2026

80-Я РЕГИОНАЛЬНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ
СТУДЕНТОВ, АСПИРАНТОВ И МОЛОДЫХ УЧЕНЫХ

СТУДЕНЧЕСКАЯ ВЕСНА

СБОРНИК НАУЧНЫХ СТАТЕЙ

VESNA.SUT.RU

СПбГУТ)))

УДК 001:061.3(082)
ББК 72
С 88

80-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна-2026»: сб. науч. ст. / Под ред. А. В. Рабина; сост. А. А. Дзюбаненко, И. М. Татарникова. СПб.: СПбГУТ, 2026. 914 с.

ПРОГРАММНЫЙ КОМИТЕТ

Председатель

Киричек Р. В. – доктор технических наук, профессор, ректор СПбГУТ

Заместитель председателя

Рабин А. В. – доктор технических наук, доцент, проректор по научной работе СПбГУТ

Ответственный секретарь

Дзюбаненко А. А. – кандидат технических наук, доцент, начальник управления организации научной работы и подготовки научных кадров СПбГУТ

Члены программного комитета

Елагин В. С. – кандидат технических наук, доцент, и.о. декана факультета инфокоммуникационных сетей и систем СПбГУТ

Владыко А. Г. – кандидат технических наук, доцент, декан факультета радиоэлектронных систем и робототехники СПбГУТ

Литвинов В. Л. – кандидат технических наук, доцент, и.о. декана факультета информационных технологий и программной инженерии СПбГУТ

Зикратов И. А. – доктор технических наук, профессор, декан факультета кибербезопасности СПбГУТ

Шутман Д. В. – кандидат политических наук, доцент, декан факультета социальных технологий и экономики данных СПбГУТ

Гирш В. А. – полковник, начальник военного учебного центра СПбГУТ

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Председатель

Абилов А. В. – кандидат технических наук, доцент, первый проректор – проректор по учебной работе

Сопредседатель

Савченко А. Ю. – проректор по молодежной политике и воспитательной работе

Ответственный секретарь

Татарникова И. М. – шеф-редактор объединенной редакции рецензируемых научных изданий

Члены организационного комитета

Ивасишин С. И. – кандидат технических наук, директор департамента организации и качества образовательной деятельности

Лысов А. Н. – директор департамента по эксплуатации и развитию материально-технического комплекса

Гуршал К. Ю. – начальник управления маркетинга и рекламы

Зыкова Н. В. – начальник управления информационно-образовательных ресурсов

Лупой Р. С. – начальник управления информатизации

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предназначено для научных работников, аспирантов, студентов старших курсов телекоммуникационных вузов, инженерно-технических работников и специалистов отрасли связи.

© СПбГУТ, 2026

10 Инфокоммуникационные сети и системы

10 Андреев Д. П. Исследование поляризационных и спектральных характеристик оптических SFP-модулей

14 Ахтырцев М. Е. Сравнительный анализ технологий DSRC, 4G LTE-V2X и 5G NR-V2X для интеллектуальных транспортных систем

20 Бадасян А. Н., Дементьев М. Е., Марочкина А. В., Юрьева А. С. Разработка и исследование системы мониторинга и управления edge-узлами в распределенных инфокоммуникационных сетях

26 Бадасян А. Н., Дементьев М. Е., Юрьева А. С. Разработка и внедрение системы V2X в городскую инфраструктуру: проблемы и особенности функционирования в условиях российских городов

31 Баскова А. Ю. Анализ полифонических аудиосигналов

36 Белов М. А., Сурков М. А., Мутханна А. С. А. От автономности к агентности: концептуальные и архитектурные основы базовых ИИ-агентов в сетях связи

40 Бугаев М. В., Кисляков С. В. Использование пограничных вычислений для построения распределенного цифрового двойника системы Network Resource Inventory

45 Ворожцов Г. С. Автономная LoRa Mesh-платформа с локальным хранением данных и журналируемой репликацией

50 Гавриленков Г. П. Способы компенсации хроматической дисперсии в волоконно-оптических системах связи

56 Доценко С. Э. Поддержание квазисолитонного режима в ВОСС с WDM при чередовании серийных типов ОМ ОВ с противоположными знаками ДГС

63 Елкин С. Д. Методы объективной оценки визуального качества в иммерсивных пространствах

69 Задимидько А. В., Тишков А. О. Имитационное моделирование системы спутниковой связи с использованием спутниковой группировки

74 Иванов Я. А. Исследование приема сигналов точек доступа Wi-Fi с использованием программно-конфигурируемого радио

79 Катыкин Д. А., Туманова Е. И. Исследование методов для анализа видеоизображений с использованием ИИ с целью обеспечения безопасности отделений Сбербанка

84 Качнов А. В. Оценка пропускной способности канала акустического трансформатора в условиях ограничения на пиковую и среднюю мощность

90 Кисляков С. В., Мамаев Е. А. Библиометрический анализ перспектив конвергенции искусственного интеллекта с цифровыми двойниками сети в качестве инструмента управления телекоммуникационными сетями

96 Колпаков С. В. Математическое моделирование работы коррелятора совместного преобразования с нелинейной обработкой совместного спектра

100 Комаха Г. Б., Плыс М. Е., Пупцев Р. И. Проектирование api для управления распределенным machine learning пайплайном

105 Коровкин В. С., Тарабанов И. Ф. Анализ методов установления прямых соединений между узлами в VPN-сетях с Mesh-топологией

110 Костылева О. А., Раковский О. В. Разработка концепции системы управления портфелем студенческих проектов

115 Кукушкин Т. Я. Сравнительный анализ технологий наземного и спутникового ТВ вещания

122 Маковец А. В. Подходы к оценке надежности инфокоммуникационных систем

126 Мананникова М. О. Таргетированная реклама: особенности и перспективы внедрения в телевизионное вещание

132 Матвеев А. О. Методы кодирования трехмерных изображений

138 Мочалов А. А. Оценка эффективности шумоподавления с использованием нейросетевой модели DTLN

142 **Пантюхин О. И., Хрусталев Н. Э.** Методы структурной оптимизации нейронных сетей для систем искусственного интеллекта в инфотелекоммуникациях

147 **Парамонов А. И., Штырляев Н. А.** Анализ эволюции технологий передачи видео

150 **Печайкин Т. В.** Прогнозирование интернет-трафика методами линейной регрессии

154 **Пимахина Ю. В.** Методика планирования систем мобильной связи

159 **Платонов С. А.** Обеспечение отказоустойчивости удаленного управления телекоммуникационным и телевизионным оборудованием с использованием SSH

163 **Помиранский Б. В., Савельева А. А.** Аналитический обзор стека протоколов уровня L2 радиоинтерфейса сетей LTE

169 **Помиранский Б. В.** Сравнительный анализ методов координации межсотовой интерференции в сетях LTE

174 **Рогова М. С., Синильников А. М.** Анализ возможностей среды MATLAB для построения модели канала спутниковой связи с морскими судами

179 **Рыбаков А. И., Соколов Н. С.** Разработка устройства передачи текстовых сообщений с использованием технологии LoRa

184 **Слесенко А. В.** Wi-Fi 6 6E 7 для задач Умного города

191 **Соромотин М. Д.** Анализ существующих интеграционных решений для сообществ в социальных сетях и мессенджерах

203 **Татаренков Д. А., Трапезникова Е. А.** Получение видеопоследовательности из архивных изображений с применением генеративных нейросетей

208 **Татаренков Д. А., Фомин П. В.** Методика цветотонального согласования 3D-объекта с видеорядом при компоновке сцены

213 **Шиманчик С. Г., Ушаков И. А.** Применение технологии SDN в сетях 6G и механизмы обеспечения безопасности

221 **Философов В. С.** Сравнительный анализ эффективности DBA-алгоритмов для сети GPON с асимметричным трафиком в многоквартирном доме

226 **Радиоэлектронные системы и робототехника**

226 **Авдеев В. В.** Сравнительный анализ использования ЛЧМ-сигналов в качестве помех в канале GSM 900

232 **Авдыш С. М., Межевова М. А.** Области использования ретрансляторов на БПЛА

236 **Акимов С. В., Люшенко А. В.** Автоматизация приемки строительно-монтажных работ в телекоммуникационной отрасли на основе компьютерного зрения

243 **Алексеев А. Э.** Влияние рефарминга RAN на качество покрытия мобильной сети

249 **Алексеев В. С., Богданов Н. И., Скалецкая И. Е.** Моделирование и расчет эффективности фонон-спиновой квантовой памяти на основе NV-центров в алмазе

254 **Андреев Б. Н., Ликонцев А. Н.** Сравнительный анализ логопериодических и рупорных антенных систем, обеспечивающих эффективное подавление каналов управления и передачи данных БПЛА

259 **Бабак Д. И., Деткова В. М.** Сравнительный анализ характеристик фотоприемного тракта при прямом детектировании на различных длинах волн излучения.

262 **Бондаренко М. В., Межевов П. А.** Проблематика управления роем БПЛА

267 **Боровков И. Ю., Калинин А. Р., Ольская М. А., Шумаков П. П.** Измеритель-характериограф нелинейных ВАХ полупроводниковых приборов

272 **Ваганов А. В., Демидов А. А.** Метамодельный подход к проектированию устройств автоматической стабилизации физических параметров на базе программируемых логических контроллеров

277 **Воищев О. С., Межевов П. А.** Влияние материала корпуса БПЛА на характеристики излучения конформной патч-антенны

282 **Володина Е. А., Макаров Л. М.** Теоретические основы компьютерного анализа лицевых экспрессий: методы, проблемы и направления развития

286 **Гаврилова Е. А., Скалецкая И. Е.** Алгоритм подбора длин волн для создания светофильтров в ИК-диапазоне

290 **Гальцова А. Д.** Сравнительный анализ методов модуляции в OFDM-системах сверхширокополосной связи

295 **Гах К. Н., Попугаев Д. Г., Шабанов А. П.** Сравнительный анализ подходов к верификации токенов доступа на основе локальной валидации и удаленной интроспекции в микросервисных решениях

300 **Гвоздецкая О. С., Татаринов Т. И., Скалецкая И. Е.** Селективный фототермолиз сосудистых патологий у пациентов с темной кожей

305 **Глушанков Е. И., Шевченко Г. С.** Моделирование фильтра Калмана в качестве интерполятора

309 **Денисов Д. А., Костоломов Н. А., Пыркин А. А., Сапрыкин А. А., Шумаков П. П., Шевченко Е. Е.** Лабораторный генератор тестовых сигналов с прямым цифровым синтезом частот

312 **Деткова В. М., Пургин Л. Б.** Цифровизация лабораторной работы «Определение горизонтальной составляющей магнитного поля Земли» и изучение сфер применения полученных данных

317 **Деткова В. М., Сидоров А. Д.** Системный анализ предельных факторов роста производительности современных вычислительных систем

322 **Долматова О. А., Пирогов В. А.** Эффективность МГД-преобразования энергии: сравнение конструкций и материалов

327 **Зайцева З. В., Кузьменков А. А., Мантуров В. М.** Сравнение энергетических показателей фильтров с разными видами фильтрующих функций

333 **Зелинский В. А., Мордовин В. Н.** Разработка портативного двухканального осциллографа для выполнения лабораторных работ по дисциплине «Компоненты электронной техники»

337 **Исаков М. В.** Влияние глубины обучения на эффективность демодуляторов на основе нейронных сетей в коротковолновом канале радиосвязи

342 **Копычко В. А., Межевова М. А.** Использование БПЛА при чрезвычайных ситуациях

346 **Коровин К. О., Чернов Г. В.** Анализ вариантов построения антенн для излучения сверхкоротких сверхширокополосных импульсов

352 **Крючков В. А.** Автоматизированный учет защищенных работ

358 **Крючков В. А., Кузичев В. А.** Метод автоматической генерации классов DTO и мапперов на основе LLM

363 **Куприянов П. А., Сидоркович Д. Р.** Повышение точности позиционирования маневрирующих целей с использованием интерактивного многомодельного алгоритма

370 **Макаров Л. М., Чаузов К. А.** Интеллектуальные матричные схемы управления промышленной роботизированной ячейкой: кейс сборки «втулка-вал»

375 **Межевов П. А., Яловицын Е. Г.** Аналитическая модель диаграммы направленности патч-антенны

381 **Меньшиков Г. К., Харьков Д. А.** Датчик движения с предварительным сканированием

386 **Меньшиков Г. К., Харьков Д. А.** Лабораторная установка измерения вольт-амперных характеристик туннельных приборов

392 **Михайлов А. В.** Моделирование и оценка точности позиционирования в помещении на основе анализа RSSI Wi-Fi устройств с учетом влияния стен

397 **Мустаев Р. Ф.** Сравнительный анализ методов оптимизации покрытия трехмерных Wi-Fi сетей в условиях больших помещений с препятствиями

401 **Нестерчук П. А.** Алгоритм управления многоканальной Bluetooth-системой с динамическим распределением устройств и адаптивным регулированием мощности

406 **Ниязгулыева А. М., Чарыярова А. Ч.** Исследование особенностей расположения базовых станций мобильных сетей 4G в условиях больших городов

410 **Рябчун Г. С.** Процесс хэндовера в спутниковых системах связи VLEO

415 **Сидоркович Д. Р., Скобкин С. А.** Роль материнского вейвлета в задачах обнаружения целей в гидроакустике: выбор оптимального базиса

420 **Смирнов Д. П.** Влияние предыскажения на сигналы передатчиков в различных системах связи

424 **Стрижкина А. М.** Разработка нейросетевой системы прогнозирования параметров распространения радиосигнала в условиях плотной городской застройки

429 **Хечуев М. И.** Адаптивное управление высокоплотными сетями Wi-Fi на основе сетей Петри

435 **Шарихина Ю. В., Шувалов Л. А.** Реализация системы беспроводной связи подвижного объекта на основе стандарта Bluetooth

441 **Информационные технологии и программная инженерия**

441 **Абакарова А. И.** Архитектура ResNet18 как основа для гибридных детекторов дипфейков: обобщающая способность и методы адаптации

446 **Аль-Нами Б. А., Стародубцев И. М.** Перспективы искусственного интеллекта в программировании

450 **Аль-Нами Б. А., Стародубцев И. М.** Развитие искусственного интеллекта в сфере персонализированного обучения

458 **Барабошкин Е. А., Коровкина Е. В.** Брокеры сообщений и их роль в распределенных системах

463 **Баразенко Д. К., Пантюхин О. И.** Минимальный состав инфраструктуры для сервиса телеприсутствия на раннем этапе разработки: подходы и риски

468 **Белов М. А., Мутханна А. С. А., Сурков М. А.** Анализ критериев оценки систем агентного ИИ в сетях связи

473 **Белый М. С., Краева Е. В.** Анализ стратегий доставки сообщений в микросервисных архитектурах в условиях деградации отдельных узлов системы

479 **Вивчарь Р. М., Рябинкин М. А., Ткач Д. М.** Архитектура метода прогнозирования корневых причин отказов производственного оборудования на основе динамических байесовских сетей

484 **Вивчарь Р. М., Рябинкин М. А., Ткач Д. М.** Поиск первопричин сбоев в микросервисных системах на основе контрфактического нейросетевого моделирования

490 **Вильготский Е. П., Коровкина Е. В.** Веб-приложение гитарный тюнер с геймифицированной средой для обучения

494 **Герасимов А. В., Перевозник Ю. Я.** Современные проблемы криптографии при появлении квантовых компьютеров

498 **Гребенщиков Д. А.** Data-informed Design в проектировании цифровых интерфейсов

502 **Губин А. Н., Райымбеков Н. Т.** Исследование методов нечеткого прогнозирования плотности транспортного потока для предотвращения образования заторов

507 **Давыдов Р. В., Никандров В. А., Устинина Ж. В.** Сравнительный анализ подходов к оценке частоты сердечных сокращений по фотоплетизмограмме: временная и частотная области

514 **Диденко А. С., Коробов А. С.** Сравнительный анализ подходов к трассировке ядра Linux для мониторинга систем хранения данных

517 **Ермакова Т. В., Новикова С. В.** Разработка программного обеспечения для логопедической диагностики и анализа динамики речевого развития младших школьников

521 **Карташов Д. И., Ушаков И. А.** Разработка учебно-методического комплекса по формированию навыков настройки сервисов L2 L3VPN в гетерогенных сетях на базе отечественных решений

525 **Ким З. В.** Гибридные интеллектуальные методы обнаружения аномалий в киберфизических системах

531 **Коретко В. М.** Анализ архитектурных подходов к разработке приложений для систематизации читательского опыта

537 **Коровкина Е. В., Куркин А. П.** Применение технологий искусственного интеллекта для персонализации систем управления задачами

541 **Лабковская Р. Я., Негина А. М., Стороженко А. А.** Интеллектуальные системы поиска и исправления уязвимостей в коде: от описания на естественном языке к защите

546 **Лебедев И. Р.** Сравнительный анализ эффективности типовых структур интеллекта в задачах управления сложными системами

551 **Ломакин В. А. , Перевозник Ю. Я.** Исследование актуальности разработки прототипа музыкального сервиса с функцией совместного прослушивания

555 **Ломакин В. А., Перевозник Ю. Я.** Исследование протоколов и алгоритмов сжатия для потоковой передачи аудио высокого качества (Hi-Fi) в веб-среде

560 **Луконин В. В., Плотников П. В.** Обеспечение целостности данных при обновлении корпоративных хранилищ: метод снапшотов в микросервисной архитектуре

565 **Марочкина А. В., Новиков К. А.** Разработка гибридных механизмов мониторинга и управления сетевым трафиком в ОС Android на базе технологий VPNService и eBPF

570 **Марушина М. Е.** Сравнительная оценка методов сбора фотоплетизмографического сигнала с умных часов

576 **Миронов К. Б.** Система обмена текстовыми сообщениями на основе протокола ESP-NOW для автономных устройств

580 **Никитин М. В.** Обзор и сравнение классов протоколов для устойчивой связи в VANET

586 **Олейников Н. Р.** Разработка подхода к визуализации музыкального сигнала на основе соответствия частот и цвета

3

591 **Пелих Д. А., Толоконникова Е. П.** Разработка информационной системы поддержки маломобильных групп населения при передвижении по городу

596 **Пелих Д. А., Ястребов Я. П.** Исследование и разработка мультиагентной системы автоматизированного составления расписания

602 **Перевозник Ю. Я., Скрябин Е. Г.** Исследование P2P-передачи данных посредством веб-приложений

607 **Раковский О. В., Турлыков И. И.** Исследования интеллектуальных методов формирования индивидуальной траектории развития

612 **Сатуев Э. А.** Разработка мобильного приложения для визуализации стереометрических задач: обзор и анализ существующих решений

619 **Старков Д. А.** Психометрия и искусственный интеллект: можно ли алгоритмам доверить оценку личности

624 **Тихиня И. П., Пупцев Р. И., Шальнов М. А.** Разработка конвейера для машинного обучения по подготовке и версионированию датасетов с использованием Git и DVC

628 **Кибербезопасность**

628 **Абзалов Т. А.** Анализ влияния архитектуры размещения ИИ-нагрузок на доступность сервисов в центрах обработки данных

633 **Алькаттан С., Мано Г., Никифоров А. В.** Разработка требований к методике автоматизированной проверки веб-сайта на соответствие 152-ФЗ

639 **Антипина С. О., Манжула А. О., Пестов И. Е., Шелкоплясова П. Е.** Анализ методов криптографической защиты информации в типовых архитектурах облачных инфраструктур

646 **Борисов С. В., Демидов Г. А., Егорова П. Ю.** Модели и алгоритм выявления аномального аккаунта в социальных сетях

651 **Ветров М. М., Мухина М. В.** Устойчивость серверных ОС к SYN-flood атаке

656 **Виткова Л. А., Трофимов Е. А.** Мониторинг дрейфа данных и концептуального дрейфа как индикаторов снижения киберустойчивости ИИ систем

661 **Гилева Д. Е., Махмутова Н. Ф.** Сравнительный анализ подходов к автоматизации управления точками доступа для образовательных целей

665 **Горковенко В. А.** Сравнительный анализ подходов к обнаружению длительных соединений в каналах управления вредоносного программного обеспечения

671 **Грибов О. С.** Методы ограничения поверхности атак в инфраструктуре центра обработки данных, основанных на штатных средствах автоматизации Zabbix

676 **Денисова Е. В., Кушнир А. Р.** Анализ угроз безопасности по уровням модели OSI

682 **Дрепа В. Е., Филимонов В. Е.** Экспериментальная оценка производительности многопользовательского веб-приложения с синхронизацией в реальном времени

688 **Дроботов А. Г.** Обнаружение атак типа удаленного выполнения кода при помощи eBPF и IoB

693 **Елагин В. С., Царёв П. Д.** Прогнозирование пользовательского трафика базовой станции LTE с использованием модели ARIMA для задач КИИ

699 **Елагин В. С., Черняков Д. А.** Анализ DoS-атак, перехвата вызовов и фрод–угроз в инфраструктуре sip

704 **Калмыков Н. Р.** Разработка подсистемы безопасного управления секретами в инфраструктуре автоматизированного управления конфигурациями

708 **Красников Д. А., Любащенко Т. Д., Шахмоведев М. А.** Оценка производительности решения на основе технологии LoRa/Meshtastic

712 **Мартыненко В. О., Николаев А. Д., Терентьев И. А., Ушаков И. А.** Анализ характеристик и функций межсетевых экранов веб-приложений

718 **Мартыненко Д. Р.** Систематизация методов обнаружения эмулятора и средств отладки в вредоносном ПО для Android

724 **Никифоров А. В., Шахмоведев М. А.** Современные методы и средства обеспечения конфиденциальности и целостности данных в системах управления базами данных

731 **Паскенова А. У.** Анализ структуры основных файлов виртуальных машин в цифрово-криминалистическом аспекте

737 **Романова Д. А.** Методика идентификации многоэтапных кибератак на прикладные сервисы в инфраструктуре сетей 6G на основе анализа сетевой телеметрии

742 **Сидельников А. С.** Комбинированный подход к аудиту информационной безопасности: интеграция сканеров уязвимостей и SIEM-системы

746 **Теровец А. А.** Контейнеризированная платформа для практического исследования и интеллектуального анализа уязвимостей смарт-контрактов

754 **Филонов А. В.** Исследование эффективности гибридной архитектуры CNN-BiGRU для обнаружения DoS- и DDoS-атак

762 **Социальные технологии и экономика данных**

762 **Berdiyeva O. P.** Linguodidactic foundations of the digital learning system for IT specialty students

765 **Андреева А. С.** Анализ роли функциональных доменов в разработке информационных систем и подхода Domain-driven Design

773 **Арипходжаев У. Т., Симонина А. А.** Анализ туристического рынка Кыргызстана и перспективы привлечения российского туриста

779 **Атаян А. М., Марченко Л. А.** Повышение эффективности бизнес-процессов сервисной компании при переходе на отечественное программное обеспечение

785 **Басиева Л. А.** Исследование инструментов принятия решений для обоснования разработки ИИ-ассистента бизнес-аналитика в банке

789 **Бородич Е. И.** Транснациональная корпорация Inditex на мировом рынке fast fashion

793 **Виноградова Ю. А.** Как китайские бесплатные gacha-игры формируют сверхдоходную бизнес-модель

800 **Володина Л. В., Парашов Д. Ш.** Современные тенденции в политических антикризисных коммуникациях

804 **Гехт А. Б., Ухалов О. А.** Неонацистские основы батальона «Азов»

808 **Гриценко Д. А., Заляжный М. М.** Влияние коротких видеороликов на потребительское поведение в современных реалиях

812 **Ждан Р. А., Петрова Е. В.** Особенности восприятия пользовательского поколения Z и Alpha

817 **Заболотник О. П., Посохова О. А.** Роль нематериального поощрения в повышении вовлеченности сотрудников и студентов в эффективности трудовой и образовательной деятельности: акцент на поколение Z

822 **Ильина К. Э.** Экосистемы цифровых сервисов как новая экономическая модель компаний

827 **Калимуллина О. В., Сидорова Е. В.** Применение технологий блокчейн в логистике и контрактах

831 **Капелюжная А. Е.** Гастродипломатия как важный фактор международных отношений

834 **Кобильняк А. А.** Политика США по противодействию четвертой волне опиоидного кризиса: федеральный, штатный и местный уровни (2021–2025 гг.)

839 **Куликов В. В., Сметанин Р. А.** Основные бизнес-процессы при управлении проектами в НПФ «Импульс»

844 **Лапков Б. Н.** Изменение роли менеджера в условиях внедрения нейросетей и искусственного интеллекта

847 **Масляк В. И.** Использование данных социальных сетей для прогнозирования потребительских трендов

851 **Михеев Д. А., Слотин М. Ю.** Влияние искусственного интеллекта на создание рекламных материалов

856 **Молчанова Т. В., Чернокозов И. Ю.** Сотрудничество государства и бизнеса в сфере креативной экономики Китая

860 **Набиев М. М., Шутман Д. В.** Лоббистская деятельность: понятие и цели регулирования

864 **Русакова А. А.** Совершенствование деятельности российского ИТ-интегратора в современных условиях

870 **Смирнова В. С.** Эволюция и роль ERP-систем в цифровой трансформации предприятия

876 **Столетова П. С.** Единая цифровая платформа в логистике как инструмент формирования прозрачного рынка перевозок (на примере «ГосЛог»)

882 **Сулейманов Д.** Экосистема как скрытая форма монополизации рынка на примере российских компаний

887 **Третьякова Ю. С.** Цифровая трансформация Saudi Aramco: бизнес-модель и экономика промышленных данных

891 **Шерстнева Д. Д.** Особенности и проблемы организации работы салона красоты и бьюти-коворкинга

895 **Сети связи специального назначения**

895 **Билиба О. В.** Энергетический расчет радиолинии спутниковой связи с учетом потерь сигнала в гидрометеорах

898 **Григорчук А. Н., Евдокимов И. А.** Подходы к построению и моделированию спутникового сегмента в сетях связи специального назначения

904 **Обухов А. Н.** Применение MIMO-архитектуры для повышения дальности и устойчивости УКВ-радиосвязи

909 **Скаредин А. А.** Повышение эффективности системы связи тактического звена управления на основе анализа опыта специальной военной операции

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 681.7

ИССЛЕДОВАНИЕ ПОЛЯРИЗАЦИОННЫХ И СПЕКТРАЛЬНЫХ ХАРАКТЕРИСТИК ОПТИЧЕСКИХ SFP-МОДУЛЕЙ

Д. П. Андреев (студент группы ИКТО-28 СПбГУТ), andreev.dp@sut.ru

Современные высокоскоростные волоконно-оптические системы связи используют одномодовые одночастотные полупроводниковые лазеры для передачи информации. Стабильная работа таких систем требует устойчивости передатчиков к внешним факторам, в частности, к температурному дрейфу. Проведено экспериментальное исследование влияния температурного дрейфа на рабочие характеристики полупроводниковые лазера в составе SFP-модуля разных марок. Показано, что в рабочем интервале изменения температур большинство SFP-модулей сохраняли свои рабочие параметры в пределах паспортных значений.

когерентность, полупроводниковый лазер, спектр, CWDM, спектральное уплотнение

Современные высокоскоростные волоконно-оптические телекоммуникационные системы предъявляют особые требования к компонентам [1, 2]. Для повышения эффективности работы волоконно-оптических систем передачи данных используется метод спектрального уплотнения каналов: несколько десятков оптических сигналов передаются по одному волоконному световоду. Для таких систем критическое значение имеет контроль частоты несущих каждого канала. Когерентные волоконно-оптические системы передачи данных позволяют повысить скорость передачи и компенсировать дисперсию [3]. Однако для стабильной системы необходимо обеспечить стабильность сигнала на приеме. Особое влияние на точность регистрации сигнала оказывает стабильность состояния его поляризации.

Целью работы является исследование влияния температуры на параметры полупроводникового лазера, встроенного в SFP модуль.

Температурный дрейф вызывает изменение таких параметров, как длина волны генерации, выходная мощность, степень поляризации.

Исследования проводились с использованием SFP-модулей для систем со спектральным уплотнением стандарта CWDM. Одной из особенностей SFP модулей для CWDM является отсутствие термической стабилизации и охлаждения входящего в его конструкцию полупроводникового лазера. Сделано это для дополнительного удешевления приемо-передающего оборудования с учетом увеличенного межканального интервала в сетях с неглубоким спектральным уплотнением. Дополнительным фактором, заставляющим обратить внимание на нагрев таких модулей, является конструкция CWDM-трансиверов со сменными лазерными модулями. SFP модуль при установке в слот находится практически полностью внутри трансивера и из-за этого быстрее нагревается.

С учетом вышеперечисленных факторов было проведено исследование зависимости длины волны излучения SFP модуля с длиной волны излучения 1310 нм и шириной спектра излучения 0,2 нм.

Для исследования поляризационных характеристик методом сферы Пуанкаре использовался поляриметр THORLABS PAX1000. Пример регистрации состояния поляризации при температуре -5°C, 20°C и 50°C приведен на рис. 1.

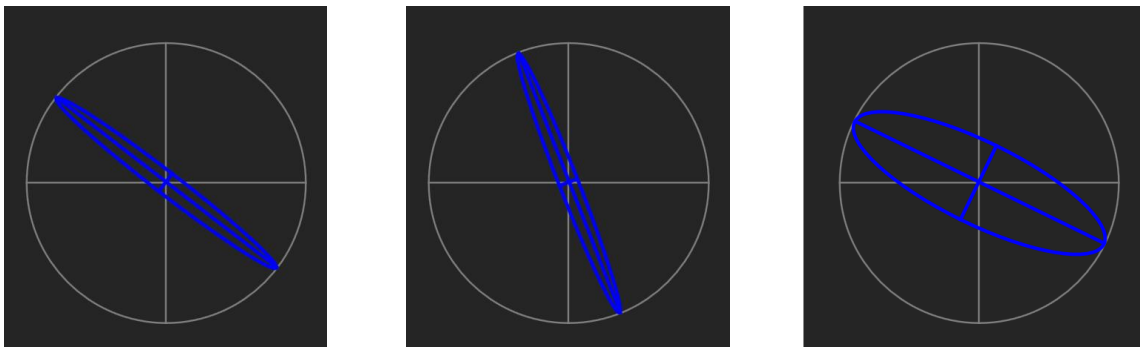


Рис. 1. Исследование состояния поляризации излучения SFP модулей от температуры. Измерения проводились при температурах -5°C (а), 20°C (б) и 50°C (в)

Экспериментальные исследования подтвердили стабильность состояния поляризации в пределах паспортных данных для рабочего диапазона температур в большинстве случаев (5 различных производителей из 6 использованных в эксперименте).

При росте температуры состояние поляризации может существенно измениться и ухудшить контраст интерференционной картины на приеме. У

полупроводниковых лазеров разных производителей этот эффект проявляется по-разному.

Исследования зависимости длины волны проводились с помощью анализатора спектра Yokogawa AQ6370C в диапазоне температур от -5°C до +50°C. Результаты исследований показали, что излучаемая мощность остается неизменной в пределах паспортных данных. Это обусловлено наличием фотодиода обратной связи, включенного в цепь питания полупроводникового лазерного диода. В то же время с ростом температуры наблюдается смещение центральной длины волны генерируемого излучения в длинноволновую область, рис. 2. Смещение центральной длины волны излучения невелико и составляет ±1 нм. С учетом межканального интервала сетей передачи данных с неплотным спектральным уплотнением подобное смещение приемлемо, однако в сетях с плотным спектральным уплотнением использование подобных модулей не представляется возможным.



Рис. 2. Исследование зависимости длины волны излучения SFP модулей от температуры. Измерения проводились при температурах -5°C (зеленый), 20°C (фиолетовый) и 50°C (желтый)

Показано, что вследствие температурного дрейфа происходит сдвиг центральной частоты излучения полупроводникового лазерного диода. При увеличении температуры несущая частота снижается, т. е. длина волны возрастает.

Список используемых источников

1. Трещиков В. Н, Листвин В. Н. DWDM-системы. 5-е изд. Техносфера. 2024.

2. Волоконно-оптическая техника: современное состояние и новые перспективы: Сб. статей под ред. Дмитриева С. А. и Слепова Н. Н. 3-е изд., перераб. и доп. М.: Техносфера 2010.

3. Дураев В., Медведев С. Одночастотные полупроводниковые РОС-лазеры, Фотоника. 2014. № 6/48. С. 40–42.

Статья представлена научным руководителем, доцентом кафедры ОКСС СПбГУТ, кандидатом физико-математических наук, доцентом Е. И. Андреевой.

УДК 621.396.93

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ DSRC, 4G LTE V2X И 5G NR V2X ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

М. Е. Ахтырцев (студент группы РМ-22 СПбГУТ), ahtyrcev.me@sut.ru

Технологии интеллектуального транспорта представляют собой важное направление систем связи, направленное на повышение безопасности, эффективности и устойчивости дорожного движения за счет обмена сообщениями между его участниками и окружающей инфраструктурой. В данной работе проводится сравнительный анализ технологий DSRC, 4G LTE и 5G NR V2X, используемых в интеллектуальных транспортных системах. Проводится оценка их ключевых характеристик: затухания, количества ошибочных блоков, пропускной способности, задержки передачи данных, что позволяет выявить преимущества и недостатки этих технологий в задачах построения систем интеллектуального транспорта.

5G NR V2X, 4G LTE V2X, DSRC, Intelligent Transportation Systems (ITS)

Согласно статистике Всемирной Организации Здравоохранения за 2023 год [1], в результате ДТП 50 миллионов человек получили травмы различной степени тяжести, а также ДТП привели к летальному исходу 1.19 миллиона человек. Кроме того, следует отметить значительные экономические потери: в 2023 году они составили 3 % мирового ВВП. Одним из возможнных решений данной проблемы является внедрение систем интеллектуального транспорта, в частности технологий V2X. Концепция V2X подразумевает организацию взаимодействия между транспортным средством и остальными участниками дорожного движения: пешеходами (V2P), другими автомобилями (V2V), дорожной инфраструктурой (V2I) и сетью (V2N). Основными технологиями применяемыми в V2X системах являются DSRC (Dedicated Short-Range Communications), 4G LTE V2X и 5G NR V2X. Характеристики каждой технологии приведены в таблице 1 [2].

ТАБЛИЦА 1. Характеристики технологий

Параметр	DSRC	4G LTE V2X	5G NR V2X
Частота	5.9 ГГц	5.9 ГГц	5.9 ГГц
Модуляция	BPSK, QPSK, 16-QAM, 64-QAM	Rel. 14: QPSK, 16-QAM Rel. 15: 64-QAM	BPSK, QPSK 16-QAM 64-QAM 256-QAM
Разделение	OFDM	SC-FDMA	OFDMA
Длительность символа, мкс	8	71	66.7 (μ = 0) 33.3 (μ = 1) 16.6 (μ = 2) 8.33 (μ = 3)
Расстояние между поднесущими, кГц	156	15	15 (μ = 0) 30 (μ = 1) 60 (μ = 2) 120 (μ = 3)
HARQ	Отсутствует	Blind	Blind

Для проведения сравнительного анализа была построена математическая модель в среде Matlab. В имитационной модели были выбраны следующие параметры: Модуляция QPSK для обеспечения достаточного уровня помехоустойчивости, вторая нумерология для $5G$, а также скорость 100 км/ч.

Далее представлены формулы [3, 4] моделей распространения для каждой технологии

$$\text{DSRC (NIST/CAMP Urban)} - \begin{cases} PL_{LOS} = PL_0 + 10 * 2.5\, log_{10}\left(\frac{d}{d_0}\right) + X_{LOS} \\ PL_{NLOS} = PL_0 + 10 * 3.5\, log_{10}\left(\frac{d}{d_0}\right) + X_{NLOS} \end{cases} \quad (1)$$

$$\text{4G C-V2X (V2V Urban Canyon)} - \begin{cases} PL_{LOS} = 22.7\, log_{10}\, d + 41.0 + 20\, log_{10}(f_c/5) \\ PL_{NLOS} = 36.7\, log_{10}\, d + 22.7 + 26\, log_{10}(f_c) \end{cases} \quad (2)$$

$$\text{5G NR V2X (Umi Street Canyon)} - \begin{cases} PL_{LOS} = 32.4 + 21\, log_{10}(d) + 20\, log_{10}(f_c) \\ PL_{NLOS} = 35.3 + 22.4\, log_{10}(d) + 20\, log_{10}(f_c) \end{cases} \quad (3)$$

На рисунке 1 представлены графики зависимости затухания сигнала от расстояния распространения в прямой видимости (LOS) и отсутствии прямой видимости (NLOS).

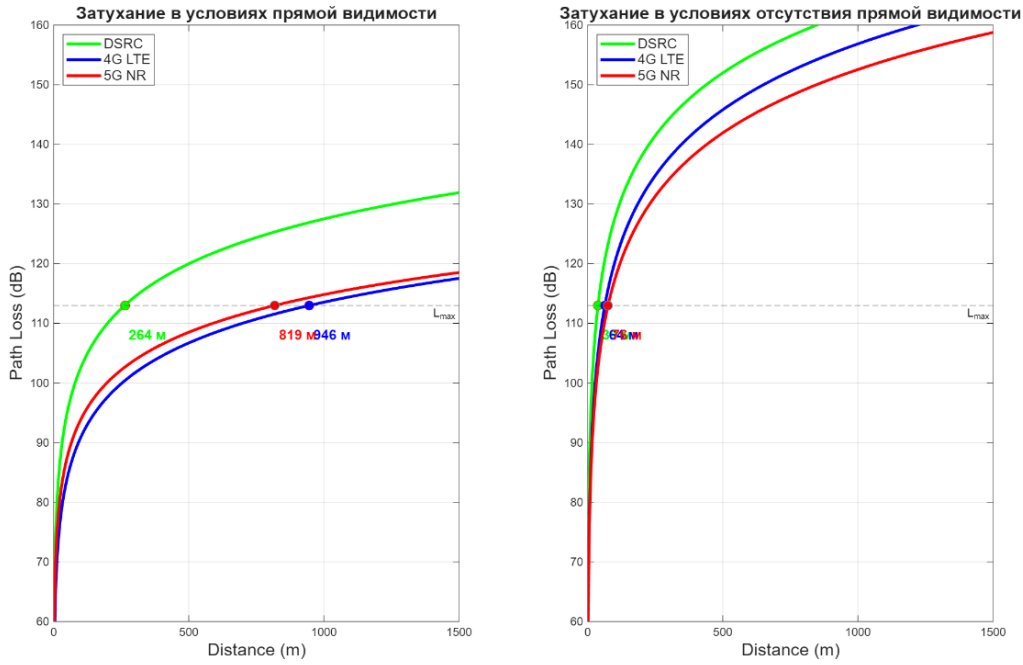


Рис. 1. График затухания

По графикам видно, что максимальные потери в 113 децибел достигаются для 5G на 819 и 76 метрах, для 4G на 946 и 64 метра, и для DSRC на 264 и 39 метрах в условиях прямой видимости и ее отсутствия соответственно.

Далее был построен график зависимости блочной ошибки от SNR.

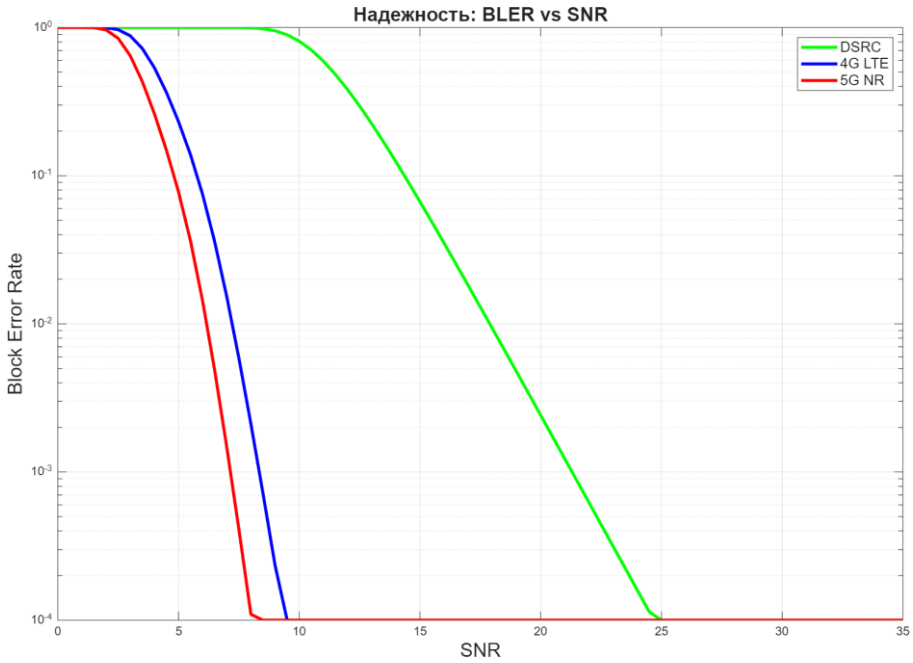


Рис. 2. График зависимости BLER от SNR

На графике можно также увидеть, что 5G превосходит более старые технологии и ему требуется меньшее SNR для отсутствия вероятности блочной ошибки.

Следующим был построен график пропускной способности в зависимости от SNR.

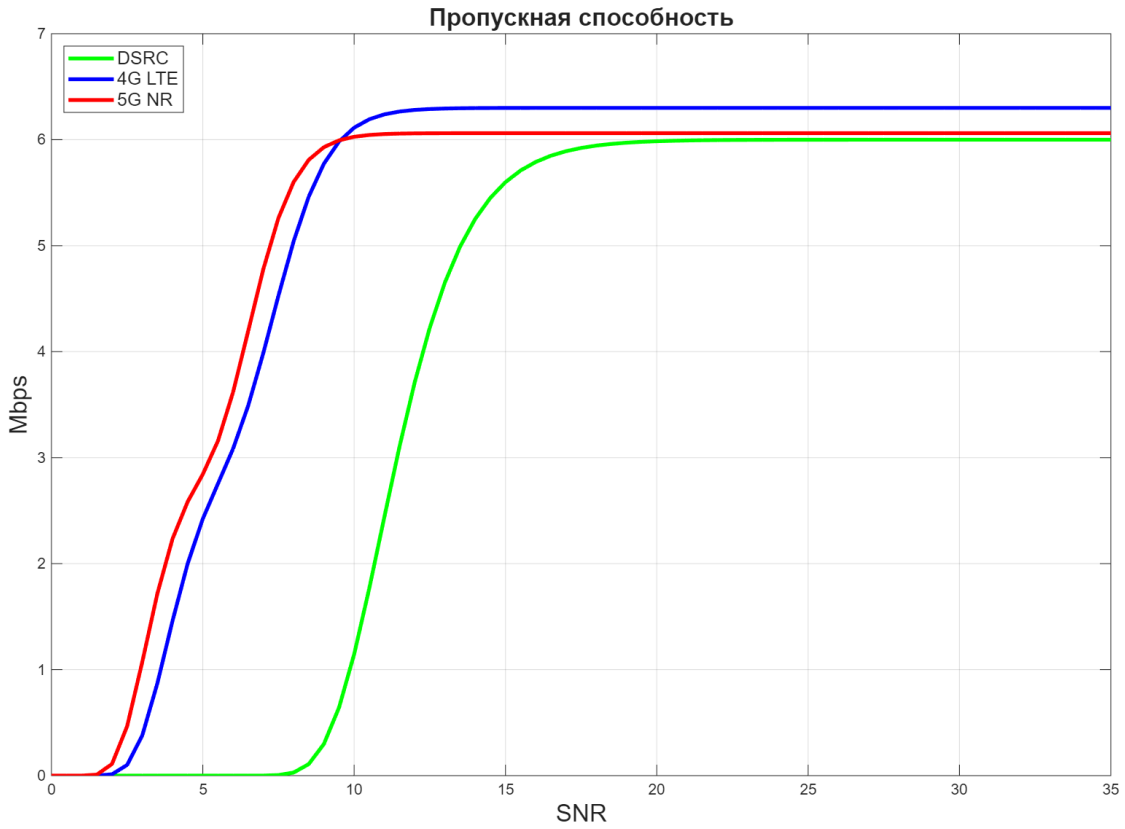


Рис. 3. График зависимости пропускной способности от SNR

На данном графике видно, что скорость в 5G начинает расти при меньшем SNR, чем у остальных технологий, что также показывает превосходство 5G над ними.

Кроме того, одним из ключевых критериев для систем интеллектуального транспорта является задержка передаваемого сигнала, далее представлены расчеты задержек для каждой из технологий, для расчета задержек в 5G была выбрана технология URLLC, так как она способна обеспечить минимально возможную задержку, что имеет критическую важность в системах интеллектуального транспорта.

$$T_{DSRC} = 1 + 22 + 0.4 + 0.00167 = 23.4 \text{ мс} \quad (4)$$

$$T_{4G} = 4 + 12.5 + 1 + 0.00167 + 1 = 18.5 \text{ мс} \quad (5)$$

$$T_{5G} = 0.5 + 0.125 + 0.25 + 0.00167 + 1 = 1.63 \text{ мс} \quad (6)$$

После расчета были построены графики задержек, представленные на рисунке 4:

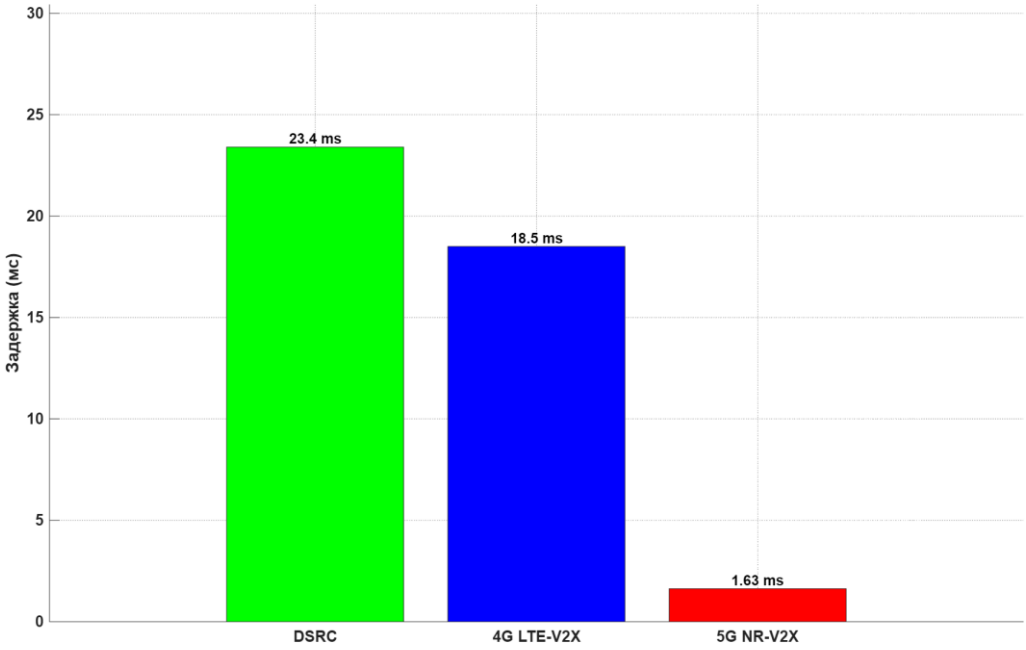


Рис. 4. График задержек

На графиках можно увидеть, что 5G превосходит 4G примерно в 11.5 раз, а DSRC примерно в 14.5 раз, обеспечивая наименьшую задержку.

По итогам построенной модели была составлена таблица 2, в которой приведены основные.

ТАБЛИЦА 2. Результирующая таблица

Параметр	DSRC	4G LTE V2X	5G NR V2X
PL_{LOS}, м	264	946	819
PL_{NLOS}, м	39	67	76
Задержка, мс	23.4	18.5	1.63
Минимальное SNR	23	11	8

Сравнительный анализ результатов моделирования показал технологической преимущество 5G NR-V2X перед стандартами предыдущих поколений. Обладая наивысшей устойчивостью в сложных условиях распространения сигнала (дальность в NLOS составляет 76 м против 67 м у 4G и 39 м у DSRC) и минимальной задержкой в 1.63 мс, данная технология обеспечивает требуемый уровень надежности для критически важных сервисов интеллектуальных транспортных систем.

Список используемых источников

1. Road traffic injuries // World Health Organization [Электронный ресурс]. URL: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries (дата обращения: 16.04.2026).

2. A comprehensive study and analysis of 3GPP's 5G New Radio for V2X communication [Электронный ресурс]. URL: https://www.preprints.org/manuscript/202311.1562 (дата обращения: 16.04.2026).

3. 3GPP TS 23.2934. Technical Specification [Электронный ресурс]. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2934 (дата обращения: 16.04.2026).

4. 3GPP TS 23.3173. Technical Specification [Электронный ресурс]. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3173 (дата обращения: 16.04.2026).

Статья представлена научным руководителем, преподавателем кафедры БТС СПбГУТ Е. С. Багаевым.

УДК 004.7

РАЗРАБОТКА И ИССЛЕДОВАНИЕ СИСТЕМЫ МОНИТОРИНГА И УПРАВЛЕНИЯ EDGE-УЗЛАМИ В РАСПРЕДЕЛЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

А. Н. Бадасян (студент группы ИКВТ-31 СПбГУТ), badasian.an@sut.ru
М. Е. Дементьев (студент группы ИКВТ-31 СПбГУТ), dementev.me@sut.ru
А. В. Марочкина (доцент кафедры СС и ПД СПбГУТ)
А. С. Юрьева (студент группы ИКВТ-31 СПбГУТ), iureva.as@sut.ru

В статье представлены результаты разработки и экспериментального исследования системы мониторинга и управления edge-узлами в распределенной инфокоммуникационной сети. Описана архитектура системы, включающая программные агенты, backend-сервер, базу данных и веб-интерфейс. Обоснован выбор технологического стека. Рассмотрены метрики производительности и надежности, механизмы управления узлами и оповещений. Проведено сравнение с системами Prometheus и Zabbix. Работа стенда проиллюстрирована скриншотами интерфейса.

edge-вычисления, мониторинг распределенных систем, метрики производительности и надежности, REST API, контейнеризация, веб-интерфейс

Введение

С развитием концепции Интернета вещей и ростом числа подключенных устройств парадигма граничных (edge) вычислений приобретает все большую практическую значимость. Перенос обработки данных на периферийные узлы позволяет снизить задержки и разгрузить центральную инфраструктуру. Вместе с тем гетерогенность и территориальная распределенность edge-узлов ставят задачу их комплексного мониторинга: отказы и деградация производительности периферийных компонентов должны выявляться оперативно.

Промышленные платформы мониторинга – Prometheus и Zabbix – ориентированы на стационарные серверные среды и требуют значительной настройки при работе с динамически изменяемыми конфигурациями [1, 2]. Это обусловливает актуальность разработки специализированного исследовательского инструмента, обеспечивающего гибкое управление параметрами наблюдаемых узлов. Целью работы является проектирование, реализация и экспериментальное исследование такой системы в контейнеризованной среде.

Архитектура и программная реализация

Система построена по многоуровневой клиент–серверной модели и включает четыре взаимодействующих компонента: агент мониторинга на каждом edge-узле, центральный backend-сервер, реляционную базу данных и веб-интерфейс оператора. Агент периодически собирает диагностические метрики и передает их на сервер по протоколу HTTP через REST API [3]. Сервер валидирует, сохраняет данные в базе и предоставляет их веб-интерфейсу для отображения текущего и исторического состояния системы. Наряду со сбором данных реализовано активное управление: команды формируются в интерфейсе, передаются через backend и исполняются на узлах, образуя двунаправленный канал взаимодействия.

Обоснование выбора технологического стека

В качестве серверного фреймворка выбран FastAPI (Python) [4]. Его ключевым преимуществом является нативная поддержка асинхронной обработки запросов на основе ASGI, что обеспечивает высокую пропускную способность при работе с множеством одновременных подключений от агентов. FastAPI автоматически генерирует интерактивную документацию API (OpenAPI/Swagger), что существенно упрощает отладку и интеграцию компонентов. По сравнению с синхронными фреймворками, в частности Flask, FastAPI демонстрирует существенно меньшие задержки при конкурентной нагрузке, что делает его предпочтительным выбором для систем мониторинга реального времени.

Пользовательский интерфейс реализован на библиотеке React [5]. Механизм виртуального DOM обеспечивает точечное обновление изменившихся элементов интерфейса без полной перезагрузки страницы, что позволяет отображать динамические графики и таблицы в потоковом режиме. Для построения временных графиков и диаграмм применялась библиотека Recharts, входящая в экосистему React.

Контейнеризация компонентов выполнена средствами Docker [6]. Данный подход обеспечивает воспроизводимость окружения независимо от хост-платформы и устраняет конфликты зависимостей. Docker Compose используется для декларативного описания топологии стенда. Топология стенда – backend, база данных, веб-интерфейс и произвольное число edge-агентов – задается единым конфигурационным файлом, а управление жиз-

ненным циклом всех сервисов осуществляется одной командой. Такой подход делает развертывание воспроизводимым и упрощает масштабирование в экспериментальных условиях.

В качестве интеграционного интерфейса между агентами и сервером выбран REST API [1]. HTTP-запросы беспрепятственно проходят через стандартные сетевые конфигурации, включая NAT и межсетевые экраны, что существенно для реалистичного моделирования edge-инфраструктуры. Данный архитектурный стиль также не исключает горизонтального масштабирования серверного компонента в дальнейшем.

Метрики системы

Собираемые метрики разделены на два класса. Метрики производительности охватывают загрузку CPU (%), использование RAM (%), сетевой трафик (КБ/с) и дисковый I/O (операций/с). Метрики надежности включают RTT до backend (мс), фактический интервал сбора метрик (с), размер локального буфера агента и долю неуспешных запросов (fail rate, %) – последний показатель отражает стабильность канала передачи данных. Аналогичные подходы к классификации метрик применяются в Prometheus и Zabbix. На уровне сервера вычисляются агрегированные значения по всем узлам, что позволяет оценить состояние инфраструктуры в целом, не анализируя каждый узел отдельно.

Управление узлами и оповещения

Система поддерживает четыре команды управления: set_interval – динамическое изменение интервала сбора метрик без перезапуска агента, restart – принудительный перезапуск, shutdown – остановка узла с возможностью последующего запуска и start – запуск узла. Возможность изменять частоту опроса на лету позволяет исследовать влияние гранулярности мониторинга на характеристики системы без изменения программного кода – это ключевое преимущество с исследовательской точки зрения. Реализован модуль пороговых оповещений: при превышении критических значений метрик формируется уведомление в журнале событий и веб-интерфейсе. История всех выполненных команд с отметками времени создания и исполнения сохраняется в разделе аналитики, обеспечивая полную аудируемость и воспроизводимость экспериментальных сценариев.

Сравнительный анализ с существующими решениями

Prometheus – система сбора и хранения временных рядов метрик, изначально разработанная для облачно-нативных сред. Архитектура Prometheus основана на модели «вытягивания» (pull): сервер самостоятельно обращается к экспортерам на наблюдаемых узлах по заданному расписанию. Система располагает мощным языком запросов PromQL и тесно интегрируется с платформой визуализации Grafana. Вместе с тем конфигурирование Prometheus для динамически добавляемых узлов требует задействования механизмов service discovery (Consul, DNS и др.), что существенно усложняет развертывание в исследовательских сценариях с часто меняющейся топологией.

Zabbix – комплексная платформа мониторинга серверной и сетевой инфраструктуры. В отличие от Prometheus, Zabbix поддерживает как pull-, так и push-модели сбора данных, располагает встроенными средствами визуализации, гибкой системой оповещений и механизмами управления конфигурацией. Платформа хорошо зарекомендовала себя в крупных производственных инфраструктурах. Однако высокий порог входа, сложность администрирования и ориентация на долгосрочную эксплуатацию делают Zabbix избыточным для задач экспериментального исследования, где требуется быстрая смена конфигурации и минимальные накладные расходы на настройку.

Разработанная система уступает обоим аналогам по функциональной полноте, однако целенаправленно оптимизирована для экспериментальных задач: она допускает оперативное изменение параметров агентов на лету, не требует предварительной настройки service discovery и предоставляет аудируемый журнал управляющих воздействий. Это делает ее пригодным инструментом для исследования зависимостей между параметрами мониторинга и характеристиками распределенной системы.

Результаты и иллюстрация интерфейса

Для проверки работоспособности системы развернут стенд на базе Docker Compose, включающий три edge-узла (node1, node2, node3), backend-сервер, базу данных и веб-интерфейс. Все узлы передавали метрики с заданным интервалом; корректность сбора, отображения данных и исполнения управляющих команд подтверждена в ходе тестирования. На рисунках 1 и 2 представлены графики метрик производительности и надежности системы, отражающие работу трех узлов в режиме реального времени.



Рис. 1. Графики метрик производительности: CPU, память, сеть и диск I/O



Рис. 2. Графики метрик надежности: интервал передачи, RTT, очередь и fail rate

На рисунке 3 показана панель управления узлами, обеспечивающая отправку команд set_interval, restart и shutdown на выбранный узел.

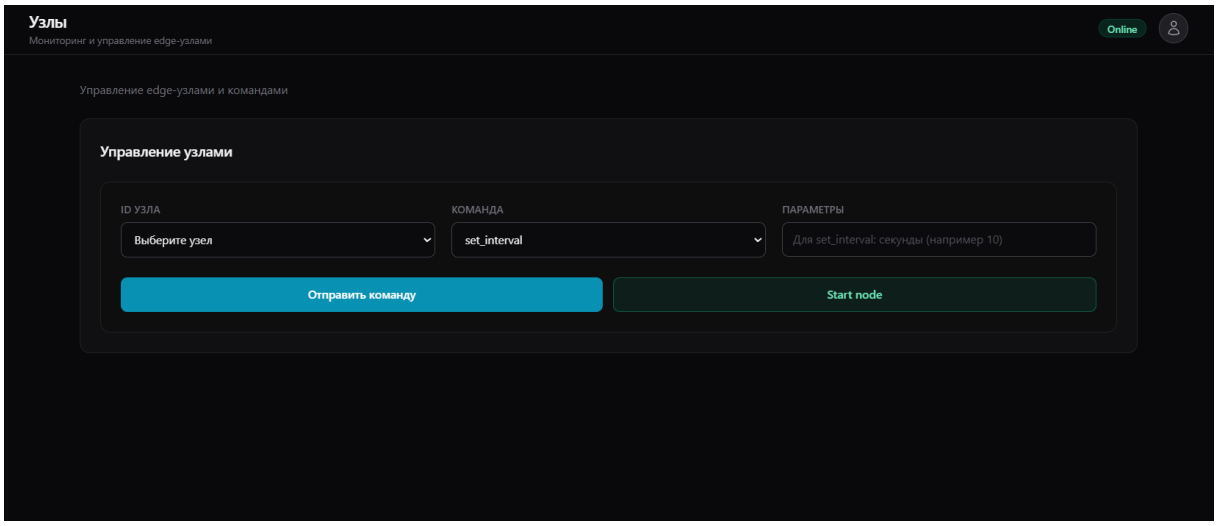


Рис. 3. Панель управления: выбор узла и доступные команды

Заключение

В работе спроектирована и реализована система мониторинга и управления edge-узлами, обеспечивающая двунаправленное взаимодействие с наблюдаемыми узлами, сбор метрик производительности и надежности, пороговые оповещения и динамическое управление агентами. Обоснован выбор технологического стека. Сравнение с существующими решениями показало, что разработанная система занимает нишу гибкого исследовательского инструмента. Экспериментальная проверка на трехузловом стенде подтвердила работоспособность всех компонентов. Дальнейшие исследования предполагают масштабирование серверного компонента, интеграцию предиктивной диагностики и анализ поведения системы при нестабильных каналах связи.

Список используемых источников

1. Prometheus. Официальная документация. [Электронный ресурс]. URL: https://prometheus.io/docs/introduction/overview/ (дата обращения: 03.04.2026).
2. Zabbix. Официальная документация. [Электронный ресурс]. URL: https://www.zabbix.com/documentation (дата обращения: 03.04.2026).
3. Исчерпывающее руководство по различным типам API [Электронный ресурс] // Habr. URL: https://habr.com/ru/companies/otus/articles/737610/ (дата обращения: 03.04.2026).
4. FastAPI. Официальная документация. [Электронный ресурс]. URL: https://fastapi.tiangolo.com (дата обращения: 03.04.2026).
5. React. Официальная документация. [Электронный ресурс]. URL: https://react.dev (дата обращения: 03.04.2026).
6. Docker. Официальная документация. [Электронный ресурс]. URL: https://docs.docker.com (дата обращения: 03.04.2026).

УДК 621.396.7:656.13

РАЗРАБОТКА И ВНЕДРЕНИЕ СИСТЕМЫ V2X В ГОРОДСКУЮ ИНФРАСТРУКТУРУ: ПРОБЛЕМЫ И ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ В УСЛОВИЯХ РОССИЙСКИХ ГОРОДОВ

А. Н. Бадасян (студент группы ИКВТ-31 СПбГУТ), badasian.an@sut.ru
М. Е. Дементьев (студент группы ИКВТ-31 СПбГУТ), dementev.me@sut.ru
А. С. Юрьева (студент группы ИКВТ-31 СПбГУТ), iureva.as@sut.ru

В статье рассматриваются архитектурные и технические аспекты построения систем межмашинного взаимодействия Vehicle-to-Everything (V2X) на основе стека протоколов ETSI ITS. Проводится сравнительный анализ двух конкурирующих технологий доступа – ITS-G5 (IEEE 802.11p) и C-V2X (3GPP). Обосновывается предпочтительность ITS-G5 для российских городских условий с учетом климатических особенностей, состояния нормативно-правовой базы и частотного регулирования. Описывается архитектура многоуровневой программной реализации передатчика и приемника CAM-сообщений, разработанной в лаборатории MegaNet СПбГУТ им. проф. М. А. Бонч-Бруевича. Рассматриваются ключевые барьеры внедрения и предлагаются пути их преодоления.

V2X, ITS-G5, C-V2X, CAM, DENM, ETSI EN 302 637, GeoNetworking, BTP, Vanetza, умный город, интеллектуальные транспортные системы

Введение

Концепция Vehicle-to-Everything (V2X) представляет собой совокупность технологий беспроводной связи, обеспечивающих обмен данными между транспортными средствами (V2V), транспортными средствами и дорожной инфраструктурой (V2I), пешеходами (V2P) и глобальными сетевыми сервисами (V2N). По оценкам международных аналитических агентств, внедрение V2X способно сократить число ДТП, вызванных человеческим фактором, на 20–30 %, а также повысить пропускную способность городских магистралей за счет кооперативного управления потоком.

Ведущие технологические юрисдикции – Европейский союз, США и Китай – уже располагают разветвленными нормативными базами и пилотными инфраструктурами. В России первые испытания V2X-оборудования на ЦКАД состоялись в 2022–2023 годах [1]. Параллельно в области ИТС исследователями разработаны смежные системы бортового ассистирования водителю на основе нейронных сетей [2] для исследования возможностей взаимодействия V2X-систем с системами распознавания дорожно-транспортной инфраструктуры. Однако массовое тиражирование технологии V2X сдерживается рядом системных факторов, которые будут рассмотрены далее.

Стандарты ETSI ITS и архитектура протокольного стека

Европейский институт стандартизации в области телекоммуникаций (ETSI) разработал комплексную нормативную базу для кооперативных интеллектуальных транспортных систем (C-ITS). Эталонная архитектура ITS-станции, описанная в стандарте ETSI EN 302 665, предусматривает четыре функциональных уровня.

Уровень доступа (Access Layer) определяется стандартом ETSI EN 302 663: физический подуровень IEEE 802.11p с каналами шириной 10 МГц в диапазоне 5,9 ГГц, дополненный механизмом децентрализованного контроля нагрузки DCC (ETSI TS 102 687), динамически регулирующим мощность передачи, частоту генерации сообщений и чувствительность приемника во избежание перегрузки канала.

Уровень сетевого взаимодействия и транспортировки включает протокол GeoNetworking (ETSI EN 302 636-4-1), обеспечивающий адресацию и маршрутизацию пакетов на основе географических координат без использования IP, и протокол Basic Transport Protocol типа B (ETSI EN 302 636-5-1) для транспортировки периодических широковещательных сообщений.

Уровень служб (Facilities Layer) реализует два ключевых примитива. Cooperative Awareness Message (CAM, ETSI EN 302 637-2) – периодическое сообщение каждой ITS-станции с частотой 1–10 Гц, которое содержит координаты, скорость, курс, тип и идентификатор станции. Decentralized Environmental Notification Message (DENM, ETSI EN 302 637-3) генерируется событийно при обнаружении опасной дорожной ситуации. Для корректного формирования обоих типов сообщений необходим модуль PoTi (Position and Time), обеспечивающий синхронизацию времени и позиционирование.

Уровень приложений (Application Layer) обеспечивает интеграцию с внешними системами.

Архитектура программной реализации V2X-платформы

В лаборатории MegaNet СПбГУТ им. проф. М. А. Бонч-Бруевича разработана программная платформа V2X – открытой реализации протокольного стека ETSI C-ITS на языке C++. Платформа реализует четырехуровневую слоистую архитектуру:

- L1 (Access Layer): поддержка IEEE 802.11p через сетевой интерфейс Ethernet (для лабораторных испытаний) или реальный 802.11p-адаптер;
- L2 (Networking & Transport Layer): GeoNetworking с поддержкой одношагового Broadcast и BTP-B для транспортировки CAM и DENM;

● L3 (Facilities Layer): модули CAM (периодическая генерация), DENM (событийная генерация) и PoTi (обеспечение синхронизации времени и координат); уровень является общим для всех приложений;

● L4 (Application Layer): разделение на tx-модуль (получение телеметрии из Redis Pub/Sub, формирование CAM/DENM) и rx-модуль (прием и публикация декодированных сообщений).

Ключевым архитектурным решением является использование единого стека протоколов для обоих направлений передачи: переключение узла между режимами tx и rx производится без изменения нижних уровней, что исключает дублирование кода и упрощает тестирование. Модульная организация уровня Facilities обеспечивает независимое подключение новых типов сообщений без переработки транспортного и канального уровней.

ITS-G5 и C-V2X: сравнительный анализ в контексте российских условий

На мировом рынке V2X конкурируют два подхода: ITS-G5 (IEEE 802.11p, ad hoc) и C-V2X (3GPP Rel. 14+, режимы PC5 и Uu). Сравнительный анализ приведен в таблице 1.

ТАБЛИЦА 1. Сравнение ITS-G5 и C-V2X по ключевым параметрам

Параметр	ITS-G5 (IEEE 802.11p)	C-V2X (3GPP Rel. 14+)
Доступ к каналу	CSMA/CA + DCC (ETSI TS 102 687)	SB-SPS (ресурсный пул)
Задержка (низкая плотность)	~0,2–1 мс	~10,5–50,5 мс
Задержка (высокая плотность)	растет из-за коллизий	стабильная
Плотность >150 уч./км^2	превосходит C-V2X	деградирует
Инфраструктура	не требуется (ad hoc)	требуется в режиме Uu
Стандартизован с	2010 г.	2017 г.
Открытое ПО	Vanetza (LGPL)	ограничено
Зависимость от оператора	нет	есть (режим Uu)

Сравнительные исследования показывают, что C-V2X демонстрирует преимущество при плотности трафика менее 150 участников/км^2, однако в условиях насыщенного городского потока ITS-G5 превосходит C-V2X по доставке пакетов [3]. Задержка доступа к каналу в ITS-G5 составляет доли миллисекунды; механизм SB-SPS в C-V2X вносит структурную задержку 10–50 мс.

Применительно к российским городам ITS-G5 является предпочтительным выбором по трем основаниям. Во-первых, режим ad hoc обеспечивает полную независимость от сотовой инфраструктуры, что критично при ее отсутствии или отказе. Во-вторых, стандарт обладает большей зрелостью (с 2010 г.) и открытой программной экосистемой – в частности, библиотека Vanetza [4] реализует полный стек ETSI C-ITS под лицензией LGPLv3. В-третьих, физический уровень IEEE 802.11p устойчив к доплеровскому сдвигу и многолучевому распространению, характерным для городских каньонов с плотной застройкой.

Особенности функционирования V2X в условиях российских городов

Климатические факторы. Значительная часть российских городов функционирует в диапазоне от -40°C до +40°C. Снег и наледь на дорожном покрытии снижают эффективную плотность трафика, смещая баланс сравнения с C-V2X в пользу ITS-G5. Туман и осадки оказывают ограниченное влияние на распространение радиоволн в диапазоне 5,9 ГГц, однако плотная городская застройка ухудшает качество GNSS-позиционирования, необходимого для корректной генерации CAM.

Нормативно-правовая база. В Российской Федерации отсутствует специализированный национальный стандарт для систем V2X, сопоставимый по детализации с семейством ETSI. Существующие ГОСТ Р в области ИТС носят общий характер, что создает правовую неопределенность при сертификации оборудования. Рекомендация МСЭ-R M.2121-1 (2023) призывает выделить полосу 5850–5925 МГц для применений ИТС [5], однако соответствующее решение ГКРЧ в России на момент написания работы принято не было.

Частотное регулирование. В Европе диапазон 5875–5925 МГц закреплен исключительно за ITS-G5 решением Еврокомиссии. В России полоса 5850–5925 МГц не имеет прямого регуляторного решения для наружного применения в транспортных системах. Это означает, что развертывание ITS-G5 в полном соответствии с ETSI EN 302 663 требует

специального разрешения ГКРЧ и является одним из ключевых барьеров коммерциализации. Принципиально важно, что ITS-G5 не требует лицензий на использование сотовой инфраструктуры, исключая зависимость от конкретного оператора связи.

Заключение

По результатам проведенного исследования установлено, что технология V2X на основе стека ETSI ITS является зрелым, стандартизованным решением, готовым к масштабному внедрению. ITS-G5 демонстрирует преимущества перед C-V2X применительно к условиям российских городов: независимость от сотовой инфраструктуры, меньшая задержка при высокой плотности трафика, зрелость стандартов и наличие открытых программных реализаций. Разработанная V2X-платформа подтвердила работоспособность многоуровневой архитектуры ETSI ITS. Для масштабного развертывания необходимы: принятие решения ГКРЧ о выделении диапазона 5875–5905 МГц для ITS-G5; разработка ГОСТ Р, гармонизированного с ETSI EN 302 637/663; развитие отечественных открытых программных платформ.

Список используемых источников

1. Нигметзянов М. На «умной» ЦКАД расширяют применение системы V2X [Электронный ресурс] // CNews. 16.03.2023. URL: https://www.cnews.ru/news/line/2023-03-16_na_umnoj_tskad_rasshiryayut (дата обращения: 04.04.2026).

2. Виницкий М. А., Дусталев Е. В., Минин Д. А., Бабич В. Н., Бобровский В. И. Разработка интеллектуальной системы помощи водителю // Информационные технологии и телекоммуникации. 2025. Т. 13. № 1. С. 40–46. DOI: 10.31854/2307-1303-2025-13-1-40-46.

3. Mannoni V., Berg V., Sesia S., Perraud E. A Comparison of the V2X Communication Systems: ITS-G5 and C-V2X // 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). DOI: 10.1109/VTCSpring.2019.8746562.

4. Riebl R. Vanetza: Open-source implementation of the ETSI C-ITS protocol stack. [Электронный ресурс] 2017–2024. URL: https://github.com/riebl/vanetza (дата обращения: 04.04.2026).

5. МСЭ-R M.2121-1. Использование полосы частот 5850–5925 МГц для интеллектуальных транспортных систем. Рекомендация. Международный союз электросвязи, 2023.

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ССиПД СПбГУТ А. В. Марочкиной.

УДК 681.84.087

АНАЛИЗ ПОЛИФОНИЧЕСКИХ АУДИОСИГНАЛОВ

А. Ю. Баскова (студент группы Р-41м СПбГУТ), baskova.aju@sut.ru

В данной работе рассматривается метод, сочетающий преобразование с постоянной добротностью, неотрицательное матричное разложение для разделения источников и кепстральный анализ для извлечения тембральных признаков. Это позволяет эффективно декомпозировать аккорд на его составляющие ноты, что открывает возможность для детального изучения характеристик полифонического сигнала.

полифония, музыка, частотный анализ

В современных задачах автоматической транскрипции музыки ключевым аспектом остается обработка полифонических сигналов. Традиционные методы спектрального анализа, такие как кепстральный анализ, демонстрирует высокую эффективность в задачах выделения основного тона и оценки речевых трактов. Однако при обработке полифонического сигнала, где одновременно звучат несколько источников с перекрывающимися обертонами, классический кепстральный подход сталкивается с рядом фундаментальных ограничений. Для возможности дальнейшей работы с полифоническим сигналом применяется метод неотрицательного матричного разложения.

Для обработки полифонического ((греч. Polyphonia – многозвучие) – вид многоголосной музыки, основанный на одновременном звучании двух и более самостоятельных мелодических линий) [1, 2] музыкального сигнала БПФ и кепстрального анализа недостаточно. Наличие нескольких голосов, звучащих одновременно приводит к наложению неосновных спектральных составляющих (обертонов) на основной тон, что делает невозможным определение частоты основного тона в мгновенный момент времени.

Для решения этой проблемы применяется неотрицательное матричное разложение (НМР), задачей которого является декомпозиция сложного полифонического сигнала на спектральные и временные составляющие [3].

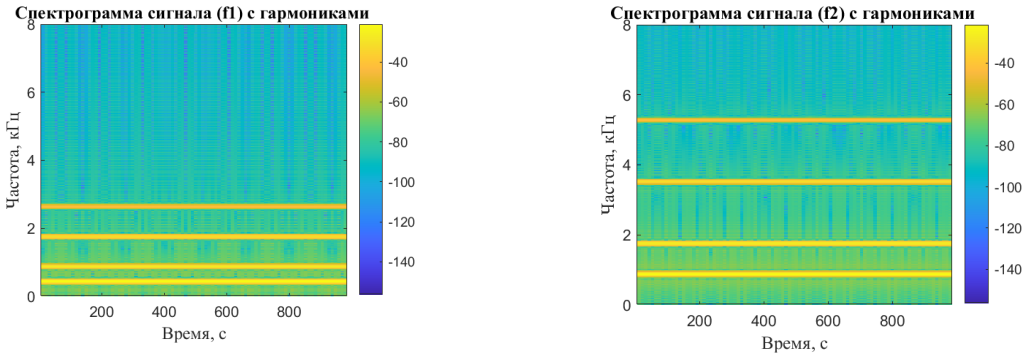
НМР раскладывает матрицу спектрограммы сигнала (V) на две матрицы [4]: матрица словаря и матрица активации. Первая матрица (W) содержит информацию о каждой частоте и ее гармонике. Вторая матрица (H) определяет момент времени, на который приходится определенная нота:

$V \cong W \cdot HV$ – матрица спектрограммы, W – матрица частотных компонент, H – матрица временных компонент.

Подбор двух матриц производится итеративно. Обе матрицы W и H заполняются случайными значениями. Далее алгоритм вычисляет ошибку между исходной матрицей V и матрицей V2, получившейся в результате перемножения W и H. По правилам обновления [4] алгоритм изменяет вес каждого элемента матрицы H при постоянных значениях матрицы W. Затем при постоянных коэффициентах H подбираются элементы W. С каждой итерацией разность между матрицами V и V2 уменьшается.

Так как НМР работает с предварительно полученной спектрограммой в матричном виде, то для корректной работы этого алгоритма вместо БПФ следует предварительно воспользоваться преобразованием с постоянной добротностью (ППД) [5], где частотная шкала формируется логарифмически, что соответствует равномерно темперированному строю из 12 полутонов, принятому за эталон для музыкальных инструментов. После ППД гармонический состав любой ноты будет инвариантен к сдвигу, что позволит алгоритму НМР отделить энергию одной ноты от другой, даже если их обертоны накладываются на основной тон.

Пусть имеются сигналы с частотой f1 = 440 Гц с тремя кратными гармониками и сигнал с частотой f2 = 880 Гц и тремя кратными гармониками. После БПФ интервал между основным тоном и следующей кратной составляющей спектра будет различное [3] при сравнении двух сигналов, рис. 1:



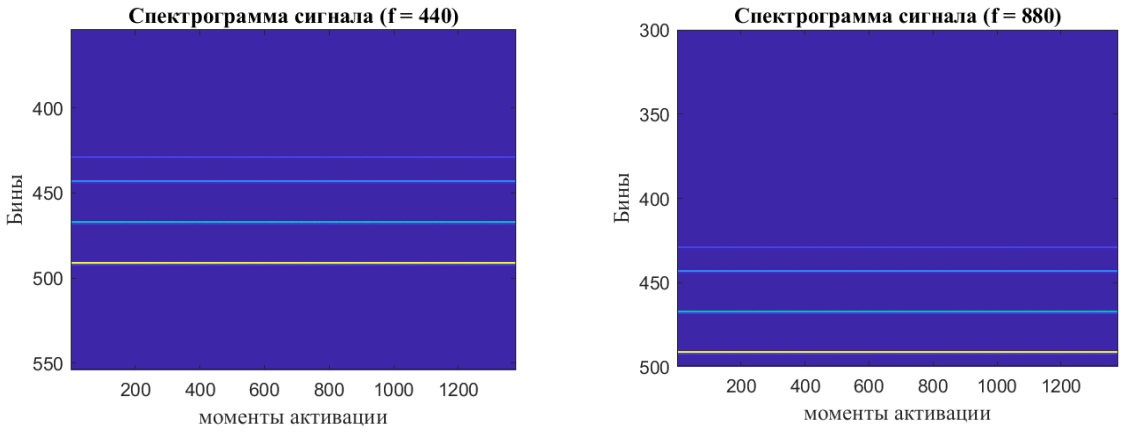
а б

Рис. 1. Спектрограммы сигналов *и* их кратных частот а) 440 Гц б) 880Гц

При одновременном звучании двух таких сигналов вторая компонента спектра первого сигнала совпадет с основной частотой второго сигнала, что

впоследствии приведет к невозможности отделения гармоники одной частоты от основного тона другой частоты. В дальнейшем НМР будет определять эти частоты как от совершенно разных источников звука.

При работе ППД структура расстояния между основным тоном и кратными частотами одинаково у двух сигналов, ввиду нелинейной шкалы частот, рис. 2:



а б

Рис. 2. Спектрограммы сигналов *и* кратных частот а) 440 Гц, б) 880Гц

Благодаря логарифмической шкале расстояние между спектральными компонентами фиксировано, что позволяет создать определенную неизменяющуюся спектральную структуру для работы алгоритма НМР. Такие структуры будут детектироваться НМР, как компоненты одного источника, что будет являться верным. Использование алгоритма НМР позволяет получить спектральные профили каждого тона. Пусть имеются два синусоидальных сигнала (ноты «До» и «Ми») fc = 261.63 Гц и fe = 293.63 Гц, с гармониками, рис. 3:

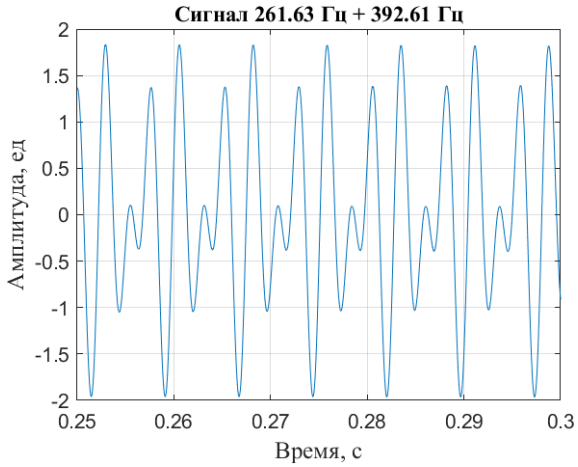


Рис. 3. График сходного аддитивного сигнала

Данный сигнал представляет собой аддитивную смесь фундаментальных частот и их кратных компонент. Спектрограмма сигнала после ППД будет представлять участки (бины) сигнала с высокой энергией, благодаря наложению кратных гармонических составляющих сигнала, рис. 4:

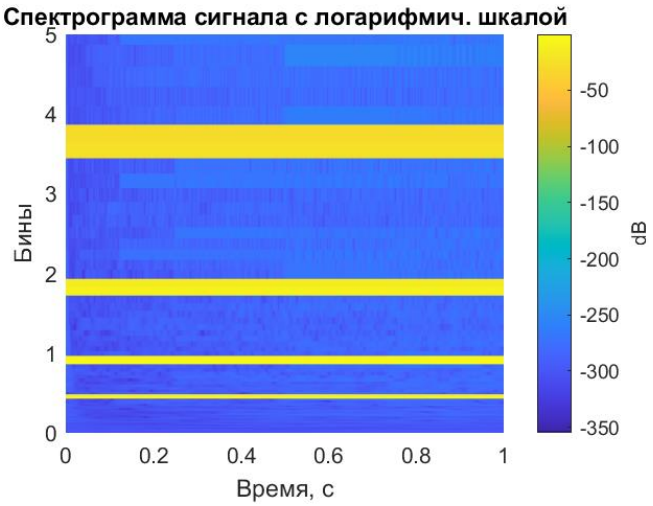


Рис. 4. Спектрограмма аддитивного сигнала после ППД

После применения алгоритма НМР умножение матриц H и матриц W позволит сформировать спектрограмму детектированных частот, рис. 5:

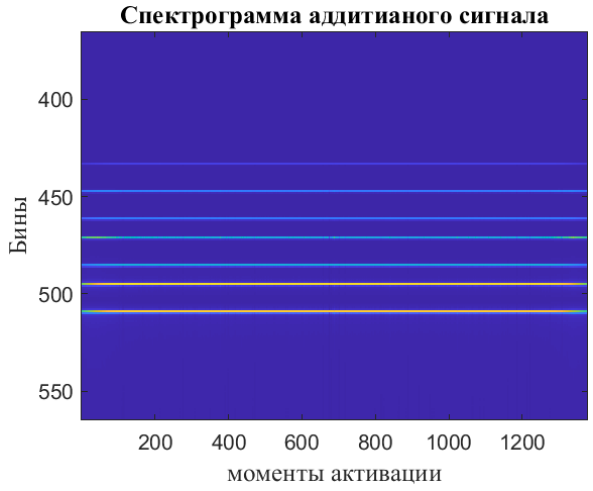


Рис. 5. Спектрограмма аддитивного сигнала после НМР

Энергия двух основных составляющих сигнала и их гармоник постоянна ввиду постоянной энергии на всем протяжении времени и отсутствия затухания.

НМР позволяет выделит спектральные профили каждой ноты, однако для корректного транскрибирования в нотную запись необходимо подавить высшие гармоники и выделить фундаментальную частоту, что достигается

путем дальнейшего применения обратного преобразования Фурье к логарифму полученных значений, как при работе кепстрального анализа, рис. 6:

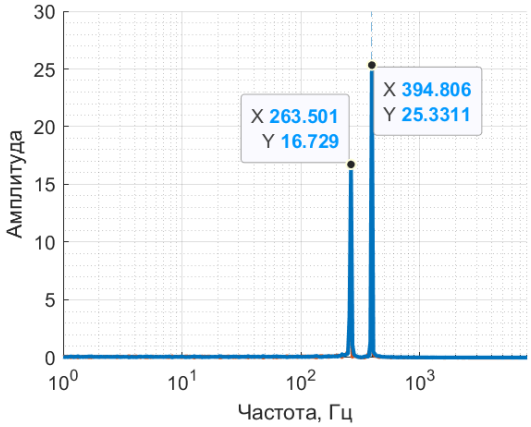


Рис. 6. Спектр сигнала после кепстрального анализа

Таким образом алгоритм HMP декомпозирует сложный полифонический сигнал на спектральные профили, в совокупности с кепстральным анализом, эффективно извлекает основные компоненты сложного полифонического сигнала, обеспечивая высокую точность для последующей транскрипции аудиофайла.

Список используемых источников

1. Дубовский И., Евсеев С., Способин И., Соколов В. «Учебник Гармонии» Изд. Музыка, Москва. 1965 г.

2. Элементарная теория музыки. Вахромеев В.А. 3-е изд. М.: 1961. 244 с.

3. Цифровая обработка сигналов / Оппенгейм А., Шафер Рональд; Боев С.Ф. (ред., пер. с англ.). Изд. 3-е, испр. М.: Техносфера, 2012. 1046 с.

4. Non-negative Matrix Factorization Techniques Advances in Theory and Applications / Ganesh R. Naik. 978-3-662-48330-5 Published: 05 October 2015, 194. URL: https://doc.ml.tu-berlin.de/bbci/material/publications/Bla_constQ.pdf (дата обращения: 30.04.26).

УДК 621.39:004.89

ОТ АВТОНОМНОСТИ К АГЕНТНОСТИ: КОНЦЕПТУАЛЬНЫЕ И АРХИТЕКТУРНЫЕ ОСНОВЫ БАЗОВЫХ ИИ-АГЕНТОВ В СЕТЯХ СВЯЗИ

М. А. Белов (студент группы МСТ-2561 СПбГУТ), belov.ma@sut.ru
М. А. Сурков (студент группы РМ-21 СПбГУТ), surkov.ma@sut.ru
А. С. А. Мутханна (профессор кафедры ССиПД, д.т.н. СПбГУТ), muthanna.asa@sut.ru

В статье рассматривается концептуальное разграничение терминов «ИИ-агент» и «Агентный ИИ» применительно к сетям IMT-2020 и IMT-2030. На основе стандартов МСЭ-Т и доклада ОЭСР № 56 описывается архитектурный фреймворк базового автономного агента, реализованного через линейный конвейер машинного обучения согласно ITU-T Y.3172. Показано, что терминологическое смешение двух парадигм ведет к архитектурным ошибкам при развертывании ИИ в сетях.

ИИ-агент, агентный ИИ, IMT-2020, IMT-2030, автономность, агентность

Генеративный ИИ меняет управление сетями связи быстрее, чем успевает формироваться единая терминология. МСЭ-Т в рамках Исследовательской группы 13 (Q20/13) ведет работы по вопросам ИИ в сетях IMT-2020 и IMT-2030 [1]: требования к архитектуре, эталонный тест для GenAI, словарь терминов, протоколы взаимодействия агентов. ОЭСР в феврале 2026 года опубликовала доклад № 56, посвященный концептуальным основам агентного ИИ [2]. Оба источника фиксируют общую проблему: понятия «ИИ-агент» и «Агентный ИИ» используются как взаимозаменяемые, хотя за ними стоят принципиально различные архитектурные решения.

В сетях с высокими требованиями к надежности – IMT-2020 и особенно IMT-2030, где автономное управление предполагается как базовый принцип [1], – смешение понятий ведет к архитектурным ошибкам: некорректному выбору механизмов оркестровки, неверной оценке допустимого уровня автономности и отсутствию надлежащего контроля.

Цель данной статьи – на основе стандартов МСЭ-Т и концептуального аппарата ОЭСР разграничить два понятия и описать архитектурный фреймворк базового автономного ИИ-агента применительно к сетям связи.

Документ МСЭ-Т YSTR.NAIA «Terms and definitions related to the AI Agent topic in future networks» [3] разграничивает два термина, которые в смежной литературе нередко приравниваются друг к другу:

● ИИ-агент (AI agent) определяется как «автоматизированная сущность, воспринимающая свое окружение и предпринимающая действия для достижения целей»; этот уровень отвечает исполнительной автономности: агент собирает данные, применяет инструменты, выполняет узко заданную задачу. Словарь МСЭ-Т дополняет это определение, указывая, что агент – «сущность, способная взаимодействовать со средой и использующая специфические ИИ-возможности для достижения целей сети» [3]. На практике в сетях IMT-2020 такие агенты функционируют как «инструктивно-управляемые» (instruction-driven) системы, работающие преимущественно на основе заранее заданных правил, рабочих процессов или явных инструкций человека.

● Агентный ИИ (Agentic AI) представляет иную парадигму. Согласно ОЭСР, агентный ИИ – это «системы, состоящие из нескольких скоординированных ИИ-агентов, способных декомпозировать задачи, взаимодействовать и автономно достигать сложных целей в течение продолжительного времени» [2]. Ключевые отличия от базового агента – делегирование подзадач, распределенное планирование, работа в непредсказуемых средах и минимальный человеческий надзор.

ОЭСР разграничивает понятия следующим образом: «автономность – способность системы действовать без прямого участия человека», тогда как «агентность предполагает способность к самостоятельной постановке целей, долгосрочному планированию и стратегической адаптации» [2]. Система может быть автономной, не будучи агентной: простой ML-модуль управления трафиком работает независимо, однако не формирует целей и не взаимодействует с другими агентами.

Таким образом, автономность – характеристика изолированного алгоритма, выполняющего конкретную задачу, тогда как полноценная агентность требует социального контекста: межагентных протоколов, механизмов координации и разделения ролей.

Стандарт ITU-T Y.3172 «Architectural framework for machine learning in future networks including IMT-2020» описывает конвейер машинного обучения (ML pipeline) как базовую структурную единицу для встраивания ИИ в сети [4]. Конвейер включает строго последовательные логические узлы:

- источник данных – точка входа данных из сетевой среды;
- сборщик данных – агрегирует и маршрутизирует потоки;
- препроцессор – нормализует, фильтрует, преобразует данные;
- ИИ-модель – выполняет вывод или обучение;

- узел политик – применяет правила оператора к результатам вывода модели для минимизации рисков при воздействии на сеть;
- распределитель – направляет результаты вывода;
- приемник/цель – точка выхода, управляющее воздействие на сеть.

Каждый узел стандартизован, интерфейсы между ними определены. Конвейер работает без постоянного участия оператора – ITU-T Y.3172 называет это «наложенной моделью развертывания» (machine learning overlay), при которой ИИ-функциональность слабо связана с сетевыми функциями через стандартные интерфейсы.

Данная архитектура соответствует концепции инструктивно-управляемого агента: принимая данные среды, обрабатывая их по заданным правилам и генерируя управляющее воздействие, конвейер автономно решает узко заданные задачи – прогнозирование загрузки ресурсов, классификацию трафика – без внешней оркестровки.

Ограничение данной архитектуры вытекает из ее достоинств – изолированности. Конвейер не предусматривает межагентного взаимодействия, делегирования подзадач или адаптивного планирования в условиях неопределенности, что не позволяет реализовать полноценную агентность в понимании ОЭСР.

IMT-2030 предполагает «автономное управление сетями средствами ИИ/МО – самомониторинг, самоорганизацию, самооптимизацию, самовосстановление без вмешательства человека» как базовый принцип. Выполнение данного принципа требует координации между множеством таких конвейеров, то есть перехода от исполнительной автономности к системной агентности в понимании ОЭСР, а также опирается на инфраструктурные принципы IMT-2030.

В статье показано, что понятия «базовый ИИ-агент» и «Агентный ИИ» описывают разные уровни интеграции ИИ в сети связи. Первый реализуется через линейный ML-конвейер согласно ITU-T Y.3172 – это автономная, изолированная и предсказуемо работающая система для точечных задач в IMT-2020. Второй предполагает координацию нескольких таких агентов, декомпозицию целей, межагентные протоколы – инфраструктуру, которая формируется в рамках стандартизационных работ Q20/13 МСЭ-Т.

Разграничение терминов имеет прикладное значение. Использование единственного изолированного конвейера в сценариях, требующих агентного ИИ, либо не дает необходимого результата, либо порождает скрытые

архитектурные уязвимости. Избыточная мультиагентная оркестровка в задачах, где достаточно инструктивно-управляемого агента, неоправданно усложняет систему без функциональной необходимости.

Архитектура базового автономного агента, описанная в ITU-T Y.3172, остается надежным инструментом для автоматизации конкретных сетевых функций в IMT-2020/2030. Переход к подлинному агентному ИИ потребует дополнительных механизмов: протоколов межагентного взаимодействия, распределенной памяти, оркестровки конвейеров – над чем в настоящее время ведут работу Q20/13, Q21/13 и Q22/13 МСЭ-Т.

Список используемых источников

1. ITU-T YSTR.IMT2030-req. IMT-2030 networks. Considerations on requirements: Draft new Technical Report, Q20/13, Study Group 13. Geneva: ITU, 2026. 25 с.

2. OECD AI Papers N 56. The agentic AI landscape and its conceptual foundations. Paris: OECD Publishing, 2026. 34 с.

3. ITU-T YSTR.NAIA. Terms and definitions related to the AI Agent topic in future networks: Draft new Technical Report, Q20/13, Study Group 13. Geneva: ITU, 2026. 9 с.

4. ITU-T Y.3172. Architectural framework for machine learning in future networks including IMT-2020: Recommendation. Geneva: ITU, 2019. 25 с.

Статья представлена научным руководителем, профессором кафедры ССиПД СПбГУТ, доктором технических наук, профессором А. С. А. Мутханной

УДК 654.1

ИСПОЛЬЗОВАНИЕ ПОГРАНИЧНЫХ ВЫЧИСЛЕННИЙ ДЛЯ ПОСТРОЕНИЯ РАСПРЕДЕЛЕННОГО ЦИФРОВОГО ДВОЙНИКА NETWORK RESOURCE INVENTORY

М. В. Бугаев (студент группы ИКТС-43м СПбГУТ), bugaev.mv@sut.ru
С. В. Кисляков (к.т.н., доцент кафедры ИКС, преподаватель базовой кафедры ИТТ СПбГУТ)

В статье рассматривается архитектурный подход к развитию системы Network Resource Inventory путем выноса ресурсоемких и чувствительных к задержкам функций на граничный уровень сети (Edge Layer). Предлагается концепция распределенной архитектуры с использованием цифровых двойников, функционирующего вблизи управляемых сетевых ресурсов. Анализируются существующие проблемы развития системы Network Resource Inventory и предлагаются пути их решения, аргументированные существующим трендам в развитии сетей нового поколения.

цифровой двойник, пограничные вычисления, ODA, NRI, машинное обучение

Неограниченный рост сетевого трафика, процессы конвергенции сетей и сетевых устройств, а также необходимость в новых бизнес-моделях определяют растущую важность новых методов снижения эксплуатационных расходов, эффективного использования сетевых ресурсов и уменьшения рисков в управлении цифровым бизнесом. Одной из важнейших проблем и серьезной болевой точкой поставщики услуг называют именно поддерживание точной и надежной информационной базы [1].

Привычной системой учета инфраструктуры сети связи является NRI (Network Resource Inventory) – один из ключевых компонентов ландшафта OSS (Operation Support System), как правило централизованная база данных, предназначенная для хранения и предоставления информации о физических и логических ресурсах инфраструктуры: устройствах, интерфейсах, связях, емкостях, логических сущностях и их взаимосвязях. Помимо этого, NRI обеспечивает возможность отслеживания изменений в сети и управления конфигурациями, а также используется для многих бизнес-процессов, например, для проверки технической возможности.

Несмотря на то, что NRI влияет на задержки из конца в конец не напрямую (как физический параметр канала связи), а опосредованно, через оптимизацию и автоматизацию процессов управления сетью, влияние задержек обработки данных на уровне NRI нельзя преуменьшать, поскольку от этого

зависит как скорость предоставления услуг, так и точность информационной базы оператора. NRI, особенно в концепциях активной инвентаризации, позволяет сократить задержки в бизнес-процессах на всех этапах, где решения принимаются на основе информации о сети.

Существующие системы управления сетями и коммуникационными услугами не в полной мере отвечают требованиям пользователей в сфере информационно-коммуникационных услуг следующего поколения, которые определяются бизнес-процессами компаний [2]. Решения для управления запасами изначально были разработаны для облегчения взаимодействия человека с данными и рабочими процессами инвентаризации, решения для управления запасами следующего поколения будут разработаны в первую очередь для более тесного взаимодействия между машинами, а взаимодействие человека с машиной будет осуществляться только там, где это необходимо [3]. По мере усложнения сетей нового поколения (4G/5G и перспективных 6G) становится очевидно, что одних только архитектурных изменений OSS-платформ недостаточно. Существенным фактором остается пространственное расположение функций управления и обработки данных. Важно и то, что при архитектуре с одним центром обработки данных, наращивание вычислительных ресурсов не сможет вечно справляться с ростом нагрузки. Такие проблемы уже возникали в сетях связи, яркие примеры – оперативные базы данных в мобильных сетях и сети CDN (Content Delivery Network). Оба случая показывают, как проблему перегрузки баз данных можно решить с помощью распределенной архитектуры.

Переход к полностью автономной сети является стратегической необходимостью (рис. 1). Он представляет собой фундаментальный сдвиг от ручных, реактивных операций к проактивным, ориентированным на намерения и самоуправляемым сетям. Открытая цифровая архитектура (ODA), приходящая на смену традиционному OSS/BSS, способна существенно упростить и автоматизировать основные бизнес-процессы используя логику распределенных вычислений, что позволяет внедрять сервисы на разрозненных сетевых узлах [2].

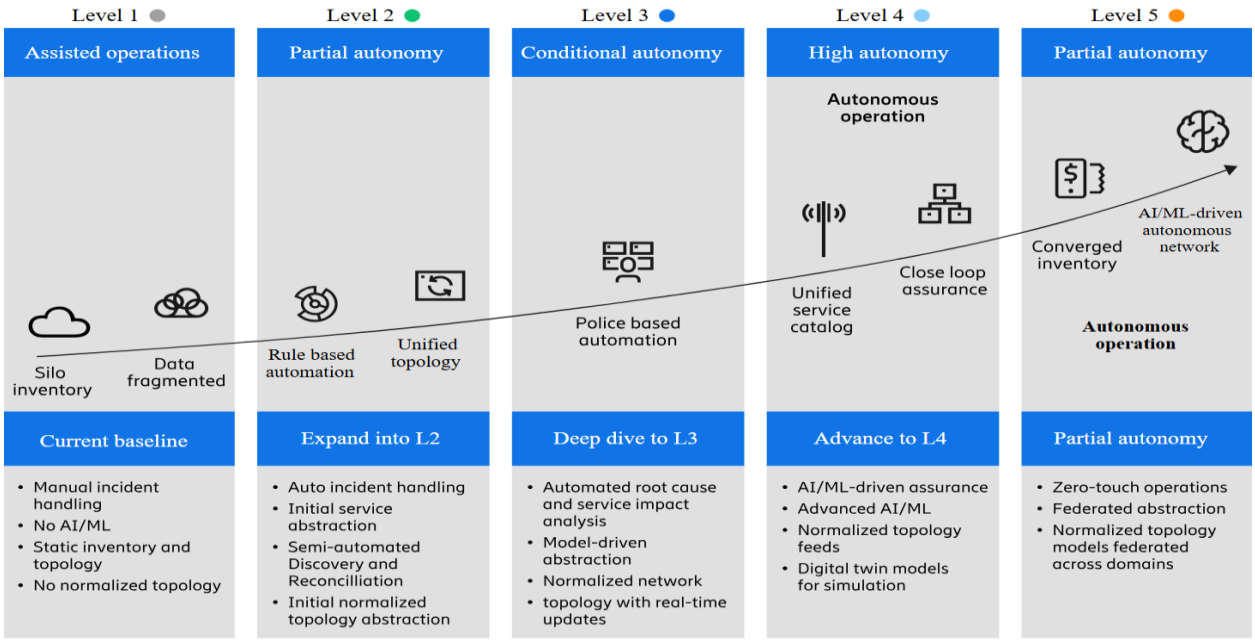


Рис. 1. План развития систем учета сетевых ресурсов [3].

Рассмотрим подробнее, какие возможности открывает использование распределенной архитектуры.

Распределенная архитектура и пограничные вычисления

В современном инвентаре изменения состояний происходят гораздо чем раньше, из-за чего первостепенно требуется обеспечить быстрое обнаружение и согласование (также известное как динамическая или активная инвентаризация) [1]. Этот процесс должен фиксировать изменения в инвентаризации и конфигурации (например, логических и виртуализированных сетевых ресурсов) практически в режиме реального времени для поддержки сценариев предоставления услуг и обеспечения качества обслуживания. Централизованные OSS-системы, традиционно развертываемые в ядре сети или в крупных дата-центрах оператора, могут становиться узким местом в сценариях, требующих оперативного доступа к данным о топологии, ресурсах и состоянии инфраструктуры. В таких условиях все более актуальным становится перенос отдельных функций управления и обработки сетевых данных ближе к месту их возникновения – на пограничный уровень сети. Такой подход позволяет сократить время доступа к данным, уменьшить задержки при принятии операционных решений и повысить масштабируемость системы управления. Кроме того, слайсинг сети хорошо себя показывает сам по себе, снижая задержки до 30 % [4], как и пограничные вычисления, будучи эффективнее обычного облачного подхода в мобильных сетях на 37-55 % [5].

Машинное обучение – планирование и предсказание емкости

Скачок популярности решений с использованием машинного обучения вполне обоснован их незаменимым на данный момент применением. Существуют решения, такие как платформа Anodot, что помогают в разработке передовых, автономных систем прогнозирования сети, многие операторы, например Nokia, используют методы искусственного интеллекта для определения масштабов проектов, понимания закономерности изменений в базе данных инвентаризации и лучшего представления о том, как и где развивается сеть [1]. В условиях усложнения сети, роста числа передающих устройств, увеличения разнообразия используемых абонентами услуг, работы с большими объемами данных, все большее влияние на результативность работы оператора связи оказывает его способность прогнозировать дальнейшие события, а также строить свою деятельность на основании этих прогнозов [6]. Надежная система учета в реальном времени, которую мы стремимся создать, служит основой для расширенной автоматизации и операций, управляемых искусственным интеллектом. Она предоставляет высококачественные данные, необходимые для обучения моделей машинного обучения, и поддерживает сетевое взаимодействие на основе намерений, в котором сеть может автономно настраиваться и оптимизировать себя для достижения конкретных целей.

Цифровой двойник NRI

Цифровой двойник NRI на пограничном уровне сети представляет собой программную модель сетевых ресурсов локального домена, синхронизированную с физической сетью с задержкой близкой к реальному времени. В отличие от центрального NRI, такой цифровой двойник ориентирован не на долгосрочное хранение данных, а на их операционную полезность. ЦД может выполнять большинство трудоемких функций, зависящих от времени отклика сети, ранее возложенных на NRI (которые мы можем делегировать благодаря микросервисному подходу ODA), проводить мониторинг своей зоны ответственности, т.е. собирать телеметрию, отслеживать состояние ресурсов и их загруженность, принимать решения при определенных инцидентах или на основе прогнозируемых с помощью машинного обучения и виртуальной модели данных. Концепция анализа «что, если?» с использованием цифрового двойника, виртуальной копии действующей сети, имеет центральное значение для обеспечения высокого уровня автономности [3].

Однако, эта среда моделирования ценна только в том случае, если она является идеальным, работающим в режиме реального времени, зеркальным отражением действующей сети. Работа NRI в реальном времени обеспечивает необходимый поток данных для создания и поддержания этого высокоточного двойника, позволяя поставщикам услуг тестировать изменения и прогнозировать результаты, не рискуя нарушить работу действующей сети.

Синтез этих подходов и их взаимодополняемость позволяет создать распределенную архитектуру, в которой цифровой двойник NRI превращается в высокоточную базу данных с возможностью автоматизированного управления и планирования развития сети, в то же время основной NRI остается единым источником истины, получая инкрементированные обновления в свою базу данных из цифровых двойников, что, теоретически, существенно снижает нагрузку на центр обработки данных.

Список используемых источников

1. Jeffery R., Crawshaw J. Inventory of the Future: Flexible, Scalable, and Highly Dynamic [Электронный ресурс] // Passionate about OSS. 2022. https://www.oracle.com/a/ocom/docs/corporate/analystrelations/inventory-of-the-future-flexible-scalable-and-highly-dynamic.pdf (дата обращения: 04.04.2026).

2. Mochalov V, Bratchenko N., Linets G., Yakovlev S. Distributed Management Systems for Infocommunication Networks: A Model Based on TM Forum Frameworks // Computers. 2019. Т. 8. № 2. С. 45. EDN: JKWPMY.

3. Whitham M., Au J. Autonomous networks: Use real-time inventory to unravel the challenge [Электронный ресурс] // The Ericsson Blog. 2025. https://www.ericsson.com/en/blog/2025/10/autonomous-networks-use-real-time-inventory-to-unravel-the-challenge (дата обращения: 04.04.2026).

4. Àlvarez-Campana M., López D. R., Moreno J. I., Rivera D., Sanz Rodrigo M. Digital Twins for 5G Networks: A Modeling and Deployment Methodology // IEEE Access. 2023. Т. 11. с. 38112-38126. EDN: YUGDQO.

5. Dalapati P., Kanellopoulos D. N., Poorzare R., Sharma V. K., Waldhorst O. P. Network Digital Twin Toward Networking, Telecommunications, and Traffic Engineering: A Survey // IEEE Access. 2025. Т. 13, с. 16489-16538. EDN: EQIWJZ.

6. Белозор А. М., Гольдштейн А. Б. Анализ применения методов машинного обучения для задач операторов связи // Информационные технологии и телекоммуникации. 2019. Т. 7. № 3. С. 26-30. EDN: BUFGNT.

УДК 621.396.2:004.7

АВТОНОМНАЯ LORA MESH-ПЛАТФОРМА С ЛОКАЛЬНЫМ ХРАНЕНИЕМ ДАННЫХ И ЖУРНАЛИРУЕМОЙ РЕПЛИКАЦИЕЙ

Г. С. Ворожцов (студент группы ИБ-31вп, ИНО СПбГУТ),
vorozhtsov.gs@sut.ru

В статье рассматривается архитектура автономной платформы передачи данных на основе радиосвязи дальнего действия LoRa. В отличие от типовой серверно-ориентированной схемы, где конечное устройство в основном отправляет короткие сообщения через шлюз в центральную инфраструктуру, предлагаемая нода хранит локальное состояние и журнал изменений. Ячеистая топология позволяет увеличивать дальность сети за счет промежуточных нод, которые выполняют ретрансляцию пакетов. Радиоканал используется для отложенной доставки и дельта-синхронизации данных при восстановлении связности. Показаны принципы компактного бинарного протокола, дедупликации, подтверждений, логических меток времени и профилей репликации по стоимости транспорта. Аппаратная конфигурация рассматривается как референсная реализация, а основной результат работы связан с сетевой и алгоритмической архитектурой платформы.

LoRa, mesh-сеть, распределенная база данных, журнал изменений, репликация данных, автономные сети, встроенные системы

Автономные узлы связи и мониторинга часто работают вне устойчивой инфраструктуры: без проводного канала, стабильной сотовой сети и постоянного доступа к серверу. Для таких условий важна не только дальность радиоканала, но и способность системы сохранять данные локально, переживать разрывы связности и восстанавливать согласованность после повторного появления соседних узлов. Поэтому задача платформы формулируется шире, чем передача отдельного сообщения: требуется сеть, в которой каждый узел является самостоятельным носителем состояния.

Сети дальнего радиуса действия с низким энергопотреблением обычно применяются для телеметрии, счетчиков и иных коротких сообщений. В типовом сценарии LoRaWAN конечные устройства передают полезную нагрузку через шлюзы к сетевому и прикладному серверам, где выполняются маршрутизация, обработка и долговременное хранение данных [1]. Такая модель хорошо подходит для централизованного интернета вещей, однако становится менее удобной там, где сервер или магистральный канал могут быть временно недоступны.

Предлагаемая платформа ориентирована на другой режим эксплуатации. Узел содержит локальное хранилище, журнал операций и механизм синхронизации с другими узлами. Если прямой путь к получателю отсутствует, изменение остается в журнале и передается позднее, в том числе через промежуточные ноды. При восстановимой связности это дает семантику отложенной доставки: данные не теряются из-за кратковременного разрыва канала, а повторная передача не приводит к повторному применению одной и той же операции.

Ячеистая топология является вторым ключевым отличием платформы. В сети типа «звезда» радиус работы ограничен возможностью конечного устройства достучаться до шлюза. В mesh-сети каждый узел может быть не только источником или получателем, но и ретранслятором. За счет многоходовой передачи зона покрытия расширяется последовательностью промежуточных нод, а отказ отдельного участка может компенсироваться перестроением маршрута. Такой подход соответствует общим принципам беспроводных mesh-сетей, где связность формируется не одним центральным каналом, а множеством соседских соединений [2].

Архитектура ноды разделена на радиоконтур и хост-уровень. Радиоконтур на базе трансивера SX1262 и микроконтроллера STM32 выполняет прием и передачу LoRa-кадров [3], адресацию, управление временем жизни пакета и первичную дедупликацию. Хост-уровень отвечает за топологию, маршрутизацию, локальную базу данных, прикладные модули и программный интерфейс. Конкретная связка STM32/SX1262 и Orange Pi используется как инженерный стенд; научно-технический фокус работы находится в протоколе доставки и репликации, а не в уникальности выбранного одноплатного компьютера.

Формат радиокадра сделан компактным и ориентированным на сверхмалую пропускную способность. Заголовок содержит идентификатор сети, адрес источника, адрес получателя, идентификатор пакета, счетчик времени жизни, флаги и длину полезной нагрузки. Пара «источник – идентификатор пакета» используется для дедупликации, а счетчик времени жизни ограничивает распространение кадра и защищает сеть от бесконечных петель. В отличие от подходов, где для работы в сетях с низкой пропускной способностью требуется специальная адаптация широких сетевых стеков, например сжатие и фрагментация заголовков [4], здесь применяется прикладно-ориентированный бинарный протокол с минимальным служебным расходом.

Для разных этапов работы используются два режима ретрансляции. Режим FLOOD предназначен для обнаружения соседей, первичного распространения служебных сообщений и работы до построения устойчивой карты сети. В этом режиме узлы пересылают широковещательный кадр дальше, если не видели его ранее, и если счетчик времени жизни еще не исчерпан. Режим DIRECTED применяется после появления маршрутной информации: решение о следующем переходе принимает хост, что снижает паразитную нагрузку на эфир и делает доставку более управляемой.

Механизм доставки строится не как абсолютная гарантия при любых отказах, а как гарантия в модели восстанавливаемой связности. Отправляемая операция помещается в локальный журнал и хранится до получения подтверждения от нужного узла или группы узлов. Повторная отправка допустима, поскольку каждая операция имеет устойчивый идентификатор и применяется идемпотентно. На транспортном уровне это соответствует повторной доставке до подтверждения, а на уровне данных – единственному эффекту применения, даже если один и тот же пакет был принят несколько раз.

Распределенная база данных проектируется вокруг журнала изменений, а не вокруг периодической передачи полного состояния. Каждая запись или операция получает логическую метку времени. При синхронизации узлы сравнивают метки последнего подтвержденного состояния и передают только дельты, отсутствующие у соседа. Логические часы позволяют упорядочивать события в распределенной системе без единого физического времени [5]. Для прикладных таблиц, где допустима политика «последняя запись побеждает», это дает детерминированное разрешение конфликтов, а спорные случаи могут фиксироваться отдельно для ручной или доменной обработки.

Дополнительно данные делятся по профилям репликации. Локальные параметры, временные сессии и диагностические сведения могут оставаться только на узле. Критичные дельты, например идентичность нод, конфигурация и минимальная телеметрия, передаются через LoRa. История большого объема, вложения, подробные журналы и массовая диагностика относятся к высокополосному профилю и синхронизируются только при наличии Wi-Fi, Ethernet или другого более дешевого транспорта. Такой механизм не блокирует развитие платформы в сторону универсальности, но защищает радиоканал от перегрузки.

Для прикладных подсистем предлагаемая архитектура задает единый уровень работы с данными и событиями. Сенсорные модули, сервисы конфигурации, журналы событий, механизмы аварийного оповещения и локальные панели управления взаимодействуют не с радиоканалом напрямую, а с локальным хранилищем и программным интерфейсом узла. Сетевая часть платформы определяет способ распространения изменений: локальное сохранение, передачу по LoRa, ретрансляцию через промежуточные ноды mesh-сети или синхронизацию по более широкополосному транспорту при его наличии. За счет этого прикладной уровень отделяется от маршрутизации, повторной передачи, подтверждений и выбора транспортного профиля.

Существенным свойством предложенной модели является переход от передачи отдельных сообщений к репликации устойчивого состояния. Событие, команда или телеметрическое значение фиксируются как запись в журнале изменений и сохраняются на узле до подтвержденной синхронизации. При временной потере связности данные не исчезают из коммуникационного контура, а остаются доступными для последующей доставки по принципу store-and-forward. Повторная передача и дедупликация позволяют приблизить транспортную семантику к модели at-least-once delivery, а идемпотентное применение операций и логические метки времени обеспечивают согласованное обновление состояния на уровне данных.

Mesh-топология расширяет область покрытия без опоры на единственный шлюз или постоянно доступный сервер. Промежуточные узлы выполняют функцию ретрансляторов и тем самым увеличивают достижимую дальность сети, а режимы FLOOD и DIRECTED позволяют разделить начальное обнаружение связности и рабочую маршрутизацию. В результате LoRa-канал используется не как простая линия доставки коротких пакетов в центральную инфраструктуру, а как часть распределенной среды, где узлы способны хранить, переносить и синхронизировать изменения даже при фрагментированной связности.

Таким образом, научно-техническая значимость работы состоит в формировании архитектуры автономной LoRa-сети, в которой основным объектом обмена является не изолированное сообщение, а изменение распределенного состояния. В отличие от серверно-ориентированных LPWAN-сценариев, где хранение и обработка данных в основном сосредоточены за пределами радиосети, предлагаемая модель переносит механизмы устойчивости, журналирования и отложенной синхронизации на уровень самих

узлов. Совмещение mesh-ретрансляции, компактного нативного протокола и дельта-репликации позволяет использовать LoRa для построения прикладно-независимого сетевого ядра, пригодного для автономных систем мониторинга, оповещения и управления в условиях нестабильной инфраструктуры связи.

Список используемых источников

1. LoRa Alliance. LoRaWAN® L2 1.0.4 Specification [Электронный ресурс]. 2023. URL: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification (дата обращения: 27.04.2026).

2. Akyildiz I. F., Wang X. A survey on wireless mesh networks // IEEE Communications Magazine. 2005. Vol. 43. № 9. P. S23-S30. DOI: 10.1109/MCOM.2005.1509968.

3. Semtech Corporation. SX1261/2 Long Range, Low Power, sub-GHz RF Transceiver. Datasheet. URL: https://www.semtech.com/products/wireless-rf/lora-connect/sx1262 (дата обращения: 27.04.2026).

4. Minaburo A., Toutain L., Gomez C., Barthel D., Zuniga J. C. RFC 8724: SCHC: Generic Framework for Static Context Header Compression and Fragmentation. IETF, 2020. URL: https://www.rfc-editor.org/rfc/rfc8724.html (дата обращения: 27.04.2026).

5. Lamport L. Time, Clocks, and the Ordering of Events in a Distributed System // Communications of the ACM. 1978. Vol. 21. № 7. P. 558-565. DOI: 10.1145/359545.359563.

Статья представлена научным руководителем, к.с.-х.н., доцентом, преподавателем кафедры СОД СПбГУТ С. А. Медведевым.

УДК 681.7.068, 621.39

СПОСОБЫ КОМПЕНСАЦИИ ХРОМАТИЧЕСКОЙ ДИСПЕРСИИ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ

Г. П. Гавриленков (студент группы ИКТО-27 СПбГУТ),
gavrilenkov.gp@sut.ru

В статье рассматривается проблема компенсации хроматической дисперсии (ХД) в волоконно-оптических системах связи (ВОСС). Известно, что ХД является одним из основных факторов, ограничивающих дальность и скорость передачи сигнала. Проведен сравнительный анализ существующих оптических и электронных методов компенсации ХД. Даны практические рекомендации по выбору методов компенсации ХД в ВОСС.

волоконно-оптические системы связи (ВОСС), хроматическая дисперсия, компенсация хроматической дисперсии, специальные оптические волокна для компенсации дисперсии, чирпированные волоконные брэгговские решетки, электронная компенсация дисперсии

Современные волоконно-оптические системы связи (ВОСС) являются основой высокоскоростных телекоммуникационных сетей. Однако с увеличением скорости передачи и длины линий возрастает влияние физических факторов, ухудшающих качество передачи сигнала, одним из которых является хроматическая дисперсия (ХД), при которой различные спектральные компоненты сигнала распространяются по оптическому волокну (ОВ) с разной скоростью. ХД приводит к искажению передаваемого сигнала и увеличению вероятности ошибок при его приеме. Для сохранения требуемого качества связи в ВОСС применяются методы компенсации дисперсии.

ХД в одномодовых ОВ и принцип ее компенсации

Основу инфраструктуры современных ВОСС составляют одномодовые (ОМ) ОВ. Наибольшее распространение на отечественных сетях получили стандартные ОМ ОВ, обладающие относительно большим коэффициентом ХД [1]. Рассмотрим распространение по ОМ ОВ оптического импульса (ОИ) с огибающей гауссовской формы, то есть зависимостью его мощности P_0 от внутриимпульсного времени T (время, отсчитываемое от середины ОИ):

$$P_0(T) = P_{0m} \cdot exp(-T^2/T_0^2), \quad (1)$$

где P_{0m} – амплитуда мощности оптического импульса (амплитуда), T_0 – полуширина оптического импульса на уровне P_{0m} / e. Будем считать ОИ

спектрально ограниченным, то есть $\Delta\omega_0 \cdot T_0 = 1$, где $\Delta\omega_0$ – полуширина спектра ОИ. В [2] показано, что в ОМ ОВ длиной z огибающая ОИ (1) принимает вид:

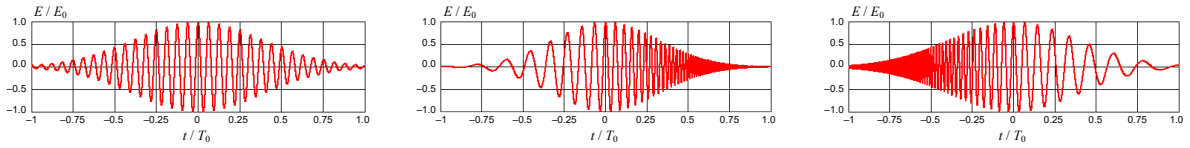
$$P_z(T,z) = \frac{P_{0m} \cdot exp(-\alpha \cdot z)}{\sqrt{1+(z/L_D)^2}} \cdot exp\left(-\frac{T^2}{T_0^2 \cdot [1+(z/L_D)^2]}\right), \quad (2)$$

где α – коэффициент затухания ОВ, L_D – дисперсионная длина ОВ:

$$L_D = T_0^2/|\beta_2|, D_x = -2\pi \cdot c \cdot \beta_2/\lambda_0^2. \quad (3)$$

В (3) β_2 – дисперсия групповых скоростей (ДГС) ОВ, связанная с коэффициентом ХД D_x, λ_0 – длина волны. Из (2) следует, что ОИ на выходе ОМ ОВ сохраняет гауссовскую форму огибающей и ширину амплитудного спектра, но его фазовый спектр меняется. ОИ приобретает внутриимпульсную линейную частотную модуляцию (рис. 1). Глубину возникающей модуляции характеризуют параметром C – чирпингом, зависящим от знака коэффициента ХД D_x:

$$C(z) = -sgn(D_x) \cdot (z/L_D). \quad (4)$$



а б в

Рис. 1. ОИ, прошедшие ОМ ОВ: а – без ХД ($\beta_2 = 0$, $C = 0$),
б – с нормальной ХД ($\beta_2 > 0$, $D_x < 0$, $C > 0$), в – с аномальной ХД ($\beta_2 < 0$, $D_x > 0$, $C < 0$)

Возможность оптической компенсации ХД основана на том, что в ОВ возникает чирпинг, знак которого зависит от знака D_x. Он может быть скомпенсирован в другом ОВ, если оно имеет противоположный знак D_x.

Компенсация ХД с помощью специальных ОМ ОВ

Для уширения ОИ в линейном тракте, состоящем из двух ОВ с длинами l_1 и l_2 и коэффициентами ХД D_{x1} и D_{x2}, справедливо выражение:

$$\Delta T = \sqrt{T_z^2 - T_0^2} = |D_{x1} \cdot l_1 + D_{x2} \cdot l_2| \cdot \Delta\lambda, \quad (5)$$

где $\Delta\lambda$ – ширина спектра ОИ [2]. Для зависимостей D_{x1} и D_{x2} от длины волны λ можно использовать выражения [1]:

$$D_{x1}(\lambda) = D_{x1}(\lambda_1) + S_{x1}(\lambda_1) \cdot (\lambda - \lambda_1), D_{x2}(\lambda) = D_{x2}(\lambda_2) + S_{x2}(\lambda_2) \cdot (\lambda - \lambda_2), \quad (6)$$

где λ_1 и λ_2 – длины волн, для которых известны значения $D_{x1}(\lambda_1)$, $D_{x2}(\lambda_2)$ и $S_{x1}(\lambda_1)$, $S_{x2}(\lambda_2)$, $S_x = \mathrm{d}D_x / \mathrm{d}\lambda$ – наклон дисперсионной характеристики.

Если D_{x1} и D_{x2} имеют разные знаки, то из (5) и (6) можно определить длину второго ОВ, необходимую для компенсации ХД:

$$l_2 = -\frac{D_{x1}(\lambda_1)+S_{x1}(\lambda_1)\cdot(\lambda-\lambda_1)}{D_{x2}(\lambda_2)+S_{x2}(\lambda_2)\cdot(\lambda-\lambda_2)} \cdot l_1 = -\frac{D_{x1}(\lambda_1)}{D_{x2}(\lambda_2)} \cdot \frac{1+RDS_{x1}(\lambda_1)(\lambda-\lambda_1)}{1+RDS_{x2}(\lambda_2)(\lambda-\lambda_2)}, \quad (7)$$

где $RDS_x = S_x / D_x$ – относительный наклон коэффициента ХД. Реальная компенсация в некотором диапазоне длин волн возможна, если: 1) D_{x1} и D_{x2}, а также S_{x1} и S_{x2} имеют в данном диапазоне разные знаки; 2) $RDS_{x1} = RDS_{x2}$.

Наиболее часто реализуется сосредоточенная компенсация ХД с помощью модулей, представляющих собой бухты со специальным компенсирующим ОВ (Dispersion Compensating Fiber, DCF) [3]. DCF имеет коэффициент и наклон ХД, знаки которых противоположны знакам коэффициента и наклона ХД основного ОВ. Абсолютная величина коэффициента ХД в DCF обычно в несколько раз превышает абсолютную величину коэффициента ХД в телекоммуникационном ОВ.

DCF разрабатывается специально для конкретного ОМ ОВ. Недостатком такого способа компенсации является увеличение затухания на участке с компенсатором. В реальной ВОСС увеличение затухания может быть скомпенсировано увеличением уровня сигнала в начале участка или установкой оптического предусилителя перед фотоприемником.

Компенсация ХД с помощью волоконных брэгговских решеток

Волоконная брэгговская решетка (ВБР) представляет собой участок ОВ, показатель преломления (ПП) сердцевины которого периодически изменяется вдоль оси ОВ. Спектр отражения ВБР сосредоточен вблизи длины волны Брэгга λ_B, зависящей от периода изменения ПП Λ [4]

$$\lambda_B = 2n_{eff}\Lambda, \quad (8)$$

где n_{eff} – эффективный ПП для основной моды.

Для компенсации ХД используются чирпированные ВБР, период которых линейно меняется вдоль ОВ от Λ_{max} до Λ_{min}, создавая разную задержку

для разных длин волн [5]. Если компенсацию ХД необходимо осуществлять для сигнала с шириной спектра $\Delta\lambda$, для Λ_{max} и Λ_{min} справедливо:

$$\Lambda_{\frac{\lambda_{B0}+\Delta\lambda/2}{2n_{eff}}}{}_{max}, \Lambda_{\frac{\lambda_{B0}-\Delta\lambda/2}{2n_{eff}}}{}_{min}, \quad (9)$$

где λ_{B0} – длина волны Брэгга для центральной части ВБР. ХД D, создаваемая такой ВБР, может быть оценена по выражению:

$$D = 2n_{eff}/(\mathrm{c} \cdot \Delta\lambda). \quad (10)$$

Для подключения компенсатора ХД на основе ВБР используют оптические циркуляторы, позволяющие разделить падающий и отраженный сигналы (рис. 2)

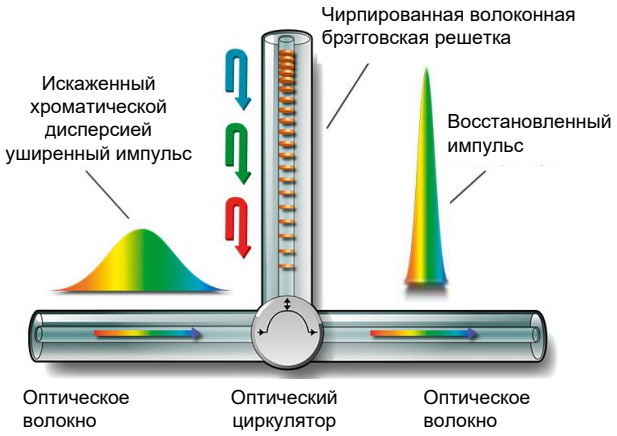


Рис. 2. Подключение компенсатора ХД на основе ВБР

Достоинствами компенсаторов на основе ВБР являются низкие вносимые потери, малая задержка сигнала при распространении, небольшие габариты, а также возможность перестройки в широких пределах [5]. К недостаткам таких компенсаторов относят необходимость стабилизации температуры и защиты от механических воздействий, сложность обеспечения линейного изменения периода при изготовлении длинных чирпированных ВБР.

Электронная компенсация дисперсии

Появление когерентных ВОСС позволило не только повысить скорость передачи благодаря использованию более эффективных многоуровневых амплитудно-фазовых форматов модуляции, но и осуществлять компенсацию ХД в электрическом тракте путем цифровой обработки принятого сигнала. Электронная компенсация ХД не вносит дополнительных оптических

потерь и обладает высокой гибкостью, однако требует вычислительных ресурсов.

Наиболее распространенными являются алгоритмы, осуществляющие линейную компенсацию ХД в частотной или во временной области [6]. Обработка сигнала осуществляется цифровым фильтром с конечной (КИХ) или бесконечной (БИХ) импульсной характеристикой, согласованной с параметрами ОВ.

Недостатком линейных алгоритмов является отсутствие учета нелинейных искажений сигнала в ОВ, которые должны компенсироваться отдельно. Существует возможность одновременной компенсации ХД и нелинейных искажений. Такие алгоритмы основаны на решении нелинейного уравнения Шредингера [7]. Они эффективны, но требуют существенно больше вычислительных ресурсов по сравнению с линейными алгоритмами.

Рекомендации по применению методов компенсации ХД

Методы оптической компенсации ХД универсальны и могут использоваться в ВОСС как с энергетическим, так и с когерентным приемом, при этом:

- компенсаторы на основе DCF предпочтительны для обработки широкополосных сигналов;
- компенсаторы на основе ВБР с возможностью перестройки предпочтительны для обработки сигналов в условиях меняющейся длины линии из-за оптической маршрутизации, а также в ВОСС с повышенной чувствительностью к остаточной ХД.

Методы электронной компенсации ХД могут использоваться только в ВОСС с когерентным приемом и являются наилучшим решением для высокоскоростных систем.

Список используемых источников

1. Рекомендация ITU-T G.652 (08/2024): Характеристики одномодового оптического волокна и кабеля [Электронный ресурс] / Международный союз электросвязи. Женева, 2024. URL: https://www.itu.int/rec/T-REC-G.652.ru (дата обращения: 12.04.2026).

2. Былина М. С. Оптические волокна в телекоммуникациях: учебное пособие / М. С. Былина, С. Ф. Глаголев; СПбГУТ. Санкт-Петербург, 2019. 108 с.

3. Былина М. С. Компенсация дисперсии в оптических линейных трактах с использованием DWDM / М. С. Былина, С. Ф. Глаголев, Н. С. Кузнецова, О. Н. Рык // Фотон-экспресс. 2009. № 7 (79). С. 32-35.

4. Варжель С. В. Волоконные брэгговские решетки: учеб. пособие / С. В. Варжель; Ун-т ИТМО. Санкт-Петербург: Университет ИТМО, 2015. 65 с.

5. Dispersion Management: Fiber Bragg Grating based DCM [Электронный ресурс]: white paper / Proximion Fiber Systems AB. Kista, Sweden. 12 p. URL: https://www.proximion.com/hubfs/bu-pr/white-paper/dispersion-compensation/ White_Paper_DCM.pdf (дата обращения: 28.04.2026).

6. Savory S. J. Digital filters for coherent optical receivers / S. J. Savory // Optics Express. 2008. Vol. 16. N 2. P. 804-817. DOI: 10.1364/OE.16.000804.

7. Бурдин В. А. Электронная компенсация в волоконно-оптических линиях передачи на основе нелинейных фазовых фильтров / В. А. Бурдин, И. В. Григоров // T-Comm: Телекоммуникации и транспорт. 2013. № 5. С. 18-24.

Статья представлена научным руководителем, заведующим кафедрой ОКСС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 621.39, 530.182

ПОДДЕРЖАНИЕ КВАЗИСОЛИТОННОГО РЕЖИМА В ВОСС С WDM ПРИ ЧЕРЕДОВАНИИ СЕРИЙНЫХ ТИПОВ ОМ ОВ С ПРОТИВОПОЛОЖНЫМИ ЗНАКАМИ ДГС

С. Э. Доценко (аспирант кафедры ОКСС СПбГУТ), dotsenko.sergey@sut.ru

В статье исследована возможность поддержания квазисолитонного режима распространения оптических импульсов в волоконно-оптических системах связи (ВОСС) со спектральным уплотнением каналов (WDM) при использовании серийных типов одномодовых оптических волокон (ОМ ОВ) с различными знаками дисперсии групповой скорости (ДГС). Рассматривается метод управления дисперсией путем периодического чередования участков ОМ ОВ с нормальной и аномальной ДГС, обеспечивающий баланс между дисперсионными и нелинейными эффектами при малом отрицательном среднем значении ДГС. Проведено имитационное моделирование четырехканальной системы WDM со скоростью передачи 10 Гбит/с на канал. Проанализированы конфигурации ВОЛТ на основе комбинаций волокон G.652 и DCF, а также G.655. Показано, что квазисолитонный режим позволяет обеспечить устойчивое распространение импульсов на расстояния до 1000 км с сохранением их формы и длительности.

квазисолитонный режим, волоконно-оптическая система связи, WDM, одномодовое оптическое волокно, дисперсия групповых скоростей, управление дисперсией, нелинейная оптика, имитационное моделирование

Непрерывный рост потребности в пропускной способности магистральных ВОСС требует внедрения новых подходов к повышению эффективности передачи информации. Одним из перспективных направлений является использование нелинейных свойств ОМ ОВ для формирования солитонных режимов распространения оптических импульсов. В идеальном случае солитонный режим обеспечивается строгим балансом хроматической дисперсии (ХД) и фазовой самомодуляции (ФСМ), что гарантирует неизменность формы импульса на сверхдальних расстояниях [1-3]. Однако в реальных ВОСС наличие потерь, дискретных оптических усилителей (ОУ) и ограничений по вводимой мощности препятствует существованию фундаментальных солитонов.

На практике в ВОСС реализуется квазисолитонный режим, при котором баланс дисперсионных и нелинейных эффектов выполняется приближенно, но импульсы сохраняют устойчивость формы на протяжении всего волоконно-оптического линейного тракта (ВОЛТ). В предыдущих работах

были исследованы механизмы поддержания квазисолитонного режима в одноканальных ВОСС с управляемой дисперсией и различными схемами ОУ [2, 3].

Целью настоящей работы является исследование влияния параметров серийных ОМ ОВ на устойчивость квазисолитонного режима в многоканальных системах WDM, а также сравнительный анализ энергетической эффективности различных комбинаций ОМ ОВ.

Распространение оптических импульсов в ОМ ОВ с учетом нелинейных эффектов и ХД описывается модифицированным нелинейным уравнением Шредингера (НУШ) [1]

$$i\frac{\partial A}{\partial z}+\frac{\beta_2}{2}\frac{\partial^2 A}{\partial t^2}+\gamma\mid A\mid^2 A=0 \qquad (1)$$

где *A(z, t)* – комплексная амплитуда огибающей электрического поля; *z* – расстояние от начала ОМ ОВ; *t* – время, отчитываемое от середины импульса; β_2 – коэффициент дисперсии групповых скоростей (ДГС); γ – коэффициент нелинейности ОМ ОВ.

В отсутствие потерь уравнение (1) имеет решение в виде фундаментального солитона [1]:

$$A(z,t)=\sqrt{P_0}sech(t/T_0)exp(iz/2L_D), \qquad (2)$$

где P_0 – пиковая мощность импульса; T_0 – его длительность; $exp(iz/2L_D)$ – фазовый множитель, определяющий набег фазы $\phi = z/2L_D$. Устойчивость такой формы сигнала достигается при точном балансе ХД и ФСМ, что характеризуется равенством дисперсионной L_D и нелинейной L_{NL} длин [1]:

$$L_D=\frac{T_0^2}{|\beta_2|},\ L_{NL}=\frac{1}{\gamma P_0}. \qquad (3)$$

Для реализации квазисолитонного режима в реальных ВОСС применяется метод управления дисперсией. В рамках данной работы рассматривается ВОЛТ, состоящий из *M* последовательно соединенных секций. Каждая секция включает два типа ОМ ОВ с противоположными знаками ДГС и длинами l_n (нормальная дисперсия) и l_a (аномальная дисперсия). Среднее значение ДГС на участке ВОЛТ определяется выражением [2]:

$$\langle\beta_2\rangle=\frac{\beta_{2n}l_n+\beta_{2a}l_a}{l_n+l_a} \qquad (4)$$

где β_{2n} и β_{2a} – коэффициенты ДГС соответствующих типов ОМ ОВ.

Формирование квазисолитона с управляемой дисперсией требует поддержания малого отрицательного значения $\langle\beta_2\rangle$, при котором нелинейность компенсирует остаточную дисперсию. При этом параметры импульса (пиковая мощность и ширина) периодически осциллируют в пределах каждой секции ВОЛТ.

Для многоканальных систем WDM необходимо учитывать зависимость параметров ОМ ОВ от несущей частоты каждого канала. Зависимость коэффициента ХД D и ДГС β_2 от длины волны λ аппроксимируется линейно [4]:

$$D_x(\lambda) = D(\lambda_0) + S(\lambda - \lambda_0), \quad \beta_2(\lambda) = -D_x(\lambda) \cdot \lambda_0^2/(2\pi \cdot c)\ , \qquad (5)$$

где S – наклон дисперсионной характеристики; c – скорость света в вакууме. Коэффициент нелинейности также является функцией длины волны [2]:

$$\gamma = \frac{2\pi n_2}{\lambda A_{eff}} \qquad (6)$$

где n_2 – нелинейный показатель преломления, A_{eff} – эффективная площадь моды ОМ ОВ.

С учетом уравнений (4)-(6) расчетная пиковая мощность P_0, необходимая для поддержания квазисолитонного режима в m-м канале WDM, определяется как [2]:

$$P_{0m} = \frac{|\langle\beta_2\rangle|}{\gamma T_0^2} \qquad (7)$$

Компенсация потерь в ВОЛТ осуществляется дискретными ОУ (EDFA), установленными в конце каждого ВОЛТ. Коэффициент усиления G выбирается равным суммарному затуханию на участке ВОЛТ: $G = \exp(\alpha L)$, где α – коэффициент затухания, $L = M(l_n + l_a)$ – длина участка [1].

Для исследования устойчивости квазисолитонного режима проведено имитационное моделирование четырехканальной ВОСС со скоростью передачи 10 Гбит/с на канал. Несущие частоты каналов выбраны с шагом 400 ГГц: $\nu_0 = 193$ ТГц, $\nu_1 = 193.4$ ТГц, $\nu_2 = 193.8$ ТГц, $\nu_3 = 194.2$ ТГц.

В качестве среды передачи рассмотрены две конфигурации ВОЛТ на базе серийных типов ОМ ОВ:

1. Стандартное ОМ ОВ (SSMF) G.652 и компенсирующего (DCF).

2. ОМ ОВ с ненулевой смещенной дисперсией (NZDSF) марки G.655 TrueWave и G.655 SMF-LS.

Параметры используемых ОМ ОВ на длине волны $\lambda = 1550$ нм, принятые в модели в соответствии с паспортными данными производителей, представлены в таблице 1 [5].

ТАБЛИЦА 1. Параметры серийных ОМ ОВ, используемых в модели ВОЛТ

Тип ОМ ОВ	α, дБ/км	D, пс/(нм·км)	S, пс/(нм²·км)	A_{eff}, мкм²	$n_2 \cdot 10^{-21}$, м²/Вт	β_2, пс²/км	γ, (Вт·км)$^{-1}$
G.652 (SSMF)	0.20	17	0.058	82	23.5	-21.6	1.16
DCF	0.40	-103	-0.35	21	27.0	131.4	5.21
G.655 (TrueWave)	0.22	4.5	0.045	52	26.0	-5.7	2.03
G.655 (SMF-LS)	0.20	-3	-0.05	48	26.0	3.80	2.20

На рисунке 1 представлена структурная схема моделируемого ВОЛТ. Каждый участок ВОЛТ включает в себя M секций с чередованием знаков ДГС для обеспечения малого среднего значения $\langle \beta_2 \rangle = -0.2$ пс²/км. В первой конфигурации секция состоит из отрезка DCF $l_n = 1$ км и SSMF $l_a = 6.1$ км. Во второй конфигурации используются ОМ ОВ G.655 SMF-LS $l_n = 6$ км и G.655 TrueWave $l_a = 4.4$ км с соответствующими длинами участков для обеспечения требуемой остаточной дисперсии.

Для компенсации затухания в ОМ ОВ в конце каждого ВОЛТ установлены дискретные усилители EDFA. Входная мощность каналов P_{in} рассчитывается с учетом коэффициента энергетического усиления K по формуле (8), что позволяет нивелировать влияние потерь и поддерживать среднюю мощность сигнала на уровне, необходимом для существования квазисолитона [3].

$$P_{in} = K \cdot P_0, \qquad K = \frac{G \ln G}{G-1}, \tag{8}$$

где G – коэффициент усиления, соответствующий потерям в ОМ ОВ на участке ВОЛТ.

Расчетные значения пиковой мощности P_{in} для формирования квазисолитонного режима (при условии обеспечения средней ДГС $\langle \beta_2 \rangle = -0.2$

пс²/км) составили: для ОМ ОВ G.655 на всех каналах 3.7 мВт; для ОМ ОВ G.652+DCF на канале 3 P_{03} = 5.6 мВт, на канале 2 P_{02} = 5.5 мВт, на канале 1 P_{01} = 5.4 мВт, на канале 0 P_{00} = 5.3 мВт.

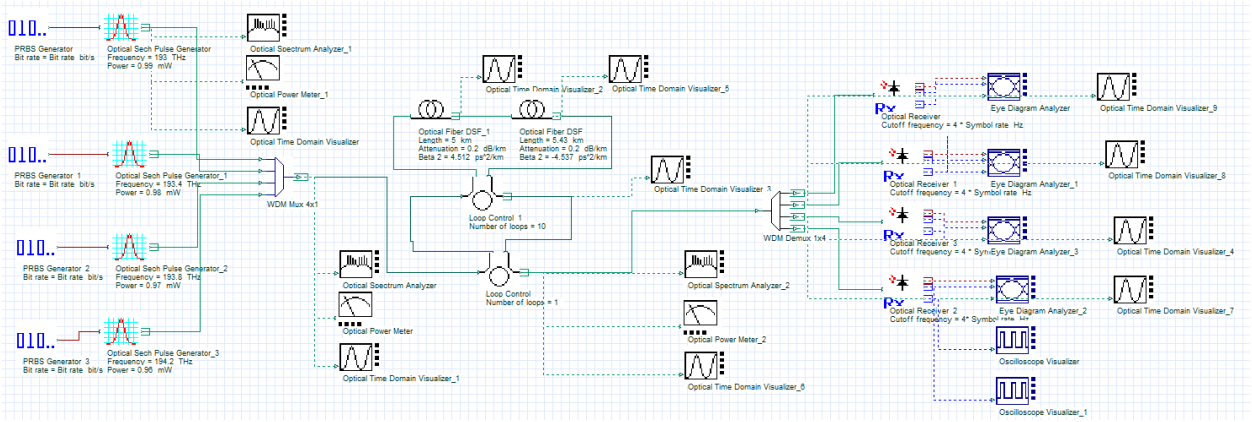


Рис. 1. Схема моделирования многопролетной солитонной ВОСС WDM с управлением дисперсией

В ходе исследования проведено моделирование четырехканальной ВОСС с WDM для двух выбранных конфигураций ВОЛТ на дистанциях до 1000 км. В таблице 2 представлены результаты для первой конфигурации, использующей комбинацию ОМ ОВ G.652 и DCF. Длина одного участка ВОЛТ составила 106.5 км (15 секций) с общим затуханием 26.4 дБ.

ТАБЛИЦА 2. Параметры сигналов в ВОЛТ на базе ОМ ОВ G.652 и DCF

Длина ВОСС, км	Q_{cp} (каналы 0–3)	P_{lm}, мВт	t_{ul}, пс
106.5	33.0–39.0	5.3–5.6	20.3–20.5
426.0	15.0–18.0	5.5–5.8	19.8–20.0
1065.0	12.0–13.0	5.4–5.8	20.5–21.4

Анализ данных таблицы 2 показывает, что в ВОСС на базе G.652 и DCF поддерживается устойчивый квазисолитонный режим. Несмотря на накопление шумов усилителей EDFA и снижение Q-фактора с ростом длины ВОСС, длительность импульсов t_{ul} сохраняется в узком диапазоне (19.8–21.4 пс), а пиковая мощность P_{lm} остается практически неизменной (5.4–5.9 мВт), что подтверждает компенсацию дисперсионного расширения нелинейными эффектами.

Результаты моделирования второй конфигурации ВОЛТ на базе ОМ ОВ G.655 TrueWave и G.655 SMF-LS) при длине участка 103,6 км (10 секций) и общем затухание 21.7 дБ представлены в таблице 3.

ТАБЛИЦА 3. Параметры сигналов в ВОЛТ на базе ОМ ОВ семейства G.655

Длина ВОСС, км	Q_{cp} (каналы 0–3)	P_{lm}, мВт	t_{ul}, пс
103.6	35.0–47.0	3.65	20.7
414.4	17.0–22.0	3.80	19.8–20.0
1036.0	12.0–13.0	3.75–3.80	20.3–20.4

Для ВОЛТ на базе G.655 характерна более высокая энергетическая эффективность: требуемая пиковая мощность импульсов для поддержания режима составила 3.7 мВт, что примерно на 35 % ниже, чем в случае комбинации G.652+DCF. При этом стабильность длительности импульсов ($t_{ul} \approx 20$ пс) остается идентичной.

Особого внимания заслуживают условия формирования квазисолитонного режима в конфигурации на базе ОМ ОВ G.655. Несмотря на то, что расчетные дисперсионные длины для данных ОМ ОВ ($L_{Dn} = 34$ км и $L_{Da} = 23$ км) существенно превышают физическую длину отдельных участков ($l_n = 6$ км и $l_a = 4.4$ км), результаты моделирования подтверждают формирование устойчивого квазисолитонного режима.

Это явление объясняется спецификой ВОЛТ с управлением дисперсией: баланс между дисперсионными и нелинейными эффектами реализуется не в пределах каждого отдельного сегмента ОМ ОВ, а усредненно по всей длине секции [1].

Дополнительно была проверена устойчивость режима при отклонении пиковой мощности от расчетной. При снижении мощности до 1 мВт наблюдалось резкое падение Q-фактора (до 5–6) и расплывание импульсов ($t_{ul} > 32$ пс). При увеличении мощности до 10 мВт возникали значительные нелинейные искажения, сокращающие длительность импульса до 14–15 пс. Это подтверждает, что именно рассчитанные значения P_{in} обеспечивают оптимальный баланс ХД и ФСМ.

Заключение

1. Метод управления дисперсией в ВОЛТ со спектральным уплотнением на базе серийных ОМ ОВ обеспечивает устойчивость квазисолитонного режима на дистанциях до 1000 км.

2. Конфигурация на основе ОМ ОВ G.655 снижает требуемую пиковую мощность импульсов на 35 % по сравнению с комбинацией G.652 и DCF при сохранении идентичной стабильности длительности импульса (~20 пс).

3. Устойчивость квазисолитонного режима подтверждается достижением баланса нелинейных и дисперсионных эффектов в среднем по длине секции, что позволяет сохранять форму сигнала даже при превышении дисперсионной длины L_D на отдельных участках ВОЛТ.

Список используемых источников

1. Agrawal G. P. Nonlinear Fiber Optics. 5th ed. Oxford: Academic Press, 2013. 629 p.

2. Былина М. С., Глаголев С. Ф., Доценко С. Э. Метод управления дисперсией для поддержания квазисолитоного режима распространения импульсов в высокоскоростной волоконно- оптической системе связи // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 16–26. DOI:10.31854/1813-324X-2024-10-4-16-26. EDN: KIGLSY.

3. Глаголев С. Ф., Доценко С. Э. Квазисолитонный режим в многопролетной волоконно-оптической системе связи с применением оптических усилителей // Труды учебных заведений связи. 2023. Т. 9. № 2. С. 47–56. DOI:10.31854/1813-324X-2023-9-2-47-56.

4. Глаголев С. Ф., Доценко С. Э., Соколов Г. Ю., Юдина Е. А. Исследование влияния хроматической дисперсии в одномодовых оптических волокнах на импульсы различной формы // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2022. С. 349-353.

6. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М.: ЛЕСАР-арт, 2003. 288 с.

Статья представлена научным руководителем кандидатом технических наук, доцентом кафедры ОКСС С. Ф. Глаголевым.

УДК 004.946

МЕТОДЫ ОБЪЕКТИВНОЙ ОЦЕНКИ ВИЗУАЛЬНОГО КАЧЕСТВА В ИММЕРСИВНЫХ ПРОСТРАНСТВАХ

С. Д. Елкин (студент группы Р-41м СПбГУТ), elkin.sd@sut.ru

В данной статье рассматривается проблема объективной оценки качества иммерсивного видео, которая требует учета сферической природы контента и интерактивных особенностей восприятия. Рассматриваются как модификации стандартных метрик, так и специализированные подходы, включая методы, основанные на глубоком обучении. Особое внимание уделяется компенсации проекционных искажений и моделированию зрительного внимания для повышения точности оценки.

иммерсивное видео, ODV, взвешенный сферический ПОСШ, параболическая проекция ПОСШ, ПОСШ всенаправленного видео

Введение

Для объективной оценки качества применяются метрики, которые необходимо коррелировать с субъективными оценками качества, полученными от зрителей. Метрики объективной оценки качества для традиционного двумерного видео не идеально подходят для видео с круговым обзором (omnidirectional video, ODV) [1]. При работе с иммерсивным видео нужно учитывать два уникальных аспекта, которых нет в обычных двумерных видео. Во-первых, иммерсивное видео имеет сферическую структуру, но обычно его хранят в двумерных плоских форматах для обеспечения совместимости с существующими стандартами хранения и потоковой передачи видео. Такое преобразование сферических изображений в плоские неизбежно влечет за собой искажения, которые не свойственны традиционному видео, поскольку плоская проекция не может полностью передать сферическую перспективу. Вдобавок, плоские изображения характеризуются четкими границами, которых нет в оригинальном сферическом представлении. Во-вторых, необходимо учитывать интерактивные особенности восприятия сферического видео. Поле зрения намного шире, чем у стандартного видео, но пользователь просматривает лишь его часть через шлем виртуальной реальности. В связи с этим, анализ контента иммерсивного видео требует обязательного учета поведения пользователей и моделирования зрительного внимания, особенно при оценке качества, поскольку искажения в наиболее заметных областях оказывают большое влияние на воспринимаемое визуальное качество.

Стандартные метрики для оценки видео

Возможный подход к оценке качества иммерсивных видео заключается в применении метрик, разработанных для стандартных видео, к сферическим видео, хранящимся в форматах сферической проекции. Хотя данный метод не является идеальным, поскольку не учитывает искажения сферической проекции. К распространенным полным эталонным метрикам для традиционного видео относятся: пиковое отношение сигнал/шум (PSNR), индекс структурного сходства (structural similarity index measure, SSIM) [2], его многомасштабная версия (multiscale structural similarity index measure, MS-SSIM) [3], точность визуальной информации (visual information fidelity, VIF) [4], показатель потери детализации (detail loss metric, DLM). PSNR представляет собой пиксельную метрику, основанную на расчете среднеквадратичной ошибки. Данная метрика широко используется для оценки эффективности методов кодирования и восстановления данных благодаря своей вычислительной простоте и математической удобности, даже если не сильно коррелируется с субъективным восприятием качества. В отличие от него, SSIM является метрикой, основанной на восприятии, которая вычисляет различия между исходным и искаженным изображениями по трем сравнительным параметрам: яркости, контрастности и структуре. Данные параметры рассчитываются для каждой позиции пикселя с учетом соседних пикселей в пределах локального окна, после чего объединяются в итоговую оценку качества. Наиболее совершенной версией данной метрики считается MS-SSIM, которая вычисляет сравнительные параметры SSIM на нескольких масштабах изображения, а не на одном, что характерно для базовой версии SSIM.

Другой перспективной полной эталонной метрикой для стандартного видео, недавно разработанной Netflix, является метрика слияния многометодной оценки видео (video multimethod assessment fusion, VMAF). VMAF – это показатель, предназначенный для оценки искажений, полученных в результате сжатия или масштабирования, и демонстрирует высокую степень корреляции с субъективными оценками качества. Алгоритм VMAF предполагает первоначальное извлечение объектов из каждого видеокадра на основе метрик DLM, VIF и анализа движения. Для каждого кадра вычисляется оценка качества. Итоговая оценка качества видео формируется путем усреднения полученных покадровых оценок. VMAF использует набор данных

с 34 эталонными и 300 искаженными видео вместе с субъективными оценками качества [5].

Всенаправленные метрики, основанные на стандартных методах

В отличие от метрик для традиционного двумерного видео, показатели оценки качества иммерсивного видео должны учитывать его специфические особенности, включая сферическую структуру контента и характеристики восприятия. Для компенсации проекционных искажений, присущих сферическим проекциям, применяются два основных подхода: использование весов искажений и методы повторной дискретизации. Веса искажений коррелируют с уровнем проекционного искажения в конкретной области и могут быть пропорциональны площади, которую пиксель занимает в сферическом представлении иммерсивного видео. Метрики на основе повторной дискретизации либо извлекают области обзора с минимальными проекционными искажениями, либо преобразуют сферическое видео в формат проекции с пониженными проекционными искажениями, либо работают с равномерно распределенными точками на сфере. Для учета характеристик просмотра сферического видео часто применяются веса визуального внимания, рассчитываемые на основе статистики просмотра или характеристик контента [6]. Архитектура большинства метрик включает два компонента: модуль извлечения признаков, идентифицирующих искажения, и модуль, преобразующий эти признаки в итоговую оценку качества. При оценке иммерсивного видео вычисляются покадровые метрики качества, которые впоследствии объединяются с использованием либо простого усреднения, либо более сложных методов временного объединения, учитывающих особенности человеческого зрительного восприятия.

Подавляющее большинство метрик качества, разработанных специально для видео с круговым обзором, представляют собой модификации стандартного PSNR. Разработано взвешенное сферическое пиковое отношение сигнал/шум (weighted spherical PSNR, WS-PSNR) [7], который включает в себя весовые коэффициенты, учитывающие проекционные искажения пикселей в плоской проекции. Эти веса пропорциональны площади, занимаемой пикселем на сфере. В отличие от этого подхода, метрика параболической проекции Крастера ПОСШ (craster parabolic projection PSNR, CPP-PSNR) [8] вычисляет значение PSNR не в исходной проекции, а в проекции, характеризующейся пониженным уровнем проекционных искажений.

Существует метод моделирования пространственно-временных искажений для объективной оценки качества иммерсивного видео, учитывающий временную динамику изменений искажений между кадрами. Разработанная полноэталонная метрика, названная ПОСШ всенаправленного видео (omnidirectional video PSNR, OV-PSNR) [7], использует в качестве базовых единиц анализа пространственно-временные сегменты. Процедура извлечения сегментов предполагает равномерное разделение каждого кадра в равнопрямоугольной проекции (Equirectangular Projection, ERP) на блоки, при этом для каждого блока формируется сегмент, включающий его соответствия в соседних кадрах вдоль траектории движения. Временной масштаб сегментов соответствует типичной продолжительности фиксации глаз. Оценка искажений осуществляется для каждого сегмента с учетом механизмов зрительного восприятия, после чего производится пространственно-временное объединение полученных значений для расчета общего уровня искажений всего иммерсивного видео.

Всенаправленные метрики, основанные на глубоком обучении

В дополнение к метрикам, основанных на стандартных методах, были разработаны метрики на основе глубокого обучения, которые демонстрируют наивысшую производительность в оценке качества сферических видео. Данные подходы состоят из двух ключевых компонентов: модуля извлечения признаков, основанных на сверточных слоях и компонентой оценке регрессии, основанном на полностью связанных слоях [6]. Большинство метрик, основанных на глубинном обучении, работают с участками, которые извлекаются либо напрямую из проекции через обрезку изображения, либо как области обзора на основе гномонической проекции. В процессе обработки для каждого участка вычисляются либо его характеристики, либо весовые коэффициенты, либо локальные оценки, которые впоследствии объединяются в одну. Для компенсации сферических искажений применяются веса искажений, либо производится выборка участков с низким уровнем проекционных искажений, либо в входные данные включаются координаты положения участка. Учет особенностей просмотра иммерсивного видео осуществляется через интеграцию данных о движении головы и глаз, которые используются для расчета весов участков и пикселей, либо для определения локации выборки участков. Прогнозирование визуального внимания реализуется через предобученные модели. Модели глу-

бокого обучения нуждаются в предварительном обучении, что предполагает наличие значительных объемов размеченных данных, содержащих экспертные оценки. Однако доступные сейчас ресурсы такого типа ограничены по размеру. Наиболее крупным набором данных для оценки визуального качества с учетом движений головы и взгляда является VQA-OD (Video Quality Assessment for Omnidirectional Video), включающий 60 оригинальных видео и 540 их модифицированных версий, которые были оценены 221 человеком. Чтобы справиться с небольшими наборами обучающих данных, используются методы увеличения, такие как извлечение участков или ротация. В дополнение к стандартному обучению, состязательное обучение также успешно применяется для решения задачи прогнозирования качества.

Заключение

Традиционные метрики, такие как PSNR и SSIM, демонстрируют ограниченную эффективность в оценке качества иммерсивного видео, поскольку не учитывают его специфику. Ключевыми проблемами являются проекционные искажения, возникающие при преобразовании сферического видео в двумерный формат. Современные специализированные метрики адаптируют стандартные подходы, путем использования весовых коэффициентов, компенсирующие пространственные искажения, и учета данных о зрительном внимании. Методы, основанные на глубоком обучении, представляют собой наиболее перспективное направление, демонстрирующее высокую точность прогнозирования.

Таким образом, создание универсальной и высокоточной метрики для иммерсивных видео остается актуальной научной проблемой.

Список используемых источников

1. Arbind Agrahari Baniya, Tsz-Kwan Lee, Peter W. Eklund, Sunil Aryal: Omnidirectional Video Super-Resolution Using Deep Learning [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/10102571 (дата обращения: 10.03.2026).

2. Varshini Appana, Tulasi Manasa Guttikonda, Divya Shree, Shahana Bano, Himasri Kurra: Similarity Score of Two Images using Different Measures [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/9358789 (дата обращения: 10.03.2026).

3. Z. Wang, E.P. Simoncelli, A.C. Bovik: Multiscale structural similarity for image quality assessment [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/1292216 (дата обращения: 10.03.2026).

4. Chenchen Peng; Mixia Wu; Kaiyuan Liu: Multiple Levels Perceptual Noise Backed Visual Information Fidelity for Picture Quality Assessment [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/10082853 (дата обращения: 10.03.2026).

5. Marta Orduna, Cesar Diaz, Lara Munoz, Pablo Perez, Ignacio Benito, Narciso Garcia: Video Multimethod Assessment Fusion (VMAF) on 360VR Contents [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/8924618 (дата обращения: 10.03.2026).

6. Simone Croci, Ashutosh Singla, Stephan Fremerey, Alexander Raake, Aljosa Smolic: Subjective and objective quality assessment for omnidirectional video [Электронный ресурс]. URL: https://www.researchgate.net/publication/367480398_Subjective_and_objective_quality_assessment_for_omnidirectional_video (дата обращения: 10.03.2026).

7. Yufeng Zhou, Mei Yu, Hualin Ma, Hua Shao, Gangyi Jiang: Weighted-to-Spherically-Uniform SSIM Objective Quality Evaluation for Panoramic Video [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/8652269 (дата обращения: 10.03.2026).

8. Jayasingam Adhuran, Chathura Galkandage, Gosala Kulupana, Anil Fernando: A Novel Spherical Video Quality Metric for 360° Video Coding [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/9900878 (дата обращения: 10.03.2026).

Статья представлена научным руководителем, заведующим кафедрой ЦТМ СПбГУТ, кандидатом технических наук, доцентом С. Л. Фёдоровым.

УДК 621.396.94

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ СПУТНИКОВОЙ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ СПУТНИКОВОЙ ГРУППИРОВКИ

А. В. Задимидько (студент группы РМ-22 СПбГУТ), zadimidko.av@sut.ru
А. О. Тишков (ассистент кафедры БТС СПбГУТ), tishkov.ao@sut.ru

В статье рассматривается процесс моделирования системы спутниковой связи между двумя наземными станциями, взаимодействие между которыми осуществляется через спутниковую группировку. Исследуемая методика основана на пакете расширения Satellite Communications Toolbox. В работе выполняется расчет и выбор оптимального маршрута передачи сигнала через спутниковую группировку с учетом расстояния между спутниками, условий видимости и продолжительности использования данного маршрута. Описанная методика может помочь в анализировании и проектировании низкоорбитальных спутниковых сетей, обеспечивающих передачу данных на большие расстояния.

спутниковая связь, низкоорбитальные спутники, моделирование, MATLAB, Satellite Communications Toolbox, визуализация сценария спутниковой связи, маршрутизация

Развитие спутниковых систем связи связано с ростом требований к передаче данных между удаленными наземными объектами. Во многих случаях прямая видимость между станциями отсутствует, а использование неземной инфраструктуры затруднено из-за географических условий. В таких ситуациях перспективным решением является применение низкоорбитальных спутниковых группировок, которые легко обеспечивают передачу сигнала через несколько промежуточных спутников.

Одним из важных направлений проектирования таких систем является выбор маршрута передачи данных. При многоскачковой передаче, сигнал последовательно проходит от начальной наземной станции к одному или нескольким спутникам, а затем к конечной станции. Эффективность маршрутов зависит от расположения спутников, углов видимости, расстояния между узлами и времени доступности линий связи [1].

Для анализа подобных систем, маршрутов, очень удобно использовать программу MATLAB, и ее пакет Satellite Communication Toolbox [2]. С их помощью можно создать разные сценарии движения спутников, воспроизвести наземные станции, рассчитать геометрическую видимость и определить интервалы доступности маршрута. Данный подход дает возможность

оценить работоспособность спутниковой сети еще на этапе предварительного проектирования маршрутов.

Исходным сценарием является связь между двумя наземными станциями, которые не имеют прямой видимости друг с другом из-за географических особенностей. Для обеспечения взаимодействия используются спутниковая группировка, которые движутся вокруг Земли.

Основные параметры моделирования включают себя:

- количество спутников в группировке;
- параметры орбит;
- максимальная длина канала;
- требуемое качество сигнала.

Моделирование спутниковой системы выполняется в несколько последовательных этапов, начиная с создания спутниковой группировки и заканчивая таблицей с интервалами передачи данных.

Первым этапом моделирования сценария является создание двух наземных станций, расположенные на фиксированных координатах, и тысяча спутников, которые движутся по определенным орбитам [3]. Для каждого спутника выбирается тип орбиты, высота, наклонение.

На данном этапе формируется базовая структура сценария, включающая в себя орбиты с тысячей спутников и двумя наземными станциями [4]. Эта структура сценария служит основой для последующей настройки параметров и анализа (рис. 1).

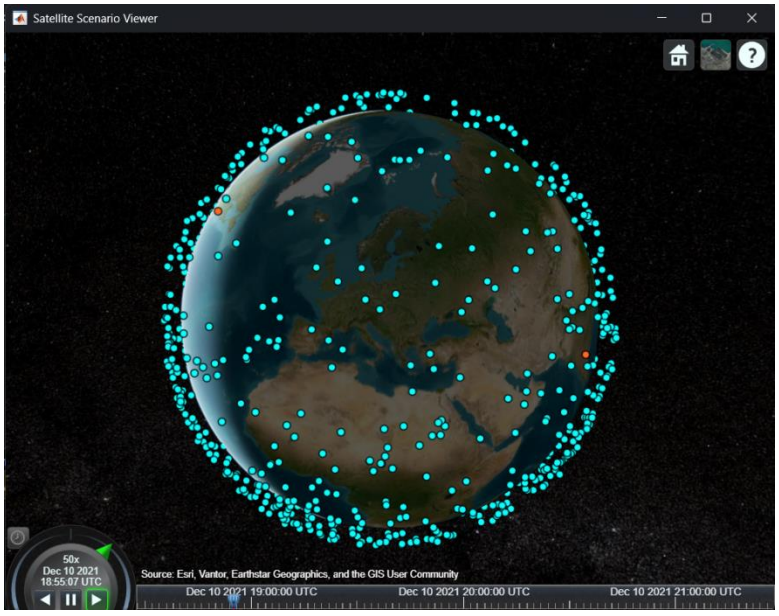


Рис 1. Визуализация базовой структуры

После создания базовой структуры сценария определяется возможность соединения между спутниками. Для этого рассчитываются расстояние между летательными аппаратами и проверяется наличие прямой видимости между спутниками.

На основе полученных данных формируется графы связности, где спутники являются вершинами, а возможные каналы связи – это ребра. Это позволяет определить все потенциальные маршруты передачи сигнала от одной наземной станции к другой. На рисунке 2 показана обобщенная схема такого пути (S1-S11 – это спутники; G1-G2, это наземные станции). Схема [5] не привязана к конкретной орбитальной плоскости, но отражает общий принцип: наземная станция получает доступ к первому спутнику, после чего данные передаются по другим спутникам и выводятся на конечную наземную станцию.

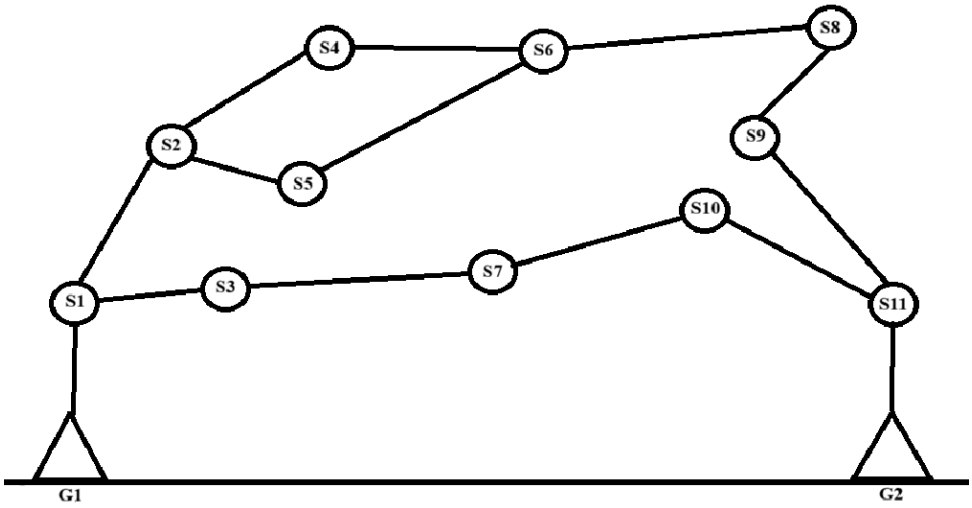


Рис 2. Концептуальная схема машрута

Вторым этапом является выборка маршрута передачи данных. Для каждого возможного пути рассчитываются:

- общая длина маршрута;
- уровень сигнала на каждом участке;
- длительность существования данного маршрута.

Оптимальным считается маршрут, обеспечивающий устойчивую связь при минимальных потерях сигнала и длительностью больше минуты.

Особенностью рассматриваемой системы является динамическое изменение конфигурации группировок. Поскольку спутники находятся в постоянном движении вокруг земли, то выбранный маршрут может перестать существовать, из-за помех [1]. В таком случае система автоматически перестраивает маршрут передачи, выбирая новый доступный путь к наземной станции (рис. 3).

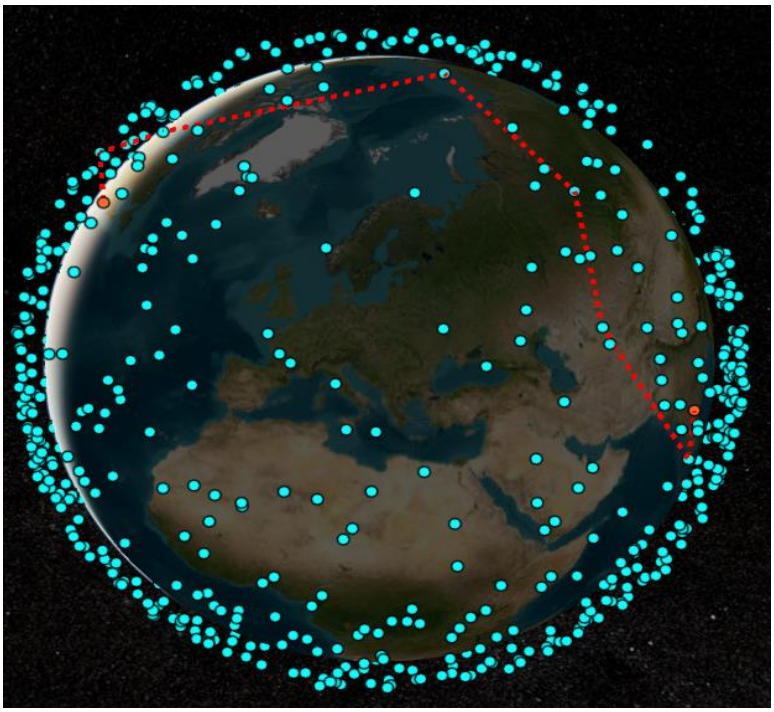


Рис 3. Визуализация одного из маршрутов

После оптимизации маршрута появляется таблица, показывающая дату и время оптимального подключения наземных станций друг к другу (таблица 1).

ТАБЛИЦА 1. Оптимальные подключения между станциями

Начало машрута	Конец маршрута	Номера интервалов	Начало связи	Конец связи	Длительность подключения
Отправитель	Получатель	1	10.12.2021 18:27:57	10.12.2021 18:29:57	120 с
Отправитель	Получатель	2	10.12.2021 20:01:57	10.12.2021 20:04:57	180 с

Полученные результаты показывают, что найденные в начальный момент пути не остаются пригодными для передачи данных, из-за чего подтверждается необходимость постоянной перестройки маршрута. Поэтому для спутниковых сетей перспективой является графовые алгоритмы, расчет маршрутов и многокритериальная оценка путей.

Таким образом, в данной статье рассмотрены возможности имитационного моделирования спутниковых систем связи. Также, можно сделать вывод, что представленная методика является достаточно эффективным инструментом для проектирования узлов связи в труднодоступной местности и выборе оптимальных маршрутов для их работы.

Список используемых источников

1. Satellite Communication Toolbox. Satellite Multi-Hop Satellite Communications Link Between Two Ground Stations. [Электронный ресурс]. URL: https://www.mathworks.com/help/satcom/ug/multihop-satellite-communication.html (Дата обращение: 12.04.2026)

2. Satellite Communications Toolbox. MathWorks. [Электронный ресурс] URL: https://www.mathworks.com/products/satellite-communications.html (Дата обращения: 12.04.2026)

3. Satellite Communications Toolbox. Getting Started Guide. MathWorks. [Электронный ресурс]. URL: https://nl.mathworks.com/help/pdf_doc/satcom/satcom_gs.pdf (Дата обращения: 12.04.2026)

4. Satellite Communication Toolbox. Multi-Hop Path Selection Through Large Satellite Constellation. [Электронный ресурс]. URL:https://nl.mathworks.com/help/satcom /ug/multi-hop-path-select-through-sat-constellation.html

5. Камнев В. Е, Черкасов В. В, Чечин Г. В. / Спутниковые сети связи: Учеб. пособие М.: «Альпина Паблишер», 2004. 536 с.: ил. ISBN 5-94599-099-X

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры БТС СПбГУТ А. Н. Степутиным.

УДК 621.396

ИССЛЕДОВАНИЕ ПРИЕМА СИГНАЛОВ ТОЧЕК ДОСТУПА WI-FI С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНО-КОНФИГУРИРЕМОГО РАДИО

Я. А. Иванов (студент группы РМ-21 СПбГУТ), ivanov.ya@sut.ru

Популярность беспроводных локальных сетей постоянно растет. Все больше домов, офисных зданий, кафе и других общественных мест оснащаются соответствующим оборудованием для подключения настольных компьютеров, ноутбуков, планшетов и смартфонов к интернету. Кроме того, беспроводные LAN позволяют двум или нескольким расположенным неподалеку компьютерам обмениваться данными и без выхода в интернет. При исследовании беспроводных сетей важное значение имеет анализ параметров сигналов точек доступа, позволяющий оценивать уровень сигнала, используемый канал, тип модуляции и особенности радиоканала. В работе исследуется прием сигналов точек доступа Wi-Fi с использованием технологий программно-конфигурируемого радио. Использование программно-конфигурируемого радио позволяет реализовать программный приемник радиосигнала и выполнять анализ сигналов физического уровня стандарта IEEE 802.11. В исследовании используется программная среда MATLAB и библиотека WLAN Toolbox для приема служебных кадров beacon и извлечения параметров беспроводных сетей.

802.11, WLAN, SDR, Beacon, анализ сигналов Wi-Fi

Современные беспроводные локальные сети широко используются для организации доступа к сети Интернет и передачи данных между устройствами. С увеличением плотности развертывания беспроводных сетей возрастает необходимость анализа параметров радиосигналов точек доступа, что позволяет изучать характеристики распространения радиоволн, оценивать качество связи и оптимизировать настройки сети. Традиционные сетевые адаптеры Wi-Fi предоставляют ограниченный доступ к параметрам сигнала и не позволяют анализировать физический уровень передачи данных. Для проведения более детального анализа радиосигналов обычно применяются специализированные измерительные комплексы, однако их использование требует дорогостоящего оборудования. Альтернативным решением является применение технологий программно-конфигурируемого радио [1-3].

Программно-конфигурируемое радио является радиооборудованием, в котором большинство функций выполняются в программном виде, а функции, выполняемые аппаратно, должны оперативно модифицироваться по требованию рабочего стандарта связи. Аппаратная часть системы

выполняет только преобразование радиочастотного сигнала в цифровую форму, после чего дальнейшая обработка осуществляется на обычном персональном компьютере или на ПЛИС (Программируемая логическая интегральная схема) с использованием алгоритмов цифровой обработки сигналов. Такой подход позволяет исследовать структуру сигналов различных стандартов связи, включая IEEE 802.11 [4].

В беспроводных сетях стандарта Wi-Fi точки доступа периодически передают служебные beacon-кадры, которые используются для объявления о наличии сети и передачи параметров ее работы клиентским устройствам. Принимая такие кадры, устройства могут обнаруживать доступные сети, синхронизировать свою работу и получать информацию о конфигурации точки доступа.

Beacon-кадр имеет стандартную структуру и включает MAC-заголовок (Media Access Control-заголовок) IEEE 802.11, тело кадра и последовательность проверки ошибок (FCS). В теле кадра содержится набор параметров, характеризующих работу беспроводной сети. Структура beacon-кадра представлена на рисунке 1.

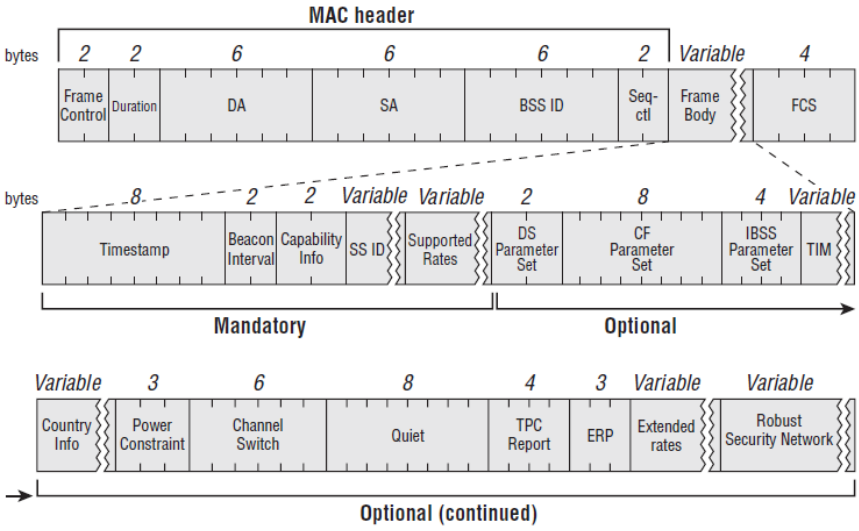


Рис. 1. Структура beacon-кадра

К основным параметрам, содержащимся в beacon-кадре, можно отнести: SSID (Service Set Identifier) – идентификатор сети, BSSID (Basic Service Set Identification) – MAC-адрес точки доступа, используемый радиоканал, ширина канала, поддерживаемые стандарты беспроводной связи, а также временные параметры синхронизации. Передача beacon-кадров осуществляется через регулярные интервалы времени, которые обычно составляют около 100 мс.

Исследование параметров beacon-кадров дает возможность оценивать состояние радиочастотной среды и анализировать работу беспроводных сетей. Для исследования параметров таких кадров может использоваться технология программно-конфигурируемого радио. В практической части работы применяется подход, реализованный в среде MATLAB, позволяющий принимать и анализировать beacon-кадры точек доступа Wi-Fi. При этом программное обеспечение выполняет сканирование каналов диапазонов 2,4 и 5 ГГц, захватывает радиосигнал с помощью SDR-приемника и обрабатывает полученные выборки в среде MATLAB. В диапазоне 2,4 ГГц маяки чаще всего передаются с модуляцией DSSS (Direct Sequence Spread Spectrum). В диапазоне 5 ГГц маяки всегда передаются с модуляцией OFDM (Orthogonal Frequency-Division Multiplexing).

В рамках работы был использован программный алгоритм приема и обработки сигналов Wi-Fi с использованием среды MATLAB. Для обработки сигналов используется библиотека WLAN Toolbox [5], содержащая инструменты моделирования и анализа сигналов стандарта IEEE 802.11. Блок-схема процедуры приема beacon-кадра представлена на рисунке 2.

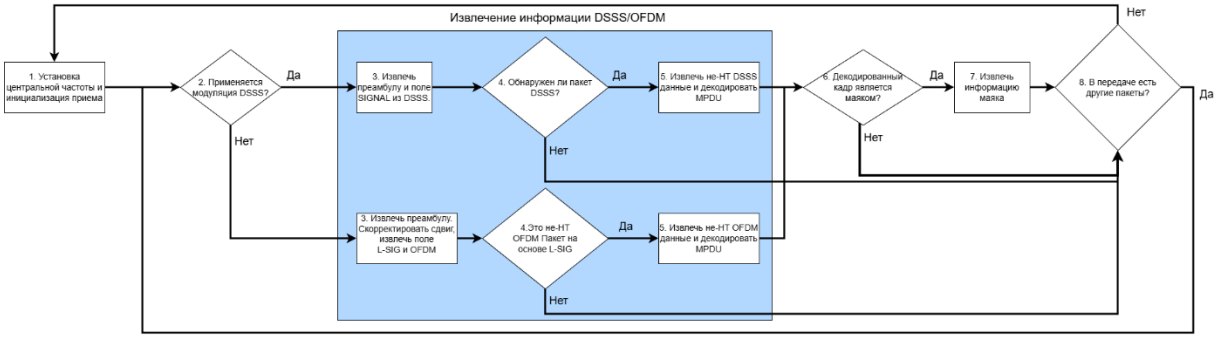


Рис. 2. Блок-схема процедуры приема beacon-кадра

В работе используется предварительно записанный сигнал Wi-Fi, содержащий радиосигналы точек доступа в диапазонах 2,4 ГГц и 5 ГГц. Данные сигналы представлены в виде комплексных отсчетов, которые могут быть получены с помощью SDR-приемника.

Работа программы начинается с инициализации параметров, определяющих диапазон частот (2,4 или 5 ГГц), тип модуляции (OFDM или DSSS), частоту дискретизации и набор сканируемых каналов. При использовании SDR дополнительно настраиваются параметры приемника, такие как центральная частота, коэффициент усиления и время захвата сигнала.

После настройки выполняется захват радиосигнала на выбранных каналах. Программа может работать как в режиме приема сигнала с SDR-

устройства, так и в режиме обработки ранее записанных данных. Полученные выборки анализируются для обнаружения beacon-кадров.

Далее выполняется декодирование обнаруженных пакетов. В зависимости от типа сигнала применяются алгоритмы обработки для сигналов OFDM или DSSS, которые обеспечивают синхронизацию, демодуляцию и извлечение данных MAC-кадра. Из успешно декодированных beacon-кадров извлекаются основные параметры точки доступа: SSID, BSSID, используемый канал, ширина канала и отношение сигнал-шум (SNR).

Полученная информация, представленная на рисунке 3, сохраняется и представляется в виде таблицы, содержащей параметры обнаруженных точек доступа. Дополнительно программа может выполнять визуализацию спектра и спектрограммы сигнала, что позволяет оценить характеристики принимаемого радиосигнала и наличие помех.

SSID	BSSID	Vendor	SNR (dB)	Primary Operating Channel	Current Channel Center Frequency Index	Channel Width (MHz)	Band	Mode
"WLAN_5G"	"04D4C451C584"	"ASUSTek COMPUTER INC."	34.57	52	50	"160"	5	"802.11ax"
"w-inside"	"B0B867F6B2D0"	"Hewlett Packard Enterprise"	26.24	56	58	"80"	5	"802.11ac"
"w-mobile"	"B0B867F6B2D1"	"Hewlett Packard Enterprise"	26.251	56	58	"80"	5	"802.11ac"
"w-guest"	"B0B867F6B2D2"	"Hewlett Packard Enterprise"	25.843	56	58	"80"	5	"802.11ac"
"w-inside"	"B0B867F3D9B0"	"Hewlett Packard Enterprise"	31.592	157	155	"80"	5	"802.11ac"
"w-mobile"	"B0B867F3D9B1"	"Hewlett Packard Enterprise"	31.971	157	155	"80"	5	"802.11ac"
"w-guest"	"B0B867F3D9B2"	"Hewlett Packard Enterprise"	33.3	157	155	"80"	5	"802.11ac"

Рис. 3. Информация, полученная из кадров-маяков для конфигурации «OFDM, band 5»

На рисунке 3 показано, что после декодирования beacon-кадров было обнаружено 7 точек доступа, работающих в диапазоне 5 ГГц. Установлено, что исследуемые сети используют рабочие каналы 52, 56 и 157, а ширина канала составляет 80 и 160 МГц.

В ходе работы была рассмотрена программная реализация приема и анализа кадров-маяков точек доступа Wi-Fi с использованием технологий программно-конфигурируемого радио. Инструменты среды MATLAB позволяют использовать ранее записанные выборки из файла или использовать программно-конфигурируемое радио для сканирования каналов диапазонов 2,4 и 5 ГГц. Полученные данные позволяют проводить анализ параметров точек доступа и исследовать особенности функционирования беспроводных сетей Wi-Fi.

Таким образом, использование технологий программно-конфигурируемого радио и средств MATLAB позволяет эффективно реализовать систему мониторинга и анализа сигналов точек доступа, что может быть применено при исследовании характеристик радиоканала и оптимизации параметров беспроводных сетей.

Список используемых источников

1. Beacon frame. Wikipedia. URL: https://en.wikipedia.org/wiki/Beacon_frame (дата обращения: 15.03.2026).

2. Фокин Г. А. Принципы и технологии цифровой связи на основе программно-конфигурируемого радио: обзор современных тенденций в области создания комплекса подготовки специалистов // Труды учебных заведений связи. 2019. № 1. URL: https://cyberleninka.ru/article/n/printsipy-i-tehnologii-tsifrovoy-svyazi-na-osnove-programmno-konfiguriruemogo-radio-obzor-sovremennyh-tendentsiy-v-oblasti (дата обращения: 15.03.2026).

3. Мещеряков Д. Е., Фокин Г. А. Исследование приема сигналов точек доступа Wi-Fi с использованием программно-конфигурируемого радио // Материалы научно-технической конференции. СПб. СПбГУТ. URL: https://conf-ntores.etu.ru/assets/files/2025/sbornik-konferencii/182-185.pdf (дата обращения: 15.03.2026).

4. IEEE 802.11 Working Group. URL: https://www.ieee802.org/11/ (дата обращения: 15.03.2026).

5. WLAN Beacon Receiver Using Software-Defined Radio. MathWorks. URL: https://www.mathworks.com/help/wlan/ug/ofdm-beacon-receiver-using-software-defined-radio.html (дата обращения: 15.03.2026).

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Г. А. Фокиным.

УДК 004.932

ИССЛЕДОВАНИЕ МЕТОДОВ ДЛЯ АНАЛИЗА ВИДЕОИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИИ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОТДЕЛЕНИЙ СБЕРБАНКА

Е. И. Туманова (к.т.н., доцент кафедры ЦТМ, СПБГУТ)
Д. А. Катыкин (студент группы Р-41м, СПБГУТ), katykin.da@sut.ru

В данной статье представлено исследование существующих методов для анализа видеоизображений. Проведен сравнительный анализ по различным критериям, а также выдвинуты трудности реализации подобных моделей для цели обеспечения безопасность отделений банков.

видео, компьютерное зрение, обеспечение безопасности, искусственный интеллект, банкинг

Ухудшение социально-экономической обстановки может привести к росту агрессивного поведения, что отразится в увеличении количества инцидентов в отделениях банков, в частности в отделениях ПАО «Сбербанк». Стремительная трансформация финансового сектора в цифровую среду, а также повсеместное внедрение алгоритмов интеллектуальных систем [1], позволят построить превентивную защиту, основанную на компьютерном зрении и машинном обучении, что будет функционировать быстрее и лучше традиционных систем видеонаблюдения [2]. Однако, при внедрении подобных видеосистем нужно учитывать стандарты комплаенса, требования к обработке данных и технические возможности реализации в данной сфере [3].

Перед переходом к описанию и сравнению методов определим терминологию анализа видеоизображений с использованием искусственного интеллекта (ИИ). Под этим понимается автоматизированное получение семантической информации из видеоряда для последующей классификации и определения объектов или выявления паттернов поведения [2]. В случаях, когда поведение отличается от указанных (заготовленных) сценариев – это называется аномалией поведения, что и является акцентом поиска. Для определения качества моделей применяются следующие критерии:

- *точность* (precision) – показывает, насколько успешно классификатор различает объекты одного класса от другого;
- *полнота* (recall) – показывает долю правильно классифицированных положительных примеров от общего числа истинно положительных примеров;

● *усредненная точность модели* (mAP) – позволяет оценить и сравнить качество моделей детекции, опираясь как на точность, так и на полноту;

● *AUC* – площадь на графике под ROC-кривой, отображающая соотношение между чувствительностью модели (True Positive Rate, TPR) и вероятностью ложного срабатывания (False Positive Rate, FPR) при различных порогах отсечения, пример графика можно наблюдать на рис. 1;

● *скорость обработки в реальном времени* [3].

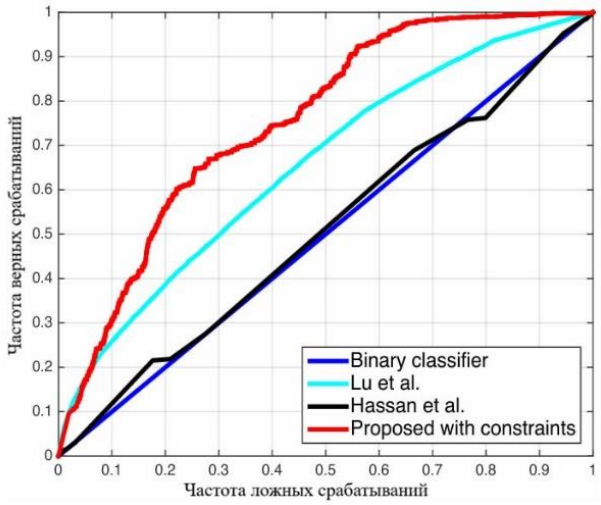


Рис. 1. Пример графика AUC

Определив термины и определения, можно описать и сравнить современные методы и решения, как для детекции объектов, так и для детекции аномалий.

Детекция объектов в основе построена на сверточных нейронных сетях. Самый частый объект обнаружения – человек. Для обеспечения безопасности отделений банка детекция человека, находящегося в закрытые часы работы отделения у входа дольше заданного периода времени, важна, так как может давать сигнал в отделы реагирования. Для этого лучше всего подходит архитектура семейства YOLO. Оно демонстрирует высокие показатели точности и полноты, в особенности YOLOv8x обеспечивает mAP в 53,9 %, а скорость обработки кадра на GPU T4 равна 14,37 мс, что затратно для реализации на Edge-устройствах в масштабах количества отделений. Однако другая модель – YOLOv8n при mAP в 53,7 % обрабатывает кадр за 1,47 мс. Это делает модель 8n более предпочтительной не только из-за скорости, но и по еще одному важному критерию – масштабируемости, поскольку отделений Сбербанка на территории РФ по состоянию на 2024 – 2026 гг. уже больше 4500. Для задач видеонаблюдения, где объект занимает

значимую часть кадра – точность детекции достигает 85-90 %. Так же стоит отметить, что обнаружение человека с помощью этого семейства не предел возможности, так как модель можно настроить и на сторонние объекты, которые не были фиксированы в кадре ранее. Это позволит обнаруживать и сообщать о теоретических взрывных и иных, наносящих урон разной степени, средствах. Сравнение с другими моделями отображено в таблице 1.

ТАБЛИЦА 1. Сравнение моделей для обнаружения объектов

Модель	mAP, %	Время обработки кадра, мс
YOLOv8n	53,7	1,47
YOLOv8s	53,9	6,06
YOLOv8x	53,9	14,37
YOLOv9c	53,8	26,32
EfficientDet-D7	53,7	128,07
Faster R-CNN	42,0	83,33

Детекция аномалий представляет больший интерес для превентивной безопасности, так как позволит описывать куда более сложные и настраиваемые сценарии. Развитие этого метода позволит с большой вероятностью прогнозировать дальнейшие действия людей, что входят или уже находятся в отделении банка. Это позволит моментально обнаружить следующие события:

1. Изучение информации об отделении. Реализуется через распознавание аномалий поведения: постоянный осмотр окружения, быстрое вращение головы, использование неяркой и неброской одежды, съемка на телефон или камеру, запись видео, общение через мессенджер и т.д.

2. Потенциальную агрессию можно определять через резкие движения, нервозное хождение из стороны в сторону, постоянные периодические взгляды в сторону со стойками менеджеров.

3. Сценарии ограблений выявляются обнаружением холодного или огнестрельного оружия в руках грабителя, выхода нескольких лиц из машины у дверей отделения или сокрытие лиц масками.

Сложность детектирования аномалий заключается в их редкости. Трудно сформировать базу данных для обучения, а инсценировка сцен может передавать аналогичные события не точно, что отразится на качестве

выявления. Для этого используется подход Multiple Instance Learning (обучение на нескольких экземплярах) [4]. Этот метод работает со слабо размеченными данными: целевой файл видео помечается как «нормальный» или «содержащий аномалию», но не указывается точное время и место события. Модель учится различать видеофрагменты с высоким и низким уровнем аномальности, что значительно снижает трудозатраты на разметку.

Подход Sultani et al (MIL) продемонстрировал хорошие результаты на сложных реальных датасетах, таких как UCF-Crime, достигнув площади под ROC-кривой в 75.41 % [4]. Это демонстрирует потенциал подобных систем детектирования для обеспечения безопасности отделений банков. Результаты сравнения других методов можно наблюдать в таблице 2.

ТАБЛИЦА 2. Сравнение моделей для обнаружения аномалий

Модель	Датасет	AUC, %	Точность, %	Полнота, %
Sultani et al. (MIL)	UCF-Crime	75.41	72.30	68.50
Liu et al. [5]	UCSD Ped2	95.40	92.10	90.50
Autoencoder-based	Avenue	78.60	74.10	71.20
GAN-based	ShanghaiTech	81.30	77.60	75.40
I3D (3D CNN)	HMDB-51	79.50	75.80	73.10

Исходя из приведенных выше данных, можно утверждать о явном потенциале подобных интеллектуальных систем, однако стоит также обратить внимание и на проблемы, что возникнут при реализации.

Первой и основной будет является сложность реализации на отечественном оборудовании, поскольку процессоры “Байкал” и “Эльбрус” имеют ограничения в поддержке специализированных инструкций для ускорения нейросетевых вычислений. Это усложнит развертывание тяжелых моделей. Также нынешний спектр видеооборудования, которое установлено в отделениях Сбербанка будет сложно интегрировать в уже готовые разработки моделей интеллектуального видеонаблюдения с уже предусмотренным для этого оборудованием. Это создаст серьезные сложности для стандартизации и расширения.

Второй проблемой станет персонал. Установка и запуск системы лишь первый шаг. Ее эффективность во многих технических и программных аспектах будет зависеть от компетентности работников, что должны уметь об-

ращаться с подобным оборудованием. Кроме того, среди группы реагирования должны быть люди, понимающие и правильно интерпретирующие сообщения от моделей интеллектуального видеонаблюдения. Эксперты безопасности должны будут отмечать неверные срабатывания и вносить корректировки в алгоритмы обработки видеопотоков.

Данное исследование методов компьютерного зрения на основе искусственного интеллекта позволяет сделать вывод о большой степени готовности технологий для реализации задачи безопасности. Переход от классической модели видеонаблюдения к превентивной будет стратегическим шагом. Технологические решения, такие как архитектуры для детекции объектов YOLO и детекции аномалий MIL, существуют и активно развиваются.

В заключении стоит отметить, что успешное внедрение таких систем требует комплексного подхода с использованием импортного ПО или написание собственного, что будет являться более предпочтительным, а отечественное оборудование на момент 2026 года не способно корректно работать с импортным ПО ИИ. Также необходимо учитывать специфику банковской среды и ограничения существующей инфраструктуры.

Список используемых источников

1. Дазмарова Т. Н. Искусственный интеллект в банковском секторе: возможности и барьеры внедрения [Электронный ресурс] // КиберЛенинка. 2022. № 4. С. 45–58. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-bankovskom-sektore (дата обращения: 20.03.2026).

2. Анализ системы видеоаналитики для мониторинга технологических процессов на основе компьютерного зрения и машинного обучения [Электронный ресурс] // КиберЛенинка. 2023. URL: https://cyberleninka.ru/article/n/analiz-sistemy-videoanalitiki-dlya-monitoringa-tehnologicheskih-protsessov-na-osnove-kompyuternogo-zreniya-i-mashinnogo-obucheniya (дата обращения: 23.03.2026).

3. Video Content Analysis for Compliance Audit in Finance and Security Industry [Электронный ресурс] // ResearchGate. 2020. URL: https://www.researchgate.net/publication/342539997_Video_Content_Analysis_for_Compliance_Audit_in_Finance_and_Security_Industry.pdf (дата обращения: 21.03.2026).

4. Sultani W., Chen C., Shah M. Real-World Anomaly Detection in Surveillance Videos // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2018. P. 1321–1330. URL: https://openaccess.thecvf.com/content_cvpr_2018/ papers/Sultani_Real-World_Anomaly_Detection_CVPR_2018_paper.pdf (дата обращения: 24.03.2026).

5. Liu W., Liao W., Ren W., Hu W., Luo W. Future Frame Prediction for Anomaly Detection A New Baseline [Электронный ресурс] // CVPR. 2018. P. 6536–6545. URL: https://arxiv.org/pdf/1803.00158.pdf (дата обращения: 24.03.2026).

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ЦТМ СПБГУТ Е. И. Тумановой.

УДК 534.8: 621.396

ОЦЕНКА ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛА АКУСТИЧЕСКОГО ТРАНСФОРМАТОРА В УСЛОВИЯХ ОГРАНИЧЕНИЯ НА ПИКОВУЮ И СРЕДНЮЮ МОЩНОСТЬ

А. В. Качнов (аспирант гр. 2213А-24 СПбГУТ), kachnov.av@sut.ru

В работе представлена оценка максимально достижимой пропускной способности канала беспроводной передачи данных через металлические барьеры с использованием ультразвуковых колебаний. Показано, что частотная характеристика такого канала является ярко выраженной гребенчатой структурой, которая описывается в виде геометрической прогрессии. Получены аналитические выражения для отношения сигнал/шум на выходе канала с учетом многократных переотражений от границ барьера. Результаты работы могут быть использованы при проектировании систем телеметрии для герметичных металлических емкостей, корпусов подводных и космических аппаратов.

ультразвуковая связь, акустический трансформатор, гребенчатая частотная характеристика, пропускная способность канала, передача через металл

Распространение ультразвуковых колебаний в ограниченной пластине (стенка корпуса) формируется волновое поле сложной структуры, обусловленное многократными переотражениями от границ раздела сред [1, 2]. Это приводит к тому, что частотная характеристика принимает гребенчатую форму, представляющую собой последовательность узких полос прозрачности, разделенных областями сильного подавления сигнала.

Для проектирования реальных систем связи необходимо провести оценку максимально достижимой скорости передачи информации в канале связи. Однако классические формулы Шеннона для канала с аддитивным белым гауссовским шумом (АБГШ) не могут быть применены напрямую, в связи с тем, что частотная характеристика канала акустического трансформатора существенно неравномерна, а передатчик имеет ограничения как по пиковой, так и по средней мощности.

Настоящая работа посвящена разработке методики оценки пропускной способности ультразвукового канала связи [3] через металлический барьер с учетом его гребенчатой структуры и реальных энергетических ограничений.

Модель канала с гребенчатой частотной характеристикой

Рассмотрим металлическую пластину толщиной *d*, на противоположных сторонах которой установлены пьезоэлектрические преобразователи. При распространении ультразвуковой волны в пластине происходит многократное отражение от границ. В частотной области передаточная функция такого канала может быть представлена в виде бесконечного числа лучей [4]:

$$H(\omega) = \sum_{n=0}^{\infty} V^{2n} \cdot e^{-(2n+1)\alpha d} \cdot e^{-j(2n+1)kd}, \quad (1)$$

где α – коэффициент затухания ультразвука в материале барьера, Нп/м;

V – коэффициент отражения от границ барьера;

d – толщина барьера, м;

$k = \omega/c_{зв}$ – волновое число, м$^{-1}$;

$c_{зв}$ – скорость звука в материале барьера, м/с;

Воспользуемся свойством геометрической прогрессии и запишем выражение (1) в компактной форме:

$$H(\omega) = \frac{e^{-\alpha d} \cdot e^{-jkd}}{1 - V^2 e^{-2\alpha d} e^{-j2kd}} \quad (2)$$

Амплитудно-частотная характеристика канала (2) может быть записана в виде

$$|H(\omega)| = \frac{e^{-\alpha d}}{\sqrt{1 - 2V^2 e^{-2\alpha d}\cos(2kd) + V^4 e^{-4\alpha d}}} \quad (3)$$

Знаменатель функции (3) достигает минимума при выполнении условия cos(2*kd*) = 1. Частоты, которые соответствуют условию могут быть рассчитаны как

$$f_m = \frac{m \cdot c}{2d} \quad (4)$$

Именно на этих частотах (4) наблюдается резонансное увеличение коэффициента передачи и образуются «окна прозрачности». Ширина этих окон определяется добротностью, которая, в свою очередь, зависит от коэффициента отражения *V* и затухания α.

Отношения сигнал/шум на выходе канала

Пусть на вход канала подается сигнал со спектральной плотности мощности $S_x(f)$. Спектральная плотность мощности сигнала на выходе канала будет определяться как $S_y(f) = |H(f)|^2 S_x(f)$. Шум на выходе приемника будем считать белым гауссовским с двусторонней спектральной плотностью $N_0/2$. В этом случае отношения сигнал/шум (ОСШ) на частоте f будет определяться как:

$$SNR(f) = \frac{|H(f)|^2 S_x(f)}{N_0} \quad (5)$$

Важной особенностью выражения (5) является сильная частотная зависимость $|H(f)|^2$. В окнах прозрачности ОСШ может быть на 20-40 дБ выше, чем вне их. Это обстоятельство делает крайне неэффективным использование равномерного спектра сигналов.

Пропускная способность при ограничениях на мощность

В соответствии с теоремой Шеннона для канала с частотно-зависимым ОСШ и ограничением на среднюю мощность сигнала P_{avg}, пропускная способность C определяется решением задачи максимизации взаимной информации:

$$C = \max_{S_x(f)} \int_0^\infty \log_2 \left[1 + \frac{|H(f)|^2 S_x(f)}{N_0}\right] df \quad (6)$$

при условии

$$P_{avg} = \int_0^\infty S_x(f) df$$

Решение задачи (6) методом множителей Лагранжа приводит к известному принципу выравнивания уровня («water-filling»):

$$S_x(f) = \max\left(0, \frac{N_0}{|H(f)|^2}\left(\frac{1}{\lambda} - 1\right)\right) \quad (7)$$

где λ – множитель Лагранжа, определяемый из условия на среднюю мощность.

Однако в реальных системах связи, в которых используются пьезоэлектрические преобразователи существует дополнительное физическое ограничение на пиковую мощность или максимальную амплитуду возбуждающего напряжения. Это величина обусловлена электрической прочностью материала пьезоэлектрика. Учет этого дополнительного ограничения накладывает верхнюю границу на допустимое значение $S_x(f)$.

$$0 \leq S_x(f) \leq S_{max}(f),$$

где $S_{max}(f)$ определяется допустимой спектральной маской излучения.

Пример расчета

Проиллюстрируем предложенный подход на примере стальной пластины толщиной 10 мм. Параметры моделирования представлены в таблице 1.

ТАБЛИЦА 1. Численные значения параметров моделирования

Параметр	Обозначение	Ед. измерений	Значение
Толщина пластины	d	мм	10
Скорость звука	$c_{зв}$	м/с	5 900
Коэффициент затухания	α	дБ/см	0.01
Полоса рабочих частот	f	МГц	0,5 – 2,5
Средняя мощность	P_{avg}	мВт	0,1
Спектральная плотность шума	N_0	Вт/Гц	10^{-9}

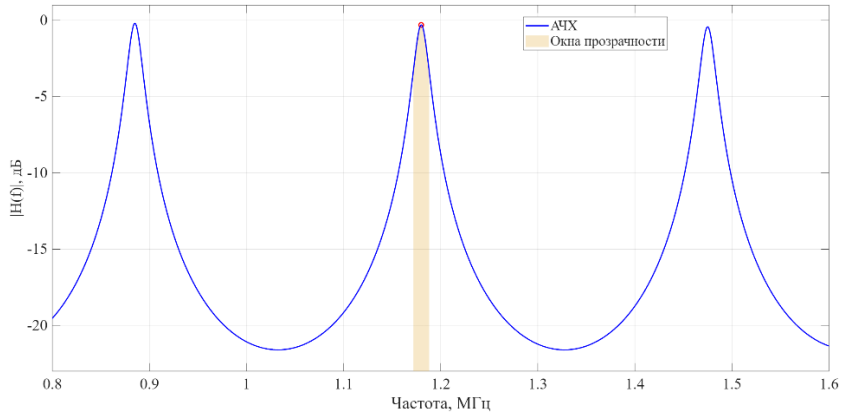


Рис. 1. Амплитудно-частотная характеристика канала

На рисунке 1 для наглядности представлена часть амплитудно-частотной характеристики канала, рассчитанной по формуле (4). Видно, что коэффициент передачи в окне прозрачности более чем на 20 дБ превышает значения в запрещенных зонах.

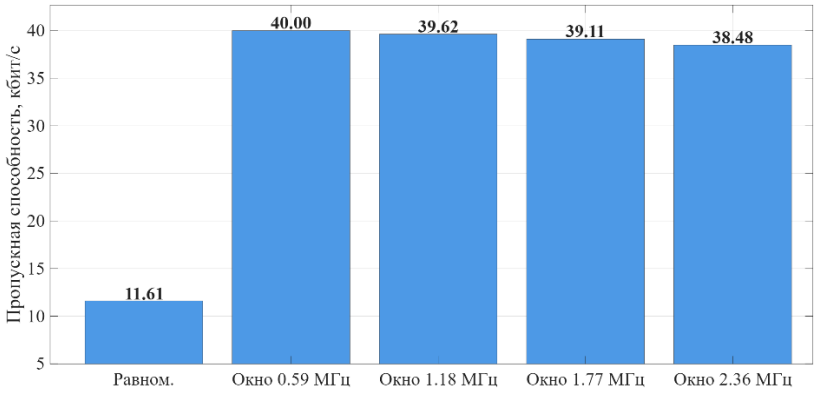


Рис. 2. Сравнение пропускной способности канала

На рисунке 2 представлено сравнение пропускной способности при равномерном распределении мощности и при концентрации мощности в некоторых окнах прозрачности. Концентрация мощности в окнах прозрачности позволяет увеличить пропускную способность более чем в 3 раза (с 11,6 бит/с до 39,5 бит/с). При этом, несмотря на изменение ширины окна прозрачности и коэффициента передачи с частотой, пропускная способность остается практически постоянной. Это объясняется тем, что увеличение ширины окна с ростом частоты компенсируется увеличением коэффициента затухания и, следовательно, уменьшением отношения сигнал/шум.

Заключение

В работе показано, что канал акустического трансформатора обладает гребенчатой частотной характеристикой, которая может быть с высокой точностью описана моделью геометрической прогрессии. Установлено, что наиболее эффективная стратегия заполнения заключается в концентрации мощности в узких «окнах прозрачности», соответствующих резонансным условиям.

Полученные результаты позволяют на этапе проектирования быстро оценить максимальную скорость передачи данных для заданных параметров барьера. Разработанная методика может быть внедрена в практику расчета систем ультразвуковой связи через структурно-неоднородные каналы.

Список используемых источников

1. Бреховский Л. М., Годин О. А. Акустика слоистых сред. М.: Главная редакция физико-математической литературы, 1989. 416 с. ISBN 5-02-014155-0.

2. Иванов А. Н. Математическое моделирование процессов распространения акустических волн в структурно-неоднородных средах: дис. … канд. техн. наук: 01.04.06 / Иванов Андрей Николаевич. Владивосток, 2008, 141 с. EDN: NQFYUL.

3. Воробьев О. В., Качнов А. В., Сидоркович Д. Р. Обеспечение информационного обмена между подводным аппаратом и донной доковой станцией // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024): Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 122-126. EDN: LERGUM.

4. Качнов А. В., Прасолов А. А., Туманова Е. И. Исследование характеристик канала акустического трансформатора с учетом многократных переотражений от границ барьера // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2025) : Сборник научных статей XIV Международной научно-технической и научно-методической конференции. В 2-х томах. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025. С. 128–133. EDN: QKYQAU.

Статья представлена научным руководителем, доцентом кафедры ЦТМ СПбГУТ, кандидатом технических наук Е. И. Тумановой.

УДК 004.896

БИБЛИОМЕТРИЧЕСКИЙ АНАЛИЗ ПЕРСПЕКТИВ КОНВЕРГЕНЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА С ЦИФРОВЫМИ ДВОЙНИКАМИ СЕТИ В КАЧЕСТВЕ ИНСТРУМЕНТА УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

С. В. Кисляков (к.т.н., доцент, доцент кафедры ИКС СПбГУТ)
Е. А. Мамаев (студент группы ИКТС-43м СПбГУТ), mamaev.ea@sut.ru

Статья посвящена исследованию перспектив конвергенции таких инновационных технологий, как искусственный интеллект и цифровые двойники сети в качестве инструмента управления телекоммуникационными сетями. На основе библиометрического анализа научных работ были выделены актуальные тенденции в исследовании слияния данных технологий, а также наиболее перспективные ниши их интеграции. Полученные результаты представляют собой данные, отражающие текущий уровень исследований в рассматриваемой области.

цифровые двойники, искусственный интеллект, сети цифровых двойников, управление сетями связи

Стремительное развитие телекоммуникационного обслуживания, как с точки зрения появления новых, более требовательных услуг, так и поддержки старых сервисов с установленным качеством, приводит к постепенному усложнению и масштабированию сети. Данная тенденция приводит к тому, что операторам связи становится необходимо искать инструменты, позволяющие производить динамический учет и управление ресурсами сети для адаптации к потребностям клиентов.

Технология искусственного интеллекта (ИИ) является быстрорастущей областью благодаря своей перспективе эффективного применения во многих сферах мировой экономики. В телекоммуникационной сфере использование искусственного интеллекта также считается перспективным направлением. ИИ-методы, такие как глубокое, генеративное и федеративное обучение, могут помочь в настройке, управлении и обслуживании сетей, на основании анализа полученных и сгенерированных данных [1].

Другой технологией, способной помочь в управлении все усложняющихся сетей, являются цифровые двойники сети (DTN). Цифровой двойник

сети является цифровым представлением реальной сети, который может получать сетевые данные в режиме реального времени, что дает возможность анализировать, диагностировать и эмулировать физическую сеть с нулевым риском и на основе этого принимать решения по управлению и эксплуатации физической сети [2].

Конвергенция искусственного интеллекта и цифровых двойников сети способно более эффективно раскрыть оба этих инструмента, устраняя ограничения присутствующие в традиционных методах управления сетью. На данный момент уже опубликовано много статей по данной теме. Среди этих публикаций существуют разные статьи, которые дают читателям представление об исследуемой области путем анализа существующих работ и выявления преимуществ, ограничений и направлений будущих исследований. Однако, существующая литература хоть и информативна, но не отражает всей полноты картины. Библиографический анализ дополняет представление о текущем состоянии исследований, что помогает определить ключевые области для дальнейших исследований.

Библиометрический анализ – это метод количественного изучения научной литературы, статей и документов с помощью статистических методов. Он используется для оценки научной продуктивности, выявления трендов и определения ведущих авторов и научно-исследовательских организаций.

При проведении библиометрического анализа используется методология проведения исследования, которая состоит из четырех этапов: определение ключевых слов для поиска, сбор данных, их обработка, а также анализ и обсуждение результатов [3]. На рис. 1 показаны этапы методологии, использованные для проведения этого исследования.

Во-первых, определяли основные поисковые слова для проведения анализа. В качестве таких слов, характеризующих тему исследования, были выбраны «Digital Twin Network» и «Artificial Intelligence», которые использовали как поисковые слова в заголовках и аннотациях статей. Затем была выбрана база данных научных публикаций, а именно Google Scholar, которая предоставляет библиометрические данные для поиска литературы. Данная база данных была выбрана на основании ее доступности в регионе, а также достаточно большого количества публикаций для проведения анализа.

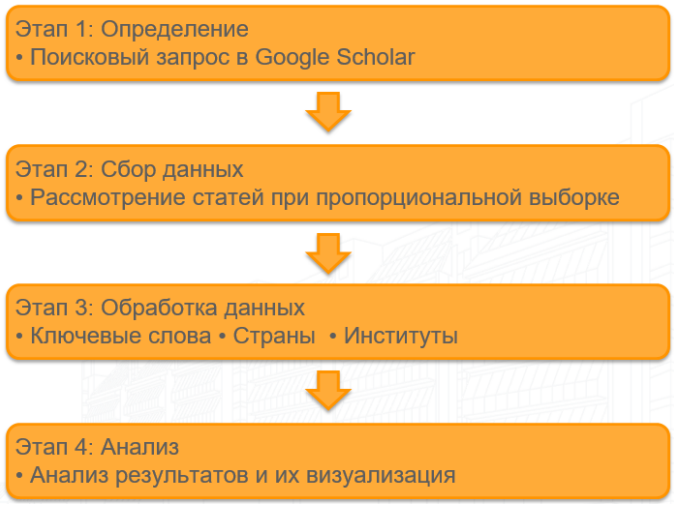


Рис. 1. Этапы методологии исследования

Второй этап включал в себя процесс сбора данных на основе выбранных поисковых слов и выбранной базы данных.

Третий этап заключался в обработке отобранных статей. На этом этапе происходил сбор и подсчет таких показателей, как ключевые слова, вклад стран в развитие данной сферы, научные организации, в которых проводились исследования, а также оценка роста числа публикаций по годам.

Наконец, на заключительном этапе этого исследования анализировали обработанные данные и визуализировали их, что позволило более наглядно проследить тенденции в исследуемой научной сфере.

Результаты

Ежегодный темп роста числа публикаций – это показатель, который позволяет понять растущий интерес к определенной сфере исследований. Используя поисковый запрос в Google Scholar, было получено 1487 статей, опубликованных в период с 2021 по 1-ю половину 2026 года.

На рис. 2 представлен график роста числа публикаций по годам. Как видно из этого графика, траектория исследований в этой области положительна. Растущее число публикаций каждый год подчеркивает пристальное внимание научных кругов и промышленности к применению ИИ и DTN вместе.

Количество публикаций от научной организации – это показатель для оценки ее академического влияния и вклада в исследование конкретной научной области.

При анализе статей была применена пропорциональная выборка для точного отражения текущих тенденций на основе уменьшенного количества статей с сохранением заданной точности. Допустимая погрешность составляла 7 %. В результате для анализа было отобрано 180 статей. При создании этих статей было задействовано 207 научно-исследовательских институтов. На рис. 3 показаны 14 ведущих организаций, отобранных на основе количества опубликованных статей из пропорциональной выборки.

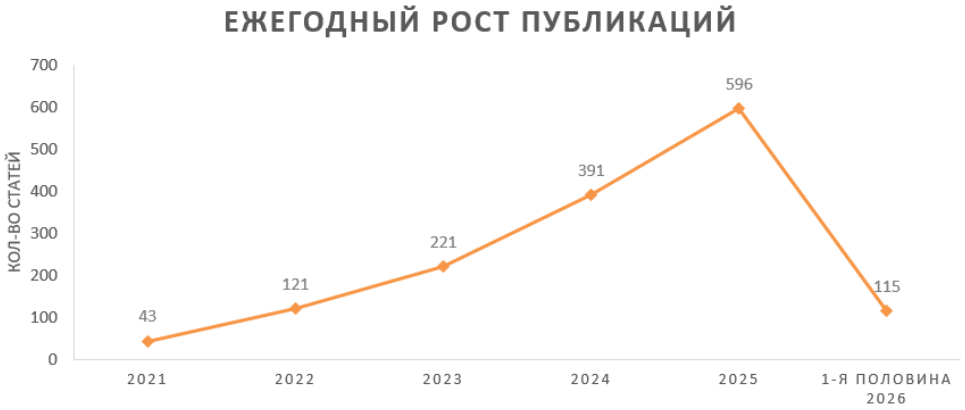


Рис. 2. Ежегодный рост публикаций

Пекинский университет почты и телекоммуникаций, Хуачжунский университет науки и технологий, а также университет Майами лидируют с 7 статьями в выборке по данной теме, заданной выбранными поисковыми словами. За ними следует Китайский мобильный научно-исследовательский институт с 6 статьями. В списке также представлены другие известные учебные заведения.



Рис. 3. Количество публикаций организаций

Можно отметить разнообразное географическое распределение среди ведущих участников. Хотя Китай остается доминирующим игроком с 9 учреждениями, наблюдается конкуренция с такими странами, как США, Канада и Норвегия. Такое распределение свидетельствует о глобальном интересе к конвергенции ИИ и DTN.

Похожий вывод можно сделать и при анализе вклада стран в исследование данной темы. Ландшафт исследований конвергенции ИИ и DTN формируется за счет вклада различных стран. Анализируемые 207 научных организаций представляли 38 стран. Оценка вклада каждой страны дает панорамное представление о динамике глобальных исследований с высоким уровнем освещения влияния и приверженности разных стран этой области.

Доминирующим игроком по-прежнему остается Китай с 34,5 % публикаций, за ним следуют США, Канада, Великобритания, Италия Испания, Южная Корея, а также Индия и Япония. На основании данных, представленных на рис. 4, можно сделать вывод о том, что в области исследования взаимодействия ИИ и DTN были сформированы два центра – Восточный, во главе с Китаем, и Западный с центром в США.

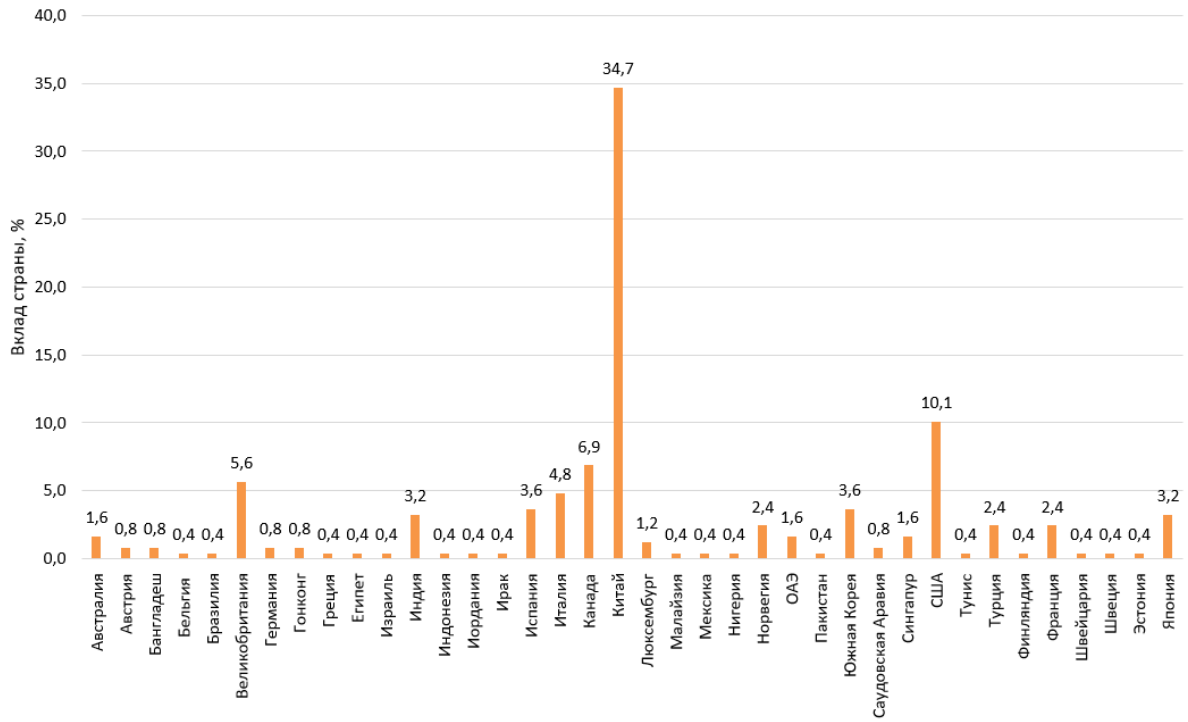


Рис. 4. Вклад стран

Ключевые слова, содержащиеся в статьях, – это показатель, характеризующий те направления внутри исследуемой темы, которые имеют наибольшее внимание в исследовательском сообществе. Так, наиболее популярными ключевыми словами, помимо искусственного интеллекта и цифровых двойников сети, являются 6G мобильная связь, глубокое обучение с подкреплением, оптимизация, управление ресурсами, системы реального времени, беспроводные сети и интернет вещей, что показано на рис. 5. На основе самых популярных ключевых слов можно сделать вывод о том, что основной упор в исследованиях делается на применение DTN с ИИ в системах мобильной связи и вопросов, связанных с их корректной работой внутри этих мобильных сетей. Это может быть вызвано тем, что сейчас при разработке современных мобильных сетей, в частности 6 поколения, применение ИИ является одним из ключевых трендов.



Рис. 5. Частота упоминаний ключевых слов

Таким образом, цифровые двойники сетей связи в совокупности с различными моделями искусственного интеллекта являются перспективным и активно изучаемым направлением, особенно в области сетей мобильной связи. Ведущими лидерами в исследовании данной области являются Китай и США.

Список используемых источников

1. Thormundsson B. Artificial Intelligence (AI) Market Size Worldwide in 2021 with a Forecast until 2030. [Электронный ресурс]. URL: https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/ (дата обращения: 11.03.2026).

2. Minerva R., Lee G. M., Crespi N. Digital twin in the IoT context: a survey on technical features, scenarios, and architectural models. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/9120192 (дата обращения: 12.03.2026).

3. Sahran F., Altarturi H. H. M., Anuar N. B. Exploring the Landscape of AI-SDN: A Comprehensive Bibliometric Analysis and Future Perspectives. [Электронный ресурс]. URL: https://www.mdpi.com/2079-9292/13/1/26 (дата обращения: 11.03.2026).

УДК 004.94:535

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РАБОТЫ КОРРЕЛЯТОРА СОВМЕСТНОГО ПРЕОБРАЗОВАНИЯ С НЕЛИНЕЙНОЙ ОБРАБОТКОЙ СОВМЕСТНОГО СПЕКТРА

С. В. Колпаков (студент группы ИКТФ-46м СПбГУТ), kolpakov.sv@sut.ru

В работе рассмотрена возможность математического моделирования работы оптического коррелятора совместного преобразования с помощью быстрого преобразования Фурье из программы Matlab. Получены выходные сигналы коррелятора при распознавании букв.

математическое моделирование, программа Matlab оптический коррелятор совместного преобразования, распознавание образов, преобразование Фурье

Коррелятор совместного преобразования (КСП) является одним из перспективных устройств оптической обработки информации. Он может использоваться для решения практически важных задач, в том числе для распознавания образов [1]. Оптическая схема коррелятора представлена на рис. 1[2]. В схеме КСП можно обойтись и одним фурье-процессором, если голограмму *H* регистрировать на матричном фотоприемнике, а результат регистрации передавать на модулятор света вместо входных сигналов.

Исследование особенностей работы КСП удобно проводить с помощью метода математического моделирования, не требующего значительных затрат времени и средств и отличающегося высокой точностью по сравнению с экспериментом. В работе было проведено моделирование работы КСП с жидкокристаллическим пространственным модулятором на входе на основе программы Matlab.

При моделировании изображения входных сигналов были заранее записаны в память компьютера. Они подавались в программу Matlab для вычисления совместного спектра входных сигналов с помощью быстрого преобразования Фурье (БПФ). После этого на основе БПФ осуществлялось обратное преобразование Фурье квадрата модуля совместного спектра, в результате чего формировались выходные функции корреляции. Сигналы, полученные в процессе моделирования для одинаковых и разных сигналов на входе показаны на рис. 2. В соответствии с теорией корреляционного алгоритма распознавания, величина максимумов корреляционных функций,

которую легко определить по ее сечениям, для одинаковых сигналов на входе были больше, чем при разных.

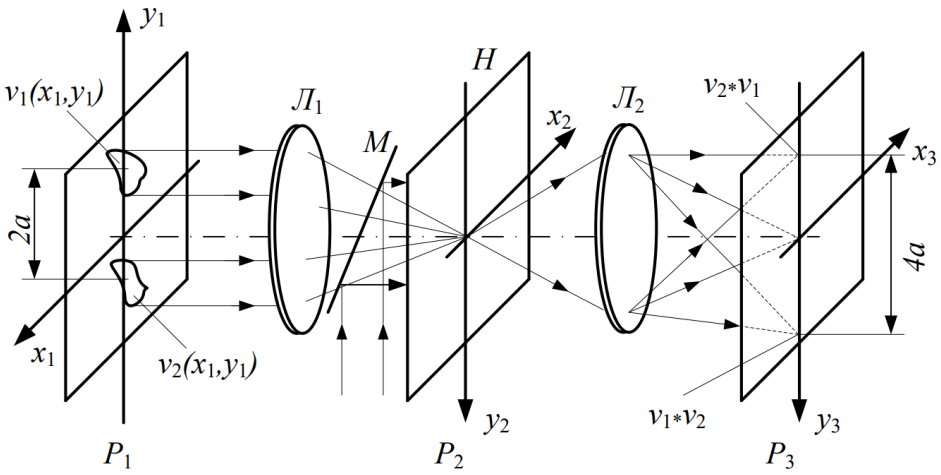


Рис. 1. Коррелятор совместного преобразования

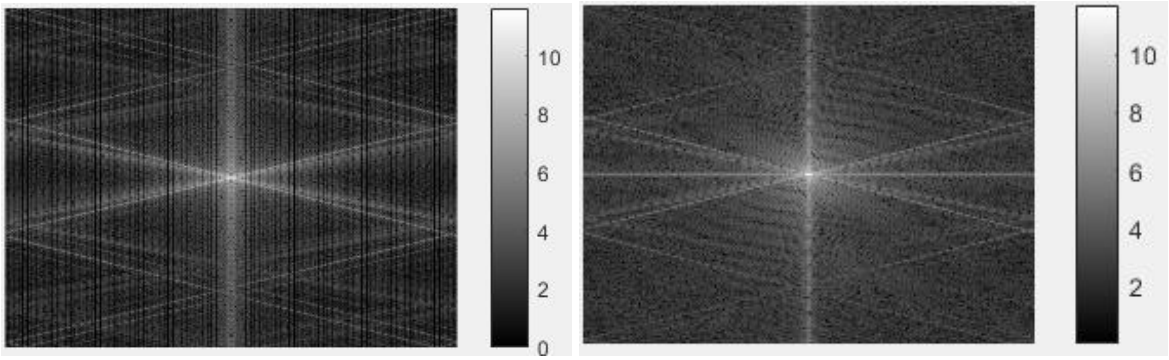
Проведенные исследования показали, что выбранный метод моделирования КСП позволяет получать его выходные сигналы, совпадающие с теоретически ожидаемыми. Эти сигналы качественно совпадают также и с полученными экспериментально на действующем макете коррелятора [3].

Развивая тему математического моделирования коррелятора совместного преобразования, были проведены вычисления с добавлением фильтра, ослабляющего низкочастотную область спектра. В результате были получены результаты (рис. 3), сопоставимые с экспериментальными, полученными на действующем макете коррелятора. На графиках с детальным изображением центральной области спектров зеленым цветом показаны исходные спектры, красным же – уже после применения фильтра низких частот.

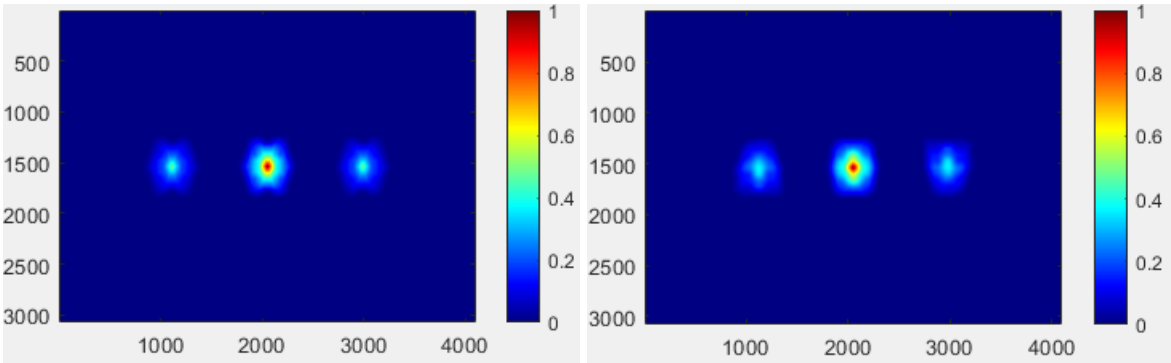
Данный метод позволяет увеличить разницу в максимумах корреляционных функций (см. рис. 3) одинаковых и разных образов, которая характеризует эффективность распознавания. Использованный подход в моделировании позволит в дальнейшем исследовать работу коррелятора и при других типах фильтров в совместном спектре.



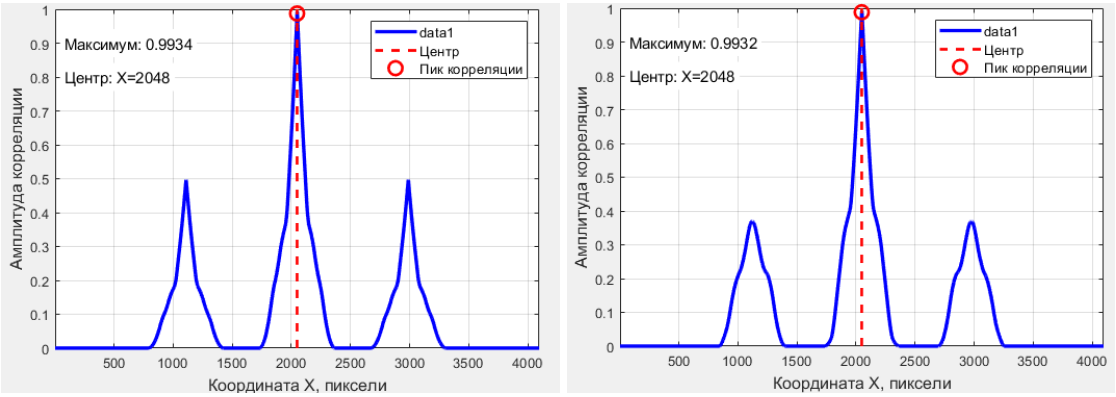
Исходное изображение AA и AB



Амплитудный спектр для AA и AB

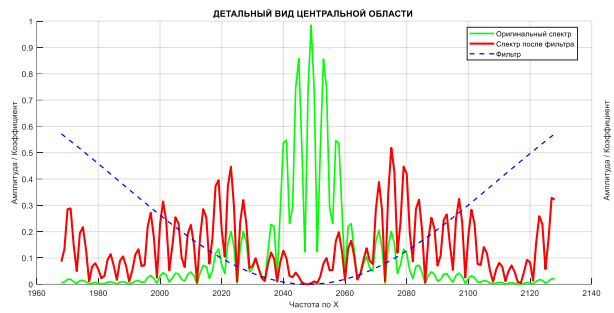


Карта корреляции для AA и AB

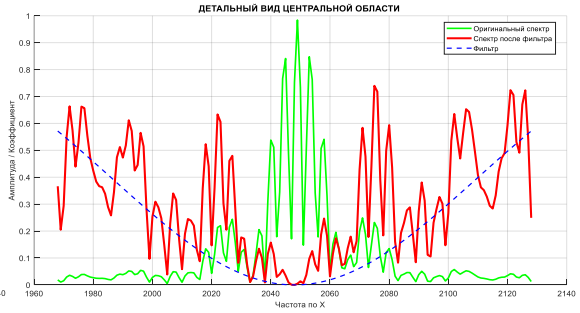


Горизонтальное сечение корреляции для AA и AB

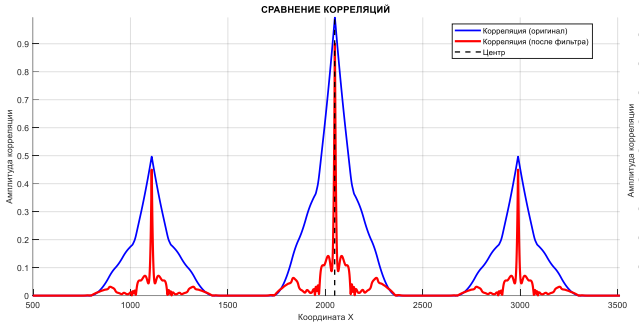
Рис. 2. Сигналы КСП при одинаковых и разных изображениях на входе



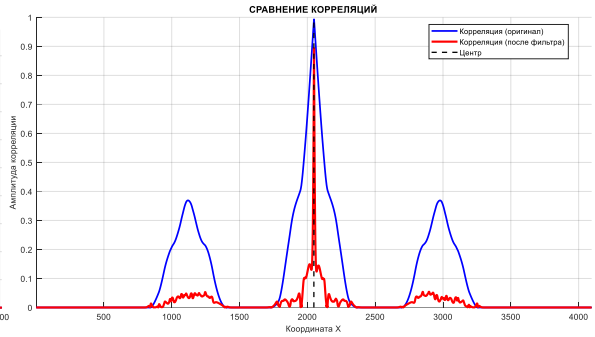
Спектр АА



Спектра АВ



Корреляция АА



Корреляция АВ

Рис. 3. Сигналы КСП при одинаковых и разных изображениях на входе после фильтра

Список используемых источников

1. Стариков Р. С. Оптические дифракционные корреляторы изображений: краткий очерк развития и новейшие достижения. 2025.

2. Математическое моделирование работы коррелятора совместного преобразования С. В. Колпаков, С. А. Рогов // Перспективные телекоммуникационные технологии и развитие цифровых кластеров в России и мире (ПКМ 2025). VI Всероссийская научно-техническая и научно-методическая конференция магистрантов, аспирантов и их руководителей: материалы конф. / Под ред. А. Н. Бучатского; сост. И. Е. Скалецкая. СПб.: СПбГУТ., 2026. 3191 с.

3. Кузьмин М. С. и др. Экспериментальное исследование коррелятора совместного преобразования // Квантовая электроника 2019. вып. 3. С. 391-397.

УДК 004.048

ПРОЕКТИРОВАНИЕ API ДЛЯ УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМ MACHINE LEARNING ПАЙПЛАЙНОМ

Г. Б. Комаха (студент группы ИКТК-21 СПбГУТ), komaha.gb@sut.ru
М. Е. Плыс (студент группы ИКТК-21 СПбГУТ), plys.me@sut.ru
Р. И. Пупцев (старший преподаватель кафедры ИКС СПбГУТ), r.pupcev@sut.ru

В статье рассматривается архитектура API-шлюза для управления распределенным контуром машинного обучения, в котором одновременно используются несколько моделей с разными данными, графиками обновления и состояниями жизненного цикла. Предлагается решение, в котором FastAPI предоставляет единый внешний интерфейс, PostgreSQL хранит данные и реестр моделей, Apache Airflow запускает пайплайны обучения, а DVC используется для версионирования датасетов и модельных артефактов. Компоненты MLflow, TeamCity и Harbor рассматриваются как опциональные расширения: они повышают удобство сопровождения, экспериментирования и развертывания, но не являются обязательными для базового функционирования системы.

FastAPI, Apache Airflow, DVC, PostgreSQL, MLflow, TeamCity, Harbor, REST API, MLOps, ML Model Management

1. Введение

В прикладных системах машинного обучения (ML) часто требуется работать не с одной универсальной моделью, а с набором специализированных моделей. Такая ситуация возникает при прогнозировании для разных географических секторов, объектов инфраструктуры, групп пользователей или отдельных показателей. Пример задачи можно найти в следующей статье [1]. У каждой модели могут отличаться входные данные, периодичность обновления, метрики качества и правила перехода в активное состояние.

При росте числа моделей ручное управление становится неэффективным. Необходимо централизованно принимать данные, запускать обучение, хранить версии датасетов и артефактов, выбирать активную модель для прогноза и контролировать доставку новой версии в эксплуатацию. Для решения этой задачи предлагается API-шлюз, который скрывает внутреннюю сложность ML-контура за единым REST-интерфейсом.

2. Общая архитектура решения

Центральным компонентом системы является API шлюз (API Gateway) [2] на FastAPI. Он принимает запросы от клиентских приложений, источни-

ков данных и внутренних сервисов, а затем маршрутизирует их к хранилищам, оркестратору обучения или worker-у прогнозирования. Клиенту не требуется знать, где физически находится модель и каким пайплайном она была подготовлена [3]. Взаимодействие компонентов системы организовано через REST API, что обеспечивает единый формат запросов для запуска обучения, получения прогнозов и работы с реестром моделей [4].

PostgreSQL используется в двух ролях: как основное хранилище предметных данных и как реестр моделей. В реестре фиксируются идентификатор модели, сектор или иной контекст применения, статус, активная версия, базовые метрики, ссылка на артефакт и параметры запуска. DVC Remote / Artifact Storage хранит версии подготовленных датасетов и обученных моделей, что позволяет воспроизвести результат обучения.

Apache Airflow [5] запускает пайплайны подготовки данных, обучения и валидации. API не выполняет обучение самостоятельно: он формирует конфигурацию запуска и передает ее в Airflow. После завершения пайплайна API обновляет реестр моделей и делает новую версию доступной для дальнейших действий.

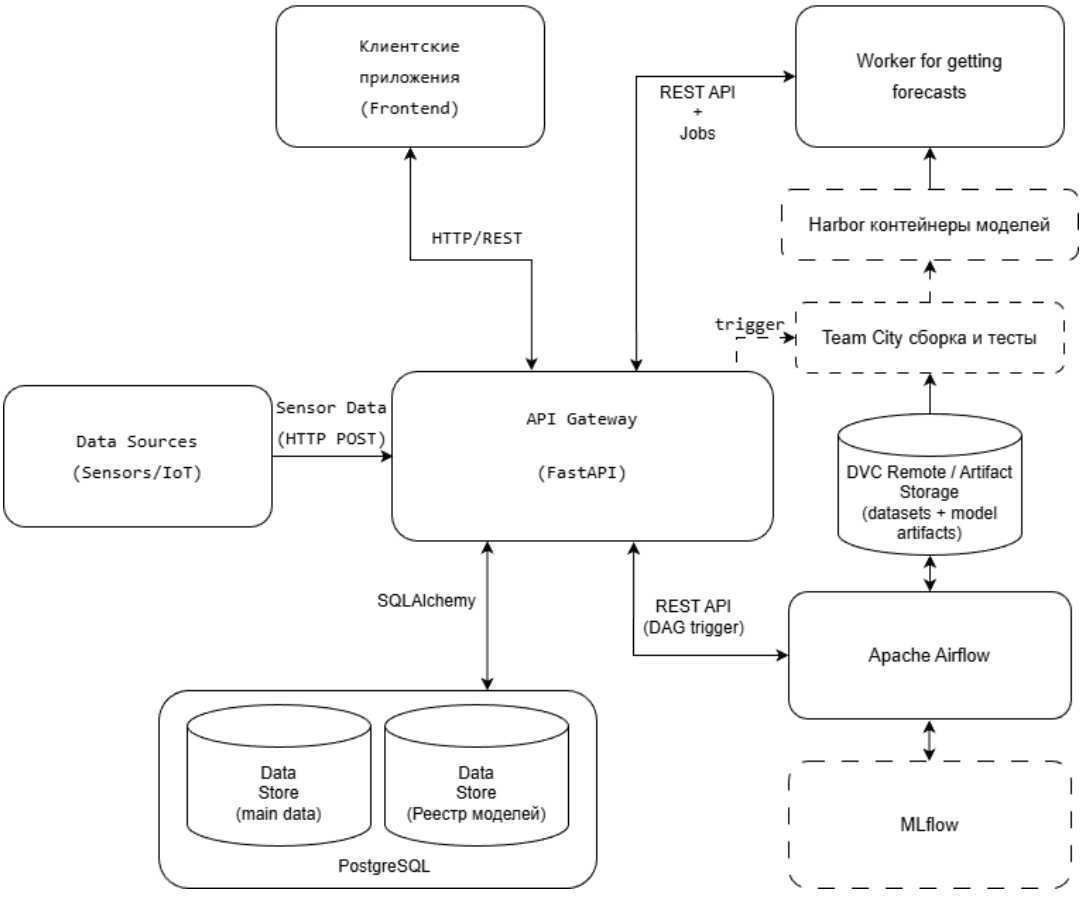


Рис. 1. Схема взаимодействия компонентов системы прогнозирования

На рисунке 1 пунктиром выделены компоненты, подключаемые по необходимости: MLflow, TeamCity и Harbor. Базовый контур может работать без них, если достаточно хранения метрик в PostgreSQL и запуска моделей непосредственно из артефактов DVC. При росте числа экспериментов и требований к развертыванию эти компоненты повышают управляемость и воспроизводимость. Состав системы и назначение ее основных частей представлены в таблице 1.

ТАБЛИЦА 1. Описние назначения всех комппонентов системы

Компонент	Статус	Назначение
FastAPI / API Gateway	основной	единый интерфейс для данных, обучения, статусов моделей и прогнозов
PostgreSQL	основной	хранение предметных данных, реестра моделей, статусов и базовых метрик
Apache Airflow	основной	запуск и контроль DAG (Directed Acyclic Graph) подготовки данных, обучения и валидации
DVC Remote / Artifact Storage	основной	версионирование датасетов и артефактов обученных моделей
Worker for getting forecasts	основной	исполнение прогноза по заданию API с использованием активной модели
MLflow	опциональный	трекинг экспериментов, сравнение параметров, метрик и кандидатов моделей
TeamCity	опциональный	сборка и тестирование контейнера модели после успешного обучения
Harbor	опциональный	хранение проверенных контейнерных образов моделей

3. Практическая реализация

Основной сценарий начинается с поступления данных от сенсоров или IoT-источников в PostgreSQL. После запроса на обучение API формирует конфигурацию для выбранного сектора и передает ее в Airflow. В DAG выполняются подготовка датасета, обучение и валидация модели; результаты сохраняются в DVC, а в реестре обновляются статус, метрики и ссылка на артефакт. MLflow в этом сценарии не является обязательным: он подключается, если требуется детально сравнивать эксперименты, параметры и кандидатов.

При прогнозировании клиент обращается к API с идентификатором сектора. API находит в реестре активную версию модели и передает задачу worker-у. Worker загружает нужный артефакт из DVC либо использует заранее подготовленный контейнер модели, выполняет расчет и возвращает результат через API.

Контейнерный вариант нужен для случаев, когда важно зафиксировать зависимости, среду исполнения, процесс тестирования и возможность отката. Тогда TeamCity может выполнять сборку и проверку образа, а Harbor – хранить готовые версии. Если таких требований нет, модель может использоваться напрямую как артефакт из DVC; поэтому TeamCity и Harbor остаются опциональными элементами контура.

Достаточный API-контракт включает следующие операции:

- POST /train/{sector_id} – запуск обучения;
- POST /predict/{sector_id} – получение прогноза;
- GET /models/{sector_id} – просмотр моделей, статусов и метрик;
- POST /models/{model_id}/activate – активация проверенной версии.

Поверх этого набора можно добавить массовое обучение, A/B-тестирование и переобучение по снижению качества. Эти функции не меняют общий принцип работы: API остается единой точкой входа, а внутренние компоненты подключаются по необходимости.

4. Заключение

Предложенная архитектура формирует единый управляемый контур для работы с распределенным набором ML-моделей: FastAPI маршрутизирует запросы, PostgreSQL хранит данные и реестр, Airflow запускает обучение, DVC фиксирует версии датасетов и артефактов, а worker выполняет прогноз.

MLflow, TeamCity и Harbor повышают удобство трекинга, сборки и развертывания, но подключаются только там, где это оправдано требованиями проекта. Это позволяет сохранить архитектуру простой в базовом варианте и масштабируемой при развитии.

Список используемых источников

1. Пупцев, Р. И. Разработка программно-аппаратного комплекса для применения в области прогнозирования лавинной опасности / Р. И. Пупцев // Снежный покров, атмосферные осадки, аэрозоли: Материалы V Байкальской международной научной конференции – стратегической сессии, Иркутск, 19–23 июня 2023 года. Иркутск: Репроцентр А1, 2023. С. 183-191. EDN: PKGRTS.

2. Нихаенко, К. М. Анализ применения машинного обучения для предсказания параметров работы системы на микросервисной архитектуре / К. М. Нихаенко, Р. И. Пупцев // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022): Сборник лучших докладов Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей, Санкт-Петербург, 06–08 декабря 2022 года / Сост. Н. Н. Иванов. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. С. 269-273. EDN: AVKWHV.

3. Пупцев, Р. И. Разработка системы автоматизированного составления прогноза лавинной опасности, с применением современных ИКТ и аппарата нейрокогнитивных архитектур / Р. И. Пупцев // Гидросфера. Опасные процессы и явления. 2022. Т. 4. № 3. С. 244-254. DOI 10.34753/HS.2022.4.3.244. EDN: EBNRRD.

4. Попов, А. А. Обзор REST API и их применение в современном web-разработке / А. А. Попов, А. Ф. Чарикова, К. С. Иванова // Тенденции развития науки и образования. 2025. № 119-4. С. 147-149. DOI: 10.18411/trnio-03-2025-166. EDN: TKIRIZ.

5. Михайлов, А. Н. Использование Apache Airflow для оркестрации процессов обработки данных / А. Н. Михайлов // Вестник науки. 2024. Т. 4. № 10(79). С. 783-787. EDN: IJIHMS.

УДК 004.724.4

АНАЛИЗ МЕТОДОВ УСТАНОВЛЕНИЯ ПРЯМЫХ СОЕДИНЕНИЙ МЕЖДУ УЗЛАМИ В VPN-СЕТЯХ С MESH-ТОПОЛОГИЕЙ

В. С. Коровкин (студент группы ИКТК-21 СПбГУТ), korovkin.vs@sut.ru
И. Ф. Тарабанов (старший преподаватель кафедры ИКС СПбГУТ)

Работа посвящена исследованию методов установления прямых соединений между узлами виртуальных частных сетей с полносвязной топологией в условиях трансляции сетевых адресов. Проведен сравнительный анализ шести методов преодоления трансляции сетевых адресов, описанных в документе Request for Comments 5128: ретрансляция, обратное соединение, прокол через межсетевой экран по протоколам с установлением и без установления соединения, предсказание порта по обоим протоколам. Обосновано, что оптимальным методом является прокол по протоколу без установления соединения, обеспечивающий прямое одноранговое соединение с совместимостью более 80 % устройств трансляции адресов. Вариант прокола по протоколу с установлением соединения отсеян ввиду сложности реализации механизма одновременного открытия и проблемы двойной инкапсуляции. Для экспериментальной проверки разработан прототип виртуальной частной сети с полносвязной топологией. Экспериментально подтверждено установление прямого туннеля и передача пакетов через виртуальный сетевой интерфейс.

преодоление трансляции сетевых адресов, прокол межсетевого экрана, виртуальная частная сеть, полносвязная топология, одноранговое соединение, сигнальный сервер

Введение

Подавляющее большинство устройств в сети Интернет находятся за механизмом трансляции сетевых адресов (NAT), побочным эффектом которого является блокировка незапрошенных входящих соединений [1]. Классические VPN-решения используют архитектуру «звезда» (централизованную), при которой весь трафик маршрутизируется через центральный сервер, что создает единую точку отказа и увеличивает задержку [2]. Альтернативой является mesh-топология, в которой каждый узел устанавливает прямое соединение с каждым другим.

Индустриальные решения Tailscale [3] и Nebula реализуют mesh-подход, опираясь на механизмы преодоления NAT. Целью данной работы является сравнительный анализ этих методов и экспериментальная проверка выбранного метода на разработанном прототипе.

1. Методы преодоления NAT

В документе RFC 5128 [4] систематизированы шесть методов, применяемых P2P-приложениями для преодоления NAT. Рассмотрим каждый из них.

Relaying (ретрансляция) – весь трафик между узлами передается через промежуточный сервер. Метод обеспечивает связность при любом типе NAT, однако соединение не является прямым: сервер увеличивает задержку и несет нагрузку по пересылке трафика [4].

Connection Reversal (обратное соединение) – узел с публичным IP-адресом инициирует соединение в обратном направлении по запросу узла за NAT. Метод неприменим, когда оба узла находятся за NAT [4].

UDP Hole Punching – оба узла одновременно отправляют UDP-пакеты друг другу. NAT создает маппинг при исходящем пакете и пропускает встречный пакет. Метод обеспечивает прямое P2P-соединение, но требует NAT с независимым отображением конечных точек (Endpoint-Independent Mapping, EIM-NAT) [4, 5].

TCP Hole Punching – аналогичный подход с использованием механизма Simultaneous Open протокола TCP. Оба узла одновременно отправляют SYN-пакеты. Однако многие NAT-устройства отслеживают состояния TCP-сессий и отбрасывают незапрошенный SYN или отвечают RST-пакетом [4].

UDP и TCP Port Prediction – модификации Hole Punching для Symmetric NAT. Методы анализируют последовательность назначения портов NAT-устройством и предсказывают следующий порт. Ненадежны: предсказание нарушается конкурирующим трафиком, а в CGNAT порты назначаются случайно [4, 5].

Результаты сравнительного анализа обобщены в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ методов NAT traversal (RFC 5128)

Метод	Прямое P2P	Оба за NAT	Symmetric NAT	Ограничения
Relaying	Нет	Да	Да	Задержка, нагрузка на сервер
Connection Reversal	Да	Нет	Нет	Один узел с публичным IP
UDP Hole Punching	Да	Да	Нет	Требует EIM-NAT
TCP Hole Punching	Да	Да	Нет	NAT отбрасывает SYN
Port Prediction	Да	Да	Частично	Порт непредсказуем

Из таблицы следует, что для mesh-VPN, где оба узла находятся за NAT, применимы только UDP Hole Punching и TCP Hole Punching.

2. Обоснование выбора UDP Hole Punching

Выбор между UDP и TCP Hole Punching обусловлен следующими факторами.

TCP Hole Punching требует механизма Simultaneous Open, при котором оба узла одновременно отправляют SYN-пакеты. NAT-устройство, получив входящий SYN при отсутствии маппинга, может ответить RST-пакетом, что приводит к разрыву соединения [4]. Протокол UDP не имеет механизма состояний: NAT создает маппинг при исходящем пакете и пропускает встречный пакет без проверки последовательности.

Кроме того, использование TCP в качестве транспорта VPN-туннеля приводит к проблеме двойной инкапсуляции (TCP-over-TCP): при потере пакета два уровня TCP конкурируют за повторную передачу, вызывая рост задержек [3].

По экспериментальным данным Ford et al. [5], UDP Hole Punching совместим с более чем 80 % NAT-устройств, тогда как TCP Hole Punching – с приблизительно 60 %. Корректность выбора подтверждается архитектурой индустриальных решений: Tailscale [3] и Nebula используют UDP Hole Punching как основной метод.

3. Архитектура прототипа и эксперимент

Для экспериментальной проверки выбранного метода разработан прототип mesh-VPN на языке Go, состоящий из двух компонентов.

Сигнальный сервер принимает периодические сообщения от клиентов по протоколу UDP и формирует карту сети – список публичных адресов всех участников, – которую рассылает каждые 5 секунд. Сервер обеспечивает обнаружение участников без непосредственного участия в передаче данных.

VPN-клиент создает виртуальный сетевой интерфейс (TUN – сетевое устройство уровня L3, работающее с IP-пакетами) с VPN-адресом из диапазона 10.0.0.0/24. При обнаружении нового участника в карте сети клиент инициирует процедуру UDP Hole Punching отправкой hello-пакетов с маркером 0x01. После получения ответного hello-туннель считается установленным. IP-пакеты, прочитанные из виртуального интерфейса, инкапсулируются в UDP-датаграммы с маркером 0x02 и отправляются напрямую другому узлу.

Структурная схема прототипа приведена на рис. 1.

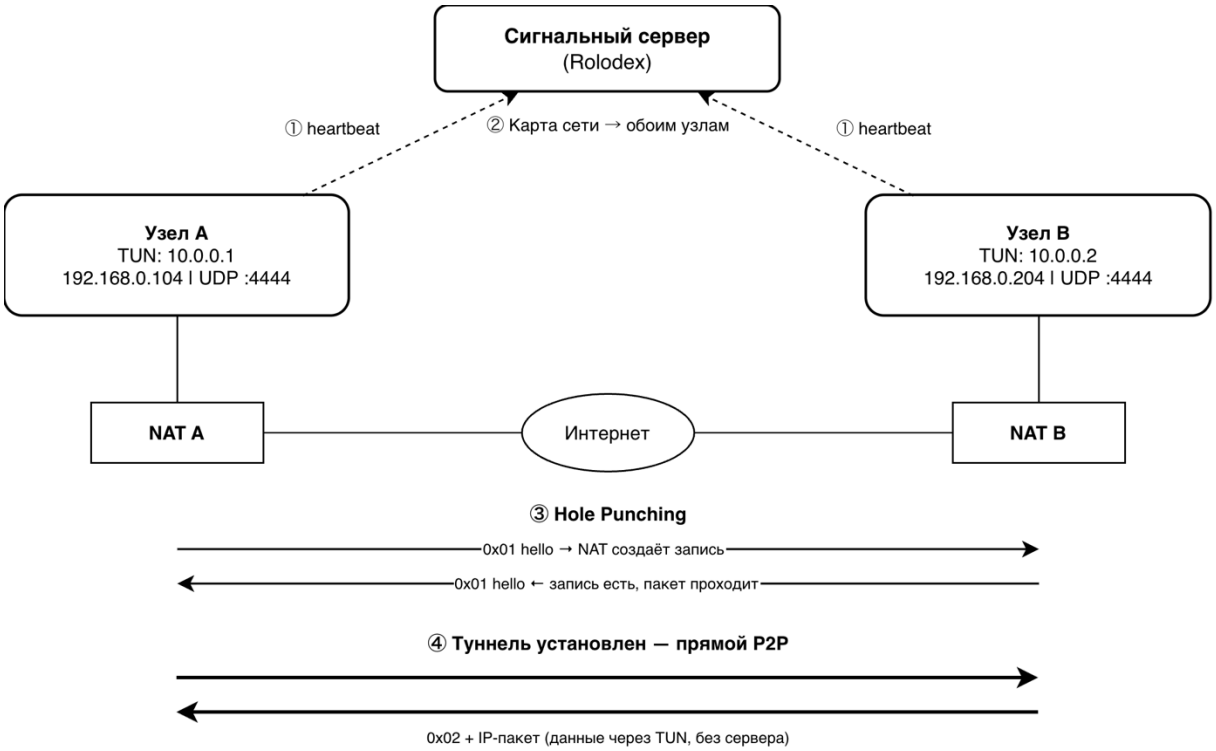


Рис. 1. Структурная схема прототипа

Эксперимент. Стенд состоит из сигнального сервера на VPS и двух клиентов. Клиенту A назначен VPN-адрес 10.0.0.1, клиенту B – 10.0.0.2. После запуска клиенты регистрируются на сигнальном сервере, обмениваются hello-пакетами (0x01), после чего туннель устанавливается. Проверка сквозной связности выполнена командой ping 10.0.0.2 с узла A – пакеты успешно доставлены через VPN-туннель.

Заключение

Сравнительный анализ шести методов преодоления NAT, описанных в RFC 5128, показал, что для VPN-сетей с mesh-топологией оптимальным является метод UDP Hole Punching. Методы Relaying и Connection Reversal не обеспечивают прямого P2P-соединения при обоих узлах за NAT. Методы Port Prediction ненадежны. TCP Hole Punching отсеян ввиду сложности Simultaneous Open и проблемы двойной инкапсуляции TCP-over-TCP.

Разработанный прототип mesh-VPN экспериментально подтвердил, что архитектура «сигнальный сервер + UDP Hole Punching + виртуальный сетевой интерфейс» достаточна для построения mesh-VPN. Данный подход соответствует решениям Tailscale [3] и Nebula.

Установлено ограничение: метод работает при условии NAT с независимым отображением конечных точек (EIM-NAT). При Symmetric NAT метод неприменим, что требует добавления relay-сервера.

Список используемых источников

1. Srisuresh P., Holdrege M. IP Network Address Translator (NAT) Terminology and Considerations // RFC 2663. 1999. DOI: 10.17487/RFC2663.

2. Gleeson B., Lin A., Heinanen J., Armitage G., Malis A. A Framework for IP Based Virtual Private Networks // RFC 2764. 2000. DOI: 10.17487/RFC2764.

3. Tailscale. How NAT Traversal Works [Электронный ресурс]. 2020. URL: https://tailscale.com/blog/how-nat-traversal-works (дата обращения: 20.03.2026).

4. Srisuresh P., Ford B., Kegel D. State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs) // RFC 5128. 2008. DOI: 10.17487/RFC5128.

5. Ford B., Srisuresh P., Kegel D. Peer-to-Peer Communication Across Network Address Translators // USENIX Annual Technical Conference. 2005. С. 179–192.

Статья представлена научным руководителем, старшим преподавателем кафедры ИКС СПбГУТ И. Ф. Тарабановым.

УДК 004.42

РАЗРАБОТКА КОНЦЕПЦИИ СИСТЕМЫ УПРАВЛЕНИЯ ПОРТФЕЛЕМ СТУДЕНЧЕСКИХ ПРОЕКТОВ

О. А. Костылева (студент группы ИСТ-213 СПбГУТ), kostyleva.oa@sut.ru
О. В. Раковский (к.т.н., доцент, доцент кафедры ИУС СПбГУТ)

В настоящее время учет студенческих проектов в вузах ведется преимущественно в табличных редакторах, что характеризуется отсутствием оперативного доступа к актуальному состоянию проектов, низкой прозрачностью вклада участников и высокой субъективностью оценки компетенций. Предлагаемая система обеспечивает централизованное управление проектами, автоматизацию отчетности, мониторинг прогресса и объективную оценку освоения студентами командных и технических компетенций.

управление портфелем проектов, студенческие проекты, информационная система, оценка компетенций, проектное обучение, ГОСТ Р ИСО 21504-2016

Сложившаяся практика учета студенческих проектов не обеспечивает быстрого доступа к состоянию проектов, прозрачности вклада участников и объективности оценки компетенций. В работе ставится цель – разработать концепцию системы управления портфелем студенческих проектов, соответствующую ГОСТ Р ИСО 21504-2016 [1] и устраняющую указанные недостатки. Дополнительно были учтены требования ГОСТ Р 54870-2011 [2], в частности процессы сбора и обработки информации и формализованного управления изменениями.

Система реализует ролевую модель RBAC (рис. 1), в рамках которой куратор наделяется полным контролем над портфелем, тимлид управляет задачами и отчетностью, а студент фиксирует выполнение собственных задач.

В состав концепции входят такие функциональные модули, как «Команды», «Заявки», «Задачи и прогресс», «Отчетность», «Календарь встреч», «Общий чат» и «Паспорт проекта».

За куратором закреплено право формировать команды, как самостоятельно, так и утверждать их самоорганизацию.

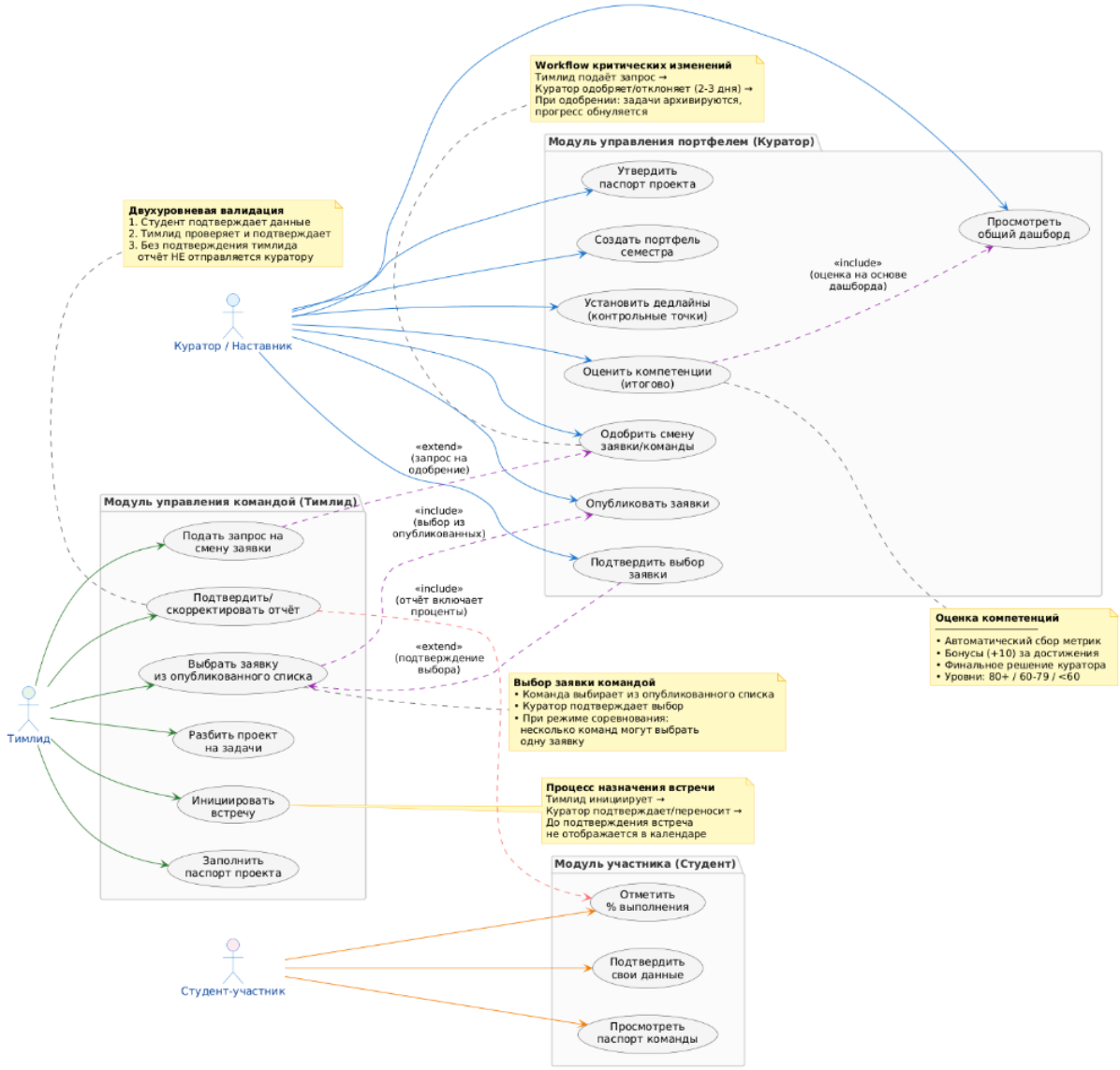


Рис. 1. Диаграмма вариантов использования системы

Механизмы контроля и отчетности

Ключевая особенность системы – двухуровневая валидация отчетности: сначала студент подтверждает свой процент выполнения, после чего тимлид проверяет и корректирует данные. Если тимлид не дал подтверждения, отчет не уходит куратору. Все корректировки сохраняются в аудит-логе, а личные проценты фиксируются для итоговой оценки. Отчет составленный тимлидом имеет общие данные по команде, а личные проценты сохраняются в системе для итоговой оценки студентов.

В концепцию также заложены автоматические уведомления о дедлайнах и дашборды куратора, показывающие только обобщенные показатели

по командам. Как отмечается в сборнике кейсов [3], такие решения снижают субъективность и повышают прозрачность.

Управление изменениями портфеля

Концепцией предусмотрен строгий порядок внесения изменений в портфель: смена заявки, состава команды или тимлида возможна только после оформления официального запроса (рис. 2). Последовательность действий выглядит так: тимлид подает запрос с обоснованием (например, риски невыполнения), куратор в течение 2–3 дней одобряет/отклоняет его, а при положительном решении предыдущие задачи архивируются, а прогресс начинается с нуля.

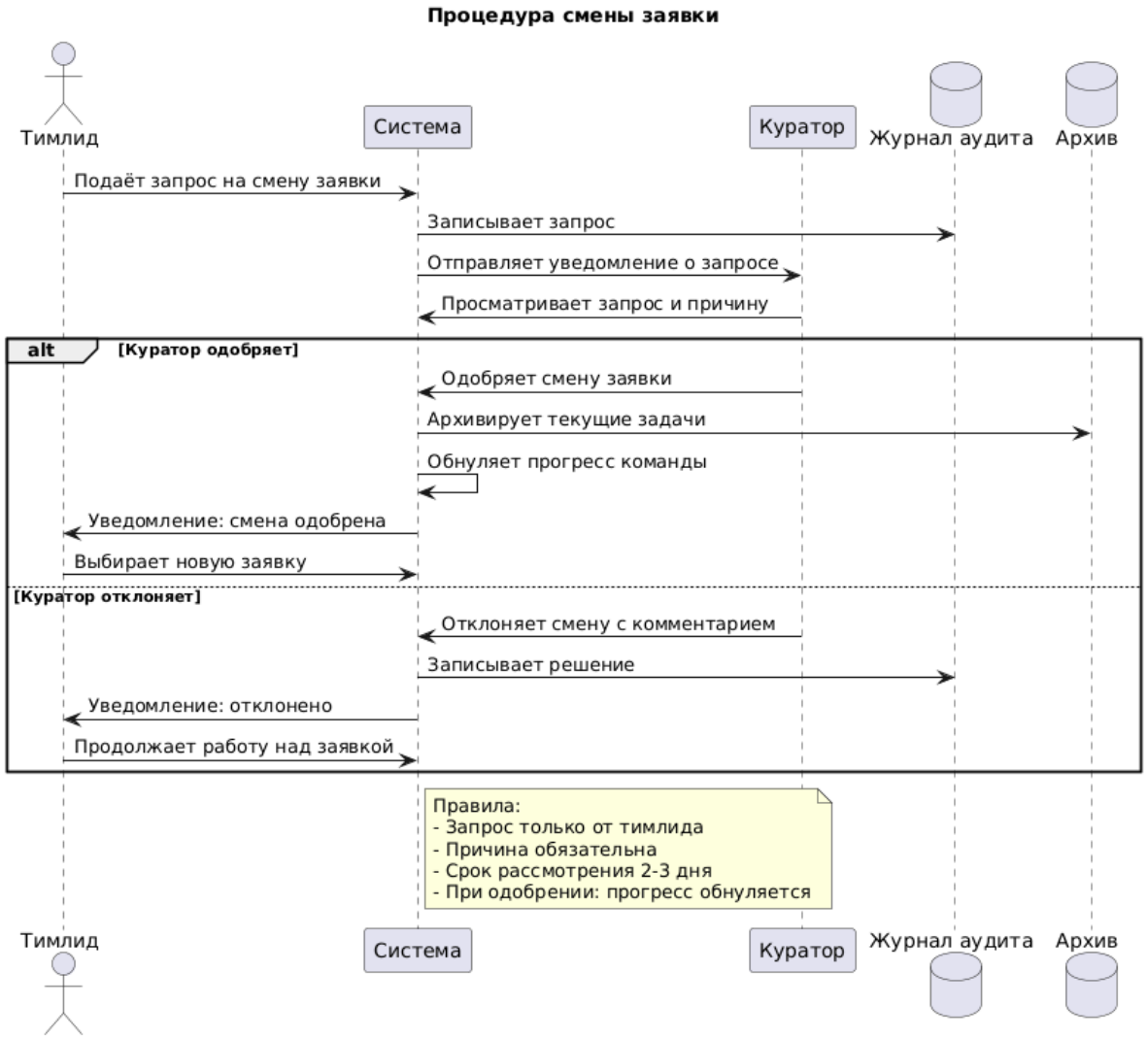


Рис. 2. Диаграмма последовательности смены заявки

Такой подход соответствует требованиям стандарта [1] к управлению изменениями состава портфеля.

Как и в случае с изменениями состава портфеля, процесс организации встреч также требует обязательного одобрения. Согласно предлагаемой концепции, инициировать встречу может только тимлид со стороны команды или сам куратор. При бронировании даты форме указывается состав участников, формат и повестку. Куратор (или тимлид) получает уведомление и принимает решение: подтвердить встречу или изменить какой-либо атрибут. Без подтверждения куратора (тимлида) встреча не считается оформленной и не попадает в календарь.

Оценка компетенций

В концепции заложен автоматический сбор количественных метрик (количество отчетов, процент выполнения, соблюдение дедлайнов). Для оценивания технических компетенций предлагается введение тимлидом отдельных задач на освоение конкретных технологий или прохождение онлайн-курсов. Такие задачи считаются выполненными только при подтверждении, например с помощью сертификата. Итоговый балл за компетенции (без учета бонусов) составляет до 100 баллов: до 50 – за командные, до 50 – за технические. Бонусные баллы (за публикации, выступления, освоения новых технологий, прохождение курсов) – до +10 начисляются куратором дополнительно и учитываются при определении итогового рейтинга, но не влияют на уровень усвоения компетенций. Окончательное решение по баллам остается за куратором и не может быть автоматически подменено расчетом системы.

Уровень усвоения (по 100-балльной шкале): 80 баллов и выше – полное усвоение, 60–79 – частичное, менее 60 – неудовлетворительное.

Предложенные в данной концепции подходы находят практическое воплощение в российских вузах. Примером служит платформа «Проектива» Тольяттинского государственного университета, где внедрены автоматический сбор цифрового следа, дашборды участников и система формирования оценки на основе проектной деятельности [4].

В результате предложенная концепция заменяет разрозненные таблицы централизованным цифровым решением, которое обеспечивает полную прозрачность хода проектов, минимизирует рутинную работу куратора и формирует объективную базу для оценки компетенций. Масштабируемость системы позволяет вести несколько курсов и групп одновременно,

а заложенные механизмы соответствуют лучшим практикам организации проектного обучения.

Список используемых источников

1. ГОСТ Р ИСО 21504-2016. Руководство по управлению портфелем проектов. М.: Стандартинформ, 2016. 24 с.

2. ГОСТ Р 54870-2011. Управление проектом. Требования к управлению портфелем проектов. М.: Стандартинформ, 2011. 16 с.

3. Проектное обучение: практики внедрения: методические рекомендации / под ред. О. В. Лешукова, Н. В. Исаевой, Л. А. Евстратовой. М.: Изд-во НИУ ВШЭ, 2018. 154 с.

4. Платформа «Проектива» Тольяттинского государственного университета [Электронный ресурс] // ТГУ: официальный сайт. URL: https://www.tltsu.ru/news/v_rossii_poiavilas_platforma_dlia_upravleniia_studproektami (дата обращения: 20.03.2026).

Статья представлена научным руководителем, профессором кафедры ИУС СПбГУТ, доктором технических наук, профессором О. В. Раковским.

УДК 621.397.13

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ НАЗЕМНОГО И СПУТНИКОВОГО ТВ ВЕЩАНИЯ

Т. Я. Кукушкин (студент группы МТВ-2531 СПбГУТ),
kukushkin.ty@sut.ru

Работа посвящена сравнительному анализу технологий наземного и спутникового цифрового телевизионного вещания с учетом особенностей их применения в Российской Федерации. Рассматриваются принципы построения и функционирования систем DVB-T2 и DVB-S2, используемое передающее и приемное оборудование, параметры модуляции и кодирования, а также эксплуатационные характеристики данных стандартов. Для оценки эффективности рассматриваемых решений проводится моделирование передачи сигнала в среде MATLAB Simulink, по результатам которого анализируются диаграммы созвездий и зависимости вероятности битовой ошибки от отношения сигнал шум для различных схем модуляции и кодовых скоростей. На основе полученных результатов определяется целесообразность применения наземного и спутникового вещания в зависимости от условий покрытия, особенностей инфраструктуры и требований к качеству телевизионного сигнала.

цифровое телевещание, стандарты DVB, DVB-T2, DVB-S2, модуляция, помехоустойчивость, BER, SNR, MATLAB/Simulink

Телевидение прошло длительный путь развития: от первых механических систем передачи изображения до современных цифровых сетей, обеспечивающих высокое качество изображения и звука. До конца XX века телевещание в основном оставалось аналоговым, что ограничивало количество каналов, устойчивость сигнала к помехам и эффективность использования радиочастотного спектра. Переход к цифровому телевидению позволил повысить качество трансляции, снизить влияние шумов и передавать в одном потоке не только видео и звук, но и дополнительные сервисы: электронную программу передач, субтитры и служебную информацию [1].

Современное цифровое телевещание в России развивается на базе стандартов семейства DVB. Для наземного эфирного вещания применяются DVB-T и DVB-T2, а для спутникового – DVB-S и DVB-S2. Стандарт DVB-T2 использует OFDM-модуляцию, которая повышает устойчивость сигнала к многолучевому распространению и помехам [2]. DVB-S2 применяется в спутниковых системах и поддерживает модуляции QPSK, 8PSK, 16APSK и 32APSK, а также помехоустойчивое кодирование LDPC/BCH [3].

Целью работы является сравнительный анализ технологий наземного и спутникового цифрового телевизионного вещания, определение их особенностей, преимуществ, недостатков и областей применения. Для этого рассматриваются архитектура сетей, используемое оборудование, нормативно-техническая база, параметры модуляции и кодирования, а также результаты моделирования передачи сигнала.

Наземное и спутниковое вещание не являются полностью взаимозаменяемыми технологиями. Они решают разные инженерные задачи и применяются в зависимости от территории, плотности населения, развитости инфраструктуры и требований к качеству сигнала. Для Российской Федерации, обладающей большой площадью, сложным рельефом и неравномерным распределением населения, особенно важно совместное использование этих технологий.

Наземное цифровое телевещание DVB-T2 строится на сети телецентров, передающих станций, ретрансляторов и пользовательских приемных устройств. Сигнал формируется в студии, проходит этап кодирования и мультиплексирования, затем поступает на передающие станции. Далее он распространяется через эфир в диапазонах VHF и UHF и принимается абонентом с помощью телевизионной антенны и цифрового тюнера [4]. Общий принцип работы наземного телевизионного вещания представлен на рисунке 1.

Главное преимущество DVB-T2 заключается в эффективном использовании частотного ресурса. В одном радиоканале шириной 8 МГц можно передавать несколько телевизионных программ, объединенных в мультиплекс. Благодаря применению OFDM сигнал делится на большое количество поднесущих, что повышает устойчивость к отражениям, городским помехам и сложному рельефу.

В России наземное вещание регулируется рядом ГОСТов, среди которых важнейшими являются ГОСТ Р 58912-2020, ГОСТ Р 55694-2013, ГОСТ Р 55696-2013 и ГОСТ Р 55947-2014. Эти документы определяют требования к параметрам сигнала, передающему оборудованию и приемникам: ширине канала, уровню пилот-сигналов, спектральной маске, стабильности частоты и чувствительности приемного оборудования [4-6].

Оборудование наземной сети включает студийные комплексы, кодеры, мультиплексоры, DVB-T2-модуляторы, усилители мощности, антенно-фидерные устройства и ретрансляторы. На стороне абонента используются те-

левизоры с поддержкой DVB-T2 или внешние приставки. При необходимости применяются активные антенны и усилители, повышающие качество приема [6, 7].

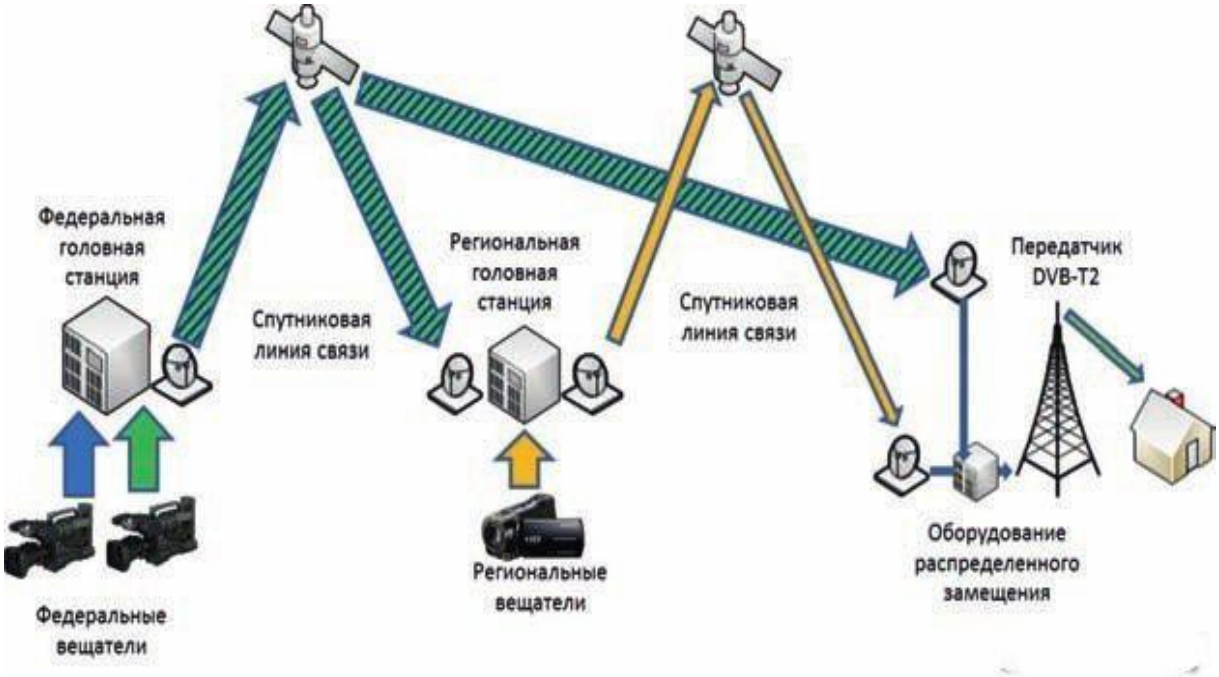


Рис. 1. Общий принцип работы наземного ТВ вещания

Основным недостатком наземного вещания является ограниченная зона покрытия одного передатчика. Радиус действия зависит от высоты антенной опоры, мощности передатчика, рельефа местности и наличия препятствий. Поэтому для покрытия больших территорий требуется сеть ретрансляторов. В городах и населенных районах это решение эффективно, но в труднодоступных и малонаселенных регионах развертывание такой инфраструктуры может быть экономически невыгодным.

Спутниковое телевещание DVB-S2 организуется по другой схеме. Сигнал формируется на головной станции, затем передается на наземную uplink-станцию, откуда направляется на геостационарный спутник. Спутник ретранслирует сигнал обратно на Землю, где он принимается пользовательской спутниковой антенной, конвертером LNB и ресивером. Общий принцип работы спутникового телевизионного вещания представлен на рисунке 2.

Главное преимущество спутникового вещания – широкая зона покрытия. Один геостационарный спутник способен обслуживать огромную территорию, включая удаленные районы, где строительство наземной сети затруднено или экономически нецелесообразно. Это особенно важно

для России, где имеются регионы с низкой плотностью населения, сложными климатическими условиями и недостаточно развитой наземной телекоммуникационной инфраструктурой.

Стандарт DVB-S2 является развитием DVB-S и обеспечивает более высокую спектральную эффективность. Он поддерживает модуляции QPSK, 8PSK, 16APSK и 32APSK, а также использует кодирование LDPC/BCH. Это позволяет передавать больше данных в пределах одного спутникового транспондера и обеспечивать трансляцию каналов высокой и сверхвысокой четкости. Спутниковые системы регулируются ГОСТ Р 58614-2019 и ГОСТ Р 58615-2019, которые устанавливают требования к параметрам DTH-вещания, приемным устройствам, уровню сигнала, шумовым характеристикам и устойчивости оборудования.

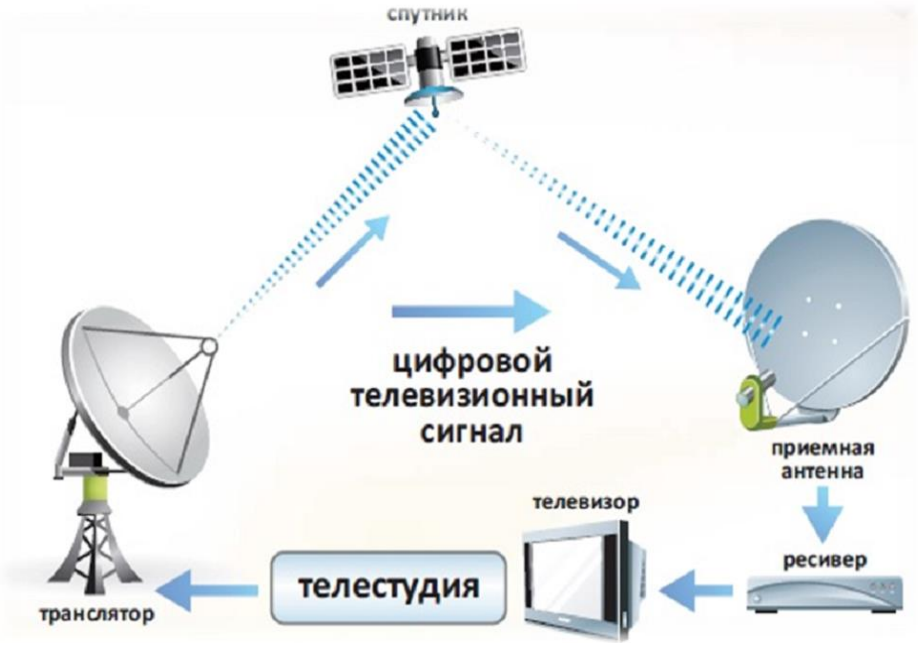


Рис. 2. Общий принцип работы спутникового ТВ вещания

Недостатком DVB-S2 является зависимость от атмосферных факторов. Сильный дождь, снег, обледенение антенны или неправильная настройка тарелки могут снижать качество приема. Кроме того, абонентское оборудование для спутникового телевидения обычно дороже, чем для наземного: требуется антенна, конвертер, кабельная линия и ресивер. Также спутниковая передача имеет большую задержку, связанную с расстоянием до геостационарной орбиты.

Для сопоставления технических и эксплуатационных параметров DVB-T2 и DVB-S2 были рассмотрены основные характеристики наземного и спутникового телевизионного вещания, представленные в таблице 1.

ТАБЛИЦА 1. Сравнение основных характеристик DVB-T2 (наземное) и DVB-S2 (спутниковое) систем

№	Характеристика	DVB-T2 (ГОСТ 58912)	DVB-S2 (ГОСТ 58614)	Комментарий
1	Рабочие частоты	УКВ/ДМВ (VHF/UHF), до 800 МГц	Сверхвысокие (Ku-диапазон, ~11-14 ГГц)	Наземный сигнал распространяется по поверхностному пути, спутник – свободно
2	Полоса телеканала	8 МГц	~36 МГц (транспондер)	Ширина канала DVB-T2 стандартизована на 7/8 МГц, DVB-S2 – на 36 МГц
3	Модуляция	CODFM (OFDM с поддержкой FEC)	QPSK/8PSK/16APSK/32APSK (LDPC+BCH)	DVB-S2 использует более высокие порядки модуляции и мощное кодирование
4	Дальность покрытия	До десятков км (зависит от мощности)	До охвата континента (~36000 км до спутника)	Спутник покрывает всю зону видимости, наземные РТС – локальную область
5	Пропускная способность мультиплекса	~20-50 Мбит/с (зависит от конфигурации)	Сотни Мбитс/с (несколько ТВ-потоков)	DVB-T2 ограничен 8 МГц, DVB-S2 использует весь транспондер
6	Пример оборудования	ТВ-передатчик на башне, приемная антенна + STB	Спутниковый трансмодулятор (uplink), тарелка + LNB + STB	Оба варианта используют специализированную технику, сертифицированную ГОСТ
7	Стандарты (ГОСТ/ETSI)	ГОСТ 58912-2020 (ETSI EN 302 755)	ГОСТ 58614-2019 (ETSI EN 302 307-1)	Российские ГОСТы привязаны к европейским стандартам DVB
8	Особенности эксплуатации	Чувствительность к рельефу, требуется повторение сигнала	Высокая зависимость от погоды (атмосферные ослабления)	Дождь/снег сильнее влияют на спутник, на наземное влияние рельефа

Для оценки параметров сигнала в работе было проведено моделирование DVB-S2 и DVB-T2 в среде MATLAB/Simulink. В моделях использовались блоки генерации битовой последовательности, кодирования, модуляции, канала с шумом AWGN, демодуляции и расчета BER. Результаты показали, что применение помехоустойчивого кодирования существенно снижает вероятность битовой ошибки. Простые схемы модуляции, например, QPSK, обеспечивают лучшую устойчивость к шумам, но меньшую скорость передачи. Более сложные схемы, такие как 64QAM, 256QAM или 32APSK, позволяют увеличить пропускную способность, но требуют более высокого отношения сигнал/шум [8].

В результате сравнительного анализа можно сделать вывод, что DVB-T2 и DVB-S2 имеют разные области оптимального применения. DVB-T2 наиболее эффективен в густонаселенных районах с развитой инфраструктурой, где можно построить сеть передающих станций и обеспечить стабильный прием при небольших затратах для абонента. DVB-S2 лучше подходит для удаленных территорий, где строительство наземной сети затруднено или экономически невыгодно. Наиболее рациональным решением для Российской Федерации является совместное применение обеих технологий: наземное вещание целесообразно использовать в городах и населенных пунктах, а спутниковое – для покрытия труднодоступных регионов, резервирования сигнала и доставки телевизионного контента на большие расстояния [2,7].

Список используемых источников

1. ГОСТ Р 54998-2012. Цифровое телевидение высокой четкости. Кодирование цифровых телевизионных сигналов для сжатия цифрового потока. Москва: Стандартинформ, 2012. 43 с.

2. ETSI EN 302 755 V1.3.1. Digital Video Broadcasting (DVB); Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2). Sophia Antipolis: ETSI, 2012. 142 p.

3. ETSI EN 302 307-1 V1.4.1. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2. Sophia Antipolis: ETSI, 2014. 113 p.

4. ГОСТ Р 58912-2020. Телевидение вещательное цифровое. Система эфирного наземного цифрового телевизионного вещания второго поколения DVB-T2. Общие технические требования. Введ. 2020-07-01. Москва: Стандартинформ, 2020. 58 с.

5. ГОСТ Р 55694-2013. Телевидение вещательное цифровое. Наземное цифровое телевизионное вещание. Структура цикловой синхронизации, методы кодирования для канала и модуляции. Введ. 2014-01-01. Москва: Стандартинформ, 2013. 52 с.

6. ГОСТ Р 55696-2013. Телевидение вещательное цифровое. Передающее оборудование для цифрового наземного телевизионного вещания DVB-T/T2. Технические требования. Основные параметры. Методы измерений. Введ. 2014-01-01. Москва Стандартинформ, 2013. 72 с.

7. Российская телевизионная и радиовещательная сеть: официальный сайт. URL: https://rtrs.ru (дата обращения: 30.04.2026). Текст: электронный.

8. Matlab Communications Toolbox User's Guide: электронный ресурс. Natick, MA: MathWorks Inc., 2022. URL: https://www.mathworks.com/help/comm/ (дата обращения: 30.04.2026).

Статья представлена научным руководителем, доцентом кафедры ЦТМ СПбГУТ, кандидатом технических наук Е. И. Тумановой.

УДК 621.39

ПОДХОДЫ К ОЦЕНКЕ НАДЕЖНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

А. В. Маковец (студент группы СИ341 БГАС), hol1ez0r@gmail.com

В статье рассматриваются основные подходы к оценке надежности инфокоммуникационных систем. Показано, что классическое описание надежности через отказы оборудования недостаточно для современных сетей и сервисов передачи данных. Сопоставляются структурный, функциональный, сервисно-ориентированный и интегральный подходы. Обосновывается необходимость многоуровневой оценки, учитывающей состояние инфраструктуры, корректность выполнения функций, качество обслуживания и последствия отказов для пользователя.

инфокоммуникационные системы, надежность, функциональная надежность, качество обслуживания, отказоустойчивость, оценка надежности

Надежность инфокоммуникационных систем представляет собой одну из базовых характеристик современных сетей связи, поскольку она определяет доступность сервисов, устойчивость передачи данных и качество взаимодействия пользователей с телекоммуникационной инфраструктурой. По мере усложнения сетей, роста доли программно управляемых решений и расширения спектра предоставляемых услуг задача оценки надежности перестала ограничиваться анализом аппаратных отказов. На практике система может сохранять физическую работоспособность оборудования, но при этом не обеспечивать требуемый результат обслуживания. Такая ситуация возникает из-за программных сбоев, ошибок конфигурации, нарушения маршрутизации, перегрузки сетевых ресурсов и деградации качества сервиса. В связи с этим в научной литературе все чаще ставится вопрос о необходимости расширения объекта оценки: от отдельного элемента сети к функции, услуге и целостному процессу обслуживания [1, 2].

Классическое понимание надежности закреплено в нормативной литературе как свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях эксплуатации [3]. Для техники связи такой подход естественным образом приводит к использованию вероятности безотказной работы, интенсивности отказов, средней наработки на отказ и коэффициента готовности. Достоинством этого подхода является высокая формализованность и наличие развитого математического аппарата. Он особенно полезен на этапах проектирования и выбора схем резервирования, когда требуется сопоставить надежность узлов, линий

связи и коммутационного оборудования. Однако для инфокоммуникационных систем такого описания уже недостаточно, поскольку оно не показывает, с какой вероятностью будет корректно выполнена прикладная задача, обеспечена доставка сообщения в требуемые сроки и сохранено приемлемое качество сервиса при частичном отказе части инфраструктуры.

В работах, посвященных функциональной надежности информационных систем, подчеркивается необходимость различать задачи структурной и функциональной надежности [1]. В первом случае рассматриваются отказы и восстановления элементов и структур системы. Во втором случае объектом анализа становится правильность и безошибочность выполнения информационных процессов. Для инфокоммуникационных систем это различие особенно важно. Исправность маршрутизатора, сервера или коммутатора сама по себе еще не гарантирует успешную передачу данных или выполнение сетевой функции. Некорректная работа программного обеспечения, ошибочные действия оператора или нарушение логики взаимодействия подсистем могут привести к функциональному отказу даже при отсутствии явных аппаратных повреждений. Следовательно, надежность сети должна рассматриваться не только как надежность составляющих ее элементов, но и как способность системы сохранять корректное функционирование в реальном эксплуатационном контуре.

Структурный подход к оценке надежности остается базовым и необходимым. В его рамках объектом оценки выступают элементы сети, узлы, линии связи, устройства питания, средства резервирования и процессы восстановления после отказов. Такой подход позволяет выявлять критические элементы инфраструктуры и количественно сравнивать различные проектные решения. Вместе с тем его ограничение состоит в том, что он ориентирован прежде всего на ответ на вопрос, исправен ли объект, а не на вопрос, выполнена ли функция в требуемом объеме и с приемлемым качеством. Для инфокоммуникационной системы, которая представляет собой многоуровневую совокупность аппаратных, программных и организационных компонентов, это различие принципиально. В обзорных работах по теории надежности указывается, что телекоммуникационные сети относятся к типам сложных систем, для которых бинарный критерий «работает – не работает» оказывается слишком грубым [4].

Следующим шагом стало развитие подходов, в которых надежность оценивается относительно выполняемых функций или функциональных подсистем. В этом случае для каждой функции задаются критерии отказа, допустимые границы отклонений и показатели надежности реализации соответствующей задачи. Достоинство такого подхода заключается в более

тесной связи оценки надежности с назначением системы. Если структурный подход отвечает на вопрос о надежности узла как технического объекта, то функциональный подход позволяет анализировать надежность обслуживания, маршрутизации, коммутации, хранения данных и мониторинга. Однако и здесь сохраняются методические трудности. Отдельные функции используют общие вычислительные и сетевые ресурсы, одно и то же программное обеспечение и тот же персонал, поэтому показатели надежности функциональных подсистем оказываются взаимосвязанными. Кроме того, в многосервисных сетях часть операций выполняется по случайным запросам, что требует учета потоков обращений и сценариев использования системы [1, 5].

В современных инфокоммуникационных системах все большую значимость приобретает сервисно-ориентированный подход. Его исходная идея состоит в том, что сеть следует рассматривать как среду обслуживания запросов, а надежность – как вероятность успешного предоставления требуемого сервиса с заданными параметрами качества. Такой подход ближе к реальным условиям эксплуатации, поскольку пользователь оценивает не исправность отдельного узла, а успешность доступа к услуге, время отклика, устойчивость соединения, задержки и потери. Частичный отказ при наличии резервирования и альтернативных маршрутов не всегда означает отказ системы в целом: сеть может сохранить обслуживание, хотя и с ухудшением отдельных показателей. По этой причине при оценке надежности инфокоммуникационных систем необходимо анализировать не только число отказов, но и последствия отказа для конкретного сервиса, пользовательского трафика и целевых функций системы. Такой ракурс естественным образом сближает задачи надежности с задачами качества обслуживания и живучести сети [2, 4].

Интегральный подход трактует надежность как совокупность свойств, обеспечивающих доверие к функционированию системы. В такой постановке учитываются готовность, безотказность, безопасность, целостность, конфиденциальность и ремонтопригодность. Для инфокоммуникационных систем данный подход представляется перспективным, поскольку позволяет учитывать не только отказы оборудования, но и ошибки программного обеспечения, нарушения информационной безопасности, воздействие внешней среды и человеческий фактор. Вместе с тем универсального показателя, который одновременно и без потери содержания описывал бы все перечисленные свойства, не существует. Поэтому для инфокоммуникационных систем целесообразно использовать многоуровневую схему оценки.

На первом уровне оценивается инфраструктура: аппаратные отказы, состояние линий связи, электропитание и средства резервирования. На втором уровне анализируется корректность выполнения задач: устойчивость маршрутизации, влияние программных ошибок и действий персонала. На третьем уровне рассматривается сервисная составляющая: вероятность успешного обслуживания запроса, задержка, потери и степень деградации качества при частичных отказах. На четвертом уровне оцениваются последствия отказов для пользователя и оператора. Такая схема не отменяет классические показатели надежности, а дополняет их с учетом особенностей современных инфокоммуникационных систем.

Таким образом, анализ существующих подходов показывает, что задача оценки надежности инфокоммуникационных систем не может быть сведена только к расчету вероятности отказа элементов сети. Надежность в этой области должна рассматриваться как комплексное свойство, включающее инфраструктурную устойчивость, корректность выполнения функций и способность системы обеспечивать сервис в условиях частичных отказов и изменяющейся нагрузки. Научная значимость такой постановки состоит в систематизации подходов к оценке надежности, а практическая – в возможности обоснованного выбора показателей для проектирования, эксплуатации и модернизации сетей связи. Перспективным направлением дальнейших исследований представляется разработка методик, позволяющих связать показатели структурной, функциональной и сервисной надежности в единую систему принятия инженерных решений.

Список используемых источников

1. Гаранин А. И. О функциональной надежности информационных систем // Интеллектуальные ИТ в управлении. 2018. № 2 (6). С. 45–50.

2. Фролов Д. Ю. Некоторые аспекты формирования понятия надежности сетей // Мир современной науки. 2011. № 3 (6). С. 18–22.

3. ГОСТ 27.002–2015. Надежность в технике. Термины и определения. М.: Стандартинформ, 2016. 23 с.

4. Ушаков И. А. Надежность: прошлое, настоящее, будущее // Reliability: Theory & Applications. 2006. № 1. С. 17–24.

5. ГОСТ Р МЭК 62628–2021. Надежность в технике. Руководство по обеспечению надежности программного обеспечения. М.: Российский институт стандартизации, 2021.

Статья представлена научным руководителем, заведующий кафедрой телекоммуникационных систем УО «Белорусская государственная академия связи», кандидатом технических наук, доцентом С. Н. Нефедовым.

УДК 621.397:659.1

ТАРГЕТИРОВАННАЯ РЕКЛАМА: ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ В ТЕЛЕВИЗИОННОЕ ВЕЩАНИЕ

М. О. Мананникова (студент группы МТВ-2531 СПбГУТ),
manannikova.mo@sut.ru

Рассматривается процесс осуществления таргетированной рекламы в цифровых телевизионных системах с использованием гибридной архитектуры вещания. Описаны элементы сигнализации рекламных вставок в транспортном потоке, выбор рекламного контента и структура взаимодействия клиентских устройств с серверной инфраструктурой. Отдельное внимание уделено стандартам DVB и принципам интеграции broadcast- и broadband-каналов.

DVB, HbbTV, MPEG-TS, SCTE-35, addressable TV, таргетированная реклама.

В цифровых системах телевизионного вещания передача контента осуществляется в виде мультиплексированного транспортного потока MPEG-TS, содержащего видеопотоки, аудиоданные и служебную информацию. Традиционная модель доставки рекламного контента предполагает его жесткую вставку в вещательный поток на стороне оператора.

Данный подход не учитывает различия в аудитории и не допускает адаптации рекламного контента на уровне пользовательского устройства. Для устранения этого ограничения используется модель адресной рекламы, при которой окончательный выбор рекламного материала переносится на клиентскую сторону.

Реализация такой модели стала возможной после внедрения гибридных стандартов, разработанных в рамках DVB, позволяющих синхронизировать вещательные и IP-потоки [1].

Функционирование таргетированной рекламы в цифровых медиасистемах основано на предварительной сегментации аудитории и последующем сопоставлении пользовательских характеристик с параметрами рекламных кампаний. В телевизионной среде источником данных выступает непосредственно пользовательское устройство, фиксирующее параметры просмотра, такие как выбранный канал, временные интервалы активности и длительность взаимодействия с контентом.

В отличие от веб-среды, где идентификация пользователя осуществляется через персональные аккаунты, в системах телевизионного вещания обработка данных, как правило, ведется на уровне устройства или домохозяйства. Это ограничивает детализацию профиля, однако позволяет

формировать устойчивые поведенческие модели, пригодные для сегментации аудитории. Формирование сегментов осуществляется на основе анализа накопленных данных с использованием алгоритмов классификации и кластеризации, что обеспечивает группировку пользователей по сходным характеристикам.

Результатом данного процесса является набор сегментов, каждому из которых могут быть сопоставлены определенные рекламные кампании. При этом выбор рекламного контента осуществляется автоматически на основе правил соответствия, заданных на серверной стороне, что позволяет реализовать динамическую персонализацию рекламных сообщений. Используемые параметры сегментации указаны в таблицах 1 и 2.

ТАБЛИЦА 1. Используемые параметры сегментации

Параметр	Источник
Время просмотра	Лог устройства
Выбранный канал	DVB-поток
Регион	IP/настройки
История просмотров	Локальное хранилище

ТАБЛИЦА 2. Параметры сегментации аудитории при таргетированной рекламе

Тип таргетинга	Описание
Демографический	Возраст, пол, социальный статус
Географический	Местоположение пользователя
Поведенческий	История просмотров и интересы
Контекстный	Соответствие рекламного сообщения контексту

Системы адресной телевизионной рекламы реализуются в рамках распределенной архитектуры, объединяющей вещательные и сетевые компоненты. Передача основного аудиовизуального контента осуществляется через инфраструктуру цифрового вещания DVB, тогда как доставка персонализированных рекламных материалов организуется через IP-сети. Такое разделение каналов передачи позволяет сохранить стабильность основного потока и одновременно обеспечить гибкость в управлении рекламным контентом.

На стороне пользователя функционирует устройство приема, например Smart TV или телевизионная приставка, которое выполняет декодирование

вещательного сигнала и одновременно обеспечивает взаимодействие с сетевыми сервисами. Встроенное программное обеспечение, реализованное, как правило, на базе HbbTV, отвечает за обработку сигналов управления и выполнение логики подстановки рекламного контента.

Серверная часть системы включает модуль принятия решений, который осуществляет выбор рекламного материала, и сервер хранения медиаресурсов, обеспечивающий доставку видеоданных. Взаимодействие между клиентской и серверной частями осуществляется по запросной модели: клиент инициирует обращение к серверу при наступлении события, связанного с необходимостью замены рекламного блока.

Такая архитектура соответствует концепции, реализуемой в стандартах DVB, где предусмотрено разделение функций передачи и персонализации контента, что обеспечивает масштабируемость и технологическую гибкость системы [1].

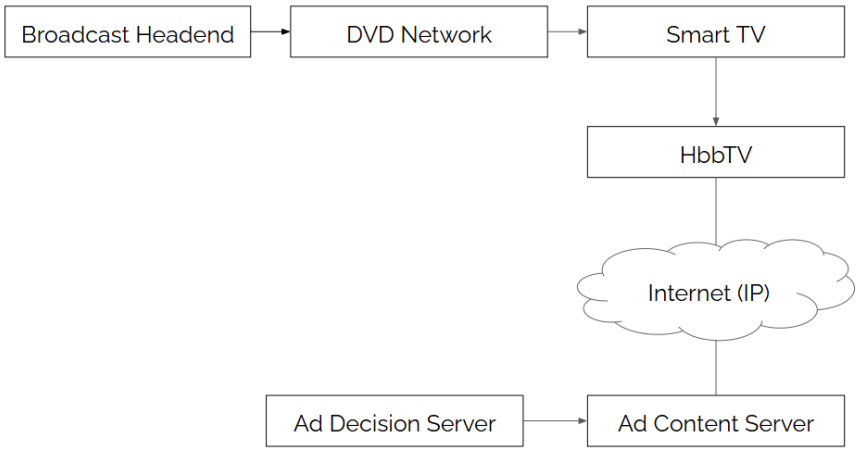


Рис. 1. Архитектура системы таргетированной рекламы в телевещании

Ключевым элементом реализации таргетированной рекламы является механизм сигнализации, позволяющий синхронизировать момент подстановки рекламного контента с вещательным потоком. В цифровом телевидении данная задача решается за счет передачи специальных управляющих сигналов в составе транспортного потока MPEG-TS.

В системах таргетированной рекламы для обозначения начала и окончания рекламных вставок применяются специальные сигнальные маркеры. На практике чаще всего используется стандарт SCTE-35, позволяющий передавать служебную информацию о параметрах рекламного блока: времени запуска, продолжительности и идентификаторах вставляемого контента. Эти данные передаются внутри транспортного потока и обрабатываются принимающим устройством.

Во время работы приемник непрерывно анализирует входящий поток данных. При обнаружении сигнала, соответствующего началу рекламной вставки, система начинает подготовку к замене стандартного рекламного блока на персонализированный контент. На данном этапе особенно важна корректная синхронизация всех процессов, поскольку даже небольшое смещение по времени может привести к заметным ошибкам воспроизведения – например, к обрыву изображения или нарушению синхронности звука и видео.

Фактически система сигнализации обеспечивает взаимодействие между вещательной частью инфраструктуры и сетевыми сервисами, отвечающими за доставку персонализированной рекламы. Благодаря этому становится возможной интеграция традиционного телевизионного вещания и IP-технологий.

Подстановка таргетированной рекламы выполняется непосредственно на стороне пользовательского устройства. Для этого приемник в реальном времени отслеживает MPEG-TS поток и фиксирует сигналы, указывающие на начало рекламного блока. После регистрации SCTE-35 маркера инициируется процедура замещения контента.

Далее устройство формирует запрос к серверу принятия решений. Вместе с запросом передаются данные о текущем сеансе просмотра: идентификатор устройства, информация о телеканале, временные параметры и характеристики пользовательского профиля. На основании этих сведений сервер выбирает рекламный материал, соответствующий заданному сегменту аудитории, после чего передает ссылку на медиаресурс.

Следующим этапом является загрузка рекламного контента по IP-каналу. Для того чтобы переключение между потоками происходило без заметных задержек, используется предварительная буферизация видеоданных. В момент начала рекламного блока устройство переключает воспроизведение с вещательного сигнала на заранее загруженный IP-контент. При корректной работе системы переход остается практически незаметным для зрителя.

После завершения рекламной вставки воспроизведение возвращается к основному вещательному потоку. Переключение синхронизируется с маркером окончания рекламного блока, что позволяет сохранить целостность аудиовизуального сигнала. Существенное значение при этом имеет скорость реакции системы: увеличение задержек может привести к появлению артефактов воспроизведения и ухудшению качества просмотра.

Управление рекламными кампаниями осуществляется на серверной стороне платформы. Для каждой кампании задаются параметры целевой

аудитории, временные ограничения показа, бюджет и допустимая частота демонстрации рекламных материалов одному пользователю.

Подбор рекламного контента выполняется с учетом характеристик аудитории и текущего контекста просмотра. В частности, анализируется соответствие тематики рекламного сообщения содержанию просматриваемой программы, поскольку контекстно связанная реклама обычно демонстрирует более высокую эффективность [2].

Дополнительно система контролирует частоту показа рекламных материалов, предотвращая чрезмерное повторение одного и того же ролика. Такой подход позволяет повысить эффективность рекламного воздействия без ухудшения пользовательского восприятия контента. В результате формируется система управления рекламными кампаниями, ориентированная на обеспечение релевантности рекламы и соблюдение заданных параметров ее распространения [3].

Для оценки эффективности рекламных кампаний используются различные количественные показатели. Одним из наиболее распространенных является CTR (Click Through Rate), отражающий отношение числа пользовательских взаимодействий с рекламным сообщением к общему количеству его показов. Данный показатель позволяет оценить степень вовлеченности аудитории и результативность применяемых методов таргетирования.

$$CTR = \frac{N_{click}}{N_{impressions}} \times 100\ \% \quad (1),$$

где N_{click} – количество взаимодействий с рекламой, $N_{impressions}$ – количество показов рекламы.

Еще одним важным показателем эффективности рекламной кампании является коэффициент конверсии (CR). Он показывает, какая доля пользователей после взаимодействия с рекламным сообщением выполнила целевое действие, например перешла на сайт, оформила заявку или совершила покупку. Данный параметр позволяет оценить не только уровень интереса аудитории к рекламе, но и ее практическую результативность с точки зрения достижения поставленных маркетинговых целей.

$$CR = \frac{N_{target}}{N_{visitors}} \times 100\ \% \quad (2),$$

где N_{target} – количество целевых действий, $N_{visitors}$ – количество пользователей, увидевших рекламу.

ТАБЛИЦА 3. Основные показатели эффективности рекламных кампаний

Показатель, единицы измерения	Описание
CTR, %	Отношение кликов к количеству показов
CR, %	Доля пользователей, совершивших целевое действие
CPM, руб.	Стоимость тысячи показов
CPA, руб.	Стоимость целевого действия

Анализ параметров, представленных в таблице 3, позволяет оценивать эффективность рекламной кампании и при необходимости корректировать параметры сегментации аудитории, а также алгоритмы подбора рекламного контента. Использование аналитических данных практически в режиме реального времени дает возможность оперативно адаптировать рекламную стратегию с учетом поведения и интересов пользователей [4-6].

Список используемых источников

1. DVB Project. Targeted Advertising and Addressable TV // DVB. URL: https://dvb.org/solutions/interactivity-personalization/ (дата обращения: 17.03.2026).

2. Галиуллина, А. Ф. Таргетирование телевизионного контента с точки зрения юмористического кодирования // Вестник Казанского государственного университета культуры и искусств. 2018. № 3. С. 95–99. URL: https://cyberleninka.ru/article/n/targetirovanie-televizionnogokontenta-s-tochki-zreniya-yumoristicheskogo-kodirovaniya (дата обращения: 17.03.2026).

3. Потапов, П. Ф., Ржанов, А. А. Роль медиапланирования в практике регионального телевещания // Вестник Воронежского государственного университета. Серия: Филология. Журналистика. 2017. № 4. С. 187–191. URL: https://cyberleninka.ru/article/n/rol-mediaplanirovaniya-v-praktike-regionalnogo-televeschaniya(дата обращения: 17.03.2026).

4. Карамышева, А. С. Увеличение трафика интернет-СМИ с помощью таргетированной рекламы ВКонтакте // Медиаскоп. 2020. № 2. URL: https://cyberleninka.ru/article/n/uvelichenie-trafika-internet-smi-s-pomoschyu-targetirovannoy-reklamy-vkontakte (дата обращения: 17.03.2026).

5. Киричек, П. Н. Информационная культура и рекламная коммуникация // Знание. Понимание. Умение. 2016. № 2. С. 156–162. URL: https://cyberleninka.ru/article/n/ informatsionnaya-kultura-i-reklamnaya-kommunikatsiya (дата обращения: 17.03.2026).

6. Жамсаранов, А. А. Особенности использования таргетированной рекламы в российском бизнесе // Экономика и бизнес: теория и практика. 2019. № 10. С. 86–90. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-targetirovannoy-reklamy-v-rossiyskom-biznese (дата обращения: 17.03.2026).

Статья представлена научным руководителем, заведующим кафедрой ЦТМ СПбГУТ, доцентом С. Л. Фёдоровым.

УДК 621.397.231

МЕТОДЫ КОДИРОВАНИЯ ТРЕХМЕРНЫХ ИЗОБРАЖЕНИЙ

А. О. Матвеев (студент группы МТВ-2531 СПбГУТ), matveev.ao@sut.ru

В современном мире кодирование занимает неотъемлемую часть в медиапроизводстве. Благодаря нему значительно снижается нагрузка на мировой видео трафик. В последние годы наблюдается рост интереса к иммерсивным технологиям, которые находят все более широкое применение в таких сферах, как медиаиндустрия, медицина, индустрия развлечений, научные исследования и других. Так как трехмерные изображения характеризуются большим объемом данных, необходимо углубиться в принципе кодирования трехмерных изображений. Эффективное кодирование позволяет существенно сократить затраты на хранение и ускорить обработку трехмерных изображений.

иммерсивные технологии, кодирование, карты глубины, облака точек, сжатие

Кодирование объемных изображений – это процесс преобразования исходных данных в формат, удобный для хранения, передачи и воспроизведения мультимедийного контента.

Причины кодирования:

1. Значительное уменьшение размера файлов для последующего хранения без существенной потери качества.

2. Сжатые файлы быстрее загружаются и скачиваются. Возможность подстраивать качество видео под текущую скорость соединения пользователя.

3. Совместимость и стандартизация:

1) Кодирование обеспечивает воспроизведение контента на разных платформах и устройствах (смартфоны, ПК, телевизоры).

2) Использование стандартных кодеков (например, H.264, H.265, JPEG 2000) упрощает обмен и обработку медиафайлов.

4. Возможность защиты контента.

5. Улучшение качества восприятия:

1) Можно удалить избыточную информацию, которую человеческий глаз не заметит.

2) Поддержка высокого разрешения и 3D.

6. Упрощение редактирования и обработки медиаконтента.

Иммерсивное пространство – это среда, которая создает эффект полного погружения в происходящее, когда человек перестает быть сторонним наблюдателем и становится частью события.

Объемное видео (Volumetric Video) – это 3D-представление реального мира, захваченное с помощью множества камер и преобразованное в 3D-модель или облако точек, которое можно просматривать с 6 степенями свободы (6DoF). Объем 3D-информации о сцене обычно намного больше, чем объем 2D-информации о той же сцене. Таким образом, сжатие является обязательным.

Используется метрика PSNR. IV-PSNR – это объективная метрика качества на основе PSNR, адаптированная для приложений с эффектом погружения в видео. По сравнению с PSNR были добавлены две основные модификации: соответствующий сдвиг пикселей и глобальный цвет. Соответствующий сдвиг пикселя устраняет влияние небольшого смещение краев объектов, вызванное репроекционными ошибками. Глобальная разница в цвете уменьшает влияние различных цветовых характеристик различных входных видов. IV-PSNR рассчитывается отдельно для каждого кадра последовательности. В конце, возвращается среднее значение IV-PSNR. Показатель качества IV-PSNR основан на PSNR; следовательно, чем больше число, тем лучше качество [1].

Проведем сравнительный анализ стандартов и методов кодирования, зафиксируем общую информацию в таблицу 1.

Кодирование многоракурсного видео

Кодирование многоракурсного видео (Multiview Video Coding, MVC) – это технология, позволяющая эффективно сжимать и передавать видеоданные, полученные с нескольких ракурсов (видов) одной сцены. Кадры одного вида могут предсказываться по времени и по другим видам для существенного снижения избыточности и повышения степени сжатия.

В потоке данных MVC выделяются базовые виды (декодируемые стандартными декодерами H.264/AVC) и дополнительные виды, которые используют информацию из базовых для реконструкции. Для передачи многоракурсного видео используются транспортные потоки MPEG-2 или MPEG-4, где каждый вид и его компоненты могут быть организованы в подпотоки [1].

Кодирование видео с несколькими ракурсами с предсказанием по сравнению с независимым кодированием дает выигрыш в 3 дБ, что примерно

соответствует 50 %-ной экономии скорости передачи данных. Для видео с несколькими просмотрами (до 8 просмотров) было зафиксировано снижение скорости передачи в среднем на 20 % по сравнению с общей скоростью одновременной трансляции (рис. 1) [2].

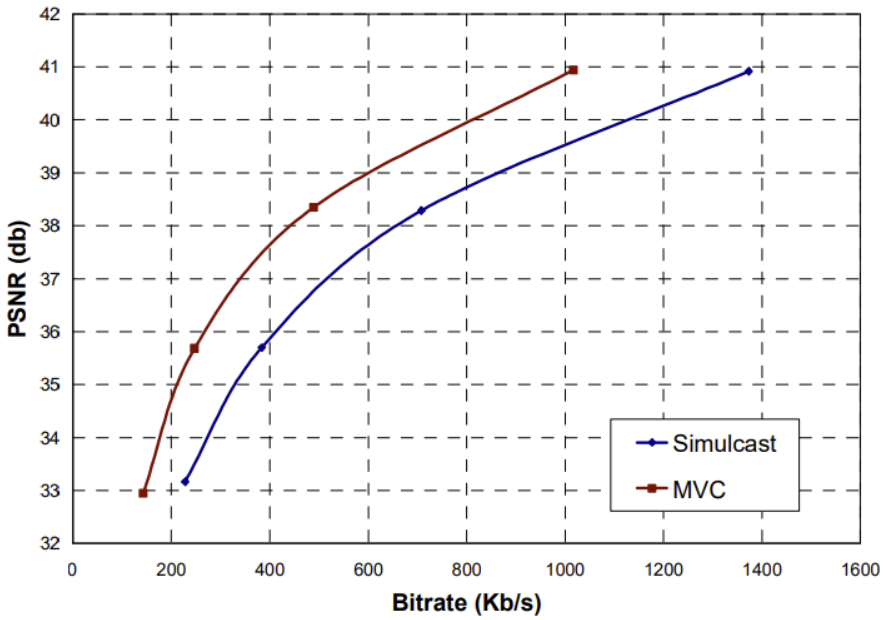


Рис. 1. Сравнение производительности одновременного кодирования с производительностью эталонного программного обеспечения MVC сигнала

Высокоэффективный стандарт эффективного видеокодирования (HEVC)

По сравнению с AVC, HEVC может достичь 50 % увеличения скорости передачи данных при субъективной оценке этих стандартов.

Расширенная версия HEVC – 3D-HEVC, предназначена для сжатия 3D-видео в формате multiview video plus depth. Это расширение включает в себя прогнозирование с компенсацией несоответствия, параметр движения между просмотром, и прогнозирование остатков между просмотром для кодирования зависимого многоракурсного видео. Для увеличения глубины просмотра добавлены новый режим внутреннего кодирования, модифицированная компенсация движения, векторное кодирование движения и концепция параметра движения. Кодировщик оптимизирует соотношение скорости и искажений на основе контроля качества нового вида между существующим видом в многоракурсном видео. Эволюция 3D-HEVC, основанная на объективной и субъективной оценке, демонстрирует прирост примерно на 20 % по сравнению с multiview-HEVC (MV-HEVC), и почти на 50 % по сравнению с HEVC simulcast.

Кодирование карт глубины

1) Принимаются исходные данные о глубине изображения.

2) Анализируется динамический диапазон и структура карты.

3) Определяются подмножества уровней для занятых/незанятых пикселей.

4) Выполняется преобразование значений глубины в карту с учетом выбранных порогов.

5) Формируется двоичный поток с картой глубины и метаданными.

Сжатие видео в формате MPEG

Подход рендеринга на основе глубины изображения (DIBR) использует несколько ракурсов камеры и связанные карты глубины. Для кодирования этих представлений, можно использовать видеокодек с несколькими ракурсами, такой как MV-HEVC, который находит пространственные и временные соответствия или избыточность в различных видах в многоракурсном видео. Однако, комитет по кодированию MPEG-I отказался от подобного подхода в пользу передача одного или нескольких эталонных видов.

Одним из вариантов – стандарт MPEG-I V3C (Volumetric Video Content Compression), который сжимает, преобразуя 3D-представление кадра в набор 2D-представлений и связанных с ними метаданных.

Для каждого компонента (геометрии и атрибутов) формируются отдельные видеопотоки или упаковываются в один «packed» компонент для устройств с ограниченными ресурсами. Полученные 2D-представления сжимаются с использованием традиционных видеокодеков (HEVC, VVC и др.). Информация о положении патчей, параметрах виртуальных камер и т. д. – кодируются отдельно и передаются вместе с видеопотоком [3].

Кодирование светового поля

Световое поле представляет собой набор изображений, полученных с множества близко расположенных ракурсов, что позволяет восстановить трехмерную структуру сцены и обеспечить возможность изменения точки обзора при просмотре.

При кодировании сначала осуществляется запись информации о световом потоке с использованием многокамерного захвата, а затем все приходит к обработке, которая может включать в себя: аппроксимацию светового

поля с помощью суммы взвешенных бинарных изображений, использование математических методов для представления светового поля в более компактной форме, или использование методов, которые используют разреженные представления. Сравнительный анализ стандартов и методов кодирования представлен в таблице 1.

ТАБЛИЦА 1. Стандарты кодирования

Стандарт/Метод	Краткое описание	Эффективность (сжатие/качество)	Особенности и применение
MPEG MVC	Расширение H.264/AVC для многоракурсного видео	Эффективнее, чем раздельное кодирование ракурсов	Используется для 3D Blu-ray, совместим с H.264
3D-HEVC (H.265/MVC)	Расширение HEVC для 3D и многоракурсного видео	На 30–50 % эффективнее H.264/MVC	Поддержка больших разрешений, выше вычислительная сложность
Кодирование карт глубины	Отдельное или совместное кодирование карт глубины для 3D-видео	Позволяет снизить битрейт (до 237 % BD-Rate для карт глубины)	Используется в сочетании с MVC/HEVC для повышения качества 3D-видео
MPEG-I V3C (Volumetric Video Coding)	Кодирование объемного видео (3D-видео с произвольными точками обзора)	Находится на стадии стандартизации, ожидается высокая эффективность для 6DoF-видео	Для AR/VR, требует значительных вычислительных ресурсов
Кодирование светового поля	Кодирование информации о световом поле (лучи света в пространстве)	Эффективность ниже, чем у MVC/HEVC, но обеспечивает свободу выбора точки обзора после съемки	Применяется для 6DoF-видео, AR/VR, научных и промышленных задач

Заключение

Исходя из данных, становится ясно, что существует множество вариантов кодирования информации, каждый из которых показывает свою эффективность в той или иной сфере. Важно правильно подобрать одну или несколько методик для достижения наилучшего результата.

Список используемых источников

1. Gauthier Lafruit, Mehrdad Teratani. Virtual Reality and Light Field Immersive Video Technologies for Real-World Applications, 2021. 377 с.

2. Vetro, A.; Wiegand, T.; Sullivan G.J. Overview of the Stereo and Multiview Video Coding Extensions of the H.264/MPEG-4 AVC Standard, 2011. 15 с.

3. An Overview of the MPEG Standard for Storage and Transport of Visual Volumetric Video-Based Coding [Электронный ресурс]. URL: https://www.frontiersin.org/journals/signal-processing/articles/10.3389/frsip.2022.883943/full (дата обращения: 08.04.2026).

Статья представлена научным руководителем, заведующим кафедрой ЦТМ СПбГУТ, доцентом С. Л. Фёдоровым.

УДК 004.357

ОЦЕНКА ЭФФЕКТИВНОСТИ ШУМОПОДАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВОЙ МОДЕЛИ DTLN

А. А. Мочалов (студент группы Р-41м СПбГУТ), mochalov.aa@sut.ru

В работе рассматривается задача оценки эффективности шумоподавления речевых сигналов на основе нейросетевой модели DTLN. Актуальность обусловлена широким применением технологий обработки речи и необходимостью повышения качества аудиосигнала в условиях шума. Выполнен сравнительный анализ нейросетевого и классических методов шумоподавления. Проведена субъективная оценка качества по результатам слепого прослушивания. Эксперимент выполнен для различных типов шумов и уровней отношения сигнал/шум. Полученные результаты демонстрируют преимущества нейросетевого подхода и подтверждают эффективность модели DTLN.

нейросети, шумоподавление, аудиосигналы

Технологии обработки речевых сигналов широко применяются в системах связи, вещания и голосовых интерфейсах. Одной из ключевых задач является подавление фонового шума, существенно влияющего на разборчивость и качество речи.

Существуют классические методы шумоподавления, основанные на спектральной обработке, и современные нейросетевые подходы. Несмотря на широкое использование объективных метрик (PESQ, STOI, SI-SDR), их значения не всегда коррелируют с субъективным восприятием, что усложняет корректное сравнение методов.

Целью работы является экспериментальная оценка эффективности шумоподавления речевых сигналов с использованием нейросетевой модели DTLN и классических алгоритмов на основе субъективного тестирования.

К классическим методам шумоподавления относятся спектральное вычитание и фильтр Винера. Спектральное вычитание основано на оценке спектра шума и его вычитании из спектра зашумленного сигнала [1]. Метод обладает низкой вычислительной сложностью и эффективен при стационарных шумах, однако в более сложных сценариях может показывать искажения и довольно чувствителен к ошибкам оценки шума. Фильтр Винера же реализует равномерную фильтрацию за счет минимизации среднеквадратичной ошибки [2]. Он обеспечивает более плавное подавление шума

и лучше сохраняет структуру речи, но при этом может сохранять часть шума неподавленным и зависит от величины сигнал/шум [3].

В качестве нейросетевого подхода рассматривается модель DTLN (Dual-Signal Transformation LSTM Network) [4]. Данная модель использует двухэтапную обработку сигнала в частотной и временной областях. Модель способна учитывать сложные нелинейные зависимости и демонстрирует высокую эффективность, особенно при нестационарных шумах, однако ее качество зависит от обучающей выборки. В рамках работы использовалась модель DTLN, обученная на наборе речевых сигналов с добавлением различных типов шумов. Обучающая выборка включала записи речи с наложением как стационарных, так и нестационарных шумов, что позволило сформировать модель, способную обобщать различные акустические условия.

Эксперимент проводился на наборе речевых сигналов, включающих записи речи. В качестве помех использовались автомобильный шум и шум ремонтных работ, что позволило рассмотреть как стационарные, так и нестационарные шумовые условия. Зашумление выполнялось путем аддитивного смешивания сигнала и шума при уровнях сигнал/шум 0, 5 и 10 дБ.

Для оценки качества использовалась субъективная шкала MOS (Mean Opinion Score) в диапазоне от 1 до 5 [5]. В тестировании приняли участие 12 слушателей, каждый из которых оценивал все аудиофрагменты длительностью 10 секунд. Аудиоматериалы предъявлялись в случайном порядке, а условия прослушивания были унифицированы, что обеспечивало корректность сравнительного анализа.

Результаты субъективной оценки показывают, что при SNR = 10 дБ наилучшее качество обеспечивает модель DTLN. Для автомобильного шума значение MOS достигает 4,5, тогда как для спектрального вычитания и фильтра Винера – 4,0 и 3,7 соответственно. Аналогичная тенденция наблюдается и для шума ремонтных работ.

На рисунках 1 и 2 представлена зависимость оценки MOS от уровня SNR для различных методов.

Для классических алгоритмов наблюдается достаточно предсказуемое поведение: с увеличением отношения сигнал/шум качество обработки постепенно возрастает. При более высоких значениях SNR полезный сигнал выделяется лучше, поэтому алгоритмам проще отделять речь от шумовой составляющей.

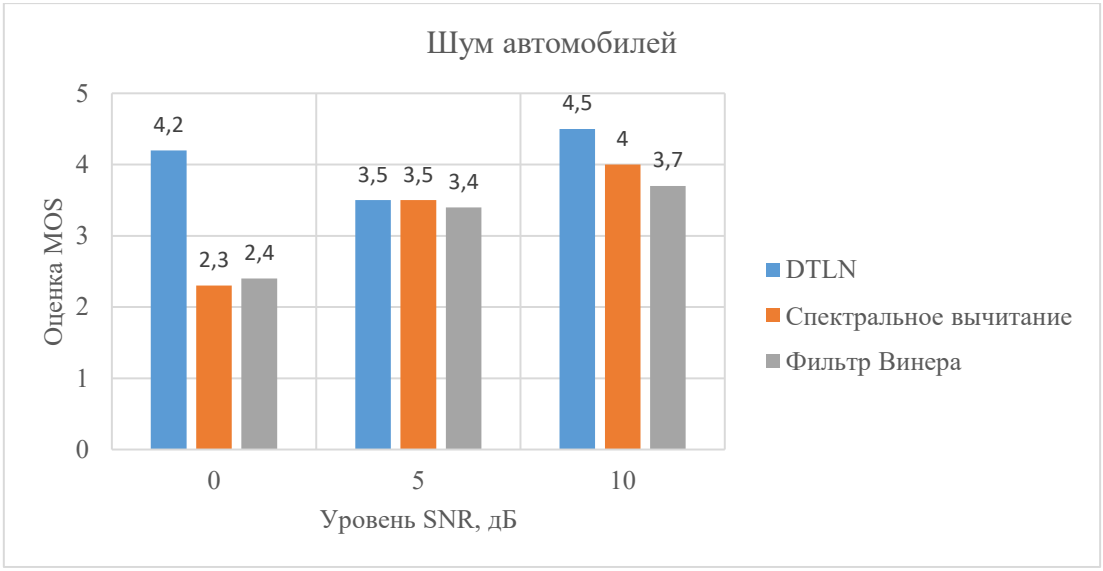


Рис. 1. Зависимость оценки MOS от SNR аудиосигнала, содержащего автомобильный шум

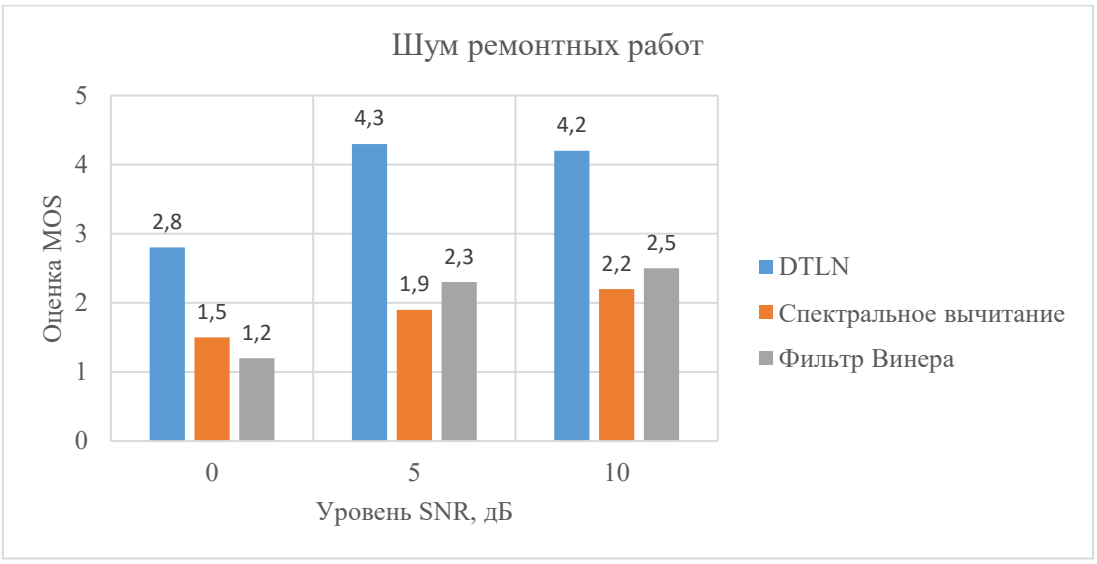


Рис. 2. Зависимость оценки MOS от SNR аудиосигнала, содержащего шум ремонтных работ

Наиболее заметные различия между методами проявляются при обработке нестационарных шумов, например, шума ремонтных работ. В таких условиях качество работы классических алгоритмов снижается значительно сильнее: MOS находится в диапазоне 1,2-2,5. При этом модель DTLN продолжает показывать более высокие значения (2,8-4,2), что еще раз подтверждает ее преимущество в сложных акустических условиях.

Различается и характер возникающих искажений после обработки сигнала. Спектральное вычитание обеспечивает наиболее интенсивное подавление шума, но вместе с этим в сигнале появляются заметные артефакты. Фильтр Винера, напротив, сохраняет речь более естественной, но часть шумовой составляющей остается в обработанном сигнале. Модель DTLN

в большинстве рассмотренных случаев позволяет получить более сбалансированный результат между степенью подавления шума и сохранением качества речи.

Полученные результаты показывают, что модель DTLN обеспечивает более высокое качество шумоподавления по сравнению с классическими алгоритмами, особенно при наличии нестационарных шумов. При этом зависимость качества обработки от уровня SNR для нейросетевого подхода выражена слабее, чем для спектрального вычитания и фильтра Винера.

Следует учитывать, что эффективность DTLN во многом определяется составом обучающей выборки. Если характеристики шумов или условия применения существенно отличаются от данных, использованных при обучении модели, качество обработки может снижаться. По этой причине для практического применения подобных систем важны как разнообразие обучающих данных, так и адаптация модели под конкретные акустические условия.

Список используемых источников

1. Boll S. Suppression of acoustic noise in speech using spectral subtraction // IEEE Transactions on Acoustics, Speech, and Signal Processing. 1979. Vol. 27. N 2. P. 113–120.

2. Haykin S. Adaptive Filter Theory. 5th ed. Pearson, 2013. – 800 p.

3. Никитин О. Р., Левин Е. К., Лабзина Е. А. Использование фильтра Винера для подавления помех в речевом сигнале // Методы и устройства передачи и обработки информации. – 2020. URL: https://rts-md.mivlgu.ru/MDjornal/article/view/141.

4. Westhausen N. L., Meyer B. Dual-Signal Transformation LSTM Network for Real-Time Noise Suppression // Interspeech 2020. PP. 2472–2476.

5. ITU-T P.800. Methods for subjective determination of transmission quality. Geneva: ITU, 1996.

Статья представлена научным руководителем, ст. преподавателем кафедры ЦТМ СПбГУТ О. А. Свиньиной.

УДК 004.032.26

МЕТОДЫ СТРУКТУРНОЙ ОПТИМИЗАЦИИ НЕЙРОНЫХ СЕТЕЙ ДЛЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОТЕЛЕКОММУНИКАЦИЯХ

О. И. Пантюхин (канд. техн. наук, доцент кафедры ССиПД СПбГУТ
Н. Э. Хрусталев (магистрант гр. МСТ-2561 СПбГУТ), hrustalev.ne@sut.ru

В работе рассматриваются методы структурной оптимизации нейронных сетей для систем искусственного интеллекта в инфотелекоммуникациях. Под такими методами понимаются подходы обрезания весов и структурной дистилляции, обеспечивающие снижение вычислительной сложности моделей при сохранении их качества. На основе анализа современных публикаций выделены принципы структурного удаления параметров и механизма переноса знаний от teacher-модели к student-модели. Основным результатом является классификация методов сжатия и оценка их применимости для edge-устройств и распределенных сетей. Показано, что указанные подходы позволяют эффективно решать задачи мониторинга трафика, обнаружения аномалий и адаптивного управления ресурсами.

нейронные сети, структурная оптимизация, обрезание весов, структурная дистилляция, инфотелекоммуникации, edge computing.

Современные инфотелекоммуникационные системы характеризуются ростом объемов передаваемых данных, увеличением числа подключенных устройств и усложнением сетевой инфраструктуры. В таких условиях искусственный интеллект становится необходимым инструментом для мониторинга состояния сети, прогнозирования нагрузки, обнаружения аномалий и адаптивного управления ресурсами. При этом практическое применение нейросетевых моделей в телекоммуникационной среде ограничивается требованиями к вычислительным ресурсам, объему памяти, времени отклика и энергопотреблению. Особенно это заметно при развертывании интеллектуальных алгоритмов на периферийных устройствах, маршрутизаторах, базовых станциях и иных узлах распределенной инфраструктуры.

В связи с этим особую актуальность приобретают методы структурной оптимизации нейронных сетей, направленные на снижение вычислительной сложности без существенной потери качества. Наиболее распространенными подходами являются методы обрезки весов и структурной дистилляции [1, 2]. Обрезка весов позволяет уменьшать избыточность модели за счет удаления малозначимых параметров, связей или структурных компонентов, а структурная дистилляция обеспечивает передачу знаний от более сложной

модели к компактной архитектуре, пригодной для работы в условиях ограниченных ресурсов. Совместное использование этих методов представляет практический интерес для задач интеллектуальной обработки трафика, анализа сетевых состояний и поддержки принятия решений в реальном времени.

Метод обрезки весов основан на предположении о наличии избыточных параметров, вклад которых в итоговую функцию потерь является незначительным. В зависимости от уровня структурирования различают неструктурное и структурное удаление. Неструктурное обрезание ориентировано на исключение отдельных весов, тогда как структурный вариант предполагает удаление нейронов, фильтров, каналов или целых блоков сети. С практической точки зрения именно структурная обрезка весов обладает наибольшей технологической значимостью, поскольку обеспечивает более предсказуемое ускорение инференса и лучше согласуется с особенностями аппаратной реализации [2]. В простейшем случае оценка значимости параметра может быть выполнена на основе его абсолютного значения, однако в прикладных сценариях предпочтение обычно отдают критериям, учитывающим влияние параметра на функцию потерь и устойчивость модели к его исключению.

Изменению функции потерь при удалении веса можно оценить так:

$$\Delta L \approx \frac{\partial L}{\partial w_i} * w_i, \quad (1)$$

где ∂L означает функцию потерь, а w_i – конкретный весовой коэффициент. Данная оценка позволяет определить параметры, удаление которых оказывает минимальное воздействие на итоговое качество работы модели. В реальных задачах обрезка весов производится поэтапно. Сначала нейронная сеть обучается до достижения требуемых показателей точности, затем выявляются и исключаются наименее значимые веса, после чего модель дополнительно дообучается. При повторении этих шагов, удается уменьшить размер сети без существенного ухудшения результатов.

Для инфотелекоммуникационных систем подобный подход особенно актуален при использовании нейросетей на периферийных устройствах и в распределенных вычислительных средах. Уменьшение количества параметров снижает нагрузку на оперативную память и ресурсы процессора. Исследования по этой тематике демонстрируют, что оптимизированные модели способны выполнять вычисления локально, уменьшая объем передаваемых в облако данных и снижая нагрузку на сеть. Но чрезмерное

сокращение структуры сети может негативно сказаться на способности модели адаптироваться к изменяющимся входным данным [3].

Другим направлением структурной оптимизации является структурная дистилляция. Ее суть заключается в том, что компактная *student-модель* обучается на основе данных более сложной *teacher-модели*. В отличие от стандартного обучения, данный подход учитывает распределение вероятностей между всеми классами. Благодаря этому удается передать дополнительную информацию о связях между категориями данных. Наиболее эффективно дистилляция применяется в условиях, когда данные характеризуются шумом, неполнотой или слабой структурированностью. Идея такого подхода была предложена Джеффри Хинтоном [1, 4].

Чтобы получить от teacher-модели более информативный вывод, применяется функция softmax с температурным коэффициентом:

$$p_i = \frac{e^{\frac{z_i}{T}}}{\sum_j e^{\frac{z_i}{T}}}, \quad (2)$$

где z_i представляет логит соответствующего класса, а T определяет степень сглаживания распределения. При T > 1 распределение вероятностей становится более равномерным. Это позволяет *student-модели* получать информацию не только он наиболее вероятном классе, но и взаимном расположении остальных классов. Общая функция потерь при дистилляции обычно объединяет два компонента:

$$L = aL_{CE} + (1 - a)L_{KD}, \quad (3)$$

L_{CE} соответствует кросс-энтропии по истинным меткам, L_{KD} основана на сравнении выходных вероятностей *teacher* и *student-моделей, a* коэффициент a задает баланс между двумя составляющими. Такой способ обучения позволяет одновременно учитывать исходную разметку и скрытые зависимости, выявленные более сложной моделью [1].

Практическая ценность дистилляции заключается в возможности построения компактных нейросетей с относительно высоким качеством работы при меньшем числе параметров. Благодаря этому подобные модели могут применяться на маршрутизаторах, edge-узлах, IoT-оборудовании и других устройствах с ограниченными вычислительными ресурсами. Дополнительным преимуществом является снижение затрат на передачу и обновление моделей в распределенной сети, что особенно важно в сценариях массового внедрения интеллектуальных сервисов. Российская публикация

по структурной дистилляции также показывает, что сочетание дистилляции с генетическим поиском может использоваться для оптимизации архитектуры сетей на практике, в том числе на примере VGG16 и ResNet18 [3].

С точки зрения прикладных задач инфотелекоммуникаций обрезание весов и структурная дистилляция наиболее востребованы в системах мониторинга состояния сети, обнаружения аномалий, классификации трафика, прогнозирования нагрузки и адаптивного управления ресурсами. В этих сценариях компактные модели позволяют обеспечить требуемое быстродействие при ограниченных вычислительных возможностях. При этом обрезание и дистилляция могут использоваться как независимо, так и совместно, образуя гибридные схемы сжатия, в которых структурное упрощение модели сочетается с переносом знаний от более сложной архитектуры. Именно такой комбинированный подход рассматривается в современных исследованиях как одно из наиболее перспективных направлений оптимизации нейронных сетей.

Перспективным направлением дальнейших исследований является разработка адаптивных механизмов сжатия, способных учитывать текущую нагрузку, требования к качеству обслуживания и доступные вычислительные ресурсы. В подобных системах степень обрезания и параметры дистилляции могут изменяться динамически в зависимости от состояния сетевой среды. Это создает предпосылки для построения самоадаптирующихся интеллектуальных решений, ориентированных на эксплуатацию в распределенных и ресурсно-ограниченных инфраструктурах. Для телекоммуникационных приложений особенно важно, чтобы такие методы не только уменьшали модель, но и сохраняли стабильность качества при изменении характера трафика и нагрузки [1, 4].

Таким образом, обрезание весов и структурная дистилляция являются основными методами структурной оптимизации нейронных сетей, обеспечивающими снижение вычислительной сложности и повышение энергоэффективности при сохранении приемлемого уровня качества. Их применение особенно перспективно в задачах анализа трафика, мониторинга сети, обнаружения аномалий и интеллектуального управления ресурсами в инфотелекоммуникационных системах. Дальнейшее развитие данного направления связано с поиском оптимальных стратегий сжатия, разработкой гибридных схем оптимизации и созданием адаптивных моделей, способных функционировать в реальном времени. С учетом роста требований к автономности

сетевых устройств и к быстродействию интеллектуальных сервисов структурную оптимизацию нейросетей следует рассматривать как один из базовых инструментов практического внедрения искусственного интеллекта в инфотелекоммуникации.

Список используемых источников

1. Hinton G., Vinyals O., Dean J. Distilling the Knowledge in a Neural Network [Электронный ресурс]. URL: https://arxiv.org/abs/1503.02531 (дата обращения: 25.02.2026).

2. Han S., Mao H., Dally W. J. Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding [Электронный ресурс]. URL: https://arxiv.org/abs/1510.00149 (дата обращения: 05.03.2026).

3. Потанин В. Ю. Оптимизация структуры сетей глубокого обучения [Электронный ресурс]. URL: http://www.machinelearning.ru/wiki/images/a/ae/Potanin2019NNStructure.pdf (дата обращения: 23.03.2026).

4. Кузьмин В. Н., Менисов А. Б., Сабиров Т. Р. Метод оптимизации нейронных сетей на основе структурной дистилляции с применением генетического алгоритма // Научно-технический вестник ИТМО. 2024. № 6 (170). С. 770-775 [Электронный ресурс]. URL: https://ntv.ifmo.ru/ru/article/23086/ (дата обращения: 13.03.2026).

5. Потанин В. Ю. Оптимизация структуры сетей глубокого обучения [Электронный ресурс]. URL: http://www.machinelearning.ru/wiki/images/a/ae/Potanin2019NNStructure.pdf (дата обращения: 23.03.2026).

УДК 631.1.017

АНАЛИЗ ЭВОЛЮЦИИ ТЕХНОЛОГИЙ ПЕРЕДАЧИ ВИДЕО

А. И. Парамонов (д.т.н., профессор кафедры СС и ПД СПбГУТ)
Н. А. Штырляев (студент группы ИКВТ-21 СПбГУТ), shtyrliaev.na@sut.ru

В докладе рассматриваются цифровые технологии формирования видео. Сопоставлены способы построения цифрового и аналогового видео. Проводится анализ параметров, влияющих на объем видеофайлов. Сравниваются различные способы сжатия, основанные на пространственных и временных характеристиках кадров. Приводятся стандарты цифрового видео. Приводится оценка особенностей голографических технологий.

аналоговое видео, цифровое видео, технологии сжатия, кадры-фреймы, голограмма

Первый этап развития технологий видео контента начинался с аналогового видео.

В 1986 году компания Sony разработала первый цифровой формат SMPTE D1. В цифровом видеоизображение разбивается на отдельные кадры-фреймы, каждый из которых состоит из дискретных фрагментов – пикселей, организованных в прямоугольную матрицу определенного разрешения. Уже ранние цифровые форматы DV, Digital Betacam и MPEG-2, использовали сжатие для уменьшения объема данных.

Качество цифрового изображения определяется разрешением, частотой кадров и глубиной цвета. Цветное кодирование чаще всего основано на модели RGB, где каждый пиксель содержит информацию об интенсивности красного, зеленого и синего компонентов. Глубина цвета, измеряемая в битах на пиксель, определяет количество оттенков, которое можно увеличить, используя 10, 12 или более бит на пиксель.

В формате видео JPEG [2] используется пространственное сжатие, что позволяет уменьшить объем данных необходимых для одного кадра. В кодеках MPEG и H.26x используется временное сжатие, которое анализирует различия между соседними фреймами и передает только изменения между соседними фреймами. Развитие технологий построения кодеков позволяет выбрать уровень четкости от стандартной к сверхвысокой (таблица 1).

ТАБЛИЦА 1. Стандарты четкости цифрового видео

Формат	Разрешение	Количество пикселей
HD	1280 × 720	921 600
Full HD	1920 × 1080	2 073 600
Широкоэкранный 4K	4096 × 1716	7 020 544
Ultra HD 4K	3840 × 2160	8 294 400
Кашетированный 4K	3996 × 2160	8 631 360
DCI 4K	4096 × 2160	8 847 360
Академический 4K	3656 × 2664	9 739 584
Полнокадровый 4K	4096 × 3072	12 582 912

В общем случае объем данных, который необходим для сохранения видео, можно оценить по формуле:

$$V_{\text{видео}} = V_{\text{фрейм}} * V_{\text{к/с}} * T_{\text{видео}},$$

где $V_{\text{видео}}$ – объем видео данных, $V_{\text{фрейм}}$ – объем одного файла, $V_{\text{кс}}$ – частота кадров (fps), $T_{\text{видео}}$ – длительность видео в секундах.

Для часового фильма в формате с высокой четкости требуются терабайты памяти.

Увеличение разрешения в четыре раза, например, переход от Full HD к 4K [1], заметно повышает детализацию картинки, но также в четыре раза увеличивает объем данных перед сжатием, поэтому инженеры разрабатывают новые технологии сжатия в видео, таких как, H.264, HEVC, VVC, которые позволяют уменьшить размер файла в сотни и тысячи раз без видимой потери качества за счет сложных математических алгоритмов.

Это означает, что исходный гигабитный поток можно сократить до мегабитных скоростей, доступных для домашних интернет-соединений. Например, для комфортного просмотра в разрешении 4K, достаточно канала со скоростью 30 Мбит/с, а для Full HD достаточно уже 8 Мбит/с, для HD – хватит 5 Мбит/с, для SD – всего 2 Мбит/с.

Для создания и вещания контента рекомендуются более высокие битрейты: для видео 720p при 60 к/с – 2,9-7,4 Мбит/с, для 1080p при 30 к/с – 3,8-7,4 Мбит/с, а для 1080p при 60 к/с – уже 5,6-11 Мбит/с. Пиксели современных дисплеев основаны на различных технологиях:

- жидкокристаллические (LCD) с светодиодной подсветкой;
- органические светодиоды (OLED), где каждый субпиксель светится самостоятельно, что обеспечивает идеальный черный цвет и высокую контрастность;
- перспективные микро-светодиоды (MicroLED), способные обеспечить еще большую яркость, долговечность и энергоэффективность.

Эти технологические изменения позволили улучшить четкость, расширить цветовой охват, увеличить яркость и, в результате, создать более реалистичное изображение. Однако даже самый совершенный плоский экран способен передать лишь двумерную проекцию мира. Очередным этапом развития стало создание объемного и иммерсивного видео, цель которого – создать иллюзию глубины.

Наиболее распространенным сегодня остается стереоскопическое 3D-видео, требующее специальных очков. Оно создает иллюзию объема, показывая каждому глазу немного разные изображения, имитируя бинокулярное зрение. Технологии очков эволюционировали от простых анаглифных (с сине-красными фильтрами), серьезно искажающих цвет, к более совершенным поляризационным и активным затворным, которые поочередно затемняют линзы в такт смене кадров. Для передачи такого видео в реальном времени требуются примерно вдвое большие скорости, чем для 2D: например, стереопара 4K 60 fps после сжатия требует 50-100 Мбит/с.

Попытки обойтись без очков привели к созданию автостереоскопических дисплеев с барьерами или линзовыми растрами, но они имеют крайне ограниченные углы обзора. Очередным этапом развития является голография, которая может использоваться для видеоконференцсвязи, чтобы повысить реалистичность изображения. Согласно рекомендации МСЭ, голографическая коммуникация будет в интерактивном режиме доставлять цифровые 3D-изображения от одного или нескольких источников к одному или нескольким целевым узлам.

Список используемых источников

1. Что такое разрешение видео 4K, HD, Full HD, UHD? Текст: электронный // movavika.ru: [сайт]. URL: https://www.movavika.ru/learning-portal/4k-resolution-video.html?ysclid=ml3xk9fi45508464022 (дата обращения: 01.02.2026).

2. JPEG/JPG. Текст: электронный // contented.ru: [сайт]. URL: https://media.contented.ru/glossary/jpeg-jpg/ (дата обращения: 01.02.2026).

3. ITU-T Recommendations by series: Y.3000-series: Representative use cases and key network requirements for Network 2030 (Y Suppl. 67 (07/2020). Текст: 145 электронный // ITU: [сайт]. 2020. URL: https://handle.itu.int/11.1002/1000/14386 (дата обращения: 01.02.2026).

УДК 004.852

ПРОГНОЗИРОВАНИЕ ИНТЕРНЕТ-ТРАФИКА МЕТОДАМИ ЛИНЕЙНОЙ РЕГРЕССИИ

Т. В. Печайкин (студент группы ИКВТ-21 СПбГУТ), pechaikin.tv@sut.ru

Прогнозирование объема сетевого трафика является важной задачей для обеспечения качества обслуживания, планирования пропускной способности и автоматического масштабирования инфраструктуры. В работе рассматривается применение метода множественной линейной регрессии для прогнозирования часовых объемов трафика на основе временных факторов и автокорреляции. Предложенная модель учитывает час суток, день недели, признак выходного дня, а также значение трафика за предыдущие 24 часа. Эксперименты на 168 наблюдениях (7 суток) показали, что на тестовой выборке коэффициент детерминации R^2 составляет 0,81, а среднеквадратичная ошибка – 18,7 Мбит/с. Полученные коэффициенты позволяют интерпретировать влияние временных закономерностей и инерционности трафика.

линейная регрессия, прогнозирование трафика, метод наименьших квадратов, временные ряды, автокорреляция

Современные телекоммуникационные сети характеризуются высокой динамикой нагрузки. Согласно данным Cisco, глобальный интернет-трафик ежегодно растет на 20–30 %, что требует внедрения методов упреждающего управления ресурсами [1]. Недостаточная точность прогнозирования приводит к перегрузке сетевых узлов (снижение QoS) либо к неэффективному использованию пропускной способности (избыточное резервирование).

В работе предлагается использовать **множественную линейную регрессию** для прогнозирования часового объема трафика y_t (Мбит/с) на основе временных факторов и автокорреляции:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_2 + \beta_4 x_4,$$

где x_1 – час суток (0…23);

x_2 – день недели (0 – понедельник, …, 6 – воскресенье);

x_3 – признак выходного дня (1 – выходной, 0 – будний);

x_4 – значение трафика 24 часа назад (лаг).

Для оценки коэффициентов β используется метод наименьших квадратов (МНК), который в матричной форме записывается как:

$$\beta = (X^T X)^{-1} X^T y,$$

где X – матрица признаков с добавленным столбцом единиц, y – вектор наблюдаемого трафика [2]. Данная формула является аналитическим решением задачи минимизации суммы квадратов отклонений.

Временной ряд формировался из 168 наблюдений (7 суток × 24 часа) с шагом 1 час. Первые 5 строк исходных данных приведены в табл. 1.

ТАБЛИЦА 1. Фрагмент исходных данных

Час	День недели	Выходной	Лаг, Мбит/с	Трафик, Мбит/с
0	0	0	52	48
1	0	0	48	45
2	0	0	45	42
3	0	0	42	40
4	0	0	40	38

Обучение модели выполнено в среде Mathcad 15. Полученные коэффициенты представлены в табл. 2.

ТАБЛИЦА 2. Коэффициенты линейной регрессии

Коэффициент	Значение	Интерпретация
β0	48,2	Базовый уровень трафика (ночные часы)
β1	3,25	Скорость изменения трафика в течение суток
β2	5,48	Влияние дня недели (рост к концу недели)
β3	–8,12	Коррекция трафика в выходные дни
β4	0,918	Коэффициент автокорреляции (инерционность)

Положительный знак β_1 отражает увеличение нагрузки в дневные и вечерние часы, что соответствует реальной сетевой активности. Коэффициент β_4 близок к единице, что указывает на высокую степень зависимости текущего трафика от трафика в предыдущие сутки – характерное свойство сетевых процессов.

На рис. 1 показано сравнение фактического трафика y и предсказанного $y\hat{}$для всего периода наблюдений.

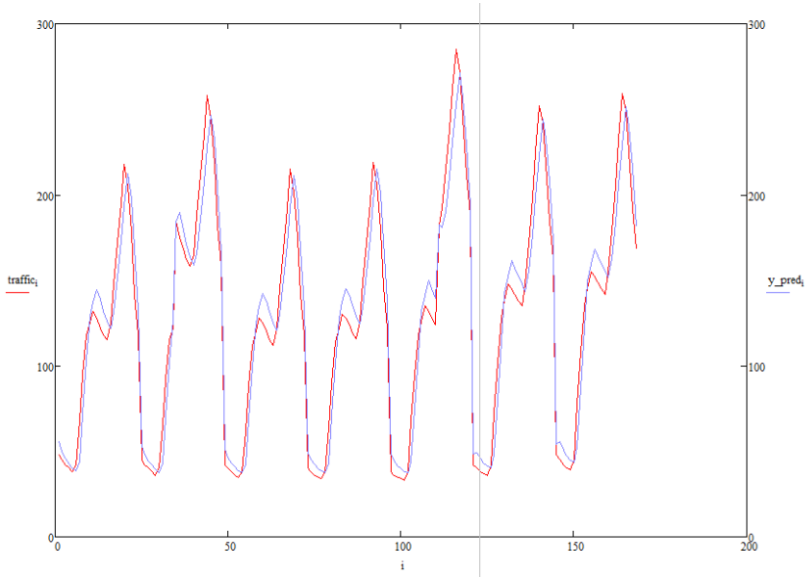


Рис. 1. Фактический и предсказанный трафик за 168 часов

Качество модели оценивалось с помощью коэффициента детерминации R^2 и среднеквадратичной ошибки RMSE:

Для предложенной модели получены следующие значения:

1. $R^2 = 0{,}81$ (модель объясняет 81 % вариации трафика);

2. RMSE = 18,7 Мбит/с (средняя ошибка прогноза).

Полученные результаты подтверждают применимость линейной регрессии для задач прогнозирования сетевого трафика при наличии ограниченного объема данных (168 наблюдений). Интерпретируемость коэффициентов позволяет использовать модель не только для предсказания нагрузки, но и для анализа суточных и недельных закономерностей, а также для выявления аномалий (например, DDoS-атак) на основе отклонения реального трафика от прогноза [3].

Дальнейшее развитие модели может включать учет праздничных дней, сезонных колебаний, а также использование нелинейных методов (XGBoost, LightGBM) при увеличении объема исторических данных [4; 5].

Список используемых источников

1. ГОСТ Р 59895-2021 Технологии искусственного интеллекта в образовании. Общие положения и терминология. М.: Росстандарт, 2021.

2. Пантюхин О. И. Основы научных исследований и проведения экспериментов: учебное пособие / Пантюхин О. И., Михайличенко А. В., Рябов Г. А., Солодухин Б. В.; СПбГУТ. Санкт-Петербург, 2024. 185 с.

3. Чаругин В. В., Чесалин А. Н.. Анализ и формирование набора данных сетевого трафика для обнаружения компьютерных атак. International Journal of Open Information Technologies, ISSN: 2307-8162. Vol. 11. № 6. 2023.

4. Хайндман Р. Дж., Атаназопулос Г. Прогнозирование: принципы и практика: пер. с англ. М.: ДМК Пресс, 2020. 482 с.

5. Дрейпер Н., Смит Г. Прикладной регрессионный анализ: пер. с англ. М.: Вильямс, 2016. 912 с.

Статья представлена научным руководителем, доктором технических наук, профессором О. И. Пантюхиным.

УДК 654.739

МЕТОДИКА ПЛАНИРОВАНИЯ СИСТЕМ МОБИЛЬНОЙ СВЯЗИ

Ю. В. Пимахина (студент группы ИКТ-2521 СПбГУТ), pimaxina.uv@sut.ru

Актуальность эффективного планирования сетей мобильной связи обусловлена развитием городской застройки и увеличением плотности абонентов. Качественное проектирование сети требует применения расчетных моделей и программных средств, учитывающих как рельеф местности, так и сложную архитектуру современных жилых комплексов. В работе рассматривается методика планирования сетей мобильной связи для условий городской застройки с применением программной среды MATLAB, позволяющей выполнять расчет радиопокрытия, моделирование распространения радиоволн и анализ показателей качества радиоканала.

мобильная связь, базовая станция, планирование сетей, MATLAB, трассировка лучей, модель Лонгли-Райса, SINR

Актуальность эффективного планирования сетей обусловлена стремительным ростом плотности абонентов в условиях современной городской застройки. Для обеспечения качественного покрытия необходимо учитывать рельеф местности, особенности застройки и условия распространения радиоволн. В данной работе рассматривается методика проектирования сети мобильной связи. Практический расчет параметров и цифровое моделирование производятся для территории поселка Шушары с учетом плотности абонентов и архитектуры жилых комплексов. Методика исследования включает несколько этапов [1].

Анализ и выбор среды моделирования

На начальном этапе исследования был проведен анализ существующих систем автоматизированного проектирования радиосетей (САПР). Рассматривались такие программные комплексы как RadioPlanner 3.0 и ONEPLAN RPLS-DB. Данные программы являются мощными коммерческими инструментами: RadioPlanner специализируется на планировании зон покрытия сетей 5G, LTE и WiMAX, а ONEPLAN предоставляет комплексное управление топологией.

Для реализации авторского алгоритма планирования и глубокого анализа данных была выбрана программная платформа MATLAB. В отличие от

узкоспециализированных САПР, MATLAB предоставляет широкие возможности для математического моделирования, разработки собственных алгоритмов трассировки лучей и гибкой настройки параметров распространения радиоволн [2].

Математический расчет

Математическая составляющая методики базируется на определении радиуса покрытия через потери на трассе и расчете необходимого количества базовых станций (БС) по абонентской емкости. [3] При расчете мощности (уровня) полезного сигнала на приемной стороне учитываются следующие параметры: выходная мощность передатчика P_{tx}, потери в антенных фидерах передатчика и приемника η_{tx}, η_{rx}, коэффициенты усиления антенн G_{tx}, G_{rx}, а также результирующее ослабление сигнала на трассе A_0. Рассчитать итоговый уровень сигнала на приеме можно по формуле (1):

$$P_{rx} = P_{tx} - \eta_{tx} + G_{tx} - A_0 - \eta_{rx} + G_{rx}, \quad (1)$$

Для определения результирующего ослабления A_0 по модели Лонгли-Райса учитываются ослабление свободного пространства A_{fs}, потери за счет дифракции и рассеяния A_{ref}, а также изменчивость условий распространения A_{var}. Расчет производится по формуле (2):

$$A_0 = A_{fs} + A_{ref} + A_{var}, \quad (2)$$

Чтобы определить необходимое число базовых станций N_{eNB}, используются данные о потенциальном количестве абонентов $N_{\text{АБ}}$ и пропускной способности (емкости) одной станции $N_{\text{АБ}.eNB}$. Данное значение может быть рассчитано по данной формуле (3):

$$N_{eNB} = \frac{N_{\text{АБ}}}{N_{\text{АБ}}.eNB}. \quad (3)$$

Для исследуемого района (пос. Шушары) был проведен детальный анализ исходных данных. Исходя из численности населения, потенциальное количество активных абонентов $N_{АБ}$ было определено как 20 % от общего числа жителей, что составило 13 400 человек. При моделировании физического уровня были рассчитаны целевые значения: мощность сигнала на границе соты -11 дБм и допустимые потери на трассе 69 дБ. На основе этих параметров и расчетной емкости одной станции стандарта LTE было определено, что для обеспечения стабильного покрытия и обслуживания всего

абонентского трафика в данной локации требуется установка 10 базовых станций.

Цифровое моделирование, трассировка и анализ SINR

Переход к топологии сети осуществляется через 3D-моделирование. Для минимизации «мертвых зон» и оценки качества сигнала в условиях плотной застройки применяется метод трассировки лучей (Ray Tracing) и анализ отношения сигнал/помеха-плюс-шум (SINR). Применение такого подхода позволяет визуализировать конкретные пути распространения радиоволн, включая отражения от зданий. Анализ SINR является критическим этапом: в условиях расстановки 10 БС на ограниченной территории необходимо минимизировать взаимное влияние станций для обеспечения высокой пропускной способности.

Фрагмент MATLAB-программы, используемый для проверки прямой видимости и трассировки сигнала, представлен в листинге 1.

Листинг 1. Фрагмент MALAB-программы трассировки сигнала

```
 % Координаты приемников
LatRX = [59.805212, 59.80471];
LonRX = [30.376073, 30.375158];

 % Создание площадки приемника с корректным именем
rx = rxsite(«Name», 'Receiver_Site', ...
'Latitude', LatRX, 'Longitude', LonRX);

show(rx);
los(tx, rx); % Проверка прямой видимости

 % Настройка модели распространения Longley-Rice
rx = rxsite(«Latitude», 59.805212, «Longitude», 30.376073);
show(rx);

pm = propagationModel(«longley-rice», ...
«AntennaPolarization», «vertical», ...
«AtmosphericRefractivity», 301);

 % Анализ трассировки лучей (Path Loss)
raytrace(tx, rx, «Type», «pathloss»);
```

Фрагмент программы, предназначенный для задания параметров базовой станции и расчета SINR, представлен в листинге 2.

Листинг 1. Код MALAB программы анализа отношения сигнал/шум

```
 % Параметры передатчика
txPowerDBm = 20;
txPower = 10.^((txPowerDBm – 30)/10); % Конвертация из дБм в Ватты
Loss = 3;
f0 = 1800e6; % Частота 1.8 ГГц
txheight = 15;

 % Координаты БС
LatTX = 59.805021;
LonTX = 30.3738;

 % Создание базовой станции
tx = txsite(«Name», 'BS_Shushary', ...
 'Latitude', LatTX, 'Longitude', LonTX, ...
 'AntennaHeight', txheight, ...
 'TransmitterFrequency', f0, ...
 'TransmitterPower', txPower, ...
 'SystemLoss', Loss);

show(tx);

 % Анализ SINR по модели Longley-Rice
sinr(tx, «longley-rice»);
```

Результатом применения, разработанной методики стало моделирование карты радио-покрытия. Код программы моделирования представлен в листинге 3.

Листинг 3. Код MALAB программы моделирования зоны покрытия

```
 % Инициализация модели распространения
pm = propagationModel(«longley-rice»);

 % Определение параметров площадки для расчета покрытия
tx = txsite(«Name», 'Shushary_Sector', ...
 «Latitude», LatTX, ...
 «Longitude», LonTX, ...
 «TransmitterFrequency», f0);

 % Генерация карты покрытия с заданными уровнями сигнала
coverage(tx, pm, «SignalStrengths», -100:5);
```

Полученное распределение покрытия для рассматриваемой территории приведено на рис. 1.



Рис. 1. Рассчитанная карта покрытия для поселка Шушары

Разработанная методика, сочетающая аналитический расчет и программное моделирование в MATLAB, позволяет с высокой точностью проектировать сети в сложных условиях. Совместное использование трассировки лучей и анализа SINR обеспечивает достаточную точность планирования и стабильность сигнала на планируемой территории.

Список используемых источников

1. Рыжков А. Е. [и др.] Сети стандарта LTE. Развитие технологий радиодоступа: монография. СПб.: СПбГУТ, 2015. 254 с.

2. Лазарев Ю. Ф. Начала программирования в среде MATLAB. К.: НТУУ «КПИ», 2003. 424 с.

3. Герасименко А. А., Киреев А. В., Романов Д. В. Расчет ослабления сигнала сетей сотовой связи 5G для частот диапазона FR1 // Инновации и инвестиции. 2021. № 6. С. 180–183. URL: https://cyberleninka.ru/article/n/raschet-oslableniya-signala-setey-sotovoy-svyazi-5g-dlya-chastot-diapazona-fr1 (дата обращения: 24.03.2026).

Статья представлена научным руководителем, доцентом кафедры ОКСС СПбГУТ, кандидатом технических наук А. С. Дюбовым.

УДК 654.197.6

ОБЕСПЕЧЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ УДАЛЕННОГО УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМ И ТЕЛЕВИЗИОННЫМ ОБОРУДОВАНИЕМ С ИСПОЛЬЗОВАНИЕМ SSH

С. А. Платонов (студент группы РЦТ-21 СПбГУТ), platonov.sa@sut.ru

Современные системы цифрового телевизионного вещания представляют собой распределенные телекоммуникационные комплексы, требующие постоянного мониторинга и управления. В условиях, когда объекты географически удалены друг от друга особую актуальность приобретает безопасное и отказоустойчивое удаленное администрирование оборудования. В статье рассматриваются особенности применения протокола Secure Shell для управления оборудованием систем цифрового телевизионного вещания.

цифровое телевидение, ЦТВ, удаленное управление, SSH, отказоустойчивость, телекоммуникационное оборудование, информационная безопасность

Системы цифрового телевизионного вещания представляют собой комплекс аппаратных и программных средств, предназначенных для формирования, обработки, передачи и распространения телевизионного сигнала в цифровом формате. В отличие от аналогового телевидения, цифровые системы обеспечивают более высокое качество изображения и звука.

Типовая архитектура системы ЦТВ (рис. 1) включает следующие элементы [1]:

- головную станцию вещания;
- кодеры и мультиплексоры;
- системы условного доступа;
- модуляторы и передающие станции;
- транспортную сеть;
- системы мониторинга и управления.

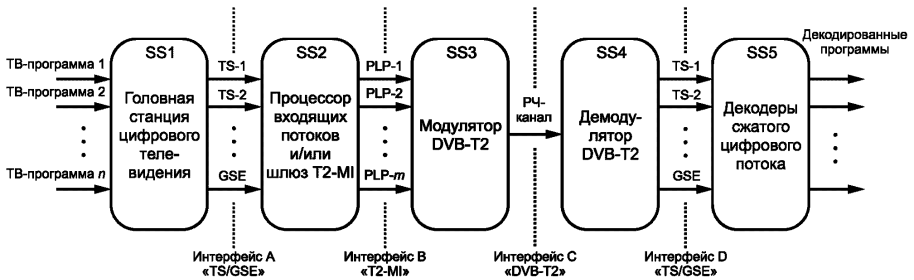


Рис. 1. Типовая архитектура системы ЦТВ

Головная станция осуществляет прием исходного медиаконтента, его кодирование и формирование транспортных потоков. Далее сигнал передается по телекоммуникационной сети на передающие узлы, где выполняется модуляция и трансляция в эфир или кабельную сеть. Системы ЦТВ часто имеют территориально распределенную структуру, включающую множество удаленных объектов. Поэтому управление оборудованием в большей степени осуществляется дистанционно.

Для удаленного администрирования традиционно применяются различные сетевые протоколы, такие как SNMP, HTTP и Telnet. Однако многие из них имеют различные недостатки с точки зрения информационной безопасности, поскольку не обеспечивают достаточного уровня шифрования и аутентификации.

Для управления наиболее важными компонентами инфраструктуры ЦТВ предпочтительно применять защищенные протоколы удаленного доступа.

Secure Shell (SSH) – это криптографический сетевой протокол, предназначенный для безопасного удаленного доступа к компьютерным системам (рис. 2). Протокол был разработан как замена небезопасному Telnet и в настоящее время является стандартным инструментом администрирования сетевых устройств и серверов [2].

Основные функции SSH: шифрование всего трафика; аутентификация пользователей; обеспечение целостности соединения; туннелирование сетевых данных.

Благодаря этому, все передаваемые данные, включая команды и учетные данные пользователей, защищены от перехвата, поэтом протокол SSH является наиболее оптимальным инструментом для удаленного управления телекоммуникационным оборудованием.

Многие производители телекоммуникационного оборудования включают SSH-сервер в стандартную прошивку устройств. Однако типовые настройки SSH зачастую ориентированы на простоту использования, а не на безопасность и отказоустойчивость.

К типичным настройкам относятся:

- использование стандартного порта 22;
- аутентификация по паролю;
- отсутствие ограничений на количество подключений;
- отсутствие механизмов резервирования.

Такая конфигурация может создавать потенциальные угрозы безопасности [2].

Поэтому стандартные настройки SSH требуют дополнительной оптимизации для использования в инфраструктуре цифрового телевидения.

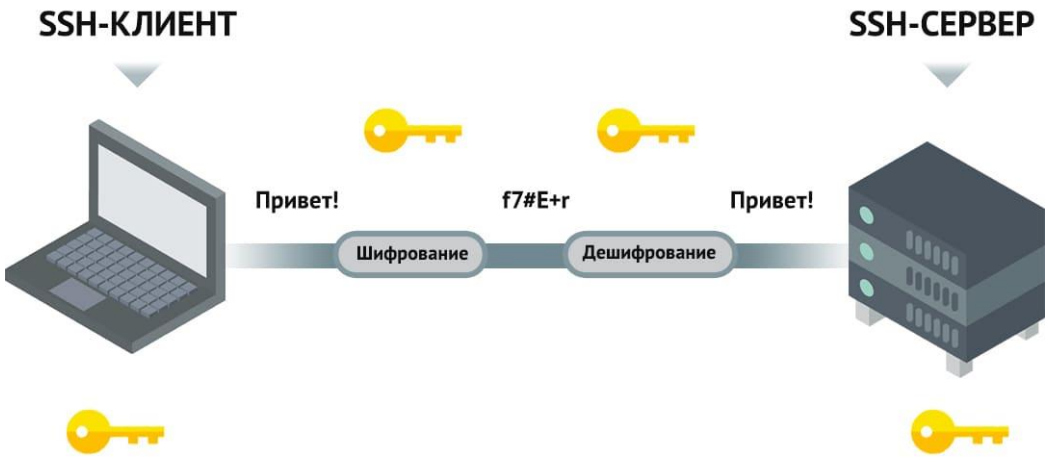


Рис. 2. Схема резервирования SSH-доступа

Повышение надежности удаленного управления может быть достигнуто за счет комплексного подхода, включающего сетевые, программные и архитектурные решения.

Проведем настройку протокола SSH для обеспечения удаленного безопасного доступа:

- Изменим стандартный SSH-порт 22 на пользовательский 2222 (рис. 3) [2, 3]:

```
### Изменяем стандартный порт 22 на пользовательский (2222) ###
Port 2222
```

Рис. 3. Изменение порта

- Используем аутентификацию по ключам (рис. 4, рис. 5) [3]:

```
### Используем аутентификацию по ключам ###
PubkeyAuthentication yes
```

Рис. 4. Аутентификация по ключу

```
### Запрещаем парольную аутентификацию ###
PasswordAuthentication no
```

Рис. 5. Запрет на аутентификацию по паролю

- Ограничиваем список пользователей (рис. 6) [4]:

```
### Разрешаем только ограниченным пользователям использовать ssh-подключение
AllowUsers client
```

Рис. 6. Ограничение списка пользователей

● Включаем механизм контроля соединений, чтобы разрывать соединения с клиентами, которые держат соединение, но не выполняют работу (рис. 7) [4, 5]:

```
### Включаем контроль активности соединения ###
### Каждые 60 секунд будет отсылаться пакет проверки активности
### У ssh-клиента будет возможность ответить на такой пакет 5 раз
### Если ssh-клиент не активен более 5 минут, то соединение разрывается
ClientAliveInterval 60
ClientAliveCountMax 5
```

Рис. 7. Механизм контроля соединения

Таким образом, удаленное управление телекоммуникационным оборудованием является важнейшим элементом эксплуатации систем цифрового телевизионного вещания. Надежность и безопасность таких систем напрямую влияют на устойчивость телевизионного вещания и качество обслуживания абонентов.

Использование протокола SSH позволяет обеспечить защищенный доступ к оборудованию и снизить риски несанкционированного вмешательства.

Предложенные решения позволяет значительно повысить устойчивость инфраструктуры цифрового телевизионного вещания и сократить время восстановления управления при аварийных ситуациях.

Список используемых источников

1. ГОСТ Р 58912-2020 Телевидение вещательное цифровое. Система эфирного наземного цифрового телевизионного вещания второго поколения DVB-T2. Общие технические требования. 2021. https://allgosts.ru/33/170/gost_r_58912-2020 (дата обращения: 10.03.2026).

2. Ylonen T. The Secure Shell (SSH) Protocol Architecture: RFC 4251 / T. Ylonen, C. Lonvick. 2006. 40 p. https://datatracker.ietf.org/doc/rfc4251/ (дата обращения: 10.03.2026).

3. Ylonen T. The Secure Shell (SSH) Authentication Protocol: RFC 4252 / T. Ylonen, C. Lonvick. 2006. 16 p. https://datatracker.ietf.org/doc/rfc4252/ (дата обращения: 10.03.2026).

4. Ylonen T. The Secure Shell (SSH) Transport Layer Protocol: RFC 4253 / T. Ylonen, C. Lonvick. 2006. 40 p. https://datatracker.ietf.org/doc/rfc4253/ (дата обращения: 10.03.2026).

5. Ylonen T. The Secure Shell (SSH) Connection Protocol: RFC 4254 / T. Ylonen, C. Lonvick. 2006. 28 p. https://datatracker.ietf.org/doc/rfc4254/ (дата обращения: 10.03.2026).

Статья представлена научным руководителем, старшим преподавателем СПбГУТ С. П. Куликовым.

УДК 621.3

АНАЛИТИЧЕСКИЙ ОБЗОР СТЕКА ПРОТОКОЛОВ УРОВНЯ L2 РАДИОИНТЕРФЕЙСА СЕТЕЙ LTE

Б. В. Помиранский (студент группы ИКТК-22 СПбГУТ),
pomiranskii.bv@sut.ru
А. А. Савельева (ст. преп. каф. ИКСС СПбГУТ)

В статье рассматриваются функции и взаимодействие подуровней канального уровня радиоинтерфейса LTE. Показано, что качество передачи пользовательского и сигнального трафика в сети LTE определяется не только характеристиками физического уровня, но и согласованной работой механизмов сжатия заголовков, сегментации, повторной передачи и распределения радиоресурсов на канальном уровне. Проанализирована роль каждого подуровня в обеспечении адаптации трафика к изменяющимся условиям радиоканала, а также в достижении допустимого баланса между задержкой, надежностью передачи и использованием радиоресурсов.

LTE, радиоинтерфейсы, канальный уровень, PDCP, RLC, MAC

Актуальность исследования обусловлена тем, что качество передачи данных в сети LTE определяется не только характеристиками физического уровня, но и согласованной работой подуровней канального уровня, обеспечивающих адаптацию трафика к условиям радиоканала [1-3]. В этой связи анализ функций данных подуровней представляет интерес как с точки зрения архитектуры LTE, так и с позиции понимания механизмов передачи данных в современных системах подвижной связи. Цель работы состоит в анализе функционального взаимодействия указанных подуровней и выявлении их вклада в обеспечение устойчивой и качественной передачи пользовательского и сигнального трафика.

Общая характеристика канального уровня радиоинтерфейса LTE

Радиоинтерфейс Uu в сети LTE обеспечивает взаимодействие между пользовательским оборудованием и базовой станцией eNodeB. Передача данных по радиоинтерфейсу реализуется на основе многоуровневой протокольной архитектуры, в которой важную роль играет канальный уровень L2 [2, 3]. Именно на этом уровне выполняются функции, обеспечивающие согласование требований приложений с переменными характеристиками радиоканала, включая обработку пакетов, управление их последовательностью, повторные передачи и распределение ресурсов [1-3].

Канальный уровень L2 в сети LTE включает три функционально взаимосвязанных подуровня:

- Packet Data Convergence Protocol (PDCP),
- Radio Link Control (RLC)
- Medium Access Control (MAC).

Каждый из них решает собственный круг задач, однако только их совместная работа обеспечивает адаптацию пользовательского и сигнального трафика к условиям радиоканала [1-3]. Поэтому рассмотрение подуровней L2 целесообразно не только как описание архитектуры LTE, но и как анализ механизмов, влияющих на параметры передачи данных в сети радиодоступа.

Функции подуровня PDCP

Подуровень Packet Data Convergence Protocol (PDCP) занимает верхнее положение в стеке L2 радиоинтерфейса LTE и обеспечивает обработку данных на границе между верхними уровнями и радиоинтерфейсом [4]. К его основным функциям относятся сжатие заголовков, шифрование, контроль целостности для сигнального трафика, а также нумерация пакетов, необходимая для переупорядочивания, обнаружения потерь и обработки дубликатов. Сжатие заголовков, в частности с использованием механизма Robust Header Compression (ROHC), позволяет уменьшить объем служебной информации, что особенно важно при передаче трафика с небольшой полезной нагрузкой [4-6].

С точки зрения задержки влияние PDCP носит преимущественно косвенный характер. С одной стороны, выполнение операций сжатия заголовков, шифрования и переупорядочивания требует дополнительной обработки пакетов. С другой стороны, сокращение объема служебной информации способствует более рациональному использованию ресурсов радиоинтерфейса и в ряде случаев уменьшает суммарное время передачи данных [1, 4-6]. Следовательно, PDCP не является основным подуровнем управления задержкой, однако влияет на нее через предварительную обработку потока данных.

Функции подуровня RLC

Подуровень Radio Link Control (RLC) обеспечивает адаптацию данных к условиям передачи на радиоинтерфейсе [7]. На передающей стороне он выполняет сегментацию или объединение блоков данных, поступающих от

PDCP, в соответствии с объемом ресурса, выделенного нижележащими механизмами. На приемной стороне RLC обеспечивает восстановление последовательности блоков и, при необходимости, повторную передачу данных. Тем самым данный подуровень задает способ передачи в зависимости от требований конкретного типа трафика [1, 7].

В LTE подуровень RLC функционирует в трех режимах: Transparent Mode (TM), Unacknowledged Mode (UM) и Acknowledged Mode (AM). Режим TM применяется в наиболее простых сценариях, где не требуется обработка заголовков и подтверждение доставки. Режим UM ориентирован на трафик, чувствительный к задержке, для которого допустимы отдельные потери пакетов, но важно минимизировать время доставки [1, 7]. Режим AM используется в случаях, когда требуется более высокая надежность передачи, поскольку в нем реализуется механизм автоматического запроса повторной передачи (ARQ).

В режиме AM приемная сторона формирует сообщения о состоянии приема, содержащие информацию о корректно доставленных и недостающих блоках данных, что позволяет передающей стороне повторно отправлять только те PDU, которые не были успешно приняты. При необходимости повторной передачи ранее сформированный PDU может быть переразбит на части, если на уровне MAC для повторной отправки выделен меньший ресурс, чем при исходной передаче. Такая схема делает RLC важным элементом обеспечения надежности передачи именно на участке радиодоступа.

С точки зрения задержки именно RLC в значительной степени определяет компромисс между быстротой и надежностью доставки. Использование режима UM позволяет избежать дополнительных временных затрат, связанных с подтверждением приема и повторной передачей, тогда как применение режима AM повышает надежность, но сопровождается увеличением задержки за счет ожидания подтверждений и выполнения повторных передач. Таким образом, влияние RLC на задержку является прямым и определяется выбранным режимом работы.

Функции подуровня MAC

Подуровень Medium Access Control (MAC) располагается между RLC и физическим уровнем и отвечает за оперативное управление доступом к радиоресурсам [8]. Функции MAC включают мультиплексирование и де-

мультиплексирование данных, приоритезацию логических каналов, реализацию механизма гибридного автоматического запроса повторной передачи HARQ, а также отображение логических каналов на транспортные. Благодаря этому MAC обеспечивает быструю реакцию на ошибки передачи, перераспределение ресурсов и согласование параметров передачи с текущим состоянием радиоканала [1, 8].

Механизм HARQ обеспечивает быструю коррекцию ошибок на радиоинтерфейсе за счет повторных передач транспортных блоков, обработки ACK/NACK и комбинирования нескольких копий принятого сигнала. В отличие от него, механизм ARQ на уровне RLC реализует более полный контроль доставки данных на участке радиодоступа [7]. При невозможности успешного декодирования средствами HARQ дальнейшее восстановление передачи обеспечивается на уровне RLC, что формирует иерархическую модель обеспечения надежности [7, 8].

Еще одной важной задачей MAC является приоритезация трафика [8]. В LTE радиоресурсы ограничены, поэтому система должна учитывать различия между потоками данных по требованиям к задержке, пропускной способности и надежности. Приоритезация реализуется как между различными пользовательскими устройствами, так и между логическими каналами одного устройства. За счет этого MAC участвует в поддержании качества обслуживания и в динамической адаптации передачи в зависимости от условий радиоканала.

С точки зрения задержки подуровень MAC играет наиболее оперативную роль. Именно на этом уровне принимаются решения о распределении ресурсов, очередности обслуживания трафика и выполнении быстрых повторных передач. Поэтому MAC непосредственно влияет на время ожидания передачи и общую задержку радиоинтерфейса.

Сценарный анализ роли подуровней

Рассмотренные функции PDCP, RLC и MAC позволяют перейти от описания отдельных подуровней к анализу их вклада в обслуживание различных типов трафика. Значимость указанных механизмов определяется не одинаково во всех случаях, а зависит от требований конкретного сервиса к задержке, надежности передачи и использованию радиоресурсов [4-6].

Для голосового трафика приоритетным параметром является минимальная задержка передачи. В таких условиях особое значение приобретают механизмы распределения радиоресурсов на уровне MAC, а также режимы

работы RLC, не связанные с дополнительными задержками из-за подтверждения доставки и повторной передачи. Роль PDCP в данном случае определяется обработкой пакетов и сокращением объема служебной информации.

Для видеотрафика характерен компромисс между задержкой передачи и устойчивостью доставки. В связи с этим на первый план выходит согласованная работа RLC и MAC: RLC обеспечивает адаптацию структуры передачи, а MAC – быстрое реагирование на изменение состояния радиоканала. PDCP дополнительно способствует снижению служебной нагрузки при передаче потоковых данных.

При передаче файлового трафика и других видов данных, критичных к полноте доставки, основное значение приобретает надежность передачи. В таких сценариях возрастает роль RLC, прежде всего в режиме AM, где реализуются механизмы повторной передачи утраченных блоков данных. MAC обеспечивает быстрое исправление ошибок на нижнем уровне, а PDCP – упорядочивание и обработку потока данных [4, 7, 8].

Заключение

Проведенный анализ показывает, что подуровни PDCP, RLC и MAC образуют согласованную систему адаптации трафика к условиям радиоканала LTE. Их вклад в обеспечение передачи данных определяется требованиями конкретного типа трафика: для сервисов реального времени на первый план выходит минимизация задержки и распределение ресурсов, тогда как для трафика, критичного к потерям, возрастает значение механизмов подтверждения и повторной передачи. При этом влияние подуровней на задержку различается: PDCP воздействует на нее косвенно, RLC определяет соотношение между задержкой и надежностью, а MAC обеспечивает наиболее быстрое управление передачей на радиоинтерфейсе. Следовательно, стек протоколов уровня L2 следует рассматривать не как совокупность изолированных функций, а как систему взаимодополняющих механизмов, обеспечивающих баланс между задержкой, надежностью передачи и использованием радиоресурсов.

Список используемых источников

1. Гельгор А. Л., Попов Е. А. Технология LTE мобильной передачи данных: учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2011. 204 с.

2. Sesia, S., Toufik I., Baker M. LTE – The UMTS Long Term Evolution: From Theory to Practice, 2011. 794 с. ISBN: 978-0-470-66025-6.

3. 3GPP TS 36.300. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Overall description. Stage 2, 2017. 195 с.

4. 3GPP TS 36.323. Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification, 2018. 39 с.

5. Bormann, C., Burmeister, C., Degermark, M., RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed. RFC 3095, 2001. 168 с.

6. Sandlund, K., Pelletier, G., Jonsson L-E., The RObust Header Compression (ROHC) Framework. RFC 5795, 2010. 41 с.

7. 3GPP TS 36.322. Evolved Universal Terrestrial Radio Access (E-UTRA). Radio Link Control (RLC) protocol specification, 2019. 39 с.

8. 3GPP TS 36.321. Evolved Universal Terrestrial Radio Access (E-UTRA). Medium Access Control (MAC) protocol specification, 2016. 93 с.

УДК 621.396.9

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ КООРДИНАЦИИ МЕЖСОТОВОЙ ИНТЕРФЕРЕНЦИИ В СЕТЯХ LTE

Б. В. Помиранский (студент группы ИКТК-22 СПбГУТ),
pomiranskii.bv@sut.ru

В статье рассматриваются методы координации межсотовой интерференции в сетях LTE. Показано влияние интерференции на пропускную способность абонентов на границе сот и спектральную эффективность сети. Проанализированы методы ICIC такие как HFR, FFR, SFR и eICIC, основанные на временной координации. Рассмотрен компромисс между снижением интерференции и эффективностью использования радиоресурсов.

LTE, ICIC, SINR, спектральная эффективность

Актуальность исследования обусловлена тем, что в сетях LTE с коэффициентом повторного использования частот равным 1 и ограниченным числом несущих базовые станции работают в общем частотном ресурсе, что приводит к межсотовой интерференции. Наиболее критично она проявляется для абонентов на границах сот, где уровни сигналов от обслуживающей и соседних базовых станций становятся сопоставимыми, что приводит к снижению SINR и, как следствие, пропускной способности и качества обслуживания.

Цель работы – провести сравнительный анализ основных методов координации межсотовой интерференции (ICIC и eICIC).

В LTE зависимость между MCS и SINR является ключевой для адаптивной модуляции и кодирования [1]. Она определяет, какой уровень модуляции и скорость кодирования можно использовать для данного канала, чтобы обеспечить приемлемый уровень ошибки. Методы ICIC позволяют повысить качество сигнала LTE на границах сот. Распределение радиоресурсов в сетях LTE осуществляется планировщиком базовой станции на уровне ресурсных блоков (PRB) во временно-частотной области.

Методы ICIC накладывают ограничения на использование этих ресурсов в частотной, временной и мощностной областях, тем самым определяя доступный набор PRB для планирования [2].

Методы координации интерференции (ICIC)

Hard frequency reuse (рис. 1) – общий частотный ресурс разделяется на несколько непересекающихся поддиапазонов, каждый из которых закрепляется за отдельной сотой (или группой сот) таким образом, чтобы соседние соты не использовали один и тот же частотный ресурс [2]. Данный подход значительно снижает межсотовую интерференцию, особенно на границах сот. Однако при увеличении коэффициента повторного использования наблюдается пропорциональное снижение спектральной эффективности сети.

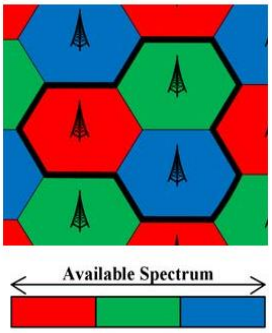


Рис. 1. Механизм HFR

Fractional frequency reuse (рис. 2) предусматривает разделение частотного ресурса на общую часть для центральных абонентов и выделенные поддиапазоны без переиспользования в соседних сотах для абонентов на границе сот, что позволяет снизить межсотовую интерференцию [2, 3].

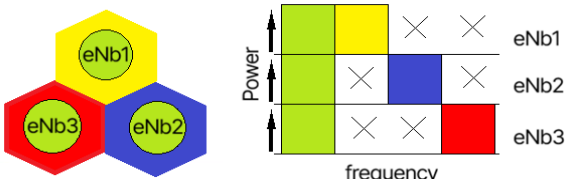


Рис. 2. Механизм FFR

Soft frequency reuse (рис. 3) позволяет использовать весть частотный ресурс во всех сотах, однако его использование предполагается с различными уровнями мощности. Для абонентов на границе сот выделяются определенные поддиапазоны с повышенной мощностью передачи, при этом в соседних сотах эти же поддиапазоны используются с пониженной мощностью для абонентов внутри соты. Такой подход позволяет снизить интерференцию на границах сот при сохранении общей емкости мобильной сети.

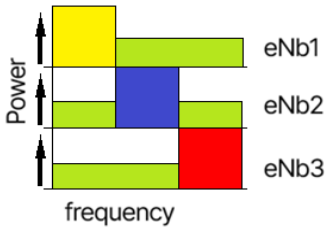


Рис. 3. Механизм SFR

Расширенные методы (eICIC)

В сетях LTE расширенные методы координации интерференции (eICIC), введенные начиная с Release 10, предназначены для снижения межсотовой интерференции в неоднородных сетях (HetNet), включающих макро-, микро- и фемто- соты [4]. В таких сценариях абоненты малых сот могут испытывать сильную интерференцию со стороны макросот с более высокой мощностью передачи. Важно уточнить, что качество радиоканала

в восходящем направлении не обязательно будет лучше, так как мощность антенн в абонентских устройствах существенно ниже [5, 6].

В отличие от классических методов ICIC, реализующих координацию в частотной и мощностной областях, eICIC дополнительно использует временную координацию. Основным механизмом eICIC являются Almost Blank Subframes (ABS) – подкадры, в которых интерферирующая макросота существенно ограничивает передачу пользовательских данных, при этом сохраняются необходимые опорные и служебные сигналы для обеспечения мобильности и обратной совместимости с абонентскими устройствами (рис. 4).

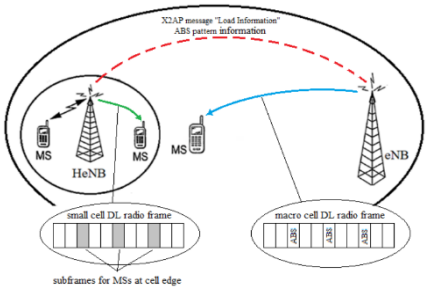


Рис. 4. Метод eICIC

Сравнительный анализ

Рассмотренные методы показывают различные подходы к решению проблемы межсотовой интерференции.

Метод Hard Frequency Reuse обеспечивает существенное снижение интерференции по причине строгого распределения частот между сотами [2]. Поэтому основным преимуществом HFR является простота реализации и нацеленность метода именно на решение проблемы, связанной с интерференцией. Однако, меньшее число ресурсных блоков влечет снижение максимальной, средней скорости передачи данных на одного абонента, а также абонентской емкости одной соты.

FFR расширяет число доступных поднесущих по сравнению с HFR за счет использования части спектра с переиспользованием во всех сотах. При этом центральные абоненты используют только общую часть спектра, а граничные – выделенные поддиапазоны без переиспользования. Несмотря на то, что в данном методе также задаются ограничения только по частотному ресурсу, при планировании сети требуется учитывать потенциальную абонентскую плотность на разном расстоянии от базовой станции. Если удаленным абонентам будет выделен ресурс, превосходящий их потребности, то ресурса может не хватить ближним абонентам. Даже при отсутствии нагрузки в граничных зонах, соответствующие им частоты не используются центральными абонентами.

В отличие от FFR, механизм SFR предполагает использование всего частотного ресурса [3]. Таким образом, базовая станция управляет всеми ре-

сурсными блоками. Управление мощностью передачи позволяет ограничивать дальность обслуживания, тем самым снижая интерференцию на границе соты. При таком подходе в случае низкой абонентской нагрузки (например, ночью) абоненту может быть предоставлен весь потенциал ширины полосы несущей, что гарантирует высокие скорости передачи данных.

Помимо статических схем, в LTE применяются и более гибкие механизмы координации, включая обмен информацией по интерфейсу X2, при котором базовые станции обмениваются информацией о загрузке и уровне интерференции, что позволяет учитывать использование PRB в соседних сотах при планировании и повышает эффективность распределения радиоресурсов по сравнению со статическими схемами.

eICIC позволяет сохранить коэффициент повторного использования сети, пользователям могут выделяться различные части спектра. Механизм ABS ограничивает передачу пользовательских данных от макросоты в различные временные интервалы в зависимости от текущей нагрузки на разных уровнях сети и удаленности абонентского терминала от базовой станции. Метод, изначально разработанный для гетерогенных сетей, лучше остальных подходит для использования в городах, где выше плотность застройки и размещения базовых станций. Использование ABS обеспечивает лучшие условия радиоканала в случаях, когда макросеть по уровням превосходит микросоты.

Заключение

Рассмотренные методы координации интерференции различаются по балансу между снижением помех и эффективностью использования радиоресурсов. Статические схемы ICIC обеспечивают предсказуемое управление интерференцией, но требуют тщательного планирования и ограничивают спектральную эффективность. Более гибкие подходы, включая SFR, динамическую координацию по X2 и eICIC, позволяют адаптироваться к текущей нагрузке и особенно эффективны в гетерогенных сетях.

Список используемых источников

1. Ахметбек А. К. LTE услуги для повышения безопасности в транспортных сетях: дис. м. телеком. сис. наук: 6M071900. Алмата, 2016. 74 с.

2. 4G/LTE – Interference // sharetechnote URL: https://sharetechnote.com/html/Handbook_LTE_ICIC.html (дата обращения: 06.04.2026).

3. Sesia, S., Toufik I., Baker M. LTE – The UMTS Long Term Evolution: From Theory to Practice, 2011. 794 с. ISBN 978-0-470-66025-6.

4. eICIC: Enhanced inter-cell interference coordination in 3GPP Release-10 // blog.3g4g.co.uk URL: https://blog.3g4g.co.uk/2011/01/eicic-enhanced-inter-cell-interference.html (дата обращения: 06.04.2026).

5. Аксенов В. А. Гетерогенные радиосети мобильного и фиксированного доступа: учеб.-метод. пособие. Минск: БГУИР, 2023. 62 с.: ил. ISBN 978-985-543-695-0

6. Комысов П. В., Надымов А. В. Исследование интерференции в гетерогенных сетях стандарта LTE-A // Известия ЮФУ. Технические науки. 2018. № 1 (195). С. 220-227.

Статья представлена научным руководителем, старшим преподавателем кафедры ИКС СПбГУТ А. А. Савельевой.

УДК 621.396

АНАЛИЗ ВОЗМОЖНОСТЕЙ СРЕДЫ MATLAB ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ КАНАЛА СПУТНИКОВОЙ СВЯЗИ С МОРСКИМИ СУДАМИ

М. С. Рогова (студент группы МБК-2581 СПбГУТ), rogova.ms@sut.ru
А. М. Синильников (к.т.н., главный инженер научно-технического центра спутниковых систем связи, радиомониторинга и вещания ФГАУ НИЦ телеком им. М. И. Кривошеева), sinilam01@gmail.com

Спутниковая связь с морскими судами широко применяется благодаря возможности обеспечения высокоскоростной передачи данных в любых районах морей и океанов. Существенное влияние на качество связи оказывает качка судна, приводящая к отклонению антенны от направления на спутник и соответственно изменению уровней мощности сигнала. Предлагается анализ возможностей среды MatLab для построения модели канала спутниковой связи с морскими судами в условиях качки.

спутниковая связь, качка судна, канал спутниковой связи, MatLab

Спутниковая связь (СС) является единственным видом высокоскоростной цифровой связи с морскими судами. Современное научно-техническое развитие привело к созданию спутниковых бортовых ретрансляционных комплексов (БРТК) высокой пропускной способности (High Throughput Satellite – HTC) и наземных терминалов с антеннами малой апертуры (Very Small Aperture Terminal – VSAT), что позволило существенно расширить область применения СС в целом и в гражданском морском флоте. Наиболее широко для связи с морскими судами используются спутники на геостационарной орбите (ГСО), обладающие очень широкой зоной охвата морских и океанских территорий.

Особенность СС с морскими судами заключается в необходимости непрерывной коррекции направления оптической оси антенной системы корабельного терминала на спутник связи, даже если он находится на ГСО. Наиболее существенными причинами коррекции является качка судна, а также изменение его курса. Указанные факторы приводят к отклонению диаграммы направленности антенны от направления на спутник, что вызывает изменение уровней принимаемого и передаваемого сигналов особенно в активно осваиваемом в настоящее время диапазоне миллиметровых волн.

Целью настоящей работы является анализ возможностей среды MatLab для построения модели канала СС с морскими судами.

Выделим основные компоненты канала СС.

1. Судовой абонентский терминал, состоящий из антенной системы со следящим приводом, обеспечивающим наведение антенны на спутник в условиях качки и изменения курса судна, малошумящий усилитель-конвертер, усилитель мощности, спутниковый модем и оборудование распределения данных. Абонентский терминал осуществляет формирование передаваемого сигнала, включая его кодирование и модуляцию, а также прием демодуляцию и декодирования входящего сигнала.

2. БРТК без демодуляции и декодирования сигналов, осуществляющий прием и усилений сигналов морских судов в восходящих лучах антенной системы, преобразование несущих частот сигналов с коммутацией по нисходящим лучам, усиление мощности и передачу сигналов в нисходящих лучах.

3. Центральная земная станция, осуществляющая формирование передаваемых сигналов, включая кодирование и модуляцию, прием демодуляцию и декодирования входящих сигналов, а также взаимодействие абонентских терминалов через спутниковый сегмент с наземной сетью связи, управление доступом к спутниковому ресурсу, синхронизацию работы терминалов и маршрутизацию передаваемых данных в наземные сети связи.

Подвижность абонентского терминала приводит к изменению параметров канала во времени, что необходимо учитывать при его дальнейшем анализе и построении математической модели.

Рассмотрим наиболее распространенный вариант сети спутниковой связи с топологией «звезда» с использованием спутника связи на ГСО и прозрачного (без обработки сигналов) спутникового БРТК, работающего в строго линейном режиме.

Для такого ретранслятора мощность W_{ER} принимаемого сигнала пропорциональна мощности W_{ET} передаваемого сигнала

$$W_{ER} = W_{ET} G. \quad (1)$$

При отсутствии качки коэффициент G передачи мощности очень медленно меняется во времени и определяется выражением [1]

$$G = \frac{G_{AET} G_{ASR} G_S G_{AST} G_{AER}}{L_{ES} L_{SE}}, \quad (2)$$

где L_{ES} и L_{SE} – коэффициенты потерь мощности сигнала на линии земля-БРТК и на линии БРТК-земля;

G_{AET} и G_{AST} – коэффициенты усиления передающих антенн земных станций и БРТК;

G_{AER} и G_{ASR} – коэффициенты усиления приемных антенн земных станций и БРТК;

G_S – коэффициент усиления транспондера БРТК.

Мощность шума АТ в полосе принимаемого сигнала

$$W_{EN} = W_{NER} + W_{NSR}\,\frac{G_S G_{AST} G_{AER}}{L_{SE}}, \qquad (3)$$

где $W_{NER} = kT_{ER}F_S$ – мощность шума антенны и приемного тракта АТ в полосе сигнала F_S;

$W_{NSR} = kT_{SR}F_S$ – мощность шума антенны и приемного тракта БРТК в полосе сигнала F_S.

Коэффициенты усиления передающей и приемной антенн судового терминала ощутимо зависят от качки судна и при отклонении максимума диаграммы направленности на угол φ от направления на спутник определяются выражением [1]:

$$G_A(\varphi) = G_A(0)J_1(u)/u, \qquad (4)$$

где $u = (\pi D_A/\lambda)\sin\varphi$;

$J_1(u)$ – функция Бесселя первого рода от действительного аргумента u;

D_A – диаметр антенны;

λ – длина волны.

Из выражения (3) видно, что коэффициент усиления $G_A(\varphi)$ существенно зависит от длины волны, особенно в Ka диапазоне частот.

При качке угол φ меняется во времени, что соответственно приводит к изменению во времени коэффициента усиления приемной и передающей антенн корабельного терминала и соответственно общего коэффициента передачи мощности спутниковой линии связи. Скорость изменения коэффициента усиления $G_A(\varphi)$ существенно выше скорости изменений других коэффициентов в выражении (2). Следует отметить, что в соответствии с выражением (4) изменение во времени коэффициента усиления приемной антенны корабельного терминала приводит не только к изменению мощности принимаемого сигнала, но и к изменению мощности шума.

Таким образом, зависимость отношения мощности сигнала к мощности шума при спутниковой связи с морскими судами имеет сложный вид

и для ее исследования необходимо моделирование. В связи с этим целесообразно использовать имитационную модель канала спутниковой связи.

Для моделирования изменения коэффициентов усиления передающей и приемной антенн корабельного терминала в условиях качки судна могут быть использованы специализированные библиотеки среды MatLab [2], предназначенные для анализа антенных систем и пространственно-временных процессов. Моделирование направленных свойств антенны и их зависимости от углового положения осуществляется с использованием пакета Antenna Toolbox. В рамках данного пакета антенна может быть представлена в виде параметрической модели, после чего с помощью функции pattern определяется пространственное распределение коэффициента усиления [3].

Результатом работы функции pattern является зависимость коэффициента усиления антенны от угловых координат (азимут и угол места), что позволяет получить численные значения усиления при отклонении антенны от направления на спутник.

Для анализа изменения усиления в одной плоскости можно использовать функцию patternAzimuth, которая определяет зависимость усиления от азимута при фиксированном угле места, а также функцию patternElevation, которая определяет зависимость усиления от угла места при фиксированном азимуте. Результатом применения указанных функций являются массивы значений коэффициента усиления, соответствующие различным углам отклонения антенны, а также графические диаграммы направленности.

Динамическое изменение ориентации антенны во времени, обусловленное качкой судна, может быть смоделировано с использованием пакета Phased Array System Toolbox [4]. В этом случае антенная система рассматривается, как пространственно ориентируемый объект. Объект phased.Platform позволяет задать движение и ориентацию антенны во времени, включая угловые отклонения, соответствующие качке судна. Объекты phased.Radiator и phased.Collector [5] используются для моделирования процессов излучения и приема сигнала с учетом текущего направления антенны.

Таким образом, результатом моделирования являются зависимости коэффициентов усиления передающей и приемной антенн от углового отклонения, временные зависимости коэффициентов усиления, обусловленные качкой судна, диаграммы направленности антенны, позволяющие оценить чувствительность системы к отклонению от направления на спутник.

Список используемых источников

1. Сомов А. М., Корнев С. Ф. Спутниковые системы связи: учебное пособие для вузов. М.: Горячая линия-Телеком, 2012. 244 с.

2. MathWorks. Antenna Toolbox Documentation (Электронный ресурс) // MathWorks. URL: https://www.mathworks.com/help/antenna/ (дата обращения: 31.03.2026).

3. MathWorks. Field Analysis – Radiation Pattern (Электронный ресурс) // MathWorks. URL: https://www.mathworks.com/help/antenna/ug/field-analysis.html (дата обращения: 31.03.2026).

4. MathWorks. Phased Array System Toolbox – MATLAB (Электронный ресурс) // MathWorks. URL: https://www.mathworks.com/products/phased.html (дата обращения: 31.03.2026).

5. MathWorks. Phased Array System Toolbox Documentation. Objects: phased.Platform, phased.Radiator, phased.Collector (Электронный ресурс) // MathWorks. URL: https://www.mathworks.com/help/phased/ (дата обращения: 31.03.2026).

УДК 621.396.73

РАЗРАБОТКА УСТРОЙСТВА ПЕРЕДАЧИ ТЕКСТОВЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ LORA

А. И. Рыбаков (ст. преподаватель, кафедра БТС СПбГУТ), lexeus.r11@gmail.com
Н. С. Соколов (студент группы ИКТР-11 СПбГУТ), sokolov1.ns@sut.ru

В статье рассматривается описание проекта по разработке устройства передачи текстовых сообщений с использованием технологии LoRa для сложных условий применения при отсутствии телекоммуникационной инфраструктуры. Предложена архитектура устройства с использованием микроконтроллера, LoRa-приемопередатчика и комбинированной системы отображения (OLED и E-Ink), обеспечивающая низкое энергопотребление и удобство взаимодействия.

LoRa, приемопередатчик, E-Ink, OLED

В современных условиях связь является неотъемлемой частью повседневной жизни человека. Она используется как для передачи критически важных сообщений (например, сигналов бедствия), так и для повседневного общения между пользователями.

Несмотря на активное развитие технологий беспроводной передачи данных, значительная часть населения в Российской Федерации по-прежнему ограничена в доступе к услугам сотовой связи. Основной причиной данного явления является высокая стоимость и сложность инфраструктуры, необходимой для функционирования современных систем связи.

Широко используемые современные стандарты связи, такие как GSM, 3G и LTE, реализуют топологию «точка–многоточка», предполагающую использование базовых станций и множества абонентских устройств. Несмотря на высокую пропускную способность таких систем, их эффективная работа требует значительной плотности размещения инфраструктуры. Так, по состоянию на 2025 год на территории Российской Федерации эксплуатируется около 950 тысяч базовых станций. Однако, даже при таком количестве в удаленных и малонаселенных регионах связь либо отсутствует, либо ее качество может быть неудовлетворительным.

Дополнительным фактором для рассмотрения актуальности описанной выше проблемы является рост стоимости услуг связи, который оказывает наибольшее влияние на социально уязвимые категории населения, включая

лиц с низким уровнем дохода и пенсионеров. Динамика изменения стоимости тарифов по годам представлена на рис. 1.



Рис. 1. Абонентская плата за пакет услуг сотовой связи по месяцам

Необходимо учитывать энергопотребление традиционных средств связи – большинство современных устройств требует регулярной подзарядки и способно функционировать автономно лишь в течение нескольких суток. В условиях нестабильного энергоснабжения это может привести к полной потере возможности коммуникации.

Одним из альтернативных решений актуальной проблемы является применение радиостанции (рации), обеспечивающей голосовую связь на значительные расстояния без необходимости использовать дорогостоящую мобильную инфраструктуру. При этом такие устройства характеризуются сравнительно высокой автономностью, но ограниченным радиусом действия. Радиостанции обладают рядом существенных ограничений. Передача информации осуществляется исключительно в голосовой форме и в реальном времени, что приводит к потере сообщения в случае отсутствия получателя в момент передачи. Таким образом, для обеспечения надежной связи требуется постоянное присутствие пользователя у устройства.

Кроме того, недорогие модели радиостанций работают лишь в нелицензируемых диапазонах частот, что может приводить к возникновению помех и пересечению с другими каналами связи. Указанные особенности ограничивают их применение в задачах, требующих надежной и фиксируемой передачи информации. Таким образом, можно сделать вывод о недостаточ-

ности доступных массовых решений, обеспечивающих автономную, энергоэффективную и надежную связь для передачи, в том числе текстовой информации, без использования инфраструктуры.

В качестве решения рассматриваемой проблематики предлагается разработка устройства передачи текстовых сообщений на основе технологии LoRa (полн. Long Range). Данная технология обеспечивает передачу данных на значительные расстояния при крайне низком энергопотреблении, что делает ее перспективной для применения в автономных устройствах связи. Однако ключевым ограничением LoRa является низкая скорость передачи данных, составляющая в среднем порядка 1 кбит/с [1, 2, 3].

Сформированы требования по проекту разработки устройства передачи текстовых сообщений на основе технологии LoRa, а именно:

- обеспечение связи на больших расстояниях в условиях отсутствия инфраструктуры;
- высокая автономность устройства;
- возможность хранения переданных сообщений;
- низкая стоимость и отсутствие регулярных эксплуатационных затрат.

Структурная схема разрабатываемого устройства представлена на рис. 2.

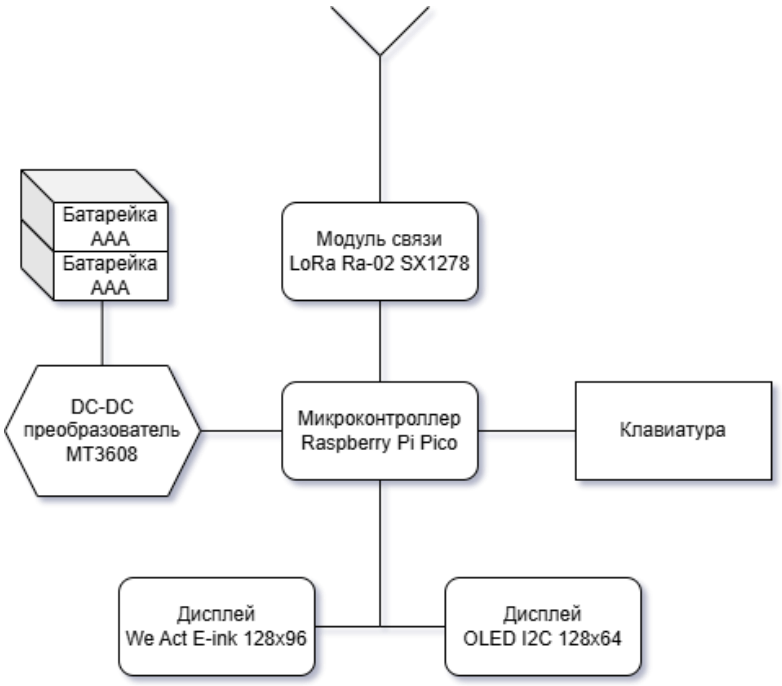


Рис. 2. Структурная схема разработанного устройства

Технология LoRa представляется оптимальным выбором для реализации подобной системы. В качестве радиомодуля был выбран приемопередатчик Ra-02 на базе чипа SX1278 [4, 5], обеспечивающий необходимый баланс между стоимостью и функциональностью.

В качестве управляющего элемента используется микроконтроллер Raspberry Pi Pico, обладающий достаточной вычислительной мощностью, объемом памяти и набором периферийных интерфейсов, включая несколько шин SPI и I2C. Использование нескольких интерфейсов является важным, поскольку LoRa-модуль взаимодействует с микроконтроллером по шине SPI.

Особенностью разработанного устройства является использование двух типов дисплеев: OLED и E-Ink. Применение E-Ink дисплея обусловлено его высокой энергоэффективностью – потребление энергии происходит только в момент обновления изображения, тогда как в остальное время информация сохраняется без затрат энергии. Это позволяет значительно увеличить время автономной работы устройства.

E-Ink дисплеи характеризуются низкой скоростью обновления, что затрудняет их использование для ввода информации. В связи с этим дополнительно используется OLED-дисплей, обеспечивающий быстрый отклик при наборе текста. Таким образом, предложенная комбинация дисплеев позволяет одновременно обеспечить низкое энергопотребление и удобство пользовательского взаимодействия.

В качестве источника питания выбраны гальванические элементы типа AAA, отличающиеся доступностью и низкой стоимостью. Для компенсации снижения напряжения при разряде батарей используется повышающий DC-DC преобразователь MT3608, обеспечивающий стабильное питание устройства.

Клавиатура реализована на основе тактовых кнопок, что позволило снизить стоимость устройства и обеспечить гибкость конструкции.

Корпус устройства изготовлен с использованием технологии 3D-печати из PLA-пластика, что позволило адаптировать конструкцию под требования проекта и сократить затраты на производство.

Внешний вид разработанных прототипов устройств представлен на рис. 3.



Рис. 3. Прототипы устройств передачи текстовых сообщений

Разработанные устройства протестированы и могут обеспечить двустороннюю передачу текстовых сообщений. Ввод осуществляется с помощью клавиатуры, включающей шесть буквенных и три функциональные кнопки. Набираемый текст отображается на OLED-дисплее, а принятые и отправленные сообщения на E-Ink дисплее.

Предусмотрена возможность подключения внешней антенны с разъемом SMA, что позволяет варьировать характеристики связи в зависимости от условий эксплуатации.

Разработанные устройства могут быть использованы для организации связи в удаленных регионах Крайнего Севера, где отсутствует развитая телекоммуникационная инфраструктура. Предложенное решение обеспечит передачу сообщений на значительные расстояния, оно характеризуется высокой автономностью и низкой себестоимостью, что делает его перспективным для использования в качестве альтернативного приемопередатчика.

Список используемых источников

1. Adelantado F., Vilajosana X., Tuset-Peiró P., Martinez B., Melia-Segui J., Watteyne T. Understanding the Limits of LoRaWAN // IEEE Communications Magazine. 2017. Vol. 55. Iss. 9. PP. 34–40. DOI: 10.1109/MCOM.2017.1600613.

2. Centenaro M., Vangelista L., Zanella A., Zorzi M. Long-Range Communications in Unlicensed Bands: The Rising Stars in the IoT and Smart City Scenarios // IEEE Wireless Communications. 2016. Vol. 23. Iss. 5. PP. 60–67. DOI: 10.1109/MWC.2016.7721743.

3. LoRa Alliance. LoRaWAN Specification v1.0.4. Fremont, CA: LoRa Alliance, 2020. 128 p.

4. Semtech Corporation. SX1276/77/78/79 – LoRa Modem Designer’s Guide. 2013. 132 p.

5. Buyya R., Dastjerdi A. V. Internet of Things: Principles and Paradigms. Amsterdam: Elsevier, 2016. 378 p. ISBN 978-0-12-805395-9.

Статья представлена научным руководителем, профессором кафедры ПМ СПбГУТ, доктором технических наук, профессором П. К. Смирновым.

УДК 654.739

WI-FI 6/6E/7 ДЛЯ ЗАДАЧ УМНОГО ГОРОДА

А. В. Слесенко (студент группы ИКТК-21 СПбГУТ), slesenko.av@sut.ru

В статье рассмотрены возможности применения Wi-Fi 6, Wi-Fi 6E и Wi-Fi 7 в инфраструктуре умного города. Актуальность исследования обусловлена ростом числа подключаемых устройств и повышением требований к качеству беспроводной связи в городской среде. Предложен сценарный подход к оценке применимости Wi-Fi нового поколения для общественного транспорта, систем видеонаблюдения и экологического мониторинга. Показано, что Wi-Fi 6 является наиболее сбалансированным решением для массового внедрения, а Wi-Fi 7 целесообразен для наиболее нагруженных участков инфраструктуры.

Wi-Fi 6, Wi-Fi 6E, Wi-Fi 7, IEEE 802.11, умный город, общественный транспорт

Развитие инфраструктуры умного города связано с ростом числа цифровых сервисов, подключаемых устройств и распределенных систем мониторинга. К ним относятся общественный транспорт, городское видеонаблюдение, экологический мониторинг и информационные сервисы для населения. Их функционирование требует надежной беспроводной инфраструктуры, обеспечивающей устойчивое соединение, достаточную пропускную способность, низкие задержки и поддержку большого числа устройств. Wi-Fi представляет собой семейство технологий беспроводных локальных сетей, основанных на стандартах IEEE 802.11 [1]. Переход от Wi-Fi 5 к Wi-Fi 6, Wi-Fi 6E и Wi-Fi 7 направлен на повышение эффективности использования радиочастотного спектра, увеличение скорости передачи данных и улучшение работы сетей в условиях высокой плотности подключений. Для городской среды данные характеристики имеют особое значение, поскольку беспроводные сети используются не только для доступа пользователей в Интернет, но и для работы транспортных, сенсорных и сервисных систем. При этом внедрение новых поколений Wi-Fi должно учитывать стоимость оборудования, необходимость модернизации сопутствующей инфраструктуры, условия радио среды и требования конкретного сценария применения.

Целью статьи является сравнительная оценка применимости Wi-Fi 6, Wi-Fi 6E и Wi-Fi 7 для отдельных сценариев умного города. В качестве основного сценария рассматривается общественный транспорт; дополнительно проводится сопоставление с системами видеонаблюдения и экологического мониторинга.

Методика сравнительной оценки

Для оценки применимости Wi-Fi 6/6E/7 в инфраструктуре умного города используется сценарный подход, который предполагает сопоставление требований конкретного городского сервиса с техническими возможностями современных стандартов Wi-Fi. В качестве критериев сравнения выбраны: плотность подключаемых устройств, требуемая пропускная способность, чувствительность к задержке, устойчивость соединения, энергоэффективность и сложность внедрения.

Выбор данных критериев обусловлен тем, что различные сценарии умного города предъявляют неодинаковые требования к беспроводной сети. Например, для общественного транспорта критична работа в условиях высокой плотности пользователей, для видеонаблюдения (стабильная передача видеопотоков, а для экологического мониторинга) поддержка большого числа маломощных IoT-устройств.

ТАБЛИЦА 1. Сравнение современных стандартов Wi-Fi

Параметр	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7
Год выхода	2013	2019	2021	2024
Стандарт IEEE	802.11ac	802.11ax	802.11ax	802.11be
Теоретическая максимальная скорость (Гбит/с)	до 3,5	до 9,6	до 9,6	до 46
Диапазоны (ГГц)	5	2.4, 5	2.4, 5, 6	2.4, 5, 6
Ширина каналов (МГц)	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160	до 320
Модуляция	256-QAM OFDM	1024-QAM OFDMA	1024-QAM OFDMA	4096-QAM OFDMA
MIMO	4×4 DL MIMO	8×8 UL/DL MU-MIMO	8×8 UL/DL MU-MIMO	16×16 UL/DL MU-MIMO
MAC (Multi-Link Operation)	-	-	-	MLO

Технологические особенности Wi-Fi 6/6E/7

В настоящее время значительная часть беспроводных сетей доступа построена на основе Wi-Fi 5. Однако рост числа подключаемых устройств и увеличение нагрузки на беспроводную инфраструктуру делают актуальным переход к более современным стандартам.

Wi-Fi 6, основанный на IEEE 802.11ax, включает ряд технологических улучшений по сравнению с предыдущими поколениями. Одно из технологических улучшений является технология OFDMA “Orthogonal Frequency Division Multiple Access”, позволяющая с помощью разделения канала дает передавать информацию одновременно на несколько устройств. Вторая технология, улучшенная в новых поколениях Wi-Fi, является улучшенная технология MU-MIMO “multiple input, multiple output”, которая дает обслуживать сразу несколько устройств, что снижает время ожидания, работая и на прием, и на передачу данных [2]. Так же усовершенствована модуляция до 1024-QAM, что дает передавать еще больше информации в одном пакете [3].

Стандарт Wi-Fi 6e, не имеет критических отличий от Wi-Fi категории 6, но улучшает его функции за счет нового диапазона частот, а именно 6 ГГц, что улучшает скорость, позволяет использовать более широкие каналы, значительно улучшая работу сети и производительность, особенно при высокой плотности подключений [4].

Стандарт Wi-Fi 7, имеет название IEEE 802.11be, появившийся в 2022 году, является последнем стандартом на данный момент. Данный стандарт сочетает в себе особенности Wi-Fi 6 и Wi-Fi 6E, при этом имея нововведения, такие как, например, объединение диапазонов. Данная технология называется MLO “Multi-Link Operation”, позволяющая различным устройствам, имеющим поддержку данного стандарта, использовать сразу несколько частотных диапазонов бесшовно, то есть без видимого переключения [5]. Подобная технология значительно увеличивает пропускную способность, способствует снижению задержек. Само внедрение стандарта требует больших вложений, так как оборудование, поддерживающее новый стандарт, значительно дороже остального оборудования.

Рассмотрим внедрение новых стандартов Wi-Fi в общественный транспорт, таких как автобусы и метрополитен. В общественном транспорте неравномерный и большой поток людей проходит каждый день, также в каждом автобусе для безопасности установлены камеры и всем посетителям метрополитена или наземного транспорта, выделанная сеть Wi-Fi. Данные

факторы, такие как большой потом устройств, создают большую нагрузку на устройства, выделяющие общественную сеть Wi-Fi, особенно в час пик. Стандарт для данных сетей используется Wi-Fi 4 или 5 в зависимости от новизны автобуса или вагонов метро. Внедрение новых стандартов, к примеру, Wi-Fi 6 за счет технологий, рассмотренных ранее, таких как OFDMA и MU-MIMO, снизят задержки при большом количестве пользователей, так как ресурсы будут распределяться более качественнее, следовательно, и снижение задержки для пользователей. Технология Wi-Fi 7 более подходит для внедрения за счет технологии MLO, ведь технология позволяет уменьшить количество точек доступа при этом с улучшением связи в близи к точке доступа, где скорость максимальная, и имеет более плотную модуляцию. Массовое внедрение упирается в стоимость точек доступа для большой инфраструктуры, так же к пользователям, у которых на устройствах должна быть поддержка новой технологии, технология MLO дает улучшенную и высокую скорость, но для практического применения Wi-Fi 6 подходит лучше для массовой замены и модернизации сети, а стандарт Wi-Fi 7 можно оставить на теоретическое будущее, когда стоимость станет более приемлемой для массовой замены городской инфраструктуры.

Рассмотрим оценку применимости стандартов Wi-Fi в городской среде (рис 1.), в частности, общественного транспорта, самый используемый стандарт, именно стандарт Wi-Fi 5, имеет множество недочетов, таких как рост задержек с большим количеством пользователей, потерей связи, снижением скорости передачи.

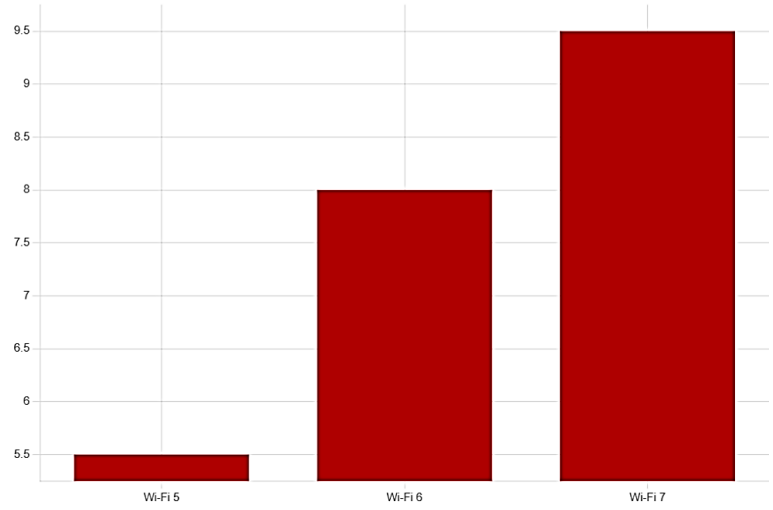


Рис. 1. Оценка стандартов Wi-Fi в общественном транспорте

Следующий критерий умного города является безопасность, что является одним из самых важных критериев в инфраструктуре города. В качестве примера можно взять город Санкт-Петербург, где реализована система «Безопасный город» [6]. Данная система включает в себя огромное количество камер видеонаблюдения, находящихся во всех частях города, что создает огромную инфраструктуру сети камер, где основными факторами являются стабильность, низкие задержки и минимальные потери сигнала, связи [7].

Новые стандарты Wi-Fi могут применятся для камер, установленных в труднодоступных местах, или для сети, где находятся скопления камер видеонаблюдения в одном месте, что позволяет убрать заполнение лишних кабелей до каждого устройства.

Использование современных стандартов Wi-Fi позволяет повысить скорость передачи данных, увеличить число одновременно подключаемых устройств и улучшить устойчивость соединения при передаче видеопотоков.

Еще одним направлением применения Wi-Fi нового поколения является экологический мониторинг. Такие системы могут включать распределенную сеть датчиков, измеряющих концентрацию твердых частиц, углекислого газа и других показателей состояния городской среды. В данном случае речь идет о сценарии с большим числом IoT-устройств, передающих небольшие объемы данных с определенной периодичностью.

Использование Wi-Fi 6/6E/7 за счет OFDMA, MU-MIMO, TWT и MLO позволяет повысить масштабируемость и устойчивость распределенных сенсорных сетей [8]. При этом полная замена существующей инфраструктуры не всегда является экономически целесообразной, поскольку требует значительных затрат на оборудование и монтаж. Более рациональным может быть поэтапное внедрение Wi-Fi нового поколения на участках с высокой плотностью устройств, в транспортных узлах, промышленных зонах, подземных коммуникациях и других труднодоступных местах.

Таким образом, Wi-Fi 6 может рассматриваться как наиболее сбалансированный вариант для развития городских IoT-сетей, поскольку сочетает поддержку большого числа устройств, энергоэффективность и относительно умеренную стоимость внедрения. Wi-Fi 7, в свою очередь, целесообразно рассматривать как перспективное решение для наиболее нагруженных и критичных участков городской инфраструктуры.

ТАБЛИЦА 2. Итоговые сценарии внедрения новых поколений Wi-Fi.

Сценарий	Основные устройства	Тип трафика	Требования	Технологии Wi-Fi	Стандарт
Транспорт	Смартфоны, бортовые системы	Смешанный (веб, видео, телеметрия)	Высокая плотность, низкая задержка	OFDMA, MU-MIMO	Wi-Fi 6
Безопасность	IP-камеры	Потоковое видео (высокий битрейт)	Высокая пропускная способность, стабильность	MU-MIMO, MLO	Wi-Fi 6/7
Экология	IoT-датчики (PM, CO_2, NO_2)	Малый периодический трафик, массовые IoT-подключения	Масштабируемость, энергоэффективность	OFDMA, TWT	Wi-Fi 6

Несмотря на технологические преимущества Wi-Fi 6/6E/7, их применение в инфраструктуре умного города связано с рядом ограничений. Во-первых, фактическая производительность беспроводной сети зависит не только от стандарта, но и от плотности пользователей, радиопланирования, уровня помех, ширины канала, характеристик точек доступа и клиентских устройств. Во-вторых, внедрение Wi-Fi 6E и Wi-Fi 7 требует поддержки соответствующих диапазонов и возможностей со стороны конечных устройств. При отсутствии совместимых клиентских устройств потенциальные преимущества стандарта могут быть реализованы не полностью. В-третьих, модернизация городской беспроводной инфраструктуры требует экономического обоснования. Наиболее затратным является не только приобретение точек доступа, но и обновление коммутаторов, контроллеров, каналов подключения, систем питания и средств мониторинга сети.

Таким образом, внедрение Wi-Fi нового поколения должно осуществляться поэтапно, с учетом технических требований конкретного городского сервиса и экономической целесообразности модернизации.

Заключение

В статье рассмотрены возможности применения Wi-Fi 6, Wi-Fi 6E и Wi-Fi 7 в инфраструктуре умного города. Показано, что современные стандарты Wi-Fi обеспечивают более эффективное использование радиочастотного спектра, поддержку плотных сетей, повышение пропускной способности и снижение задержек. На основе сценарного анализа установлено, что Wi-Fi 6 может рассматриваться как наиболее сбалансированное решение

для массового внедрения в транспортной инфраструктуре, городских IoT-сетях и публичных цифровых сервисах. Wi-Fi 6E целесообразен при перегруженности существующих диапазонов, а Wi-Fi 7 – для наиболее нагруженных участков, требующих высокой пропускной способности и минимальной задержки.

Внедрение новых поколений Wi-Fi должно осуществляться поэтапно, с учетом требований конкретного сценария, плотности устройств, стоимости оборудования и условий эксплуатации. Наиболее рациональным подходом является использование Wi-Fi 6 как базового стандарта с последующим внедрением Wi-Fi 7 в критически нагруженных зонах.

Список используемых источников

1. IEEE Std 802.11ax-2021. IEEE Standard for Information technology – Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. 2021.

2. Cisco. Wi-Fi 6 (802.11ax): High-Efficiency Wireless // Cisco White Paper. 2020.

3. Intel. Introduction to Wi-Fi 6 (802.11ax). Intel Corporation. 2019.

4. Qualcomm. Wi-Fi 7: The Next Generation of Wi-Fi Technology. 2023.

5. IEEE Std 802.11be-2024. IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks – Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment: Enhancements for Extremely High Throughput (EHT). IEEE, 2025.

6. Приказ Минстроя России от 25.12.2020 № 866/пр – Об утверждении Концепции проекта цифровизации городского хозяйства «Умный город». 2020.

7. Zhang Y., Chen X., Li L. Smart City Architecture and Technologies: A Survey // IEEE Access. 2018. Vol. 6. PP. 434-452.

8. Cisco Annual Internet Report (2018-2023). Cisco Systems. 2020.

Статья представлена научным руководителем, старшим преподавателем кафедры ИКС СПбГУТ А. А. Савельевой.

УДК 004.738.5

АНАЛИЗ СУЩЕСТВУЮЩИХ ИНТЕГРАЦИОННЫХ РЕШЕНИЙ ДЛЯ СООБЩЕСТВ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

М. С. Соромотин (студент группы ИКТК-21 СПбГУ),Т soromotin.md@sut.ru

В статье рассмотрены основные классы интеграционных решений, применяемых для управления сообществами в социальных сетях и мессенджерах. Актуальность исследования обусловлена ростом числа каналов коммуникации, усложнением сценариев администрирования и необходимостью объединять сообщения, заявки, платежи, аналитику и клиентские данные в едином информационном контуре. Проанализированы API-интеграции, no-code/low-code платформы, CRM-решения, middleware, ESB и событийные архитектуры. Предложена формальная модель сравнительной оценки, учитывающая стоимость, скорость внедрения, масштабируемость, безопасность, гибкость и зависимость от внешнего поставщика. Показано, что универсального интеграционного решения не существует: выбор архитектуры должен зависеть от типа сообщества, нагрузки, критичности процессов и требований к хранению данных.

социальные сети, мессенджеры, онлайн-сообщества, API, webhooks, CRM, no-code, middleware, ESB, интеграционная архитектура

Социальные сети и мессенджеры в последние годы стали не только средствами личного общения, но и инфраструктурой для образовательных проектов, медиаканалов, интернет-магазинов, профессиональных клубов и клиентских сообществ. Администратор такого сообщества работает одновременно с публикациями, комментариями, личными сообщениями, заявками, оплатами, рассылками и аналитикой, при малом количестве участников эти процессы могут выполняться вручную, однако при росте аудитории ручная обработка приводит к задержкам, ошибкам маршрутизации и потере данных о пользователях.

Основная проблема состоит в разрозненности цифровых каналов. Один пользователь может написать в Telegram, второй – во ВКонтакте, третий – через форму на сайте, а история сделки или обращения при этом должна храниться в CRM, если каналы не связаны между собой, администратор вынужден копировать сведения вручную. Это увеличивает операционные затраты и снижает качество обслуживания. Интеграционное решение устраняет данный разрыв за счет автоматического обмена событиями между платформами и внутренними информационными системами.

Интеграция в рамках данной статьи рассматривается как процесс объединения независимых программных систем для обеспечения совместной

обработки данных и событий, для сообществ в социальных сетях и мессенджерах типовая интеграционная цепочка выглядит следующим образом: пользователь совершает действие в канале коммуникации; платформа фиксирует событие; событие передается во внешнюю систему через API, webhook или коннектор; сервер или платформа автоматизации обрабатывает данные; результат записывается в CRM, базу данных или систему аналитики; при необходимости пользователю отправляется ответное сообщение.

Целью статьи является анализ существующих интеграционных решений для сообществ в социальных сетях и мессенджерах и определение областей, в которых каждый класс решений является наиболее эффективным, для достижения цели необходимо рассмотреть основные виды интеграций, сопоставить их по техническим и организационным критериям, выделить типовые сценарии применения и сформулировать рекомендации по выбору архитектуры.

Методика сравнительной оценки

Для анализа используется сценарный подход, который предполагает, что интеграционная технология оценивается не абстрактно, а относительно конкретной задачи сообщества: прием заявок, выдача платного доступа, рассылка, публикация контента, техническая поддержка, модерация или сбор аналитики, такой подход позволяет учитывать не только функциональность инструмента, но и ограничения эксплуатации: стоимость лицензий, необходимость разработчиков, требования к безопасности, возможность масштабирования и сложность сопровождения.

В качестве критериев оценки выбраны: скорость внедрения, стоимость владения, гибкость бизнес-логики, масштабируемость, надежность, безопасность, удобство сопровождения и степень зависимости от поставщика. Для формального сравнения можно использовать взвешенную модель:

$$S_j = \sum(i=1..m)\ w_i \cdot q_{ij},\ \sum(i=1..m)\ w_i = 1,\ q_{ij} \in [0; 5],$$

где S_j – итоговая оценка j-го интеграционного решения, w_i – вес i-го критерия, q_ij – экспертная оценка решения по данному критерию. Например, для стартапа больший вес получает скорость внедрения, а для крупного сообщества с платежами и персональными данными – безопасность и надежность.

Нагрузку интеграционного контура можно приблизительно описать выражением:

$$\lambda = \sum(k = 1..n)\ N_k \cdot f_k,\ \rho = \lambda / \mu < 1,$$

где N_k – число активных пользователей k-го канала, f_k – среднее количество событий от одного пользователя за единицу времени, λ – суммарная интенсивность входящих событий, μ – пропускная способность обработчика, ρ – коэффициент загрузки. Условие $\rho < 1$ показывает, что система в среднем успевает обработать поток событий. При приближении ρ к единице возрастает время ожидания, поэтому требуется очередь сообщений, горизонтальное масштабирование или переход к более производительной архитектуре.

ТАБЛИЦА 1. Основные классы интеграционных решений

Класс решения	Принцип работы	Типовые инструменты	Основное назначение
API и webhooks	Обмен данными через HTTP-запросы, события и методы платформ	Telegram Bot API, VK API, WhatsApp Cloud API	Боты, заявки, модерация, платный доступ, кастомная логика
No-code / low-code	Сценарии вида «триггер → действие» без полноценной разработки	Zapier, Make, n8n, Albato	Быстрые связки, уведомления, таблицы, простая автоматизация
CRM и омниканальные хабы	Объединение сообщений и клиентских данных в едином интерфейсе	Bitrix24, amoCRM, Helpdesk-системы	Продажи, поддержка, распределение обращений, история клиента
Middleware и ESB	Промежуточный слой маршрутизации, преобразования и контроля сообщений	Apache Camel, Mule ESB, брокеры сообщений	Корпоративная интеграция, высокие нагрузки, сложные регламенты
Собственные микросервисы	Набор специализированных сервисов с очередями и базами данных	Node.js/Python backend, RabbitMQ, Kafka, PostgreSQL	Независимая архитектура для критичных и нестандартных процессов

API-интеграции и webhooks

API-интеграция является наиболее гибким способом объединения сообщества с внешними системами. В этом случае разработчик обращается к официальному интерфейсу платформы, получает события, обрабатывает их

на собственном сервере и отправляет ответные действия. Telegram Bot API, например, описывает HTTP-интерфейс для создания ботов; обновления могут поступать через getUpdates или webhook, а запросы к API выполняются по HTTPS [1]. Подобная модель хорошо подходит для чат-ботов, систем выдачи доступа, модерации сообщений, обработки команд и построения персонализированных сценариев общения.

В ВКонтакте для сообществ применяются механизмы событий, включая Callback API и Bots Long Poll API. В первом случае платформа отправляет уведомления на сервер администратора, во втором – сервер интеграции самостоятельно запрашивает накопленные события, для мессенджеров бизнес-класса характерна сходная логика: WhatsApp Cloud API построен на HTTP-запросах Graph API [2], а входящие сообщения и статусы доставляются через webhooks [3]. Следовательно, общий принцип для современных платформ одинаков: событие преобразуется в JSON-объект, после чего обрабатывается внешней системой.

Преимущество API-подхода заключается в высокой степени контроля. Разработчик может реализовать собственные правила маршрутизации, подключить базу данных, платежную систему, антиспам-модуль, аналитику и CRM. API также позволяет соблюдать идемпотентность: повторно пришедшее событие не должно создавать дублирующую заявку или повторно выдавать доступ, для этого каждому событию присваивается уникальный идентификатор, который проверяется перед выполнением действия.

Недостатки API-интеграции связаны с необходимостью разработки и сопровождения. Требуется серверная инфраструктура, мониторинг, хранение токенов, обработка ошибок, защита webhook-эндпоинтов, учет лимитов платформы и адаптация к изменениям документации, кроме того, не все социальные платформы предоставляют одинаково открытый доступ к данным: часть методов может быть ограничена политиками платформы, типом аккаунта или требованиями к бизнес-верификации.

No-code и low-code платформы автоматизации

No-code и low-code платформы применяются тогда, когда требуется быстро связать несколько сервисов без написания полноценного программного кода. Типовой сценарий строится по принципу «триггер → действие»: новое сообщение, заполненная форма или добавленная строка запускают автоматическое действие, например создание лида в CRM, отправку уведом-

ления или запись данных в таблицу. В документации Zapier интеграция описывается через три базовых сущности: аутентификацию, триггеры и действия [4]. В n8n аналогичную роль выполняют узлы workflow: trigger nodes запускают процесс, а action nodes выполняют операции с данными [5].

Главное достоинство no-code – скорость внедрения. Администратор сообщества может за короткое время настроить автоматическую отправку заявок из формы в CRM, пересылку новых сообщений в канал модераторов или уведомление менеджера о платеже, для малых и средних сообществ это часто экономически выгоднее, чем разрабатывать собственный backend. Дополнительным преимуществом является наличие готовых коннекторов к популярным сервисам.

Ограничения no-code проявляются при усложнении логики. Сложные условия ветвления, большие объемы данных, нестандартная авторизация, требования к задержке и необходимость полного контроля над хранением данных могут сделать no-code недостаточным. Еще один риск – зависимость от тарифов и доступности платформы, если автоматизация построена полностью на внешнем сервисе, изменение тарифа, лимитов или правил использования напрямую влияет на работу сообщества [6-11].

Middleware, ESB и событийная архитектура

Middleware представляет собой промежуточное программное обеспечение, обеспечивающее связь между разнородными приложениями. IBM определяет middleware как программный слой, который обеспечивает коммуникацию и связанность приложений в распределенной сети, фактически выполняя роль «программного клея» между системами [7]. В контексте сообществ middleware может принимать события из Telegram, VK, сайта и CRM, преобразовывать их к единому формату и маршрутизировать в нужные сервисы.

ESB (Enterprise Service Bus) является более формализованным корпоративным вариантом middleware. Все системы подключаются не напрямую друг к другу, а через общую шину. Шина отвечает за маршрутизацию, преобразование форматов, логирование, контроль ошибок, повторные попытки и интеграцию с корпоративными сервисами, такая архитектура оправдана для крупных организаций, где сообщество связано с складом, службой поддержки, системой лояльности и корпоративной аналитикой.

Современной альтернативой монолитной ESB является событийная архитектура, в ней производители событий публикуют сообщения в канал,

а потребители подписываются на интересующие события. Microsoft описывает event-driven architecture как модель, в которой producers создают поток событий, consumers прослушивают их, а event channels передают события между сторонами, для сообщества это означает, что событие «пользователь оплатил подписку» может одновременно запустить выдачу доступа, отправку приветственного сообщения, обновление CRM и запись в аналитическое хранилище [10].

Главное преимущество middleware и событийной архитектуры – масштабируемость и слабая связанность, если один сервис временно недоступен, сообщение может быть сохранено в очереди и обработано позже. Главный недостаток – сложность внедрения: требуются архитекторы, разработчики, DevOps-практики, мониторинг и регламенты сопровождения, поэтому такие решения обычно применяются не на стартовом этапе, а при росте сообщества или при наличии корпоративных требований.

ТАБЛИЦА 2. Сравнительная оценка интеграционных решений

Критерий	API/webhook	No-code/low-code	CRM-хаб	Middleware/ESB
Скорость запуска	Средняя: требуется разработка	Высокая: готовые сценарии	Средняя: нужна настройка процессов	Низкая: проектирование архитектуры
Стоимость на старте	Низкая или средняя	Низкая, но зависит от тарифа	Средняя или высокая	Высокая
Гибкость логики	Высокая	Средняя	Средняя	Очень высокая
Масштабирование	Высокое при правильной архитектуре	Ограничено тарифом и лимитами	Зависит от CRM и лицензии	Высокое
Безопасность	Зависит от реализации	Зависит от провайдера	Есть роли и журналы, но возможен lock-in	Высокая при грамотной настройке
Сопровождение	Нужны разработчики	Доступно администратору	Нужны администратор CRM и обучение	Нужна команда сопровождения
Оптимальная область	Критичные и нестандартные процессы	Простые автоматизации	Продажи и поддержка	Крупные распределенные системы

Сценарии применения для разных типов сообществ

Онлайн-сообщества различаются по целям и характеру нагрузки. Образовательные сообщества нуждаются в управлении доступом к материалам, уведомлениях о занятиях, проверке оплат и сборе обратной связи. Коммерческие сообщества ориентированы на заявки, продажи, поддержку и повторные коммуникации. Медиасообщества чаще решают задачи публикации контента, аналитики вовлеченности и модерации комментариев. Профессиональные клубы и закрытые сообщества требуют идентификации участников, контроля ролей и сохранения истории взаимодействия.

Для публикации одинакового контента в несколько каналов рационально использовать no-code или специализированные сервисы автопостинга, если задача сводится к переносу текста, ссылки и изображения из одной системы в другую, собственный API-сервер может быть избыточным, но для сценария платного доступа требуется более строгая логика: платеж должен быть подтвержден, пользователь должен быть найден в нужной платформе, доступ должен быть выдан один раз, а информация о подписке должна сохраниться в CRM или базе данных. Здесь предпочтительна связка API + CRM.

Для поддержки клиентов наиболее эффективны CRM и омниканальные решения. Пользователь пишет из привычного мессенджера, но оператор видит диалог в едином интерфейсе и может связать обращение с карточкой клиента, для аналитики крупного сообщества целесообразно использовать промежуточный слой: события собираются из разных каналов, нормализуются и поступают в хранилище, где строятся отчеты по активности, источникам заявок, скорости ответа и конверсии.

ТАБЛИЦА 3. Рекомендации по выбору решения для типовых задач

Задача сообщества	Критичные требования	Рекомендуемая архитектура	Комментарий
Публикация контента в несколько каналов	Быстрый запуск, минимум кода	No-code/low-code	Подходит при простой логике и умеренной частоте публикаций
Платный доступ к закрытому чату	Идемпотентность, безопасность, связь с оплатой	API + CRM + база данных	Нужна проверка платежа и контроль срока подписки
Обработка заявок на обучение	Сохранение контактов, статусы, ответственный	CRM-хаб + коннекторы	CRM становится центральным узлом для менеджеров

Задача сообщества	Критичные требования	Рекомендуемая архитектура	Комментарий
Модерация и антиспам	Низкая задержка, кастомные правила	API-бот + очередь событий	Возможна интеграция с ML-фильтрами и черными списками
Клиентская поддержка	История общения, распределение нагрузки	CRM/Open Channels	Важны очереди операторов и отчеты по качеству
Корпоративная аналитика	Сбор данных из многих систем	Middleware/event bus + DWH	Оправдано при большой аудитории и нескольких внутренних системах

Риски интеграционных решений

Интеграции повышают эффективность управления сообществом, но одновременно создают новые риски, для API-интеграций наиболее значимыми рисками остаются утечка токенов, ошибки в настройке авторизации, отсутствие проверки подписи webhook-запросов, превышение установленных лимитов, повторная обработка одних и тех же событий, а также зависимость от изменений на стороне внешней платформы. В документе OWASP API Security Top 10 2023 отдельно выделяются такие угрозы, как нарушения авторизации и аутентификации, неограниченное потребление ресурсов, SSRF-атаки и небезопасная работа со сторонними API, а для Telegram-сообществ эти риски особенно существенны, поскольку интеграционные механизмы могут получать доступ к сообщениям пользователей, контактной информации, платежным статусам и персональным данным [8].

В no-code-решениях основная проблема связана с зависимостью от внешнего сервиса. Данные обрабатываются через стороннюю платформу, сценарии ограничены возможностями выбранного тарифа, а обработка ошибок часто зависит от того, какие инструменты предоставляет интерфейс конструктора, поэтому такие решения оправдано использовать для некритичных задач или на этапе быстрого прототипирования, при увеличении нагрузки и усложнении бизнес-процессов часть сценариев целесообразно переносить на собственный API-слой, оставляя no-code-платформы для вспомогательных уведомлений, простых автоматизаций и административных операций.

CRM-системы, в свою очередь, могут формировать организационную зависимость и со временем процессы сообщества начинают подстраиваться под логику конкретной CRM: структуру карточек, статусы, воронки и правила обработки заявок, если система не поддерживает нужный сценарий,

возникает необходимость в дополнительной кастомизации или подключении внешних интеграций, что увеличивает стоимость сопровождения, так же эффективность CRM зависит не только от технической настройки, но и от подготовки сотрудников, если администраторы и операторы не умеют корректно работать с карточками, статусами и очередями, даже правильно настроенная система не обеспечит ожидаемый результат.

Ключевыми вопросами для ESB и middleware-решений, становятся сложность архитектуры и устойчивость к сбоям. Центральная интеграционная шина может превратиться в единую точку отказа, если заранее не предусмотрены резервирование, репликация, мониторинг и процедуры восстановления, а в микросервисной архитектуре возникает другая сложность: по мере роста числа сервисов становится труднее отслеживать ошибки, контролировать обмен сообщениями и поддерживать согласованность данных, без централизованного логирования, трассировки и управления схемами сообщений сопровождение такой системы быстро усложняется, поэтому сложные интеграционные архитектуры следует внедрять постепенно, начиная с процессов, которые имеют наибольшее значение для работы сообщества.

ТАБЛИЦА 4. Риски и меры снижения

Класс решения	Основные риски	Меры снижения
API/webhook	Утечка токенов, дубли событий, ошибки авторизации, зависимость от лимитов	Хранение секретов в vault, TLS, проверка подписи, идемпотентность, rate limiting
No-code/low-code	Lock-in, тарифные ограничения, слабая обработка нестандартных ошибок	Использовать для простых задач, документировать сценарии, выносить критичные процессы в API
CRM-хаб	Сложность настройки, обучение персонала, ограниченная кастомизация	Регламенты, роли доступа, пилотное внедрение, API-слой для нестандартных процессов
Middleware/ESB	Высокая стоимость, единая точка отказа, сложность сопровождения	Резервирование, очереди, мониторинг, поэтапное внедрение, событийная декомпозиция

Рекомендации по проектированию интеграционной архитектуры

Первой рекомендацией является использование гибридной модели, но на практике редко бывает достаточно одного класса решений. Простые уведомления и автопостинг можно оставить в no-code, клиентскую историю вести в CRM, а критичные операции – оплату, выдачу доступа, модерацию

и синхронизацию ролей – реализовать через API, такой подход снижает стоимость внедрения и одновременно сохраняет контроль над важными процессами.

Второй принцип связан со снижением зависимости от одного сервиса**.** Важные данные следует хранить в собственной базе данных или CRM, а не только внутри мессенджера либо платформы автоматизации, что позволяет системе продолжить работу даже в ситуации, когда связь с отдельным каналом временно нарушена. Например, после восстановления соединения она сможет повторно отправить сообщение или завершить ранее начатую обработку, для этого обычно применяются очереди сообщений, журналы событий и механизмы повторных попыток с заранее заданным лимитом.

Третья рекомендация заключается в приведении данных к единому формату. Разные платформы по-разному передают идентификаторы, вложения, статусы и типы событий, поэтому в интеграционном слое целесообразно использовать внутреннюю модель события, такой подход упрощает подключение новых каналов и уменьшает количество отдельных условий в бизнес-логике.

Четвертый принцип – закладывать требования безопасности уже на этапе проектирования. Токены доступа нельзя хранить прямо в коде или в общих таблицах, Webhook-эндпоинты должны работать по HTTPS, проверять секретные ключи и подписи, ограничивать размер входящих запросов и фиксировать подозрительные ошибки, кроме того, для администраторов необходимо разграничивать права доступа: например, сотрудник поддержки не должен иметь возможность изменять настройки платежей.

Пятая рекомендация связана с наблюдаемостью. Интеграционная система должна отвечать на вопросы: сколько событий получено, сколько обработано успешно, сколько завершилось ошибкой, какой канал дает максимальную нагрузку, где возникают задержки. Даже простое логирование с идентификатором события и статусом обработки позволяет быстрее находить ошибки и доказывать факт выполнения операции.

Заключение

В статье рассмотрены существующие интеграционные решения для сообществ в социальных сетях и мессенджерах. Показано, что основными классами являются API/webhook-интеграции, no-code/low-code платформы, CRM и омниканальные хабы, middleware, ESB и собственные микросервисные решения. Каждый класс имеет свою область эффективности: no-code

обеспечивает быстрый запуск простых сценариев, CRM удобна для поддержки и продаж, API дает максимальную гибкость для критичных процессов, а middleware и событийная архитектура применяются при высокой нагрузке и сложной корпоративной интеграции.

На основании анализа можно сделать вывод, что универсального решения не существует. Выбор архитектуры должен определяться задачами сообщества, числом каналов, интенсивностью событий, требованиями к безопасности и доступным ресурсом сопровождения. Для большинства развивающихся сообществ рациональной является гибридная модель: CRM используется как центральное хранилище клиентских данных, no-code – для вспомогательных автоматизаций, а API-сервер – для критичных процессов, требующих контроля и надежности. По мере роста нагрузки архитектура может дополняться очередями сообщений, middleware и аналитическим хранилищем.

Практическая рекомендация заключается в поэтапном внедрении. На первом этапе следует автоматизировать наиболее повторяемые операции: прием заявок, уведомления и запись данных в CRM. На втором этапе – вынести критичные процессы в собственный API-слой и обеспечить журналирование событий. На третьем этапе, при росте количества каналов и пользователей, целесообразно переходить к событийной архитектуре с очередями, нормализацией данных и централизованным мониторингом. Такой путь позволяет снижать операционные затраты без избыточного усложнения системы на ранних стадиях.

Список используемых источников

1. Telegram Bot API. Официальная документация. URL: https://core.telegram.org/bots/api (дата обращения: 30.04.2026).

2. VK API. Bots Long Poll API и Callback API. Официальная документация. URL: https://dev.vk.com/ru/api/bots/getting-started (дата обращения: 30.04.2026).

3. Meta. WhatsApp Cloud API Overview. Официальная документация. URL: https://developers.facebook.com/docs/whatsapp/cloud-api/overview (дата обращения: 30.04.2026).

4. Zapier Platform Docs. How Zapier works. URL: https://docs.zapier.com/platform/quickstart/how-zapier-works (дата обращения: 30.04.2026).

5. n8n Docs. Nodes and Webhook node. URL: https://docs.n8n.io/workflows/components/nodes/; https://docs.n8n.io/integrations/builtin/core-nodes/n8n-nodes-base.webhook/ (дата обращения: 30.04.2026).

6. Bitrix24 REST API. Open Channels in Bitrix24: API for Lines and Connectors. URL: https://apidocs.bitrix24.com/api-reference/imopenlines/index.html (дата обращения: 30.04.2026).

7. IBM. What is middleware? URL: https://www.ibm.com/topics/middleware (дата обращения: 30.04.2026).

8. OWASP API Security Top 10 – 2023. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (дата обращения: 30.04.2026).

9. Hohpe G., Woolf B. Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Addison-Wesley Professional, 2003.

10. Microsoft Azure Architecture Center. Event-driven architecture style. URL: https://learn.microsoft.com/en-us/azure/architecture/guide/architecture-styles/event-driven (дата обращения: 30.04.2026).

11. Make. Scenarios Integration / Workflow Automation. URL: https://www.make.com/en/integrations/scenario-service (дата обращения: 30.04.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры ИКС СПбГУТ А. А. Савельевой.

УДК 004.932

ПОЛУЧЕНИЕ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ ИЗ АРХИВНЫХ ИЗОБРАЖЕНИЙ С ПРИМЕНЕНИЕМ ГЕНЕРАТИВНЫХ НЕЙРОСЕТЕЙ

Д. А. Татаренков (ст. преподаватель кафедры ЦТМ СПбГУТ)
Е. А. Трапезникова (студент группы Р-41м СПбГУТ), katu.ush@sut.ru

В статье рассматривается подход к получению видеопоследовательности из набора архивных двумерных изображений с использованием генеративных нейросетей. Исследуется работа модели, реализующей концепцию виртуальной камеры, позволяющей синтезировать новые ракурсы сцены на основе ограниченного набора исходных данных. Представлены результаты демонстрационного эксперимента на основе архивных фотографий, подтверждающие возможность формирования согласованной видеопоследовательности при отсутствии информации о глубине и геометрии сцены.

генеративные нейросети, виртуальный ракурс, 3D-реконструкция

В условиях цифровизации медиапроизводства возрастает интерес к технологиям восстановления и реконструкции визуального контента на основе архивных данных. Особую актуальность данная задача приобретает в сфере телепроизводства, где использование исторических материалов позволяет расширять визуальные возможности повествования, создавать реконструкции событий и формировать новые форматы медиаконтента.

Одной из ключевых проблем при работе с архивными визуальными материалами является их фрагментарность и статичность – как правило, это набор разрозненных изображений, полученных с различных ракурсов в разное время, что затрудняет их использование в динамических видеопоследовательностях. Отсутствие непрерывного движения камеры и согласованного пространственного представления сцены ограничивает возможности интеграции таких материалов в современный видеоконтент.

Современные модели генеративных нейросетей открывают новые перспективы в решении данной задачи. Они позволяют не только интерполировать недостающие данные, но и синтезировать новые ракурсы сцены, обеспечивая эффект виртуального перемещения камеры. В частности, применение моделей, реализующих концепцию виртуальной камеры, позволяет преобразовывать набор статичных изображений в связную видеопоследовательность. Генеративные нейросети способны не только интерпретировать пространственные отношения между изображениями, но

и реконструировать недостающие фрагменты, опираясь на вероятностные представления [1].

Для решения задачи синтеза видеопоследовательности из изображений в работе применяется модель Stable Virtual Camera, представляющая собой генеративную архитектуру для построения новых ракурсов сцены [2, 3, 4]. В основе модели лежат диффузионные методы генерации, а ее работа реализуется с помощью энкодера, модуля пространственного сопоставления, латентной диффузионной модели и декодера.

Для оценки возможностей предложенного подхода был проведен демонстрационный эксперимент, направленный на воспроизведение виртуального движения камеры и анализ качества синтезированных изображений. В качестве входных данных использовалось 8 изображений: 4 архивные фотографии внешнего вида здания и 4 изображения интерьера, полученные с различных ракурсов (рис. 1). Исходные данные не содержат информации о глубине или точной геометрии сцены, что позволяет рассматривать эксперимент в условиях, приближенных к реальным архивным сценариям, характеризующимся фрагментарностью и неполнотой визуального материала.



Рис. 1. Входные изображения

На этапе предварительной обработки каждое изображение преобразуется в набор информативных признаков, отражающих форму объектов, пространственную структуру и особенности сцены. Это позволяет модели перейти от покомпонентного представления (набора пикселей) к более высокоуровневому описанию содержания изображений и их взаимосвязей. На рис. 2 слева представлен набор исходных изображений в перспективном представлении, а справа – результат внутренней работы модели, соответствующий обобщенному латентному описанию сцены, используемому на последующих этапах реконструкции.

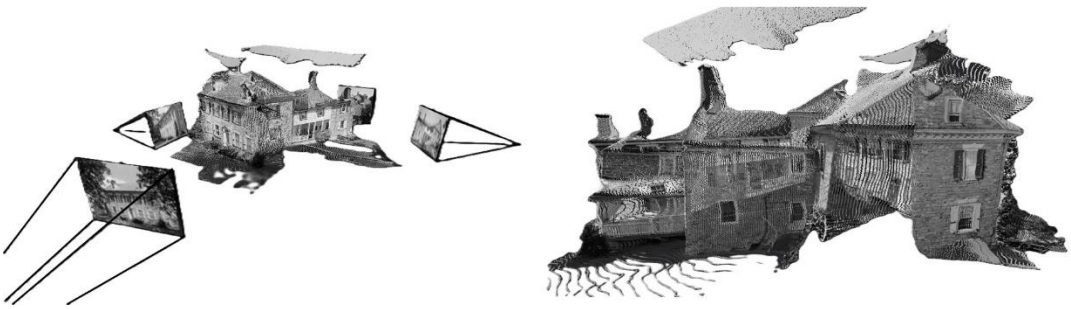


Рис. 2. Визуализация реконструкции сцены на основе входных изображений

После преобразования входных данных в латентное пространство выполняется их приведение к единой системе координат. Для этого применяется механизм пространственного сопоставления [2, 4], учитывающий положение и ориентацию виртуальных камер относительно сцены. Данный этап обеспечивает установление соответствий между изображениями, коррекцию геометрических несоответствий и согласование элементов сцены. В результате разрозненные данные интегрируются в целостное многомерное представление, сохраняющее пространственную структуру, включая глубину, перспективу и взаимное расположение объектов, а также частично отсутствующие в отдельных кадрах детали. Это формирует полный контекст, необходимый для последующей генерации.

Диффузионная модель выполняет синтез изображений в латентном пространстве путем постепенного преобразования шумового распределения в структурированное изображение [2, 4]. На каждом этапе происходит уточнение геометрии и текстур с учетом статистических закономерностей, усвоенных в процессе обучения. Поэтапный характер генерации: от грубой структуры к детализированному представлению обеспечивает реалистичность и согласованность синтезируемых ракурсов.

В результате работы модели формируется последовательность изображений, имитирующая непрерывное перемещение камеры в виртуальной сцене. На рис. 3 слева представлена исходная конфигурация с областями, не охваченными входными данными, справа – пример сгенерированного кадра, демонстрирующий заполнение недостающих участков.

Аналогичный эксперимент был проведен для интерьерной сцены (рис. 4), в которой входные данные представлены серией фотографий помещения. В данном случае задача усложняется более выраженной трехмерной структурой сцены, а также усиленным влиянием перспективных искажений на согласованность изображений.



Рис. 3. Пространственная визуализация входных изображений (слева) и пример результата после генерации (справа)

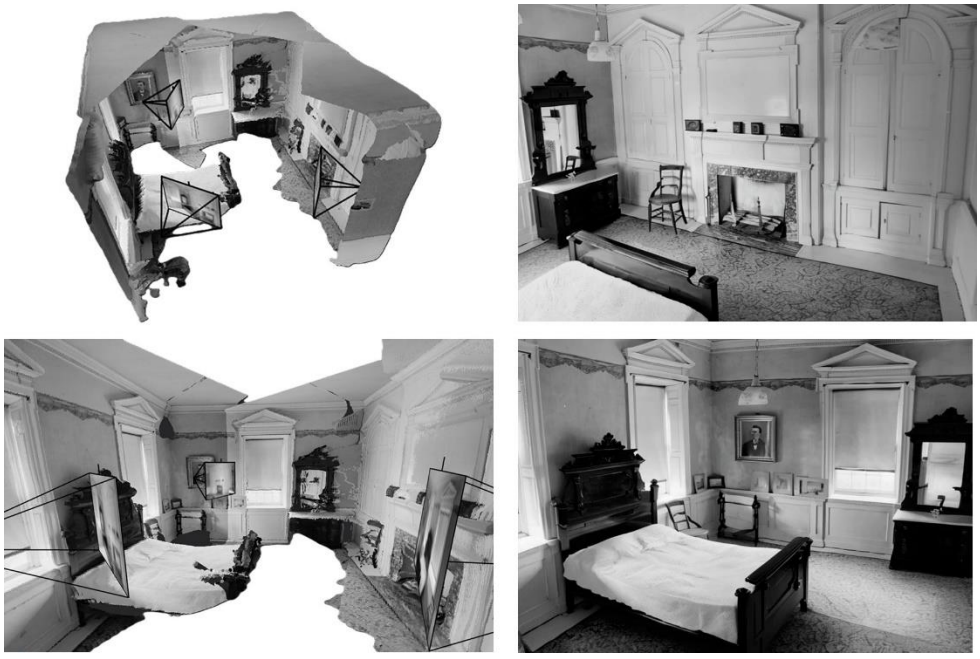


Рис. 4. Визуализация реконструкции сцены и генерация недостающих фрагментов

Развитие генеративных нейросетей открывает новые подходы к работе с визуальным наследием, позволяя переосмыслить роль архивных изображений в медиапроизводстве. Если ранее такие материалы воспринимались как статичные и ограниченные по выразительным возможностям, то современные методы синтеза ракурсов трансформируют их в основу для создания динамического визуального контента [5].

Полученные результаты демонстрируют, что даже фрагментарные и неполные наборы изображений могут служить достаточной базой для реконструкции пространственно-согласованных сцен. Это позволяет не только восстанавливать утраченные элементы визуальной информации, но и формировать новые способы представления пространства, приближенные к естественному восприятию движения камеры.

Особую значимость данный подход приобретает в контексте телепроизводства и цифровых медиа, где возрастает потребность в гибких инструментах работы с архивными материалами. Возможность синтеза видеопоследовательностей из статичных изображений расширяет границы визуального повествования и создает предпосылки для появления новых форматов контента.

Таким образом, применение генеративных моделей для реконструкции сцен из архивных данных представляет собой перспективное направление, объединяющее методы компьютерного зрения и медиатехнологий и способствующее развитию интеллектуальных инструментов обработки визуальной информации.

Список используемых источников

1. Применение генеративных адверсариальных сетей (GANs) для синтеза данных. URL: https://habr.com/ru/companies/otus/articles/754978/ (дата обращения: 25.03.2026)

2. Zhou, J. J., Gao, H., Voleti, V., Vasishta, A., Yao, C. H., Boss, M., ... & Jampani, V. STABLE VIRTUAL CAMERA: Generative View Synthesis with Diffusion Models // arXiv preprint arXiv:2503.14489. – 2025.

3. Stability AI. Stable Virtual Camera. URL: https://github.com/Stability-AI/stable-virtual-camera (дата обращения: 25.03.2026).

4. Татаренков Д. А., Трапезникова Е. А. Применение генеративных нейросетей для формирования виртуальных ракурсов // Студенческая весна – 2025: сб. науч. ст. 79-й региональной научно-технической конференции студентов, аспирантов и молодых ученых / под ред. А. В. Рабина; сост. А. А. Дзюбаненко, И. М. Татарникова. СПб.: СПбГУТ, 2025. С. 100–103.

5. Stable Virtual Camera: Generative View Synthesis with Diffusion Models. URL: https://stable-virtual-camera.github.io/ (дата обращения: 25.03.2026).

Статья представлена научным руководителем,
старшим преподавателем кафедры ЦТМ СПбГУТ Д. А. Татаренковым.

УДК 004.921

МЕТОДИКА ЦВЕТОТОНАЛЬНОГО СОГЛАСОВАНИЯ 3D-ОБЪЕКТА С ВИДЕОРЯДОМ ПРИ КОМПОНОВКЕ СЦЕНЫ

Д. А. Татаренков (ст. преподаватель СПбГУТ)
П. В. Фомин (студент группы Р-41м СПбГУТ), fomin.pv@sut.ru

Задача цветотонального согласования трехмерного объекта с изображенным пространством является важным этапом при компоновке сцены в задачах визуальных эффектов. В статье показано, что даже при точном трекинге камеры и корректной геометрической стыковке объект может выглядеть искусственно из-за расхождения по яркости, контрасту, насыщенности и общей тональности с фоновым видеорядом. Предлагается последовательность практических действий, ориентированная на использование программных средств Nuke и Autodesk Maya. Цветотональное согласование является самостоятельным этапом методики вписывания 3D-объектов в изображенное пространство и существенно влияет на визуальную достоверность результата.

3D-графика, комбинированные съемки, композитинг, цветокоррекция, визуальные эффекты

Теоретические основы цветотонального согласования

Современные технологии визуальных эффектов все чаще требуют не просто размещения трехмерного объекта в кадре, а его убедительного включения в уже существующее изображенное пространство. В практической работе над такими сценами обычно уделяют внимание трекингу камеры, совмещению перспективы, расчету освещения и подбору материалов. Однако на конечный результат не меньшее влияние оказывает цветотональное соответствие объекта и фона. Даже при правильной геометрии и согласованном освещении объект может восприниматься как «вклеенный», если его яркость, цветовой баланс и контраст отличаются от параметров исходного видеоряда. Именно поэтому цветотональное согласование следует рассматривать как отдельный этап методики вписывания 3D-объектов в изображенное пространство [1].

В подобных проектах Maya обычно применяется для рендера трехмерной сцены, а Nuke – для создания виртуальной камеры и, соответственно, самой трехмерной сцены. Такой подход уже хорошо проявил себя в практической работе с трекингом, освещением и совмещением 3D-графики с видеорядом. Однако именно цветотональный этап нередко остается недооцененным, хотя он напрямую влияет на восприятие сцены зрителем.

Под цветотональным согласованием понимается приведение виртуального объекта к такому визуальному состоянию, при котором он не выбивается из общей структуры кадра по яркости, цвету и контрасту [2]. На практике это означает, что объект должен учитывать не только параметры источника света, но и свойства самой съемки: экспозицию камеры, характер цветопередачи, уровень общей освещенности сцены, а также наличие цветовых рефлексов от окружения. В комбинированных съемках именно нарушение этих параметров чаще всего делает вставленный объект заметным как посторонний элемент.

Практический процесс цветотонального согласования можно условно разделить на несколько этапов. Сначала анализируется исходный кадр. Из него выделяются области, которые можно считать опорными для оценки тональности фона: участки с близкой яркостью, нейтральные поверхности, зоны без резких цветовых переходов и участки, на которые не попадают слишком сильные блики. Далее по этим участкам производится сопоставление цветовых параметров графического объекта и сцены. Если объект заметно светлее или темнее фона, его экспозиция корректируется еще на стадии рендера или в композитинге. Затем уточняется цветовой баланс: при необходимости объект смещается в сторону более теплого или холодного оттенка, а также подгоняется по насыщенности и локальному контрасту. Завершающим шагом становится проверка объекта в составе итогового кадра и, при необходимости, мягкая корректировка на уровне всего изображения.

Дополнительная точность цветотонального согласования достигается при анализе не отдельных значений, а распределения яркости в выбранных опорных областях изображения. Яркость пикселя вычисляется как взвешенная сумма цветовых каналов [3]:

$$Y = 0{,}2126R + 0{,}7152G + 0{,}0722B \quad (1)$$

Для сопоставления объекта с фоном используются устойчивые характеристики распределения, такие как медиана или значения, делящие диапазон яркости на части, что позволяет учитывать основную тональную массу изображения. На основе выбранного опорного значения выполняется масштабирование яркости объекта с целью приведения его к уровню сцены:

$$Y'_{obj} = k \cdot Y_{obj} \quad (2)$$

где коэффициент k определяется отношением яркости фона к яркости объекта. При этом важно учитывать не только общий уровень яркости, но и локальный контраст, который влияет на восприятие объема и глубины [4]. Избыточный контраст делает объект визуально «чужим», тогда как его

недостаток приводит к потере детализации. Дополнительно проводится корректировка цветового баланса с учетом общего температурного смещения сцены и влияния отраженного света. В результате объект адаптируется к характеристикам видеоряда не только по освещенности, но и по структуре тональных переходов. Такой подход обеспечивает более убедительное включение трехмерного элемента в изображенное пространство.

Также требуется учитывать и цветовое различие. Для этого удобно использовать расстояние между цветами в пространстве CIE Lab, где восприятие цвета человеком описывается более естественно, чем в обычной модели RGB. Цветовое расхождение можно выразить как:

$$\Delta E = \sqrt{(L_1 - L_2)^2 + (a_1 - a_2)^2 + (b_1 - b_2)^2} \quad (3)$$

где L, a, b – координаты цвета в пространстве Lab для объекта и фона [5]. Чем меньше значение ΔE, тем ближе объект по цвету к окружению. Это не означает, что объект должен полностью сливаться с фоном; напротив, он может иметь собственную цветовую индивидуальность. Но при этом его отличие не должно нарушать единство сцены. В задачах визуальных эффектов важна не одинаковость цветов, а их правдоподобная совместимость.

Практическая реализация в Nuke и Maya

В программе Maya цветотональное согласование начинается уже на этапе подготовки материала к рендеру. При настройке материалов следует учитывать не только отражающую способность поверхности, но и то, как объект будет вести себя в итоговом освещении. Если объект обрабатывается слишком «чисто» и равномерно, без учета цветовых рефлексов и атмосферного влияния, он будет выглядеть отделенным от реальной сцены. Поэтому полезно предварительно сопоставить свойства объекта с кадром: определить, находится ли сцена в холодной или теплой гамме, преобладают ли мягкие или жесткие тени, насколько сильна общая контрастность изображения. Эти данные позволяют задать материалам более реалистичные параметры и заранее приблизить рендер к итоговому фону.

В Nuke цветотональное согласование удобно выполнять на этапе компоновки сцен, поскольку программа позволяет точно контролировать яркость, контраст, гамму, цветовые сдвиги и локальные коррекции по маске. Здесь особенно важно не допустить грубой обработки, которая разрушит естественность изображения. Коррекция должна быть локализованной: изменять только те зоны, которые действительно требуют подгонки под фон.

На практике это означает использование мягких масок, корректирующих узлов и последовательной проверки результата на нескольких кадрах. Такой подход позволяет избежать эффекта «пластиковой» графики, который часто возникает при чрезмерной цветокоррекции.

Отдельное значение имеет согласование объекта с цветовой температурой кадра. Если съемка выполнена при теплом освещении, а 3D-объект сохраняет нейтральный или холодный оттенок, возникает ощущение разрыва между реальным и синтетическим элементами. Аналогичная проблема возникает при вечернем или ночном освещении, когда фоновое изображение имеет низкую насыщенность и смещенный цветовой баланс. В таких случаях объект необходимо не только подогнать по яркости, но и скорректировать по общей тональности. Визуально это достигается за счет применения цветовых фильтров, изменения баланса белого и подстройки глобального освещения в сцене.

Следует отметить, что цветотональное согласование тесно связано с освещением и рендером, но не совпадает с ними полностью. Освещение определяет, как объект освещается в сцене, а цветотональное согласование отвечает за то, как этот объект воспринимается внутри готового кадра. Иными словами, объект может быть физически корректно освещен, но все равно выглядеть несоответствующим сцене из-за различий в постобработке или из-за особенностей съемочного материала. Поэтому в методике вписывания 3D-объектов цветотональный анализ следует считать самостоятельным контрольным этапом, стоящим после рендера, но до финальной сдачи изображения.

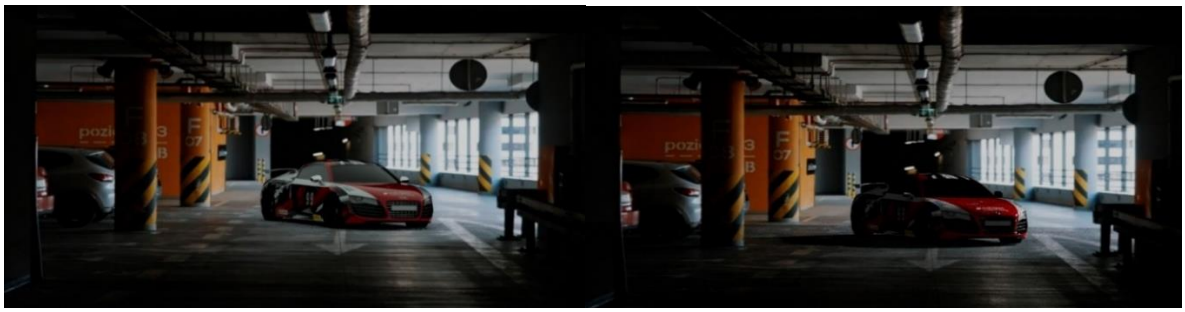


Рис. 1. Сравнение рендера изображения до цветотонального согласования (слева) и после (справа)

Практический результат такого подхода состоит в повышении визуальной достоверности сцены. Зритель не анализирует отдельные технические параметры, но мгновенно замечает несоответствие по свету, тону и цвету. Если же объект точно совпадает с общим визуальным строем кадра, он воспринимается как естественная часть сцены. Именно это и является конечной

целью методики вписывания 3D-объектов в изображенное пространство. В этом смысле цветотональное согласование выступает не вспомогательной, а обязательной составляющей процесса интеграции.

Заключение

Успешное совмещение 3D-объекта с видеорядом требует не только точного трекинга и корректного рендера, но и тщательной подгонки по яркости, цвету и контрасту. Предложенные формулы позволяют точно подобрать значения для наилучшего соответствия объекта и фона, а практическую последовательность действий эффективно использовать при работе в Nuke и Maya. Рассмотренный подход может быть включен в общую методику вписывания трехмерных объектов в изображенное пространство и использован как основа для последующей разработки более полной технологической схемы.

Список используемых источников

1. Искусство и наука цифрового композитинга / Р. Бринкманн. М.: ДМК Пресс, 2013. 448 с.

2. Multiple View Geometry in Computer Vision / R. Hartley, A. Zisserman. 2nd ed. ambridge: Cambridge University Press, 2004. – 655 p.

3. ITU-R BT.709. Parameter values for the HDTV standards for production and international programme exchange. – Geneva: International Telecommunication Union, 2015.

4. Рендеринг на основе законов физики. От теории к практике / М. Фарр, В. Джейкоб, Г. Хамфрис. М.: ДМК Пресс, 2023. 1024 с.

5. CIE 1976 Lab Colour Space. Colorimetry Part 4: CIE 1976 Lab* Colour space. Vienna: International Commission on Illumination (CIE), 2007.

УДК 004.725.2

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ SDN В СЕТЯХ 6G И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Шиманчик С. Г. (студент группы МЗС-2512 СПбГУТ), shimanchik.sg@sut.ru
Ушаков И. А. (к.т.н., доцент, и. о. зав. кафедрой ИБКС, доцент кафедры ИКС СПбГУТ)

Развитие сетей 6G требует кратного роста пропускной способности и снижения задержек. В условиях роста числа подключенных устройств и ужесточения требований к безопасности традиционные сетевые архитектуры становятся неэффективными. Ключевым решением выступает технология программно-определяемых сетей (SDN), которая обеспечивает гибкое управление ресурсами через программные интерфейсы. Отделение плоскости управления от плоскости данных позволяет динамически переконфигурировать инфраструктуру в реальном времени без вмешательства в физическое оборудование. Цель работы – определить соответствие архитектуры SDN экстремальным требованиям сетей 6G путем комплексного изучения ее ключевых механизмов управления трафиком и безопасности, подкрепленного экспериментальной оценкой производительности.

сети 6G, программно-определяемых сетей (SDN – Software-Defined Networking), зеркалирование, пропускная способность, задержка, потери

Развитие телекоммуникационных сетей шестого поколения (6G) предполагает кратное увеличение пропускной способности и снижение задержек передачи данных. В условиях экспоненциального роста количества подключенных устройств, появления новых сервисов и требований к гарантированной безопасности, традиционные подходы к построению сетей становятся недостаточными.

Одной из ключевых становится технология программно-определяемых сетей (SDN – Software-Defined Networking), которая обеспечивает гибкость, масштабируемость и управление сетевыми ресурсами через программные интерфейсы. Технология SDN предоставляет возможность разделения плоскостей управления и передачи друг от друга, тем самым предоставляя возможность динамического конфигурирования сетевой инфраструктуры без вмешательства в физическое оборудование.

В статье рассмотрена возможность применения технологии SDN в сетях 6G. Описаны основные механизмы логической сегментации, а также рассмотрено управление ip-адресацией, обеспечение отказоустойчивости

маршрутизации и реализация микросегментации. В ходе работы проведено нагрузочное тестирование технологии SDN в системе виртуализации, для проверки возможности использования SDN в сетях 6G.

Технология SDN реализована с помощью стека компонентов OVS/OVN. В качестве виртуального коммутатора, работающего на канальном уровне, выступает компонент Open vSwitch (OVS). Он устанавливается на каждом хосте в системе виртуализации. Коммутатор Open vSwitch обеспечивает коммутацию трафика между виртуальными машинами, а также поддерживает изучение MAC-адресов, агрегацию каналов, создание таблиц коммутации и VLAN [1]. OVN в данном стеке является дополнением OVS, позволяет охватить множество хостов виртуализации [2]. Он работает на сетевом уровне, тем самым обеспечивая распределенную маршрутизацию между созданными сетями.

Архитектура OVN использует две базы данных. Северная база данных содержит информацию о логической структуре сети, которая задается в веб-интерфейсе системы виртуализации. Южная база данных хранит информацию о физической реализации заданных объектов.

На каждом хосте виртуализации функционирует агент ovn-controller, который согласовывает состояния между указанными БД и преобразует логическую архитектуру в конкретные правила для Open vSwitch. Для связи OVN с платформой виртуализации применяется провайдер ovirt-provider-ovn.

Механизмы логической сегментации

Сегментация сети – это разделение сетевой инфраструктуры на изолированные широковещательные домены, хосты которых находятся в одной подсети и могут взаимодействовать друг с другом без маршрутизатора.

В традиционном подходе сеть делится на VLAN (Virtual Local Area Network). Каждый VLAN имеет уникальный идентификатор (от 1 до 4094) и требует конфигурации транков на физических коммутаторах для передачи тегированного трафика между коммутаторами [3].

В программно-определяемой сети понятие VLAN отсутствует. Вместо него используются логические сети (логические коммутаторы). Благодаря наличию логической сети, сегментация реализуется без trunk-соединений с коммутаторами инфраструктуры предприятия. Достаточно иметь сетевую связность между хостами кластера через сеть управления.

Каждая логическая сеть имеет уникальный идентификатор в базе данных OVN. При отправке пакета виртуальной машиной, ovn-controller на хосте добавляет к пакету заголовок GENEVE, который содержит идентификатор логической сети. При приеме пакета на другом хосте, ovn-controller проверяет идентификатор и доставляет пакет только тем виртуальным машинам, которые подключены к соответствующей логической сети.

Широковещательные запросы (broadcast) и многоадресный трафик (multicast) доставляются всем виртуальным машинам в пределах одной логической сети. Это необходимо для работы протоколов ARP, DHCP и других протоколов канального уровня. Широковещательный трафик не выходит за пределы логической сети.

Механизм обеспечения безопасности порта используется для контроля используемых виртуальной машиной IP и MAC-адресов. Это базовый уровень защиты, который предотвращает спуфинг (подмену) адресов.

Правило безопасности порта содержит список адресов, которыми ВМ может пользоваться для отправки и получения одноадресного (unicast) трафика. Широковещательный (broadcast) и многоадресный (multicast) трафики не фильтруются – они всегда разрешены.

Когда виртуальная машина отправляет пакет, OVN проверяет соответствие MAC-адреса источника разрешенному в правиле безопасности, а также соответствие IP-адреса источника разрешенному в правиле безопасности (в случае если он указан). Если проверка не пройдена, пакет отбрасывается [4].

Правила безопасности порта могут быть использованы совместно с правилами, указанными в группах безопасности. При этом:

- правила безопасности порта работают на уровне адресов (контроль MAC/IP);
- группы безопасности работают на уровне сетевого трафика (контроль протоколов, портов, направлений).

Оба механизма применяются последовательно, обеспечивая многоуровневую защиту.

Логический маршрутизатор может преобразовывать трафик между логическими сетями и внешней сетью. Преобразование трафика между логическими сетями не производится – они взаимодействуют напрямую.

Существует четыре типа трансляции адресов:

1. NAT (Network Address Translation)

Правило NAT осуществляет преобразование исходящего и входящего трафика за счет сопоставления «один к одному» внутреннего адреса с внешним адресом.

Для проходящих пакетов используется замена полей IP-адресов:

1. Исходящий пакет: адрес источника заменяется с внутреннего на внешний.

2. Входящий пакет: адрес назначения заменяется с внешнего на внутренний.

2. SNAT (Source NAT)

Правило SNAT осуществляет преобразование исходящего трафика за счет замены IPv4-поля адреса источника пакетов на указанный внешний адрес. В результате применения трансляции, внешний сетевой узел воспринимает исходящий пакет как отправленный с адреса логического маршрутизатора. Для обеспечения корректной доставки ответного трафика система автоматически выполняет модификацию номера порта источника в заголовке транспортного уровня. Декапсуляция и обратная подстановка исходных адресов для входящих пакетов осуществляются прозрачно для конечных узлов. Все операции преобразования трафика выполняются на том хосте виртуализации, где в текущий момент активен логический маршрутизатор.

3. DNAT (Destination NAT)

Правило DNAT осуществляет преобразование входящего трафика за счет замены IPv4-поля адреса назначения пакетов на указанный IP-адрес внутренней сети. Обратное преобразование ответных пакетов производится автоматически. Преобразование производится на хосте, к которому в данный момент прикреплен логический маршрутизатор.

4. FIP (Floating IP)

Правило FIP обеспечивает преобразование исходящего и входящего трафика за счет сопоставления «один к одному» внутреннего адреса с внешним адресом. Трансляция осуществляется децентрализованно, преобразование производится на том хосте, где расположена виртуальная машина, а не на хосте с маршрутизатором.

Микросегментация представляет собой технологию сетевой безопасности, позволяющую логически разделять объекты виртуализации на сегменты на основе правил сетевого трафика. Группы безопасности выступают контейнерами для этих правил, которые присваиваются логическим портам. Каждое правило безопасности содержит критерии проверки заголовков па-

кетов уровней L3 и L4, включая направление трафика, тип действия и приоритет. Действия могут разрешать трафик с отслеживанием состояния или без него, либо запрещать его с уведомлением или без. Приоритет определяет очередность обработки, причем запрещающие правила всегда имеют преимущество над разрешающими, а обработка завершается глобальным правилом блокировки всего остального трафика [5].

Источниками правил могут выступать другие группы безопасности, адресные пулы или конкретные IP-адреса, а фильтры позволяют уточнять правила по протоколам и портам. Создание правил осуществляется через генератор, формирующий комплексные правила из атомарных, где порядок исполнения зависит от настроек приоритета, а не от порядкового номера в имени. Управление группами безопасности включает их создание и удаление, при этом удаление невозможно, пока к группе подключены порты.

Для аудита предусмотрено логирование срабатывания правил на хостах виртуализации с ограничением частоты записей и возможностью поиска по уникальному идентификатору правила. Настройка уровней логирования и лимитов производится в интерфейсе управления. Применение защиты требует включения поддержки групп безопасности на уровне сети, назначения групп конкретным портам и прикрепления виртуальных машин к соответствующим группам безопасности через портал администрирования.

Подсистема управляемых сетей поддерживает зеркалирование трафика логических портов для диагностики сетевых проблем, анализа системами IDS/IPS, аудита безопасности и мониторинга производительности, при этом операция зеркалирования потребляет ресурсы хостов виртуализации. Зеркалирование работает с портами-источниками (откуда копируются фреймы) и портами-слушателями (куда направляются копии), поддерживая фильтрацию по направлению трафика: входящий, исходящий или оба.

Реализовано два типа зеркалирования.

Локальное зеркалирование копирует трафик на логический порт-слушатель, расположенный на том же хосте виртуализации, что требует наличия приемника на всех хостах домена миграции ВМ, иначе зеркалирование не выполнится.

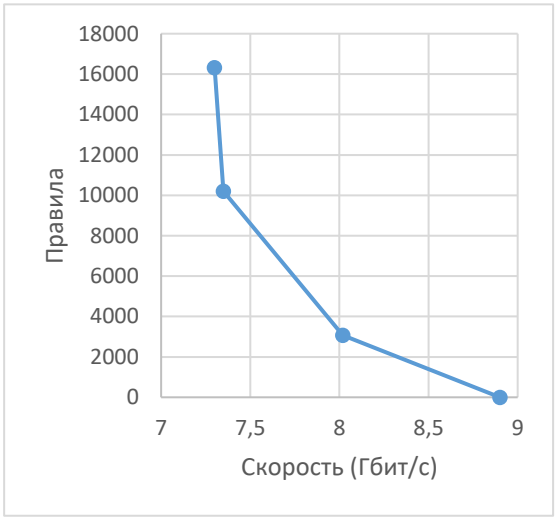
Удаленное зеркалирование передает копии трафика на внешний IP-адрес по протоколам GRE или ERSPAN, используя 32-битный идентификатор ключа (GRE Key) для тегирования туннелей.

Инструмент «Монитор сетевой активности» позволяет отслеживать трафик виртуальных машин в реальном времени для проверки соблюдения

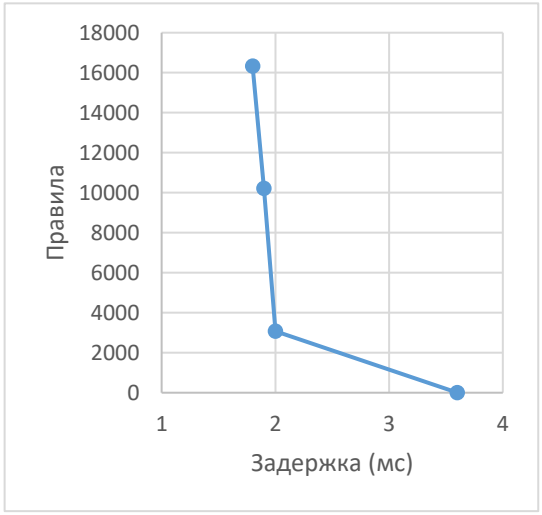
правил безопасности, диагностики сетевых взаимодействий, выявления аномалий и отладки конфигураций. Мониторинг работает только с трафиком, соответствующим правилам микросегментации, и при создании сессии типа ACL поддерживает наблюдение за одним портом без возможности запуска нескольких сессий одновременно.

Для оценки критериев SDN было проведено нагрузочное тестирование под различным количеством правил.

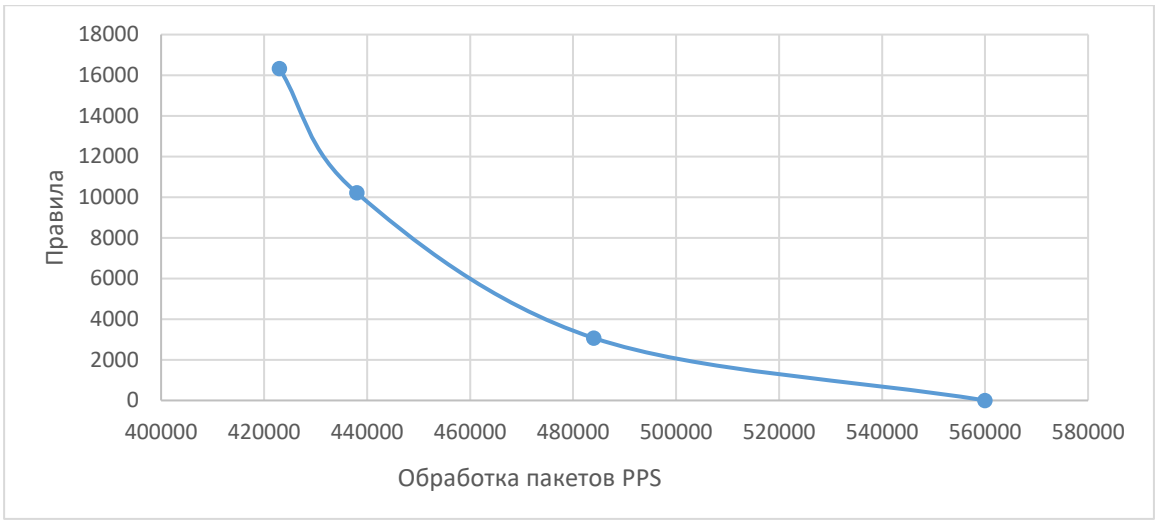
Основные метрики: пропускная способность (TX), PPS, задержка, потери пакетов. На рисунке 1(а, б, в) приведены основные результаты тестирования производительности сети в зависимости от количества правил.



а



б



в

Рис. 1а. График зависимости пропускной способности от количества правил, 1б – График зависимости задержки от количества правил, 1в - График зависимости PPS от количества правил

Потери пакетов отсутствуют при любом числе правил. Независимость показателя потерь от количества активных правил указывает на то, что алгоритмы обработки трафика в OVN/OVS не вносят дополнительной нагрузки, влияющей на целостность потока.

В рамках исследования было проведено нагрузочное тестирование подсистемы управляемых сетей zVirt в условиях отсутствия фоновой нагрузки. Ключевые метрики представлены ниже:

Сравнительный анализ представлен в таблице 1.

Таблица 1. Сравнение требований к сетям 6G и полученных результатов.

Метрика	Требование 6G	Результат SDN	Отклонение
Задержка	≤ 100 мкс	1200–3600 мкс	×12–36 выше
Пропускная способность	≥ 1000 Гбит/с	7,3–8,9 Гбит/с	×112–137 ниже
Плотность сессий	~10^7 подключений	~36 тыс. на хост	×277 ниже
Обработка пакетов	≥ 100 млн PPS	~560 тыс. PPS	×178 ниже

На основании представленной сравнительной таблицы можно сделать вывод, текущая реализация архитектуры SDN не соответствует базовым требованиям сетей шестого поколения (6G) по ключевым метрикам производительности.

Заключение

В данной работе представлены результаты выполнения практического тестирования технологии SDN. Были протестированы основные метрики для анализа возможности применения SDN в сетях 6G.

В архитектуре SDN реализован полный функционал управления сетевыми ресурсами. Внедренные механизмы безопасности обеспечивают многоуровневую защиту за счет механизма микросегментации. Проведенное нагрузочное тестирование показало стабильность работы технологии SDN системы виртуализации даже при высокой нагрузке. Потери пакетов нулевые при любом количестве правил микросегментации.

Сравнительный анализ ключевых метрик производительности сети демонстрирует несоответствие текущей реализации технологии SDN требованиям сетей 6G. Реализация SDN является перспективной для сетей шестого поколения, однако текущая реализация на базе OVS/OVN не удовлетворяет экстремальным требованиям 6G по производительности. Перспективным

вектором развития является реализация интеграции программных контроллеров с сетевым оборудованием. Такой подход позволит сохранить преимущества программной гибкости и устранить проблему недостаточной физической скорости передачи данных.

Список используемых источников

1. Benzekki K., Software-defined networking (SDN): a survey / K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui // Security and Communication Networks. 2016. Vol. 9(18). pp.5803–5833; URL: https://tesble.com/10.1002/sec.1737.

2. Yiyang Zhou "Research on large-scale container networks in OVN", Proc. SPIE 13397, Fourth International Conference on Green Communication, Network, and Internet of Things (CNIoT 2024), 1339703; URL: https://doi.org/10.1117/12.3052587.

3. Correa Chica J. C., Imbachi J. C., Botero J. F. Security in SDN: A comprehensive survey // Journal of Network and Computer Applications. 2020. Vol. 159. p. 102595. URL: https://colab.ws/articles/10.1016 %2Fj.jnca.2020.102595 (дата обращения: 05.01.2026)

4. Захаров А. А., Попов Е. Ф., Фучко М. М. Аспекты информационной безопасности архитектуры SDN // Вестник СибГУТИ. 2016. № 1 (33). URL: https://cyberleninka.ru/article/n/aspekty-informatsionnoy-bezopasnosti-arhitektury-sdn (дата обращения: 01.02.2026).

5. Сахаров Д. В. Защищенная модель программно-определяемой сети в среде виртуализации KVM / Д. В. Сахаров, А. В. Красов, И. А. Ушаков, Г. А. Орлов // Электросвязь. 2020. № 3. С. 26–32. DOI: 10.34832/ELSV.2020.4.3.004.

УДК 621.39

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ DBA-АЛГОРИТМОВ ДЛЯ СЕТИ GPON С АСИММЕТРИЧНЫМ ТРАФИКОМ В МНОГОКВАРТИРНОМ ДОМЕ

В. С. Философов (студент группы ОБ-26с СПбГУТ), filosofov.vs@sut.ru

В статье выполнен сравнительный анализ трех алгоритмов динамического распределения полосы пропускания (DBA) – Fixed, Limited и Status Reporting (SR-DBA) – для сети GPON в условиях асимметричной нагрузки абонентов. В представленной работе проведена количественная оценка эффективности алгоритмов применительно к многоквартирному жилому комплексу в городе Кудрово (Всеволожский район Ленинградской области). Предложен усовершенствованный подход к распределению ресурсов, учитывающий приоритеты трафика и текущую загрузку сети. Полученные результаты позволяют повысить эффективность использования сетевых ресурсов и улучшить показатели качества обслуживания. Рассмотрена типичная конфигурация сети: OLT Huawei MA5600T, ONU Huawei EchoLife HG8245, каскад сплиттеров 1:16+1:4 (64 ONU на один PON-порт).

GPON, DBA, Fixed, Limited, Status Reporting, асимметричный трафик, Кудрово, MA5600T

Введение

Главная проблема GPON-сетей – разделяемый восходящий канал, требующий грамотного распределения пропускной способности. Для этого применяют механизмы динамического выделения полосы (DBA), подстраивающиеся под нагрузку. Особенно это актуально в густонаселенных районах, например в кудровских многоэтажках. Там одни пользователи («тяжелые») создают пиковый трафик (видеозвонки, торренты), другие («легкие») – минимальный. Без эффективного механизма распределения восходящего канала «тяжелые» пользователи могут монополизировать временные слоты, вызывая рост задержек для всех.

GPON: ключевые характеристики и особенности применения в многоквартирных домах

GPON (Gigabit-capable Passive Optical Network) – одна из основных технологий пассивных оптических сетей, разработанная консорциумом FSAN и принятая ITU-T [1].

Архитектура GPON (рис. 1). Архитектура GPON строится по схеме «OLT → пассивный сплиттер → до 64 ONU», скорость восходящего канала – 1,25 Гбит/с, дальность – до 20 км.

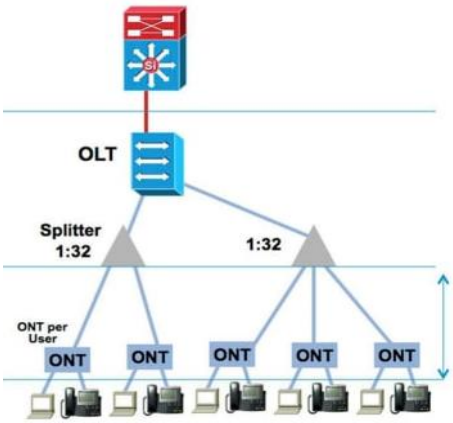


Рис. 1 – Архитектура GPON

Существует несколько особенностей GPON:

GPON использует метод инкапсуляции GEM (GPON Encapsulation Method), поддерживающий фрагментацию кадров и гибкую передачу Ethernet/TDM-трафика с QoS. Передача ведется на трех длинах волн: 1490 нм (данные вниз), 1310 нм (данные вверх) и 1550 нм (аналоговое/цифровое ТВ). Для защиты от ошибок применяется прямая коррекция FEC, а шифрование AES (128-256 бит) обеспечивает безопасность.

Механизмы динамического распределения полосы пропускания (DBA) в GPON: Fixed, Limited и Status Reporting

DBA управляется OLT и распределяет восходящую полосу между ONU на основе отчетов об их буферах [2]. В OLT MA5600T реализованы три типа DBA (табл. 1).

Fixed DBA – OLT выделяет фиксированную полосу независимо от потребности ONU. Используется для трафика, критичного к задержкам (VoIP, TDM).

Limited DBA – OLT ограничивает максимальный размер окна: выделяемая полоса = min(запрошенная, W_max).

Status Reporting DBA – OLT получает от ONU точные отчеты о загрузке. Если суммарный запрос превышает емкость цикла, полоса распределяется пропорционально запросам, что обеспечивает высокую утилизацию и минимальные задержки.

ТАБЛИЦА 1. Сравнительный анализ подходов DBA

Fixed DBA	Limited DBA	Status Reporting DBA
Принцип работы		
OLT выделяет каждой ONT фиксированный и неизменный временной слот. Даже если ONT не передает данные, слот остается пустым и не может быть использован другими.	OLT выделяет ONT полосу, но ограничивает максимальный размер одного выделяемого окна. Это предотвращает монополизацию канала одной ONT и уменьшает задержки.	ONT сама сообщает OLT о количестве данных в своем буфере. OLT на основе этих отчетов динамически выделяет полосу, точно соответствующую текущей потребности.
Использование полосы		
Очень низкое. Значительная часть пропускной способности теряется впустую.	Высокое. Полоса используется более эффективно за счет динамического перераспределения, но с контролем.	Очень высокое (достигается >80 % утилизации). Полоса выделяется точно под потребности, что минимизирует потери.
Латентность		
Минимальная для назначенного трафика. Для незапланированных всплесков – высокая (до ~100 мс).	Умеренная. Алгоритм обеспечивает компромисс между задержкой и эффективностью.	Очень низкая (в современных реализациях <10 мс). Быстрая реакция на изменение потребностей.
Преимущества		
Простота и предсказуемость. Идеально для постоянного трафика с жесткими требованиями к задержке.	Хороший баланс между эффективностью и справедливостью. Предотвращает захват канала одной ONT.	Максимальная эффективность и гибкость. Оптимально для пульсирующего трафика (например, веб-серфинг).
Недостатки		
Крайне неэффективно. Не подходит для пульсирующего трафика.	Может быть неоптимальным при сильных всплесках трафика.	Создает дополнительный служебный трафик для отчетов. Более сложная реализация.

Параметры сети и характеристика трафика

Рассматривается один GPONпорт OLT MA5600T, к которому через каскад сплиттеров 1:16 (первый уровень, в распределительном шкафу) и 1:4

(второй уровень, в подъезде) подключено 64 ONU HG8245 – полное использование емкости порта. Скорость восходящего канала – 1,25 Гбит/с (GPON). Длительность цикла DBA – 2 мс.

Трафик моделируется как смесь двух типов пользователей:

- «Тяжелые» (20 % от общего числа, 13 ONU): средняя нагрузка 80 Мбит/с (ON/OFF модель: 10 мс передачи на пиковой скорости 100 Мбит/с, затем 2,5 мс паузы).
- «Легкие» (80 %, 51 ONU): средняя нагрузка 5 Мбит/с (пуассоновский поток, пакеты 500 байт).
- Общая предлагаемая нагрузка варьируется от 0,2 до 0,95 от пропускной способности канала (коэффициент загрузки ρ). Буфер ONU – 1 Мбайт, [2].

Методика и результаты аналитической оценки

Для количественного сравнения алгоритмов DBA в условиях сети г. Кудрово использованы аналитические зависимости. Для Limited выявлена линейная зависимость задержки от числа ONU. SR-DBA при нагрузке выше (ρ>0,8) и асимметрии дает выигрыш в задержке до 30-40 % против Limited. Fixed DBA – по сути статическое TDM. Алгоритм Fixed DBA оценивался аналитически как статическое TDM-распределение. Полученные в результате расчетов значения сведены в табл. 2.

ТАБЛИЦА 2. Средняя задержка (мс) для 64 ONU

Алгоритм	ρ=0,5	ρ=0,8	ρ=0,95
Fixed	12,3	35,7	98,4
Limited	5,2	14,8	32,5
SR-DBA	4,1	10,2	14,3

Исходя из полученных данных, алгоритм Fixed DBA демонстрирует неприемлемо высокие задержки уже при ρ = 0,5 из-за статического выделения. Limited DBA значительно лучше, однако при ρ = 0,95 задержка достигает 32,5 мс. Алгоритм *Status Reporting DBA* обеспечивает наименьшую задержку (14,3 мс при ρ = 0,95) и наиболее эффективное использование канала [3, 4].

Для жилых домов Кудрово, где в вечерние часы нагрузка может достигать ρ = 0,9, применение SR-DBA является предпочтительным.

Рекомендации для настройки оборудования

На основе проведенного анализа для OLT Huawei MA5600T, установленного в узле связи г. Кудрово, рекомендуется:

- Использовать режим SR-DBA с максимальным окном G_max = 2 Мбайт и циклом 2 мс.
- Для особо загруженных домов (ЖК «Новое Кудрово», где плотность абонентов максимальна), настроить приоритетные очереди (QoS) совместно с SR-DBA.

Заключение

В работе выполнен аналитический обзор трех алгоритмов DBA для GPON-сети жилого района на примере г. Кудрово при полном заполнении порта (64 ONU, каскад сплиттеров 1:16+1:4). На основе аналитических зависимостей из показано, что алгоритм Status Reporting DBA превосходит Fixed и Limited по задержкам и эффективности использования канала, особенно при высокой нагрузке (ρ>0,8). Полученные оценки могут быть использованы при настройке оборудования MA5600T в спроектированной сети. Перспективным направлением является комбинирование SR-DBA с приоритизацией трафика для поддержки услуг реального времени.

Список используемых источников

1. Кодиров Ф. Э., Ачилова Ф. К. «Технология GPON». Сборник научных трудов Тюменского государственного университета, 2018. С. 176-181.

2. Симонов В. С. Эффективность применения алгоритмов динамического распределения полосы пропускания в пассивной оптической сети связи / В. С. Симонов, А. А. Малявко // Наука. Технологии. Инновации: сб. науч. тр.: в 9 ч., Новосибирск, 2-6 дек. 2019 г. Новосибирск: Изд-во НГТУ, 2019. Ч. 1. С. 108-110.

3. Kramer G., Mukherjee B., Pesavento G. IPACT: Динамический протокол для Ethernet PON (EPON) // Журнал IEEE по связи. 2002. С. 74-80.

4. McGarry M.P., Maier M., Reisslein M. Ethernet PONs: Динамическое распределение полосы пропускания // Журнал IEEE по связи. 2004. Vol. 42. № 8. С. 40-48.

Статья представлена научным руководителем, доктором физико-математических наук, профессором кафедры ОКСС С. А. Роговым.

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА

УДК 621.396.96

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИСПОЛЬЗОВАНИЯ ЛЧМ СИГНАЛОВ В КАЧЕСТВЕ ПОМЕХ В КАНАЛЕ GSM 900

В. В. Авдеев (студент гр. МРД-2521 СПбГУТ), avdeev.vv@sut.ru

В работе представлены результаты имитационного моделирования воздействия шести типов ЛЧМ-помех на канал связи GSM 900 с GMSK-модуляцией. Определены пороговые значения отношения сигнал/помеха (SIR), при которых вероятность битовой ошибки (BER) превышает 0,1 %. Показано, что наиболее эффективной является помеха с переключением несущей (SingleLFM_Hopping), требующая наименьшей мощности для нарушения связи.

GSM 900, GMSK, ЛЧМ-помеха, BER, SIR, имитационное моделирование, помехоустойчивость

Помехи с линейной частотной модуляцией (ЛЧМ) широко применяются в системах радиоэлектронной борьбы благодаря возможности концентрации мощности в заданной полосе частот и адаптации формы спектра [1]. В отличие от шумовых помех, ЛЧМ-сигналы требуют меньшей мощности для нарушения связи, что делает их эффективным инструментом подавления. Однако сравнительный анализ различных структур ЛЧМ-сигналов (одиночные, многокомпонентные, с переключением несущей и др.) при воздействии на реальные стандарты связи проведен недостаточно. В качестве модельного канала выбран стандарт GSM 900, который, несмотря на развитие 4G/5G, остается широко распространенным и уязвимым для преднамеренных помех. Цель работы – оценить влияние шести типов ЛЧМ-помех на вероятность битовой ошибки (BER) в канале GSM 900 и определить пороговые отношения сигнал/помеха (SIR).

Модель GSM-900 реализована в соответствии со стандартом 3GPP TS 45.001. Согласно нормативным документам [2, 3], допустимый остаточный

коэффициент битовых ошибок (RBER) для класса II в речевом канале TCH/FS при статических условиях составляет 2 %. Однако для обеспечения надежной передачи данных в реальной городской среде (с учетом замираний и интерференции) в работе используется более жесткий порог BER = 0.1 % как консервативная оценка качества связи.

GMSK (Gaussian Minimum Shift Keying) формируется путем пропускания NRZ сигнала через гауссовский фильтр с последующей частотной модуляцией. Комплексная огибающая сигнала имеет вид:

$$s(t) = \exp\left(j \int_{-\infty}^{t} \sum_{k} a_k g(\tau - kT_b) d\tau\right),$$

где $a_k \in \{-1,+1\}$ – биполярные символы, $g(t)$– гауссовский импульс, $T_b = \frac{1}{R_b}$. Демодуляция осуществляется согласованным фильтром и последующим дифференциальным декодированием.

Принимаемый сигнал представляет собой сумму полезного сигнала, помехи и шума $r(t) = s(t) + j(t) + n(t)$, где $j(t)$ – сигнал помехи, $n(t)$ – аддитивный белый гауссовский шум (AWGN) с нулевым средним и дисперсией $\sigma^2 = \frac{P_n}{2}$.

Отношение сигнал-помеха (SIR) определяется как [4]:

$$SIR(\text{дБ}) = 10 \log_{10} \frac{P_{\text{сигнала}}}{P_{\text{помеха}}}.$$

В моделировании мощность полезного сигнала нормирована к единице ($P_{\text{сигнала}}$=1), а мощность помехи варьируется в соответствии с заданным SIR.

Метрика оценки качества связи – вероятность битовой ошибки (BER):

$$BER = \frac{N_{\text{ошибок}}}{N_{\text{общее}}}.$$

Каждая помеха описывается комплексной огибающей $j(t)$ с мощностью $P_{\text{помеха}}$. Все помехи имеют одинаковую среднюю мощность на входе приемника, что позволяет сравнивать их при фиксированном SIR.

- SingleLFM: одиночный чирп, частота которого линейно изменяется от f_0 до $f_0 + B$ за время T_{frame}. Параметры: $f_0 = 0$, $B = 200$ кГц.

● MultiLFM: сумма трех независимых LFM сигналов с центральными частотами −100 кГц, 0 и +100 кГц, каждый с полосой $B = 200$ кГц. Амплитуда каждого компонента уменьшена в $\sqrt{3}$ раз для сохранения суммарной мощности.

● SignalLike: Сигналоподобная помеха, имитирующая структуру GSM-сигнала (GMSK-модуляция, BT = 0.3) со случайными битами данных.

● SingleLFM_Hopping: Одиночный ЛЧМ-сигнал с переключением несущей частоты между тремя значениями в течение кадра. В отличие от MultiLFM, вся мощность концентрируется в одном сигнале в каждый момент времени.

● MultiLFM_UpDown: сумма трех чирпов, каждый из которых сначала возрастает от f_0 до $f_0 + \frac{B}{2}$, а затем убывает до $f_0 - \frac{B}{2}$.

● FullUpDown_Single: один чирп, который за время T_{frame} поднимается от f_0 до $f_0 + \frac{B}{2}$ и опускается обратно до $f_0 - \frac{B}{2}$.

Модель реализована в среде MATLAB с использованием библиотек Communications Toolbox. Алгоритм включает генерацию случайных битов, GMSK модуляцию, формирование помехи заданного типа, сложение с аддитивным белым гауссовским шумом (AWGN), GMSK демодуляцию и расчет BER с учетом возможной задержки и инверсии (оптимальное сравнение битов).

Для каждого сочетания SNR (5, 10, 15, 20 дБ) и SIR (от –10 до +10 дБ с шагом 1 дБ) выполнено усреднение по 100 независимым кадрам. Значение SNR = 10 дБ выбрано как типичное для городской среды согласно 3GPP TS 45.001, где уровень сигнала близок к порогу чувствительности приемника (–104 дБм), а суммарные потери и интерференция снижают эффективное отношение сигнал/шум до 10–15 дБ. Использование AWGN в качестве базовой модели канала обеспечивает корректное сравнение различных типов LFM помех.

На рисунке 1 представлены зависимости BER от SIR для всех шести типов помех при SNR = 10 дБ. Дополнительные горизонтальные линии соответствуют уровням BER = 1 % и BER = 0,1 %.

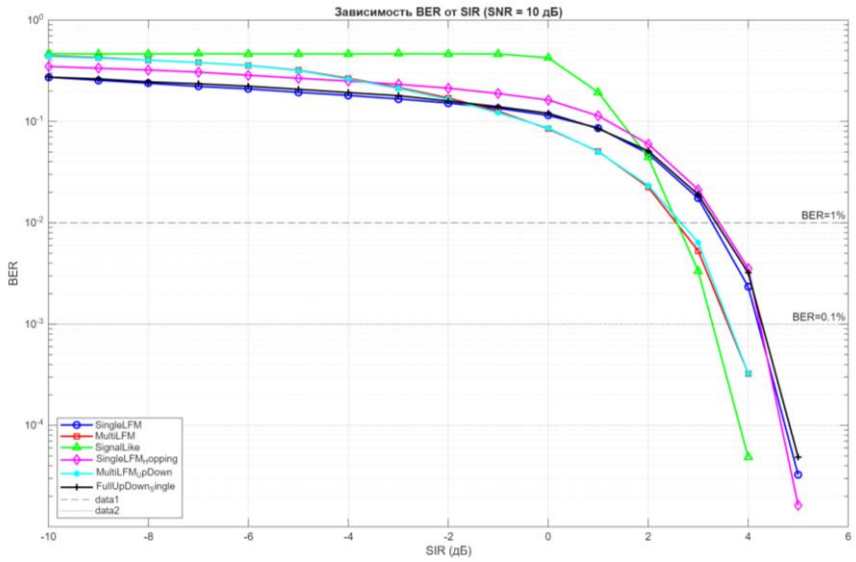


Рис. 1. Зависимости BER от SIR при фиксированном SNR

Анализ графика показывает наличие двух зон эффективности:

1. SIR < 2 дБ (помеха мощнее или сравнима с сигналом): помеха типа SignalLike демонстрирует наивысший BER (0.35–0.47), что объясняется структурным сходством с полезным сигналом.

2. SIR > 2 дБ (сигнал мощнее помехи): помеха типа SingleLFM_Hopping становится наиболее эффективной, обеспечивая BER = 0.003–0.06 при SIR = 2–4 дБ.

В таблице 1 приведены пороговые значения SIR, при которых BER превышает 0,1 % (неудовлетворительное качество связи).

ТАБЛИЦА 1. Пороговые значения SIR

Тип помехи	Порог SIR (дБ)
SingleLFM_Hopping	4,262
FullUpDown_Single	4,249
SingleLFM	4,206
MultiLFM_UpDown	3,646
MultiLFM	3,509
SignalLike	3,217

Чем выше порог SIR, тем меньшая мощность помехи требуется для превышения BER > 0,1 %. Следовательно, SingleLFM_Hopping является самой эффективной помехой, так как имеет наибольший порог. SignalLike оказалась наименее эффективной.

На рисунке 2 показаны зависимости BER от SIR для различных значений SNR. Видно, что при SIR < 0 дБ влияние SNR незначительно – помеха доминирует над шумом. При SIR > 4 дБ увеличение SNR приводит к быстрому восстановлению связи.

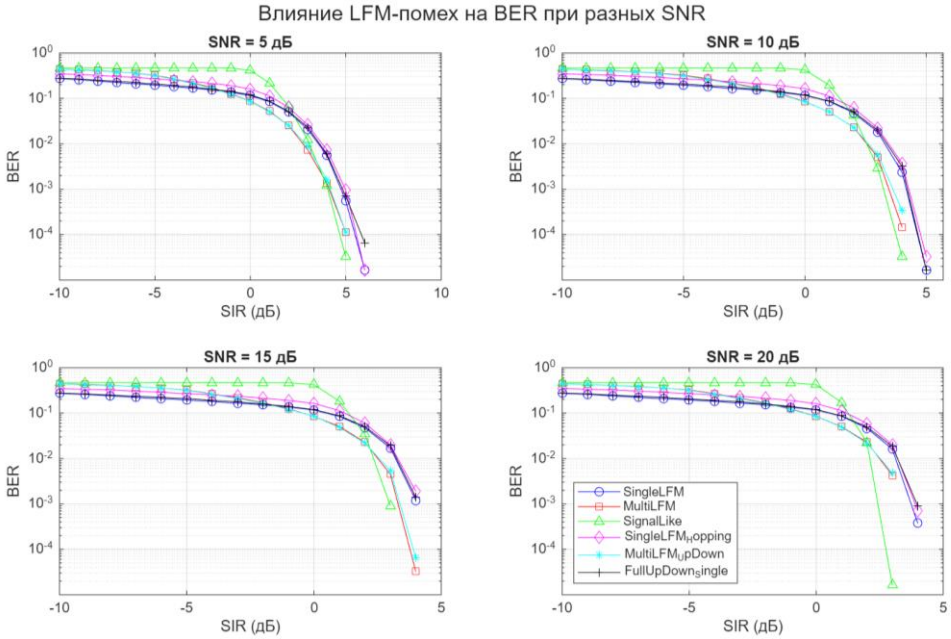


Рис. 2. Зависимость BER от SIR для различных значений SNR

Полученные результаты позволяют сделать несколько важных выводов:

1. SingleLFM_Hopping оказалась самой опасной помехой, потому что она сочетает широкую полосу (переключение между тремя частотами) и сохранение пиковой мощности (один генератор, не деленный на компоненты). В результате равномерно «размазывается» энергия по спектру полезного сигнала, создавая максимальные фазовые искажения, которые демодулятор не может полностью компенсировать.

2. Помеха SignalLike, имеющая ту же модуляцию, что и полезный сигнал, оказалась наименее эффективной. Согласованный фильтр GMSK-демодулятора настроен именно на форму сигнала GMSK. Помеха, представляющая собой другой GMSK-сигнал, частично коррелирует с полезным сигналом, и демодулятор способен ее частично подавить. В отличие от широкополосных LFM-помех, которые создают не скомпенсированные флуктуации фазы.

На практике наиболее выгодно использовать помеху SingleLFM_Hopping, так как она требует наименьшей мощности для срыва связи. Для разработчика систем защиты – необходимо предусмотреть меры против таких широкополосных скачкообразных помех.

Таким образом, в работе разработана имитационная модель канала GSM 900 с GMSK-модуляцией и проведен сравнительный анализ устойчивости системы к шести типам LFM-помех. Основные результаты:

1. Наиболее эффективной (требующей наименьшей мощности) помехой является SingleLFM_Hopping, порог SIR = 4,3 дБ при SNR = 10 дБ. Это делает ее предпочтительной для систем с ограниченной мощностью (БПЛА, портативные станции РЭБ).

2. Наименее эффективной оказалась SignalLike (GMSK со случайными данными), порог SIR = 3,2 дБ.

3. При увеличении SNR пороговые значения SIR снижаются, но относительное ранжирование помех сохраняется.

Направления дальнейших исследований включают исследование помех против LTE и 5G, учет многолучевого распространения в городской среде, разработка адаптивных помех с машинным обучением.

Список использованных источников

1. Устинов А. А., Ланцов К. В., Оков И. Н. Сравнительный анализ эффективности воздействия помех различной структуры на радиолинию, использующую интерфейс LoRa // Информация и Космос, 2025. № 2.

2. ITU-R SM.337-5, «Frequency sharing between systems in the fixed-satellite service and the fixed service». 2015.

3. РД 45.301-2002. «Руководящий документ отрасли. Средства радиосвязи. Нормы и методы измерений параметров.» Москва, 2002.

4. Приказ Министерства информационных технологий и связи РФ от 12 апреля 2007 г. № 45 «Об утверждении Правил применения базовых станций и ретрансляторов систем подвижной радиотелефонной связи. Часть II. Правила применения подсистем базовых станций и ретрансляторов сетей подвижной радиотелефонной связи стандарта GSM 900/1800».

Статья представлена научным руководителем, доцентом кафедры РТ СПбГУТ, кандидатом технических наук О. А. Симониной.

УДК 621.396.2

ОБЛАСТИ ИСПОЛЬЗОВАНИЯ РЕТРАНСЛЯТОРОВ НА БПЛА

С. М. Авдыш (студент гр. РТ-2511 СПбГУТ), avdysh.sm@sut.ru
М. А. Межевова (ассистент кафедры радиотехники СПбГУТ), mezhevova.ma@sut.ru

Статья посвящена применению беспилотных летательных аппаратов в качестве воздушных ретрансляторов для расширения зоны радиопокрытия. Показано, что ограниченная дальность наземных УКВ-радиостанций в пересеченной местности, лесах и городской застройке может быть преодолена подъемом ретрансляционного оборудования на БПЛА, что увеличивает дальность связи до 150 км и более. Приведены примеры отечественных разработок: «Орлан-10», «Тахион», привязной «Гранад ВА-1000», Z-16RELAY-VR. Обоснован переход от ненаправленных антенн к узконаправленным фазированным и кольцевым решеткам для повышения помехозащищенности и энергоэффективности, а также необходимость компенсации нестабильности БПЛА в полете. Определены области применения: экстренные службы, гражданские задачи.

БПЛА, ретранслятор, радиосвязь, антенные решетки, фазированная антенная решетка (ФАР), кольцевая антенная решетка, мобильный комплекс связи, привязной беспилотный летательный аппарат, УКВ-диапазон

Обеспечение устойчивой радиосвязью удаленных и труднодоступных территорий остается актуальной задачей для экстренных служб и гражданских операторов связи. Традиционные наземные средства связи в УКВ-диапазоне (включающем ОВЧ и УВЧ частоты) обладают существенным недостатком – малой дальностью из-за распространения радиоволн в пределах прямой видимости. Цель данной работы состоит в анализе возможностей применения беспилотных летательных аппаратов (БПЛА) в качестве воздушных ретрансляторов для преодоления этих ограничений. Для достижения цели были поставлены следующие задачи: выявить основные проблемы организации наземной радиосвязи, изучить существующие типы БПЛА и ретрансляционного оборудования, определить технические требования к антенным системам и обозначить перспективные области применения.

Проблема наземной радиосвязи

Дальность связи в УКВ-диапазоне при условии прямой видимости рассчитывается по формуле:

$$R = 4{,}1 \cdot (\sqrt{h_1} + \sqrt{h_2}), \quad (1)$$

где h_1 и h_2 – высоты подъема антенн корреспондентов (в метрах), R – дальность (в километрах).

Для наземных стационарных станций высота антенн редко превышает 30 м, для подвижных узлов – 15 м. В лесистой или горной местности реальная дальность падает до 20–25 км. Этого недостаточно для оперативного управления силами в зонах чрезвычайных ситуаций. Как показано в [1], применение БПЛА позволяет поднять ретранслятор на высоты от сотен метров до нескольких километров, что кратно увеличивает зону радиопокрытия.

Типы БПЛА и ретрансляционного оборудования

В таблице 1 приведены характеристики отечественных разработок, которые могут использоваться в качестве носителей ретрансляторов.

ТАБЛИЦА 1. Примеры БПЛА-ретрансляторов

БПЛА	Тип	Высота висения, м	Масса полезной нагрузки, кг	Время полета	Дальность связи, км
«Орлан-10»	самолетный	6000	5	до 18 ч.	до 120
«Тахион»	самолетный	4000	5	до 6 ч.	до 100
«Гранад ВА-1000»	привязной мульти коптер	100	до 5	неограниченно	до 50
Z-16RELAY-VR	мульти коптер	до 500	2	40 мин.	до 40

Привязные БПЛА, такие как «Гранад ВА-1000», имеют юридическое преимущество: полеты до 150 м не требуют специальных разрешений, а питание по кабелю обеспечивает неограниченное время работы. Самолетные БПЛА («Орлан-10», «Тахион») обеспечивают большую дальность и продолжительность полета, но нуждаются во взлетно-посадочной полосе или катапульте. Мультикоптеры способны зависать и точно позиционироваться, однако их время полета ограничено 20–60 минутами [2].

Технические требования к антенным системам

Для эффективной ретрансляции необходим отказ от ненаправленных антенн, обладающих низкой помехозащищенностью. Современные системы

переходят на узконаправленные антенные решетки – фазированные (ФАР) и кольцевые. Это позволяет повысить коэффициент усиления, подавлять помехи и работать в широкой полосе частот [3, 4]. Однако возникает проблема нестабильности: БПЛА постоянно колеблется под воздействием ветра. Чтобы удержать узкий луч антенны точно на наземной станции, требуется прогнозирование положения дрона и электрическое сканирование лучом в реальном времени. В работе [5] предлагается использование кольцевой антенной решетки на основе излучателей Вивальди, которая обеспечивает широкополосность и круговой обзор без механического поворота.

Области применения

На основе проведенного анализа можно выделить две ключевые области гражданского использования ретрансляторов на БПЛА:

1. **Экстренные службы (МВД, МЧС).** Обеспечение связи в зонах чрезвычайных ситуаций, в лесистой и горной местности, при проведении поисково-спасательных операций. Воздушный ретранслятор развертывается за считанные минуты и не зависит от разрушенной наземной инфраструктуры.

2. **Гражданские задачи.** Временное развертывание сетей связи на массовых мероприятиях, обеспечение широкополосного доступа в интернет для удаленных поселков и промышленных объектов.

В результате работы сделаны следующие выводы:

1. Применение БПЛА-ретрансляторов является наиболее эффективным способом оперативного создания зон радиопокрытия на сложной местности, позволяя увеличить дальность связи со стандартных 30–50 км до 120–150 км и более.

2. Необходим системный подход – разработка не отдельного дрона, а единого мобильного комплекса, включающего транспортное средство, БПЛА, наземную станцию питания и ретрансляционное оборудование.

3. Ключевое направление развития – создание интеллектуальных, узконаправленных и энергоэффективных антенных систем (кольцевые и полусферические решетки) для повышения дальности, помехозащищенности и устойчивости связи в условиях нестабильного положения БПЛА.

Список используемых источников

1. Карпычев В. Ю. Беспилотные авиационные системы – ретрансляторы: современные решения // Вестник Воронежского института МВД России. 2022. № 1. С. 60–68. EDN: LQOXKV

2. Блинова О. В., Васьковский С. В., Рыков Я. В. Проектирование сетей связи быстрого развертывания с использованием программного приложения анализа конфигурации сети // Управление большими системами: сборник трудов. 2021. № 90. С. 121–137.

3. Алешин М. Г., Дьяконов С. В., Сивов А. Ю. Обоснование основных характеристик антенной системы и параметров управления мощностью передатчика ретранслятора связи на беспилотном летательном аппарате // Журнал радиоэлектроники. 2011. № 12. 21 с. EDN: OXTAHB

4. Коровин К. О., Межевов П. А. Разработка антенных систем БПЛА для развертывания временных сетей связи // Военная связь будущего. Квантовый скачок как неизбежность: материалы международной научно-практической конф., СПб, 10–11 нояб. 2023 г. СПб.: ФГКВОУ ВО «ВАС» МО РФ, 2023. С. 200–204. EDN: GATAAX

5. Межевов П. А., Коровин К. О., Ликонцев А. В. Создание кольцевой антенной решетки на основе излучателей Вивальди для широкополосного канала связи с ретрансляцией // Известия высших учебных заведений России. Радиоэлектроника. 2023. Т. 26. № 3. С. 58–66. EDN: VCWALX

Статья представлена научным руководителем, ассистентом кафедры РТ СПбГУТ М. А. Межевовой.

УДК 004.8:658.5

АВТОМАТИЗАЦИЯ ПРИЕМКИ СТРОИТЕЛЬНО-МОНТАЖНЫХ РАБОТ В ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ НА ОСНОВЕ КОМПЬЮТЕРНОГО ЗРЕНИЯ

С. В. Акимов (к.т.н., доцент, доцент кафедры САР)
А. В. Люшенко (студент группы МАП-2512 СПбГУТ), lushenko.av@sut.ru

В статье рассмотрен опыт внедрения системы дистанционной приемки строительно-монтажных работ базовых станций на базе платформы Digital Mobile Construction (DMC) в ПАО «ВымпелКом». Описаны архитектура объектов, состав оборудования и этапы строительства. Представлены функции фотоотчета, выявлены ограничения ручной экспертной оценки. Сформулирована задача разработки модуля автоматической приемки на основе компьютерного зрения, рассмотрены направления его применения и ожидаемый результат внедрения.

компьютерное зрение, базовые станции, фотоотчет, Digital Mobile Construction, DMC, BBU, RRU, строительный контроль, машинное обучение, детекция объектов, распознавание текста

Современный этап развития телекоммуникационной отрасли характеризуется ростом требований к качеству и скорости развертывания сетей связи [1]. Увеличение объемов передаваемых данных, обусловленное распространением видеосервисов, облачных технологий и устройств интернета вещей, формирует устойчивый спрос на наращивание инфраструктурной емкости и плотности покрытия сетей мобильной связи. В этих условиях операторы связи вынуждены интенсифицировать строительство новых базовых станций и модернизацию существующих объектов, стремясь минимизировать временной разрыв между проектированием и вводом в коммерческую эксплуатацию.

Фактором, лимитирующим темпы строительства, выступает процедура контроля и приема выполненных работ. Традиционная модель строительного надзора предполагает регулярные выездные проверки, которые, обеспечивая визуальный контакт с объектом, сопряжены с существенными издержками. Транспортные расходы, временные затраты на перемещение персонала, необходимость координации графиков формируют временную задержку, негативно влияющую на продолжительность инвестиционно-строительного цикла. При масштабном строительстве совокупные потери времени и ресурсов вступают в противоречие с требованиями к оперативности запуска сетей.

Осознание ограничений традиционных методов контроля обуславливает поиск иных подходов к организации приемочных процедур, способных обеспечить баланс между достоверностью верификации и оперативностью. Альтернативным решением выступает переход к дистанционным форматам взаимодействия с подрядчиками на основе специализированных информационных платформ и методов фотофиксации. Внедрение таких систем позволяет делегировать первичный сбор данных исполнителю, трансформируя роль инженера от физического присутствия на объекте к экспертной оценке материалов в удаленном режиме.

Настоящая статья посвящена рассмотрению практических аспектов реализации указанного подхода в деятельности ПАО «ВымпелКом». Цель работы – описание функционирующей в компании системы дистанционной приемки на базе платформы Digital Mobile Construction (DMC), а также обоснование необходимости ее дальнейшей эволюции в направлении автоматизации контрольных процедур с использованием технологий компьютерного зрения.

Базовые станции (рис. 1) классифицируются по нескольким признакам, определяющим особенности их строительства и контроля [2]. По месту размещения выделяют крышные (на крышах зданий), мачтовые и башенные (отдельно стоящие сооружения), контейнерные (в технологических контейнерах или шкафах), а также мобильные станции на транспортных шасси для временного усиления емкости сети. По поддерживаемым стандартам связи объекты могут обеспечивать работу сетей 2G, 3G, 4G и 5G, причем значительная часть современных станций проектируется как мультистандартные решения.



Рис. 1. Пример размещения АФУ операторов связи

Современная базовая станция представляет собой распределенный аппаратный комплекс с разделением функций обработки сигнала и радиочастотной части. Центральным компонентом выступает блок базовой полосы частот – BBU (Base Band Unit), устанавливаемый в защищенных помещениях или телекоммуникационных шкафах. На BBU возлагаются задачи кодирования и модуляции данных, управления радиоресурсами, обработки сигнализации, синхронизации и взаимодействия с сетью. Вторым компонентом является выносной радиоблок – RRU (Remote Radio Unit), размещаемый вблизи антенн для минимизации потерь сигнала в фидерном тракте. Соединение BBU и RRU осуществляется посредством оптоволоконных линий с использованием интерфейса CPRI.

Помимо радиооборудования, в состав объекта входят системы электропитания с аккумуляторными батареями, системы климат-контроля, а также коммутационное оборудование для интеграции станции в транспортную сеть оператора.

Процесс возведения базовой станции включает несколько этапов: подготовка площадки и устройство фундамента; установка антенно-мачтового сооружения; монтаж оборудования в техническом помещении; монтаж антенно-фидерных устройств с ориентацией антенн в соответствии с проектом; прокладка кабельных трасс, устройство заземления и молниезащиты.

Фотоотчет в системе строительного контроля представляет собой структурированную совокупность изображений, сопровождаемых идентифицирующей информацией (дата съемки, наименование объекта, этап работ). В рамках приемочных процедур фотоотчет выполняет три функции: идентификационную (подтверждение факта выполнения работ), верификационную (подтверждение соответствия проектной документации и нормам) и юридическую (основание для подписания актов и взаиморасчетов).

Для обеспечения сопоставимости информации разрабатываются требования к методологии фотофиксации. Масштаб изображения должен позволять идентифицировать как общую компоновку оборудования, так и отдельные элементы. Применяется сочетание общих планов и детальных снимков для фиксации болтовых соединений, читаемости бирок и качества разделки кабеля.

Реализация методологии в масштабах предприятия обеспечивается корпоративной системой Digital Mobile Construction (DMC). Система выступает единой средой для загрузки, хранения и экспертизы фотоотчетов. Под-

рядчик загружает фотоматериалы через интерфейс системы, которая автоматически привязывает их к объекту и этапу работ. Экспертиза осуществляется инженером в удаленном режиме: получив доступ к материалам, специалист производит визуальный анализ каждого снимка на соответствие чек-листу приемки.

Процедура приемки построена на экспертной оценке. Чек-лист содержит десятки позиций: наличие крепежных элементов, целостность кабельных трасс, читаемость бирок, отсутствие мусора, соответствие ориентации антенн проектным значениям. Инженер последовательно просматривает каждый кадр, фиксирует несоответствия и по завершении формирует протокол замечаний, направляемый подрядчику.

Рассмотренный способ организации приемки, хотя и позволяет проводить контроль удаленно, не устраняет влияния человека на результат проверки. Анализ практического применения данной схемы позволяет выделить три типа проблем, связанных с участием человека в процессе экспертизы. Первая проблема обусловлена неизбежной долей субъективизма при визуальной оценке фотоматериалов. Один и тот же снимок, демонстрирующий, например качество укладки кабеля, может быть по-разному истолкован разными инженерами. Поскольку многие параметры не имеют формализованных количественных критериев, решение о соответствии или несоответствии часто принимается на основе личного опыта конкретного специалиста. Это приводит к неоднородности требований, предъявляемых к подрядным организациям, и создает почву для спорных ситуаций.

Вторая проблема связана с утомляемостью и снижением концентрации внимания. Специфика работы с фотоотчетами предполагает длительное изучение большого количества однотипных изображений, поскольку базовые станции разных объектов визуально схожи между собой. Как показывают исследования в области эргономики, способность человека замечать аномалии в однородном информационном потоке с течением времени снижается. Это ведет к пропуску ошибок и снижает общую достоверность контроля.

Третья проблема заключается в ограниченной производительности ручной проверки. Скорость обработки снимков напрямую зависит от физических возможностей человека. Даже высококвалифицированный специалист может просмотреть лишь определенное количество кадров за единицу

времени, не теряя при этом качества проверки. В условиях, когда предприятие ежегодно строит и модернизирует сотни объектов, пропускная способность инженерного подразделения становится «узким горлышком» всего процесса. Перед руководством возникает дилемма: либо наращивать штат проверяющих, увеличивая затраты, либо смириться с увеличением сроков рассмотрения отчетов, что отодвигает ввод объектов в эксплуатацию. В рамках данной задачи компьютерное зрение рассматривается как средство автоматического анализа фотографий, способное заменить визуальный контроль, выполняемый человеком.

Важным направлением применения CV является автоматическое распознавание типа каждого снимка. Нейросетевые модели, построенные на архитектурах трансформеров [3] и сверточных нейронных сетей [4], анализируют содержание изображения и относят его к определенной категории: общий вид объекта, узел крепления оборудования, радиоблок RRU, идентификационная бирка заземления и так далее. На основе результатов такой классификации система автоматически проверяет полноту фотоотчета, то есть наличие всех типов снимков, которые регламент предписывает выполнить на данном этапе строительства. Если какой-либо обязательный кадр отсутствует, это фиксируется как нарушение.

Следующим направлением выступает детекция объектов. Система сканирует фотографии с целью обнаружения заранее заданных элементов, подлежащих контролю. К числу таких элементов относятся, в частности, кабель-каналы и лотки, элементы заземления (шины, проводники, зажимы), антенные фидеры. Путем сопоставления факта наличия или отсутствия этих объектов с требованиями чек-листа система выявляет возможные пропуски в монтаже.

Современные методы компьютерного зрения позволяют реализовать и более сложные проверочные функции, выходящие за рамки простой классификации и детекции. В частности, функция распознавания текста (OCR) реализована с использованием мультимодальной большой языковой модели QWEN3-VL:32b. Это дает системе возможность считывать серийные номера и другие данные с заводских табличек оборудования, а также текст на маркировочных бирках, нанесенных на кабели и элементы конструкции. Полученная в машиночитаемом формате информация может быть в дальнейшем сопоставлена с проектной документацией для подтверждения соответствия установленного оборудования утвержденным спецификациям.

Сегментация изображений, необходимая для контроля отсутствия посторонних предметов в зоне размещения оборудования (например, на полу технического помещения), находится в стадии планирования. Предполагается использование модели YOLOv10 [5] в сочетании с большой языковой моделью для классификации обнаруженных объектов и фиксации наличия нарушений к требованиям к чистоте на объекте. Интеграция модуля CV в DMC трансформирует процесс приема работ. После загрузки комплекта изображений система автоматически выполняет анализ. При соответствии всех параметров система подтверждает приемку без участия человека. При обнаружении нарушений генерируется протокол замечаний с указанием конкретных пунктов чек-листа. Роль инженера трансформируется к контролеру второго уровня: участие требуется только в спорных случаях, при низкой уверенности модели или сложных нарушениях.

Проведенное исследование позволяет заключить, что развитие систем дистанционного контроля представляет собой закономерный этап цифровизации строительной отрасли. Внедрение платформы DMC обеспечило переход от выездных проверок к экспертной оценке фотоотчетов, сократив издержки. Вместе с тем существующий процесс сохраняет зависимость от человеческого фактора, что актуализирует задачу дальнейшей автоматизации.

Предлагаемое внедрение модуля компьютерного зрения направлено на трансформацию процесса приемки: алгоритмы машинного обучения принимают на себя функции классификации, детекции, распознавания текста и сегментации, обеспечивая формализацию критериев и единообразие применения требований. При этом автоматизированная валидация не исключает человека, а трансформирует его роль от рутинного просмотра к контролю второго уровня, сосредоточенному на сложных случаях.

Список используемых источников

1. Andrews J.G., Buzzi S., Choi W. et al. What Will 5G Be? // IEEE Journal on Selected Areas in Communications. 2014. Vol. 32. N 6. PP. 1065–1082. DOI: 10.1109/JSAC.2014.2328098 (дата обращения: 03.03.2026).

2. Dahlman E., Parkvall S., Sköld J. 5G NR: The Next Generation Wireless Access Technology. London: Academic Press, 2018. 560 p. ISBN 978-0-12-814323-0.URL:https://ie.uryukyu.ac.jp/~wada/system18/5G_Book.pdf (дата обращения: 03.03.2026).

3. Vaswani A., Shazeer N., Parmar N. et al. Attention Is All You Need // Advances in Neural Information Processing Systems. 2017. Vol. 30. PP. 5998-6008. URL: https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aaPaper.pdf (дата обращения: 15.03.2026).

4. Krizhevsky A., Sutskever I., Hinton G.E. ImageNet Classification with Deep Convolutional Neural Networks // Advances in Neural Information Processing Systems. 2012. Vol. 25. PP. 1097–1105. URL: https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf (дата обращения: 17.03.2026).

5. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2016. PP. 779–788. URL:https://www.cvfoundation.org/openaccess/ content_cvpr_2016/papers/Redmon_You_Only_Look_CVPR_2016_paper.pdf (дата обращения: 15.03.2026).

Статья представлена научным руководителем, кандидатом технических наук, доцентом С. В. Акимовым.

УДК 621.396

ВЛИЯНИЕ РЕФАРМИНГА RAN НА КАЧЕСТВО ПОКРЫТИЯ МОБИЛЬНОЙ СЕТИ

А. Э. Алексеев (студент группы РТ-42м СПбГУТ), alekseev.ae@sut.ru

В статье представлены теоретические основы и результаты рефарминга частотного спектра в диапазоне 2100 МГц, выполненного в Мурманском филиале оператора связи. На основе анализа распределения частотных ресурсов до и после рефарминга показано, что суммарный частотный ресурс LTE увеличился на 32 % при росте количества сот на 49 %. Проведен анализ изменения ключевых показателей сети: средневзвешенной пользовательской скорости (3G+4G), скоростей в LTE и 3G, объемов пакетного и голосового трафика, доли VoLTE. Сравнение теоретической оценки прироста скорости с фактическими данными позволило объяснить, почему средняя скорость выросла на 7 % в LTE и на 11 % средневзвешенно, тогда как объем трафика LTE увеличился на 45 %. Показано, что рефарминг эффективно повысил емкость сети при сохранении стабильности KPI.

рефарминг, LTE, UMTS, диапазон 2100 МГц, пользовательская скорость, VoLTE, пакетный трафик, GTP Loss, KPI

Введение

В условиях непрерывного роста потребления мобильного трафика операторы связи сталкиваются с проблемой дефицита радиочастотного спектра. Одним из наиболее эффективных способов увеличения пропускной способности сетей LTE является рефарминг – процесс перераспределения частотных полос, занятых устаревшими технологиями (2G, 3G), в пользу современных стандартов [1]. Особую ценность представляет диапазон 2100 МГц, который изначально использовался для сетей UMTS, но обладает более низкими потерями при распространении по сравнению с высокочастотными диапазонами (например, 2600 МГц) и лучшей проникающей способностью внутрь зданий и может быть использован для развертывания LTE без значительного ухудшения покрытия [2].

В статье анализируются теоретические основы и основные результаты этого проекта: изменение частотного ресурса, динамика пользовательских скоростей, объемов трафика, ключевых показателей качества (KPI) и абонентского опыта, выполненного в Мурманском филиале оператором ПАО «ВымпелКом».

Теоретические основы рефарминга

Скорость передачи данных в беспроводной сети описывается формулой Шеннона (1) [3]:

$$C = B \cdot log_2\left(1 + \frac{S}{N}\right) \quad (1)$$

Здесь C – максимально возможная скорость (Мбит/с), B – ширина полосы (МГц), S/N – отношение сигнал/шум. Из формулы следует, что при прочих равных условиях скорость прямо пропорциональна ширине полосы. Рефарминг увеличивает полосу для LTE за счет частот, ранее занятых UMTS. В рассматриваемом проекте до рефарминга LTE использовала полосы 10, 15 и 20 МГц в диапазонах 1800 и 2600 МГц. После рефарминга к этим конфигурациям добавились 10-мегагерцевые несущие в диапазоне 2100 МГц. В идеальных условиях (один пользователь, отсутствие помех) расширение полосы с 10 до 20 МГц позволяет увеличить максимальную скорость передачи данных в два раза. Однако на практике средняя пользовательская скорость зависит не только от полосы, но и от распределения ресурсов между абонентами, помеховой обстановки, потерь на трассе, многолучевости, помеховой обстановки и загрузки соты [4].

Методика измерения показателей

Для оценки результатов рефарминга использовались методы, регламентированные стандартами 3GPP и внутренними процедурами оператора.

Пользовательская скорость измерялась на основе агрегированных данных от всех активных абонентов в течение часа наибольшей нагрузки (ЧНН) с помощью системы мониторинга радиоресурсов. Средневзвешенная скорость (3G+4G) рассчитывалась по объему трафика в каждой технологии (2):

$$V_{\text{общ}} = \frac{V_{LTE} \cdot T_{LTE} + V_{3G} \cdot T_{3G}}{T_{LTE} + T_{3G}}, \quad (2)$$

где V_{LTE}, V_{3G} – средние скорости в соответствующих технологиях, T_{LTE}, T_{3G} – объемы переданных данных в ЧНН. Такой подход позволяет учесть фактическое распределение трафика между технологиями.

Объемы пакетного трафика фиксировались по счетчикам узлов пакетной сети (PGW, SGW) с разбивкой по технологии радиодоступа. Доля VoLTE определялась как отношение количества минут разговора, переданных через IMS, к общему объему голосового трафика.

GTP Loss (потери пакетов на интерфейсе S1-U между базовой станцией и шлюзом) измерялся с помощью протокола GTP-U с использованием порядковых номеров пакетов в соответствии с 3GPP TS 29.281. Увеличение числа базовых станций с GTP Loss >0,1 % свидетельствует о росте нагрузки на транспортную сеть.

Базовые KPI (RAB_DR_PS – частота обрывов соединений для пакетных услуг, CunSSR – успешность установления соединений, CDR – доля обрывов голосовых вызовов) вычислялись по стандартным формулам 3GPP на основе журналов базовых станций и контроллеров.

Анализ результатов рефарминга

До рефарминга сеть LTE Мурманского филиала насчитывала 1249 сот с суммарной полосой 19 300 МГц. Основные конфигурации включали сочетания диапазонов 1800 и 2600 МГц с шириной 10, 15 и 20 МГц. После перераспределения спектра UMTS 2100 в LTE количество сот увеличилось до 1865, а суммарный частотный ресурс вырос до 25 460 МГц (прирост 32 %). Добавленные соты в диапазоне 2100 МГц имеют полосу 10 МГц и входят в различные комбинации с другими диапазонами. В таблице 1 приведены ключевые параметры.

ТАБЛИЦА 1. Изменение спектрального ресурса

Параметр	До рефарминга	После рефарминга	Изменение
Количество сот	1249	1865	+49 %
Суммарный спектр LTE, МГц	19 300	25 460	+32 %
Средняя полоса на соту, МГц	~15,5	~13,7	−12 %

Увеличение числа сот при одновременном снижении средней полосы на соту объясняется тем, что добавленные соты имеют меньшую ширину (10 МГц), но обеспечивают дополнительную емкость и снижают нагрузку на существующие сектора.

Изменение пользовательских скоростей после рефарминга представлено в таблице 2.

ТАБЛИЦА 2. Изменение пользовательских скоростей

Показатель	Изменение
Средневзвешенная скорость (3G+4G)	+11 %
Скорость в сети LTE	+7 %
Скорость в сети 3G	−20 %
Скорость на сегменте ARS	+20 %

Рост скорости на 11 % свидетельствует о положительном эффекте рефарминга. Снижение скорости в 3G связано с сокращением выделенной полосы.

Динамика объемов трафика приведена в таблице 3.

ТАБЛИЦА 3. Динамика объемов трафика

Показатель	Изменение
Общий пакетный трафик	+38 %
Пакетный трафик LTE	+45 %
Пакетный трафик 3G	−68 %
Доля VoLTE	С 55 % до 62 %

Рост трафика LTE на 45 % свидетельствует о высокой загрузке высвобожденного спектра. Увеличение доли VoLTE до 62 % отражает успешную миграцию голосовых вызовов в сеть LTE.

После рефарминга зафиксировано увеличение количества базовых станций с показателем GTP Loss (потери пакетов на интерфейсе S1-U). Это связано с перераспределением трафика и ростом нагрузки на транспортную сеть. Базовые KPI (RAB_DR_PS, CunSSR, CDR) остались стабильными, деградаций не выявлено. Абонентские жалобы значимо не изменились.

Сравнение теории и практики

Формула Шеннона предсказывает пропорциональный рост максимальной скорости при увеличении полосы. Если бы добавленная полоса 2100 МГц была равномерно распределена по всем сотам и не сопровождалась изменением количества сот, можно было бы ожидать роста скорости, близкого к росту суммарной полосы (+32 %). Однако в результате произошло следующее:

● количество сот увеличилось на 49 % (с 1249 до 1865), причем большинство новых сот имеют ширину 10 МГц. Это привело к снижению средней полосы на одну соту, при этом общая емкость сети повысилась за счет большего числа секторов, обслуживающих абонентов;

● добавленный спектр был распределен неравномерно: некоторые соты получили дополнительную полосу 10 МГц (например, конфигурации 2100 10M+1800 15M), другие остались без изменений, а на части БС были введены новые соты с полосой 10 МГц;

● эффективная скорость для пользователя зависит не только от ширины полосы, но и от степени использования ресурсов соты. Увеличение числа сот позволило разгрузить существующие сектора, что частично компенсировало снижение средней полосы на соту.

Таким образом, теоретическое удвоение скорости при добавлении 10 МГц к 10 МГц реализуется лишь в идеализированных условиях (один пользователь, идеальный канал). В реальной сети с большим количеством абонентов и неоднородной конфигурацией сот прирост средней пользовательской скорости составил 7 % в LTE и 11 % средневзвешенно. При этом объем переданного трафика в LTE вырос на 45 %, что свидетельствует о значительном увеличении емкости сети – именно это является одной из основных целей рефарминга.

Заключение

Рефарминг диапазона 2100 МГц в Мурманском филиале позволил:

● увеличить суммарный частотный ресурс LTE на 32 % (с 19 300 до 25 460 МГц);

● повысить пользовательскую скорость на 11 %;

● увеличить объем пакетного трафика LTE на 45 %;

● повысить долю VoLTE до 62 % при стабильности KPI.

Детальный анализ распределения частотного ресурса (таблицы 1 и 2) показал, что прирост числа сот (49 %) и изменение структуры спектра объясняют умеренный рост средней пользовательской скорости на фоне существенного увеличения емкости сети. Выявленный рост количества базовых станций с GTP Loss указывает на необходимость последующей оптимизации транспортной сети – типовой эффект при расширении спектра и росте нагрузки. Полученные результаты подтверждают целесообразность рефарминга UMTS 2100 для развития LTE и подготовки к внедрению 5G.

Список использованных источников

1. Государственная комиссия по радиочастотам. Заседание ГКРЧ от 23.10.2006, протокол № 06-17. М.: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 2006. 15 с.

2. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Vol. 27. № 3. P. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

3. 3GPP TS 36.104: Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception. Version 15.0.0. 3rd Generation Partnership Project, 2018. 150 p. URL: https://www.3gpp.org/ftp/Specs/archive/36_series/36.104/ (дата обращения: 10.04.2026).

4. Бабков В. Ю. Подходы к планированию и оптимизации сетей LTE. СПб.: СПбГУТ, 2012. 108 с. ISBN 978-5-89160-083-6.

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. А. Прасоловым.

УДК 535.14

МОДЕЛИРОВАНИЕ И РАСЧЕТ ЭФФЕКТИВНОСТИ ФОНОН-СПИНОВОЙ КВАНТОВОЙ ПАМЯТИ НА ОСНОВЕ NV-ЦЕНТРОВ В АЛМАЗЕ

В. С. Алексеев (студент гр. РФ-42 СПбГУТ), alekseev.vs@sut.ru
Н. И. Богданов (студент гр. РФ-42 СПбГУТ), bogdanov.ni@sut.ru
И. Е. Скалецкая (к.ф-м.н., доцент кафедры физики СПбГУТ)

Квантовая память – ключевой элемент для квантовых сетей и распределенных вычислений. Перспективным видом принципом работы квантовой памяти является преобразование фотона в фонон (квант звука) с последующей записью в спиновое состояние дефекта кристалла. В работе представлена теоретическая модель памяти на основе NV-центров в алмазе и волновода из ниобата лития. Выполнен ряд расчетов, в результате которых показано, что при комнатной температуре время хранения может достигать 0,35 мс, а эффективность записи до 20 %. Предложена схема считывания состояния спина методом оптически детектируемого магнитного резонанса (ОДМР). Результаты расчетов согласуются с экспериментальными данными.

квантовая память, фонон, спин, NV-центр, волновод, вынужденное рассеяние Мандельштама–Бриллюэна, оптически детектируемый магнитный резонанс

Развитие классических кремниевых электронных технологий неумолимо приближается к своему физическому пределу. Миниатюризация транзисторов, долгое время двигавшая прогресс, сталкивается с квантовыми эффектами, которые из полезных инструментов превращаются в источник помех. Это ограничение тормозит прогресс в области искусственного интеллекта, моделирования сложных молекулярных процессов и создания новых лекарственных препаратов. Закономерным решением данной проблемы становится переход к квантовым вычислениям, использующим в качестве носителей информации фотоны. Однако для маршрутизации и синхронизации оптических сигналов необходима квантовая память – устройство, способное принять и хранить информацию в течении некоторого промежутка времени.

Целью данной работы является Теоретическое моделирование системы и расчет параметров фонон-спиновой квантовой памяти на основе NV-центров в алмазе и волновода из ниобата лития. В основе предлагаемой архитектуры лежит система, объединяющая оптическую, акустическую и спиновую платформы. Ключевая идея заключается в цепочке преобразований: фотон → фонон → спин.

Для практической реализации такого интерфейса критически важен выбор материалов. В качестве среды для генерации акустических волн предложен волновод из ниобата лития ($LiNbO_3$). Причинами этого выбора являются уникальные физические свойства кристалла. Во-первых, сильная фотоупругость и нелинейность обеспечивают эффективное преобразование оптического сигнала в акустический за счет вынужденного рассеяния Мандельштама-Бриллюэна (ВРМБ). Во-вторых, кристаллическая решетка ниобата лития поддерживает распространение гиперзвуковых волн на частотах порядка гигагерц, что необходимо для резонанса со спиновыми переходами. В-третьих, $LiNbO_3$ демонстрирует сильную оптоакустическую связь и технологически совместим с существующими интегральными фотонными чипами (LNOI-платформы), что открывает путь к созданию компактных устройств.

В качестве квантового носителя для хранения информации используются NV-центры в алмазе. NV-центр – это дефект кристаллической решетки, представляющий собой атом азота, расположенный рядом с вакансией (отсутствующим атомом углерода). Данный объект не создается «вручную» как отдельный элемент, а формируется в алмазной пленке сложным технологическим процессом. Атомы азота внедряются в кристалл либо непосредственно в процессе роста CVD-алмаза с примесями, либо методом ионной имплантации (бомбардировки ионами). Далее для создания вакансий образец облучают высокоэнергетическими электронами, после чего производят отжиг при температурах 800–1000 °C, чтобы вакансии диффундировали и заняли места рядом с атомами азота. Полученный NV-центр обладает спином $S = 1$ с характерным нуль-полевым расщеплением $D = 2{,}87$ ГГц [1], что позволяет хранить бит квантовой информации в состояниях «вверх» или «вниз» и считывать его оптически по интенсивности красной флуоресценции при возбуждении зеленым лазером (532 нм).

Общая схема работы квантовой памяти (рис. 1):

1. Лазерный фотон ($\lambda = 1550$ нм) входит в волновод из ниобата лития.
2. В результате ВРМБ фотон превращается в фонон (акустическую волну).
3. Фонон распространяется по волноводу со скоростью звука.
4. Фонон достигает NV-центра в алмазе и за счет деформации переворачивает его спин (запись информации).
5. Спин сохраняет состояние (хранение).

6. Считывание происходит оптически: зеленый лазер (532 нм) возбуждает NV-центр, а интенсивность красной флуоресценции зависит от состояния спина.

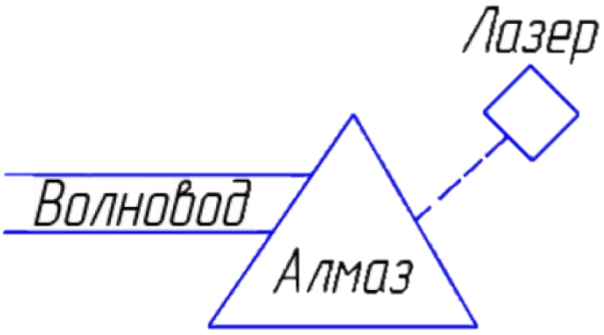


Рис. 1. Общая схема работы

Процесс ВРМБ является нелинейным взаимодействием, при котором падающий фотон преобразуется в рассеянный фотон меньшей энергии и фонон.

Для расчета максимально возможной частоты фонона используется выражение [2]: $\Omega_{max} = \frac{4\pi n v_C}{\lambda}$, где n – показатель преломления среды, v_c – скорость звука, λ – длина волны. $\Omega_{max} = \frac{4\pi \cdot 2{,}2 \cdot 7{,}4 \cdot 10^3}{1{,}55 \cdot 10^{-6}} \approx 1{,}32 \cdot 10^{11} \frac{\text{рад}}{\text{с}} \approx 21$ ГГц. Полученная величина в 21 ГГц указывает верхнюю границу частоты фононов, возбуждаемых в данной конфигурации. Для резонансного взаимодействия со спином NV-центра необходима частота фонона Ω = 2.87 ГГц [3], что лежит в пределах этого диапазона и является технически достижимым путем выбора подходящего угла рассеяния или материала волновода.

Эффективность преобразования фотон → фонон рассчитывается по формуле: $n_{\text{фт}\to\text{фн}} = h^2\sqrt{\frac{g_{\text{в}} P_P L}{2A_{\text{эфф}}}}$ [4], где $g_{\text{В}}$ – бриллюэновский коэффициент усиления (характеризует нелинейную восприимчивость среды) [2], $P_{\text{р}}$ – мощность лазера накачки, L – длина волновода, $A_{\text{эфф}}$ – эффективная площадь поперечного сечения оптической моды ≈0.85 = 85 % при идеальных условиях. Реалистичная оценка: $n_{\text{фт}\to\text{фн}} \approx 0{,}3 \div 0{,}5$. Принимаем для расчета: $n_{\text{фт}\to\text{фн}} = 0{,}4$ [4]. Это означает, что только 40 % энергии фотона переходит в энергию фонона. Это значительно ниже идеализированных 85 %, но достаточно для демонстрационных экспериментов.

Распространение фонона и его время жизни: $T_{\text{фн}} = \frac{1}{\alpha v_s}$, где $\alpha - \cdots$, $v_s - \cdots$. Для частот ~10 ГГц в ниобате лития при комнатной температуре: $T_{\text{фн}} \approx 1$ нс $= 10^{-9}$с. Максимальное расстояние распространения: $L_{max} = v_s \cdot T_{\text{фн}} = 7{,}4\times10^{3} \times 10^{-9} = 74$ мкм. Таким образом фонон затухает уже на расстоянии ~74 микрон. Это значит, что NV-центры должны располагаться в непосредственной близости от точки генерации фонона. Технически это реализуемо при интеграции алмазной пленки на волновод.

Проведем сравнение времени жизни фонона (~10 нс) и времени переворота спина (~300 нс): $t_\pi = \frac{\pi}{\Omega_R}$ [5], где $\Omega_R -$ частота Раби (частота, с которой амплитуды вероятности двух уровней атомной энергии колеблются в колеблющемся электромагнитном поле), то есть $t_\pi = 3{,}14 / 10^7 \approx 3{,}14\times10^{-7}$ с = 314 нс, при $T_{\text{фн}} = 1$ нс. Время показывает, что фонон затухает раньше, чем происходит полный переворот спина. Следовательно, процесс записи информации не является полностью когерентным и носит вероятностный характер. Вероятность успешной записи оценивается на уровне ~0.7. Необходимо увеличивать время жизни фонона (чистые волноводы, низкие температуры) или использовать резонансные структуры для увеличения Ω_R.

Время спиновой когерентности NV-центра при комнатной температуре: $T_2 = 0{,}35$ мс. Вероятность сохранения состояния за время хранения t: $P_{\text{записи}} = e^{\left(-\frac{t}{T_2}\right)}$ [6]. Выбираем время хранения t = 0,1 мс: $P_{\text{записи}} = \eta_{\text{хр}} = e^{\left(-\frac{0{,}1}{coscos\,35}\right)} \approx 0{,}75$. Исходя из вычислений получаем, что через 0,1 мс после записи спин с вероятностью 75 % все еще находится в нужном состоянии. Это хороший результат для комнатной температуры.

Считывание информации осуществляется методом оптически детектируемого магнитного резонанса (ОДМР). При облучении зеленым лазером NV-центр испускает флуоресценцию, интенсивность которой зависит от состояния спина. Контраст сигнала составляет порядка 30 % [7] а отношение сигнал/шум достигает значений около 30, что обеспечивает надежное различение состояний. Эффективность считывания близка к 0.95 [8].

Общая эффективность квантовой памяти определяется произведением эффективностей всех этапов: $\eta_{\text{всего}} = \eta_{\text{фт}\to\text{фн}} \cdot \eta_{\text{фн}\to\text{спин}} \cdot \eta_{\text{хр}} \cdot \eta_{\text{чт}} = 0{,}4 \cdot 0{,}7 \cdot 0{,}75 \cdot 0{,}95 = 0{,}1995 \approx 20$ %, однако с учетом реальных потерь более реалистичный диапазон составляет 1–10 %.

Таким образом, теоретическое моделирование показало, что предложенная модель фонон-спиновой квантовой памяти на основе гибридного

волновода из ниобата лития и NV-центров в алмазе является физически реализуемой. Безусловным преимуществом является возможность работы при комнатной температуре и принципиальная совместимость с технологиями интегральной фотоники. Однако достигнутые значения эффективности невелики, что указывает на слабые места архитектуры: короткое время жизни фонона и недостаточная скорость его взаимодействия со спином. Дальнейшая оптимизация системы должна быть направлена на использование низкотемпературного охлаждения и создание акустических резонансных структур, локализующих звуковую волну в микрообъеме. Это позволит увеличить время жизни фонона и повысить частоту Раби, что в перспективе сделает данный тип памяти значимым конкурентом элементов квантовых вычислительных сетей.

Список используемых источников

1. High-gain lithium niobate brillouin laser with tunable phonon frequency of 1∼31 GHz // frontiers URL: https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2024.1402002/full (дата обращения: 10.04.2026).

2. Optical antenna gain. 3: The effect of secondary element support struts on transmitter gain // OPTICA Publishing Group URL: https://opg.optica.org/ao/abstract.cfm?uri=ao-15-4-977 (дата обращения: 10.04.2026).

3. Andrey E. Miroshnichenko, Sergej Flach, and Yuri S. Kivshar Fano resonances in nanoscale structures // American Physical Society, 2010. 42 с.

4. Huiyao Chen, Noah F. Opondo, Boyang Jiang, Evan R. MacQuarrie, Raphaël S. Daveau, Sunil A. Bhave, Gregory D. Fuchs Engineering electron-phonon coupling of quantum defects to a semi-confocal acoustic resonator // New York: Cornell University, 2019. 29 с.

5. Dobrovitski V. V., G. de Lange, D. Rist`e, and R. Hanson Bootstrap tomography of high-precision pulses for quantum control. GA Delft: Kavli Institute of Nanoscience Delft, Delft University of Technology, 2018. 5 с.

6. Can Liu, Ruifang Liu and 12 others MicroRNA-141 suppresses prostate cancer stem cells and metastasis by targeting a cohort of pro-metastasis genes // Shanghai: NATURE COMMUNICATIONS, 2017. 14 с.

7. Xiang Shen, Liye Zhao, Fei Ge Structural Optimization and MEMS Implementation of the NV Center Phonon Piezoelectric Device. Southeast University, Nanjing: Key Laboratory of Micro-Inertial Instrument and Advanced Navigation Technology, Ministry of Education, School of Instrument Science and Engineering, 2022. 13(10) с.

8. Luca Pezz`e, Augusto Smerzi, Markus K. Oberthaler, Roman Schmied, Philipp Treutlein Quantum metrology with nonclassical states of atomic ensembles // Largo Enrico Fermi: QSTAR, INO-CNR and LENS, 2018. 76 с.

3. Цуканов А. В. NV-центры в алмазе. Часть I. Общие сведения, технология изготовления, структура спектра //Микроэлектроника. 2012. Т. 41. № 2. С. 104-104.

УДК 623.76

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЛОГОПЕРИОДИЧЕСКИХ И РУПОРНЫХ АНТЕННЫХ СИСТЕМ, ОБЕСПЕЧИВАЮЩИХ ЭФФЕКТИВНОЕ ПОДАВЛЕНИЕ КАНАЛОВ УПРАВЛЕНИЯ И ПЕРЕДАЧИ ДАННЫХ БПЛА

Б. Н. Андреев (студент гр. МВТ-2511 СПбГУТ), andreev.bn@sut.ru
А. Н. Ликонцев (к.т.н., доцент, доцент кафедры РТ СПбГУТ)

Антенные системы, использующиеся в системах радиоэлектронной борьбы для противодействия беспилотным летательным аппаратам, с каждым днем требуют большей избирательности к себе. Необходимость модернизации имеющихся систем является актуальным направлением развития радиотехнической отрасли. В данной статье рассмотрены два основных типа антенных систем, представлен их сравнительный анализ и вывод о практическом применении.

логопериодические, рупорные, антенные системы, БПЛА

Существующие средства радиоэлектронной борьбы применяются с использованием двух основных типов антенных системы: направленные и всенаправленные антенные системы.

В условиях применения современных энергоэффективных и широкополосных каналов передачи данных возникает необходимость повышения эффективности существующих средств радиоэлектронной борьбы [1].

Использование направленных антенных систем является более эффективным методом, ввиду большего коэффициента направленного действия, относительно всенаправленных антенных систем. Они, в свою очередь, подразделяются на антенны с линейной и круговой поляризацией. В системах радиоэлектронной борьбы противодействия беспилотным летательным аппаратам используют антенны с линейной поляризацией. Данный выбор следует из анализа принципов построения антенных систем. В антенне с линейной поляризацией отсутствуют потери мощности при разделении сигнала на ортогональные составляющие, что приводит к значительному снижению КПД. Основными представителями направленных антенных систем с линейной поляризацией являются логопериодические и рупорные антенны.

Логарифмически периодические (логопериодические) антенны относятся к классу частотно-независимых антенн и могут работать в диапазоне частот с коэффициентом перекрытия 10 и более. Эти антенны строятся с использованием принципа подобия, который заключается в следующем [2].

Основные характеристики и параметры антенны зависят от формы излучающих и их волновых размеров. С увеличением размеров антенны и длины волны в m раз ее характеристики не меняются. Это позволяет создать антенну из последовательно расположенных вдоль некоторой линии подобных элементов и возбудить их бегущей вдоль этой линии волной. Если при этом обеспечить интенсивное излучение только элементов, с заданными волновыми параметрами. В такой антенне создается «активная зона» из элементов, волновые размеры которых близки к заданным, и эта зона с изменением частоты перемещается вдоль линии расположения подобных элементов.

Антенна схематически показана на рис. 1 и состоит из двухпроводной линии и системы симметричных вибраторов (показано 7 вибраторов). Двухпроводная линия перекрещивается между каждой парой вибраторов.

Первый вибратор делается полуволновым на минимальной длине волны заданного рабочего диапазона, а седьмой вибратор делается полуволновым на максимальной длине волны этого диапазона. Расстояние между соседними вибраторами равно четверти минимальной длины волны. На этом расстоянии фаза волны тока, распространяющейся в двухпроводной линии, уменьшается на 90º. Поля такой пары вибраторов в одном направлении складываются синфазно, а в противоположном направлении вычитаются [3].

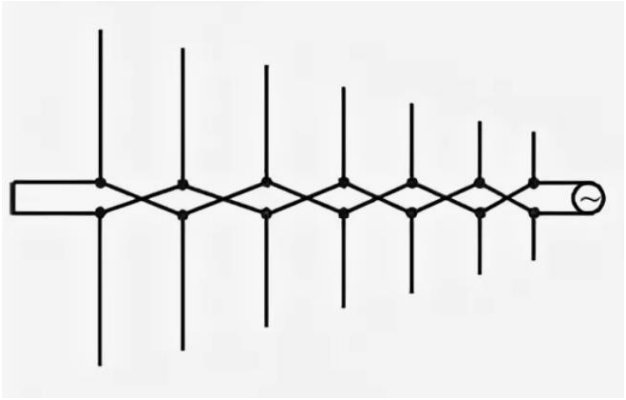


Рис. 1. Логопериодическая вибраторная антенна

На рис. 2 и рис. 3 представлены результаты расчетов и измерений КУ, КСВН и диаграммы направленности для рассматриваемой антенны.

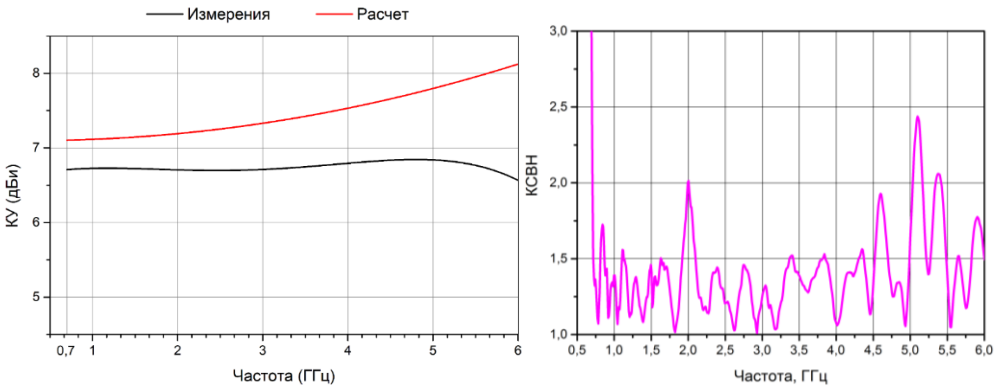


Рис. 2. Результат измерения коэффициента усиления и коэффициента стоячей волны по напряжению

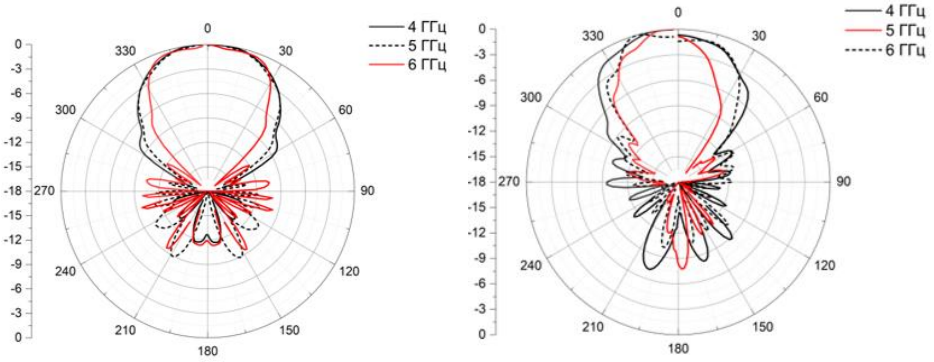


Рис. 3. Диаграмма направленности антенны в H и E плоскостях

В свою очередь, рупорные антенны относятся к классу апертурные антенны. Это антенны, излучающие с раскрыва. Элементарным излучателем в них является элемент Гюйгенса. Раскрыв – это воображаемая поверхность, отделяющая внутреннюю полость рупора от внешнего пространства. В соответствии с принципом Гюйгенса поле на раскрыве однозначно определяет поле во всем внешнем пространстве. На рис. 4 показана рупорная антенна [4].

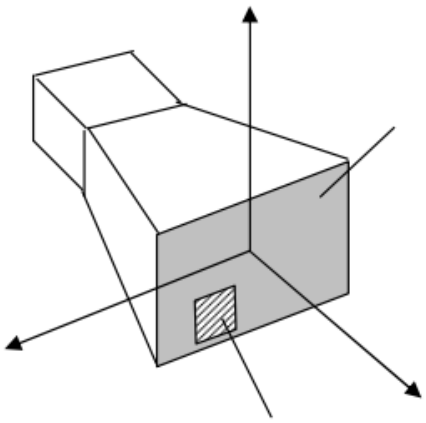


Рис. 4. Рупорная антенна

На рис. 5, рис. 6 представлены результаты расчетов и измерений КУ, КСВН и диаграммы направленности для рупорной антенны.

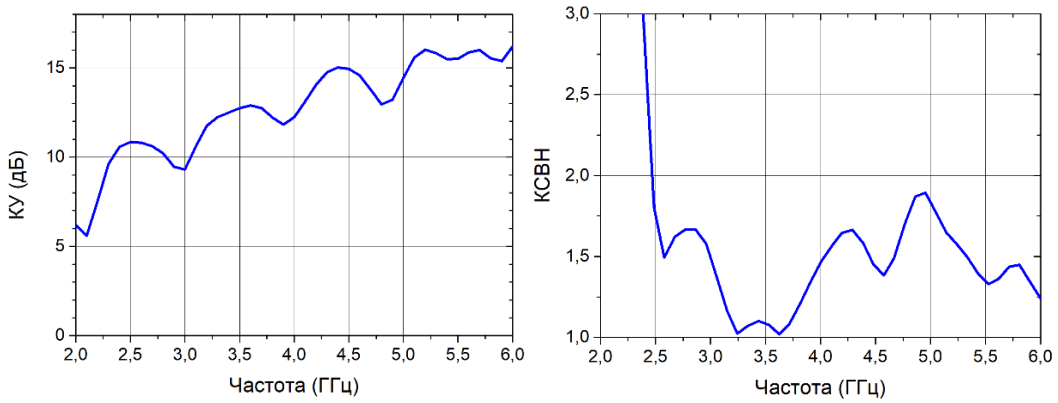


Рис. 5. Результат измерения коэффициента усиления и коэффициента стоячей волны по напряжению

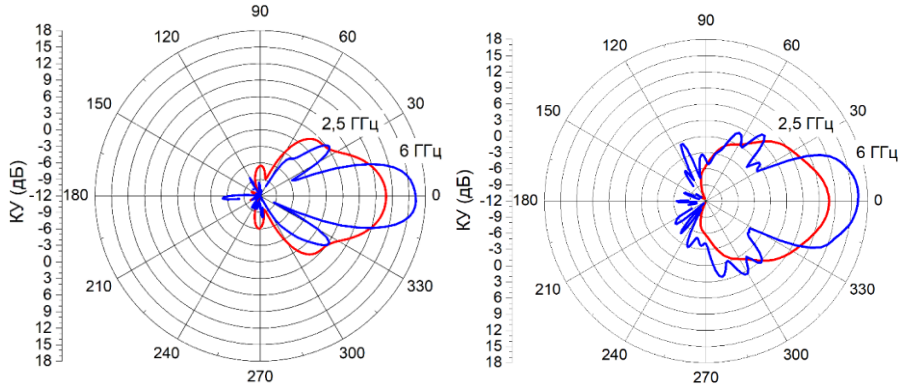


Рис. 6. Диаграмма направленности антенны в H и E плоскостях

Проведя сравнительный анализ представленных антенных систем, была составлена сравнительная характеристика для непосредственного применения антенных систем на практике, она представлена в таблице 1. Рассматриваемый диапазон каналов видеосброса для беспилотных летательных аппаратов: 5600 – 5900 МГц [5].

ТАБЛИЦА 1. Основные характеристики рассмотренных антенных систем

	Логопериодические	Рупорные
Диапазон частот, МГц	390 – 6000	2500 – 6000
Коэффициент усиления, дБи	3 – 9	9 – 16
КСВн	<2.5	<1.9
Поляризация	Линейная	Линейная

Исходя из полученных результатов логопериодических и рупорных антенн, можно сделать следующие выводы.

Оба типа антенн демонстрируют высокую эффективность в задачах радиоэлектронного подавления, однако каждая из систем обладает преимуществами, определяющими области их применения.

Логопериодические антенны характеризуются своим широким диапазоном рабочих частот, способных перекрывать большинство стандартных каналов связи БПЛА. Их постоянство характеристик и стабильная диаграмма направленности позволяют эффективно применять в комплексах радиоподавления. Кроме того, логопериодические антенны обеспечивают хорошее соотношение усиление – масса – габариты. Главным ограничением является более низкое усиление по сравнению с эквивалентными по размеру рупорными антеннами, что требует увеличения выходной мощности с передатчика для достижения той же плотности потока мощности в зоне подавления [6].

Рупорные антенны, напротив, обеспечивают максимальное усиление и высокую направленность, что позволяет концентрировать энергию в узком луче и достигать предельной дальности подавления при ограниченной выходной мощности. Это делает их более актуальными для точечного воздействия на БПЛА на больших дистанциях. Однако узкополосность и необходимость более точного наведения на цель, относительно логопериодических антенн, требуют дополнительных внедрения в комплексы антенных систем, разделенных по диапазонам.

Список используемых источников

1 Michel A. H. Counter-drone systems // Center for the Study of the Drone at Bard College, 2018. 23 с.

2. Гололобов Д. В., Кирильчук В. Б., Юрцев О. А. Распространение радиоволн и антенно-фидерные устройства. Часть 3. 2006. С. 36–58.

3. Ротхаммель К., Кришке А., Энциклопедия антен.: Пер. с нем. М.: ДМК Пресс, 2016. 812 с.: ил. // Типы антенн 2016. С. 69–74.

4. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101-175. DOI: 10.24411/2410-9916-2020-10205.

5. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). IEEE, 2016. С. 205-221.

6. Vaas L. Sound: Yet another way to smack down drones. Naked Security by Sophos, 06.08.2015. Available at: nakedsecurity.sophos.com/2015/08/06/sound-yetanother-way-to-smack-down-drones/ (accessed 14 May 2020).

Статья представлена научным руководителем, доцентом кафедры РТ СПбГУТ, кандидатом технических наук, А. Н. Ликонцевым.

УДК 53.08

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАРАКТЕРИСТИК ФОТОПРИЕМНОГО ТРАКТА ПРИ ПРЯМОМ ДЕТЕКТИРОВАНИИ НА РАЗЛИЧНЫХ ДЛИНАХ ВОЛН ИЗЛУЧЕНИЯ

Д. И. Бабак (студент гр. ИКФ-21 СПбГУТ), babak.di@sut.ru
В. М. Деткова (доцент кафедры физики СПбГУТ)

Современная фотоника и оптоинформатика базируются на умении управлять оптическими сигналами и использовать их для передачи, обработки и хранения информации. Статья посвящена ключевым компонентам любых оптико-электронных систем. Они являются источниками и приемниками излучения. Полупроводниковые источники света – лазерные диоды и светодиоды – благодаря своей миниатюрности, высокой эффективности, надежности и возможности прямой модуляции интенсивности вытеснили традиционные лампы из многих областей науки и техники. Однако каждый тип источника обладает уникальным набором характеристик: спектральным составом, диаграммой направленности, когерентностью, которые необходимо учитывать при разработке конкретных устройств.

фотоника, лазерные диоды, светодиоды, оптоинформатика

Целью работы является экспериментальное исследование и сравнительный анализ интенсивности излучения и основных характеристик источников (полупроводникового лазера, инфракрасного и белого светодиодов), а также исследование параметров приемников излучения.

Практическая значимость работы заключается в экспериментальном определении и сопоставлении ключевых параметров излучателей и приемников для подбора оптимальных приборов, составляющих фотоприемный тракт.

Фотоприемный тракт состоит из источников света, приемников света, усилителей, модуляторов и т.д.

Основные приборы, влияющие на качество формирования сигнала и его приема, это источники и приемники излучения.

В работе использовались в качестве источников излучения полупроводниковый лазер, ИК-светодиод и белый светодиод на основе синего/УФ-кристалла с люминофором. Их основные параметры это спектральная, энергетическая и светотехническая характеристика.

Особенностями излучения светодиода является относительно узкополосность (ширина спектра 20–50 нм), которая определяется материалом активной области. Для ИК-светодиодов (на основе GaAs или подобных соединений) максимум излучения лежит в ближней ИК-области (~850–950 нм)

Приемники излучения – фоторезистор и фотодиод [1, 2].

Фоторезистор. Его принцип действия основан на эффекте фотопроводимости – изменении электрического сопротивления полупроводника под действием света. Это неселективный приемник с относительно низким быстродействием, удобный для измерения интегральной интенсивности, особенно в ИК-области.

Фотодиод. Работает на основе явления внутреннего фотоэффекта в p-n-переходе. Может работать в фотогальваническом (без смещения) или фотодиодном (с обратным смещением) режиме. Обеспечивает более высокую чувствительность и линейность преобразования «свет-ток» по сравнению с фоторезистором.

Основу современной оптоэлектроники составляют полупроводниковые излучатели, работа которых основана на явлении электролюминесценции – излучении света при прохождении тока через p-n-переход в результате рекомбинации неравновесных носителей заряда.

Свойства фотодиода можно охарактеризовать вольтамперной характеристикой. Она представляет собой зависимость обратного тока от напряжения при неизменном световом потоке.

Фоторезистор – это фотоэлектрический полупроводниковый приемник излучения, принцип действия которого основан на эффекте фотопроводимости.

Для фоторезисторов характерны стабильность фотоэлектрических характеристик во времени, простота устройства, допускающая различные конструктивно-технологические решения, невысокая стоимость, высокие фотоэлектрические свойства, малые габариты. Фоторезисторы выгодно отличаются от фотодиодов почти линейной вольтамперной характеристикой, что важно при точных измерениях и отсутствием паразитных гармоник при переменных сигналах.

В неактивном состоянии полупроводник проявляет свойства диэлектрика. Для того, чтобы он проводил ток, необходимо воздействие на вещество внешнего стимулятора. Таким стимулятором может быть термическое воздействие или световое.

Экспериментально изучалась зависимость фототока от напряжения для исследуемых приемников [3-5]. Фототоком называется величина, на которую возрастает обратный ток при освещении фотодиода. Сила этого тока пропорциональна падающему на кристалл световому потоку (при не очень больших освещенностях) [5] (рис. 1). Сравнивая рисунок 1 и рисунок 2, видим, что линейность сохраняется, и полученные данные хорошо согласуются с теоретическими.

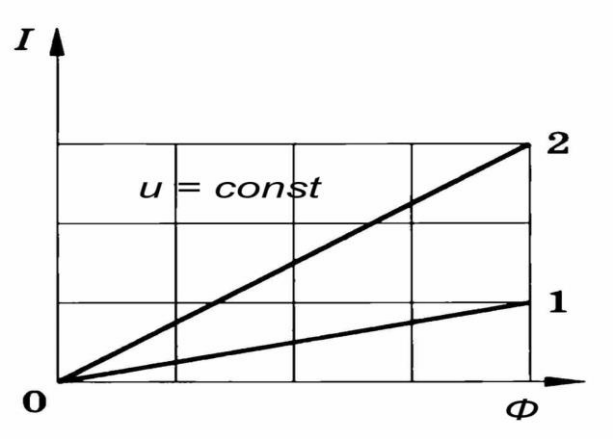


Рис. 1. Теоретический вид зависимости фототока от светового потока

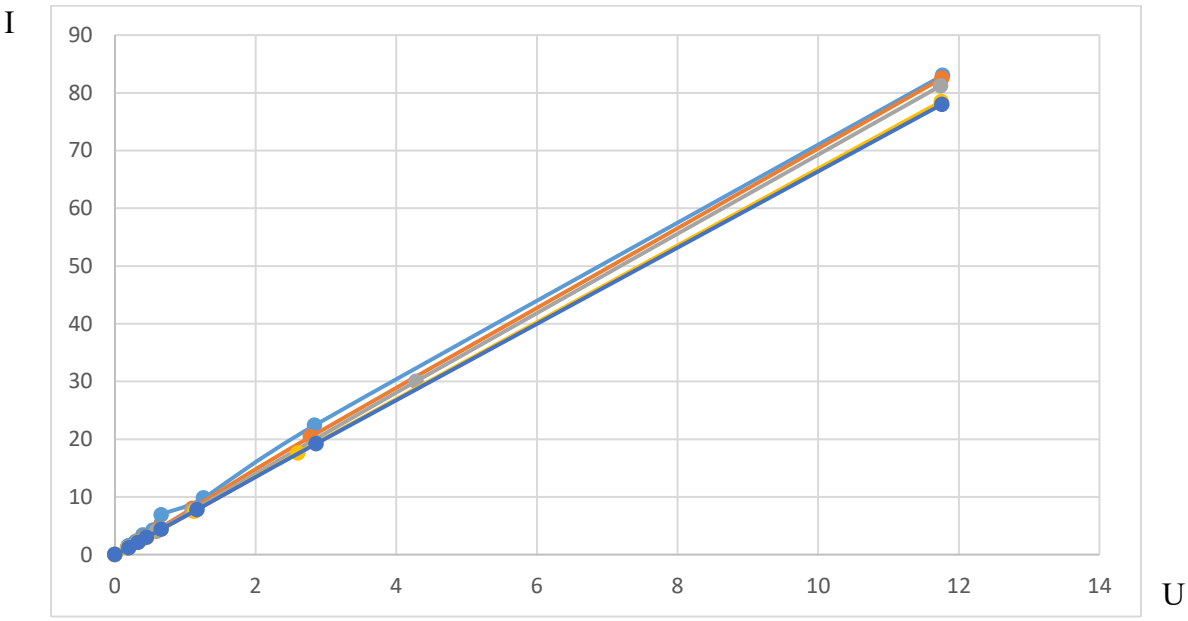


Рис. 2. Экспериментальная зависимость фототока фоторезистора от напряжения при различных световых потоках

Экспериментальные исследования элементов фотоприемного тракта являются важными для оптимального подбора элементов под конкретные практические задачи.

Список используемых источников

1. Шуберт Ф. Е. Светодиоды / Пер. с англ. под ред. А. Э. Юновича. 2-е изд. М.: Физматлит, 2008. 495 с.

2. Коган Л. М. Полупроводниковые светоизлучающие диоды. М.: Энергоатомиздат, 1983. 208 с.

3. Звелто О. Принципы лазеров / Пер. с англ. 5-е изд. М.: Лань, 2008. 720 с.

4. Ландсберг Г. С. Оптика: учебное пособие. 6-е изд. М.: Физматлит. 2023. 848 с.

5. Афонькин, М. Г., Магницкий, С. А. Оптические измерения: учебное пособие. СПб: СПбГУ ИТМО, 2008. 114 с.

УДК 623.746.-519

ПРОБЛЕМАТИКА УПРАВЛЕНИЯ РОЕМ БПЛА

М. В. Бондаренко (студент гр. РТ-41 СПбГУТ), bondarenko.mv@sut.ru
П. А. Межевов (старший преподаватель кафедры РТ СПбГУТ)

В настоящее время методы исследования и управления группами беспилотных летательных аппаратов (БПЛА) приобретают широкую популярность в различных технических и научных областях. Интерес к роевым системам объясняется их преимуществом в виде эффективности в выполнении комплексных задач и отказоустойчивостью. В статье рассматриваются ключевые проблемы в функционировании и проектировании роевых систем таких как неопределенность, вызванная внешними возмущениями, воздействующими на отдельные летательные аппараты роя, и особенности аппаратного обеспечения беспилотников. Анализ литературных источников демонстрирует отсутствие универсального подхода к организации движения роя БПЛА в подобных условиях. Большинство существующих топологий управления не в полной мере учитывают основные свойства роя, такие как масштабируемость и адаптивность.

беспилотные летательные аппараты, роевое управление, рой БПЛА, адаптивные системы

Развитие группового применения беспилотных летательных аппаратов продолжает оставаться актуальной наравне с вопросом управления целыми системами таких аппаратов. БПЛА призваны решать широкий спектр задач гражданского применения. Возможность использования БПЛА в качестве основы создания сетевой инфраструктуры рассматривается как привлекательный подход для эффективного увеличения коммуникационных возможностей сетей [1]. Интенсивное развитие электронной компонентной базы, микропроцессорной техники, теории и практики ИИ и нейросетевых технологий в сочетании с практическим опытом человека по повышению результативности за счет коллективизации усилий и их сосредоточения на приоритетных направлениях привело к тому, что одним из основных эволюционных направлений развития перспективных способов применения БПЛА сегодня является их групповое применение в виде так называемых стай или роев, связанных между собой сенсорно-сетевыми алгоритмами управления полетом [2]. Однако, несмотря на очевидные преимущества роя, такие как масштабируемость, живучесть и повышение эффективности выполнения задач, существует ряд фундаментальных проблем, требующих глубокой проработки и инновационных решений.

Формирование роя БПЛА определяется двумя базовыми обстоятельствами: поставленной задачей и аппаратно-программными возможностями, заложенными в наземные и бортовые элементы системы управления беспилотными летательными аппаратами [2], из чего можно выделить следующие проблемы: разработка робастных алгоритмов управления роем в условиях высокой неопределенности и динамической изменчивости операционной среды. Это включает в себя создание и валидацию релевантных алгоритмов траекторного управления для каждого индивидуального БПЛА в составе роя, обеспечивающих поддержание заданной формации и координацию действий для достижения общей целевой функции. В данном контексте критически важным является учет таких параметров, как отсутствие конфликтов между отдельно взятыми единицами роя, т.е. поддержание пространственно-временной когерентности роя и адаптация к стохастическим возмущениям.

Выбор той или иной стратегии группового управления определяет и структурную организацию соответствующей системы группового управления БПЛА (СГУ БПЛА). Существуют централизованные, децентрализованные и иерархические системы группового управления [3]. Централизованные системы, воспринимающие группу дронов как единое целое, на данный момент являются распространенными системами, ведь таким роем управляет оператор. Такие системы можно разделить на структуры с внешним управлением, где для каждого дрона требуется оператор, и на структуры с автономным управлением, где оператор требуется только для управления дроном-лидером. Преимущество обоих подходов заключается в их структурной простоте, отсутствии сложного технического решения, но они характеризуется низкой живучестью, поскольку отказ центрального управляющего элемента (связи с оператором или действующим дроном-лидером) приводит к коллапсу функционирования всей системы. Также недостаток таких централизованных структур заключается в необходимости присутствия оператора в сети для управления такими системами.

Децентрализованные системы, напротив, базируются на принципах локального взаимодействия между индивидуальными БПЛА, что обеспечивает повышенную адаптивность и устойчивость к единичным отказам. Данная система ориентирована на совместное использование ИИ и аппаратно-программных средств. Такие системы называют мультиагентными, т.к. управление каждым элементом роя выполняется ИИ-агентом. Характерной

особенностью мультиагентных систем является их способность к коллективному поведению с целью решения общей задачи. При этом каждый БПЛА самостоятельно управляет процессом своего функционирования, т.е. определяет свои действия и согласовывает их с другими агентами роя для наиболее эффективного, т.е. с минимальными затратами времени и ресурсов и наибольшей выгодой для роя, решения целевой задачи [2]. Тем не менее, реализация эффективного децентрализованного управления крупномасштабными роями БПЛА является нетривиальной научно-технической проблемой, требующей разработки архитектур управления и систем поддержки принятия решений, где стратегическое планирование осуществляется на высших уровнях абстракции, а тактическое выполнение траекторно-навигационных задач по формированию строя – на низших.

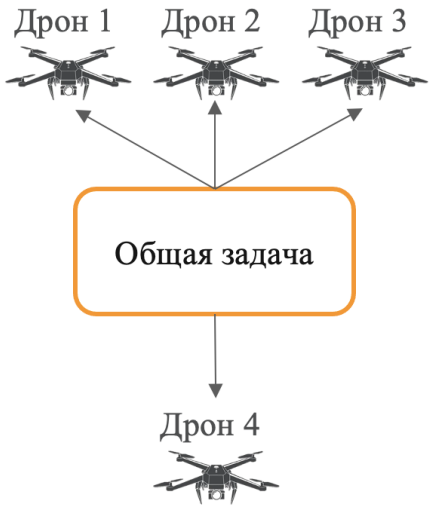


Рис. 1. Схема децентрализованной системы управления БПЛА

Иерархическая организация может сочетать в себе элементы централизованных и распределенных систем управления, т.е. реализовывать комбинированную стратегию управления [3]. Задача, заданная перед роем, разбивается на подзадачи, которые будут поставлены перед подгруппой роя со своим дроном-лидером. При потере лидера, внутри подгруппы выбирается новый, однако в таких системах параметр отказоустойчивости зависит от алгоритма делегирования управления. Однако, как и с децентрализованными системами, реализация такой системы требует сложного технического подхода, что непосредственно отразится на стоимости производства такой системы.

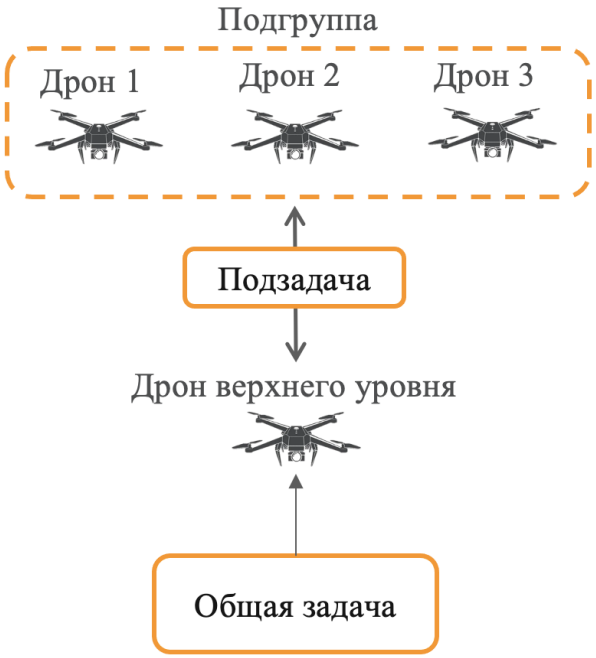


Рис. 2. Схема иерархической системы управления БПЛА

Критически значимой актуальной проблемой для всех трех типов систем является уязвимость роя к средствам радиоэлектронного подавления (РЭП). Высокая зависимость БПЛА от беспроводных каналов связи и систем спутниковой навигации делает их сугубо подверженными воздействию РЭБ. В условиях интенсивного электронного противодействия рой может утратить способность к синергетическим действиям, фрагментируясь на изолированные и легко уязвимые компоненты. Решением такой проблемы будет являться выбор децентрализованной (или иерархической) системы, где связь между единицами роя происходит по специальному каналу внутрироевого взаимодействия, или выбор подходящего протокола передачи данных. Последнее решение зависит от специфики задачи и условий эксплуатации. Для военных целей предпочтительнее использовать протоколы с высокой степенью безопасности и помехоустойчивости, в то время как в горнодобывающей промышленности и агропромышленности акцент стоит на дальности связи и энергоэффективности, а DSSS является надежным протоколом для связи с БАС [4].

Дополнительно, как было рассмотрено ранее, существует фундаментальная проблема оптимального выбора лидера и обеспечения надежной сетевой связности в рое, особенно в условиях отсутствия внешней инфраструктуры. В случаях, когда нельзя полагаться на инфраструктуру, а также в случаях, где возможно уничтожение отдельных БПЛА, необходим алгоритм выбора лидера роя [5]. Алгоритмы выбора лидера должны интегрировать критерии, такие как минимизация задержек в передаче данных и оптимизация энергопотребления для поддержания устойчивости роя. Для

обеспечения высокоэффективного функционирования роя необходима разработка высокопроизводительных и отказоустойчивых каналов связи, что представляет собой значительный вызов при масштабировании системы и увеличении численности дронов в составе роя.

Проблематика управления роем БПЛА также охватывает сложности поддержания динамической топологии роя, обеспечение адекватной динамики отдельных аппаратов, а также управление крупными плотными группами БПЛА как системами с распределенными параметрами. Необходима разработка механизмов, позволяющих дронам эффективно обмениваться данными о своем состоянии и намерениях, минимизируя при этом коллизии данных и перегрузку сетевых ресурсов, что является критически важным для масштабируемости системы при увеличении числа агентов (в децентрализованных системах).

В итоге, управление роем БПЛА представляет собой междисциплинарную исследовательскую область, требующую дальнейшей разработки в таких областях, как автономная навигация, децентрализованные мультиагентные системы, самоорганизация, избыточные архитектуры, стохастическое управление и локальные системы позиционирования. Разрешение обозначенных проблем позволит реализовать полный потенциал роевых технологий, существенно расширяя возможности беспилотных систем в широком спектре приложений.

Список используемых источников

1. Погодин Р. А., Широков И. Б. Система управления роя БПЛА // Современные проблемы радиоэлектроники и телекоммуникаций «РТ-2022»: материалы 18-й междунар. молодежной науч.-техн. конф. (Севастополь, 10–14 окт. 2022 г.) / под ред. И. Л. Афонина. Севастополь: Изд-во СевГУ, 2022. С. 43.

2. Ступницкий М. М., Мырова Л. О., Королев П. С. Рой БПЛА – новая парадигма применения малоразмерных БПЛА [Электронный ресурс] // Электросвязь. 2023. № 4. С. 2–10. URL: https://elsv.ru/wp-content/uploads/2026/01/ES-2023-04.pdf (дата обращения: 09.04.2026).

3. Мустаев А. Ф. Стратегии управления роем беспилотных летательных аппаратов [Электронный ресурс] // Вестник науки. 2019. № 3 (12). Т. 5. С. 96–99. URL: https://www.вестник-науки.рф/archiv/journal-3-12-5.pdf (дата обращения: 09.04.2026).

4. Евсеев Д. А., Дорошенко В.М. Актуальные протоколы передачи данных для беспилотных автоматизированных систем // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2025. № 2.

5. Ярмолик В. И. Новый алгоритм выбора лидера при автономном управлении роем БПЛА / В. И. Ярмолик, Т. С. Боброва, А. К. Ючков [Электронный ресурс] // Информационные технологии и системы 2023 (ИТС 2023) = Information Technologies and Systems 2023 (ITS 2023): материалы Международной научной конференции, Минск, 22 ноября 2023 / Белорусский государственный университет информатики и радиоэлектроники; редкол.: Л. Ю. Шилин [и др.]. Минск, 2023. С. 211–212. URL: https://libeldoc.bsuir.by/handle/123456789/54150 (дата обращения: 10.04.2026).

УДК 621.317.35

ИЗМЕРИТЕЛЬ-ХАРАКТЕРИОГРАФ НЕЛИНЕЙНЫХ ВАХ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

Боровков И. Ю. (студент гр. ФП-31 СПбГУТ)
Калинин А. Р. (студент гр. ФП-31 СПбГУТ)
Ольская М. А. (студент гр. ФП-31 СПбГУТ), olskaya.ma@sut.ru
Шумаков П. П. (к.т.н., заведующий кафедрой электроники СПбГУТ)

Разработка каждого электронного устройства начинается с анализа элементной базы. Одним из основных параметров нелинейного полупроводникового элемента является его вольтамперная характеристика (ВАХ). В связи с имеющейся потребностью в недорогом, простом и эффективном устройстве для анализа компонентов, была поставлена задача разработки подобного инструмента. Изготовленное в рамках работы над проектом устройство решает задачу автоматизации снятия вольтамперных характеристик, и тем самым обеспечивает студентов и радиолюбителей доступным инструментом для изучения полупроводниковых элементов.

полупроводниковые, компоненты, элементы, приборы, вольтамперные, характеристики, ВАХ, измерение, характериограф, Arduino, ЦАП, АЦП

Измеритель вольтамперной характеристики (ВАХ) – это устройство, предназначенное для получения и визуализации зависимости тока, протекающего через полупроводниковый прибор, от приложенного к нему напряжения. ВАХ является основной паспортной характеристикой любого полупроводникового элемента [1], так как она позволяет определить его ключевые параметры. Промышленные анализаторы обладают высокой стоимостью для учебных лабораторий или радиолюбительской практики.

Цель проекта: реализация программно-аппаратного комплекса с микроконтроллерным управлением для автоматического измерения и графического отображения ВАХ полупроводниковых приборов.

Задачи проекта: разработка принципиальной схемы, обоснование выбора компонентов, описание схемотехнического решения, алгоритмов измерений, представление программной реализации.

При разработке измерителя ВАХ были определены ключевые требования к его характеристикам. Диапазон измерений охватывает выходное напряжение от 0 до 5 В и измеряемый ток до 50 мА с шагом дискретизации в 101 точку измерения. Точность измерений должна обеспечивать погрешность не более ±5 % при разрешении 12 бит (ЦАП) и стабильной работе в рабочем диапазоне.

Требования к визуализации предусматривают графическое отображение ВАХ в реальном времени с четкой индикацией текущих значений напряжения и тока, возможностью масштабирования графика и наглядным представлением результатов измерений.

Для реализации измерителя была выбрана оптимальная элементная база. В качестве центрального управляющего устройства выступает микроконтроллер Arduino Uno, обеспечивающий достаточную вычислительную мощность, наличие встроенного 10-битного АЦП и поддержку интерфейса SPI. Цифро-аналоговый преобразователь MCP4921 с 12-битной разрядностью обеспечивает высокую точность формирования испытательного напряжения. Дисплей ILI9341 предоставляет цветной TFT-экран с высоким разрешением для детальной визуализации графиков. Дополнительными компонентами системы являются измерительный резистор 470 Ом, ZIF-панель для установки исследуемых приборов и стабилизатор напряжения LM1117. Выбранные компоненты обеспечивают оптимальное соотношение характеристик и стоимости, полностью удовлетворяя всем техническим требованиям проекта.

На рисунке (рис. 1) представлена принципиальная схема устройства, которая состоит из микроконтроллера, микросхемы цифроаналогового преобразователя, дисплея, ZIF-панели для установки исследуемого устройства и измерительного резистора 470 Ом. Микроконтроллер Arduino UNO выбран из-за доступности библиотек и простоты написания кода. ЦАП MCP 4921 разрешением 12 бит служит для формирования напряжения, которое будет подаваться на неизвестное устройство. Номинал резистора в 470 Ом выбран исходя из того, что необходимо ограничить ток, протекающий в измерительной цепи, чтобы не допустить повреждения входов микроконтроллера.

Микроконтроллер Arduino Uno посредством интерфейса SPI передает цифровой код на двенадцатибитный ЦАП MCP4921, который преобразует его в аналоговое напряжение в диапазоне 0-5 В. Это напряжение подается на измерительную цепь, состоящую из резистора номиналом 470 Ом и исследуемого прибора, подключенных последовательно. Измерение значений напряжения на калибровочном резисторе и исследуемом приборе осуществляется через аналоговые входы микроконтроллера Arduino. На основе полученных данных в соответствии с законом Ома производится расчет силы тока, протекающего через измерительную цепь [2].

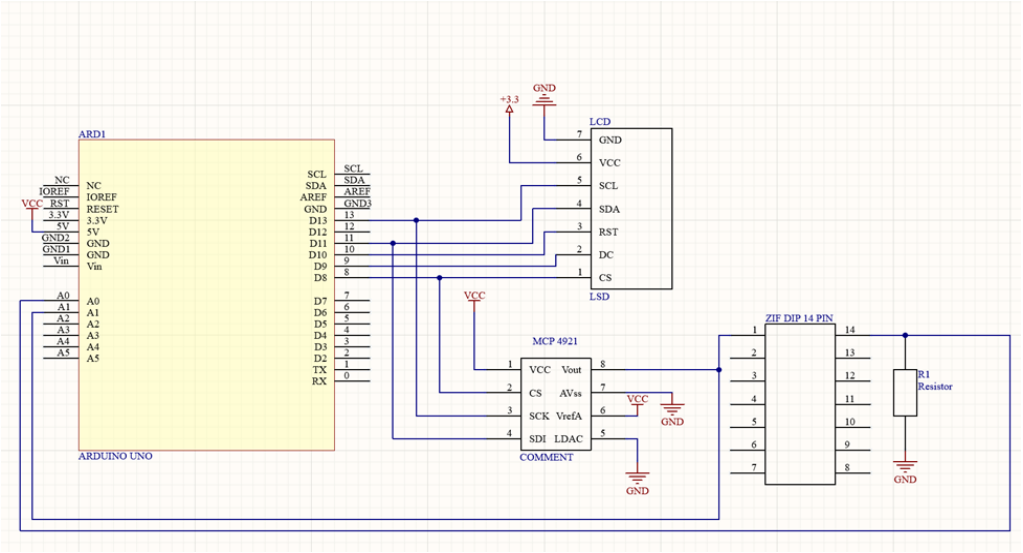


Рис. 1. Принципиальная схема устройства

Программа для микроконтроллера написана на языке C++ в среде Arduino IDE. Оперативная память используется для хранения измеренных данных, для них предусмотрены массивы фиксированного размера.

В программе задействованы три основные библиотеки. SPI.h библиотека для обмена данными с периферийными устройствами по протоколу SPI. Adafruit_GFX.h базовая графическая библиотека. Adafruit_ILI9341.h обеспечивает работу с дисплеем на контроллере ILI9341.

Алгоритм измерения. Сначала задается начальное напряжение и конечное. ЦАП последовательно устанавливает напряжения, соответствующие равномерно распределенным точкам, шаг вычисляется автоматически. На каждом шаге после короткой задержки, необходимой для стабилизации напряжения в измерительной цепи, производится многократное считывание аналоговых входов. Полученные значения усредняются – это позволяет подавить случайные помехи и повысить точность. Далее средние значения АЦП пересчитываются в милливольты с учетом опорного напряжения и разрядности АЦП. По закону Ома рассчитывается ток через диод в миллиамперах по формуле $I = \frac{(Vdac_{avg} - Vdiode_{avg})}{470}$, где $Vdac_{avg}$ – усредненное напряжение на выходе ЦАП, $Vdiode_{avg}$ – усредненное напряжение на аноде диода, 470 – сопротивление токоизмерительного резистора в омах. Если рассчитанный ток превышает 50 мА, точка отбрасывается – это реализует защиту от перегрузки как исследуемого прибора, так и измерительной цепи. В момент, когда ток впервые превышает порог 1 мА, фиксируется пороговое напряжение, которое затем используется при анализе и отображении. Все достоверные точки сохраняются в массивы для последующей отрисовки.

Построение графика на дисплее происходит после завершения цикла сканирования. Программа находит минимальное и максимальное значения напряжения среди сохраненных точек, а также максимальное значение тока. Далее отрисовываются оси координат и дополнительные информационные поля. Вертикальной линией отмечается найденное пороговое напряжение. В нижней части экрана отображается количество полученных точек, диапазон напряжений и пороговое напряжение.

Передача данных на компьютер организована через последовательный порт. В режиме отладки в Serial Monitor выводятся подробные текстовые отчеты о каждом шаге измерения – номер точки, напряжение на ЦАП, напряжение на диоде, рассчитанный ток. В ходе выполнения работы был успешно разработан и изготовлен программно-аппаратный комплекс для автоматического измерения и графического отображения вольтамперных характеристик полупроводниковых приборов. Основные итоги работы включают:

1. Создание работоспособного устройства с микроконтроллерным управлением.
2. Реализацию автоматического режима снятия ВАХ.
3. Внедрение системы визуализации результатов измерений.

Созданный комплекс обладает следующими ключевыми преимуществами:

1. Полная автоматизация процесса измерения ВА
2. Наглядное графическое отображение результатов в реальном времени.
3. Высокая точность измерений (погрешность не более ±5 %).
4. Широкий диапазон измеряемых параметров (0-5В, 0-50мА).
5. Компактные размеры и автономность работы.
6. Простота использования благодаря интуитивно понятному интерфейсу.
7. Возможность работы с различными типами полупроводниковых приборов.

Для дальнейшего совершенствования устройства планируется реализация следующих направлений развития:

1. Расширение функциональных возможностей.
2. Добавление гибкого выбора диапазона рабочего напряжения.
3. Внедрение функции экспорта полученных данных.
4. Модернизация системы крепления микроконтроллера.
5. Оптимизация конструкции корпуса с использованием современных материалов.

Список использованных источников:

1. Наумчик В. В., Спиридонов Л. К. Полупроводниковые приборы: Учеб. для вузов по спец. «Полупроводниковые и микроэлектронные приборы». 4-е изд., перераб. и доп. М.: Высш. шк., 1987. 479 с.: ил.

2. Хоровиц, Пауль. Искусство схемотехники [Текст] / П. Хоровиц, У. Хилл; пер. с англ. Б. Н. Бронина [и др.]. Изд. 7-е. Москва: Бином, 2015. 704 с.: ил.; 24 см.; ISBN 978-5-9518-0351-1.

УДК 681.2.082

МЕТАМОДЕЛЬНЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ УСТРОЙСТВ АВТОМАТИЧЕСКОЙ СТАБИЛИЗАЦИИ ФИЗИЧЕСКИХ ПАРАМЕТРОВ НА БАЗЕ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ КОНТРОЛЛЕРОВ

А. В. Ваганов (ст. преп. кафедры САР СПбГУТ)
А. А. Демидов (студент гр. ИСТ-441м СПбГУТ), demidov.aa@sut.ru

В статье рассматривается система стабилизации мощности оптического излучения для турбидиметрических измерений мутности жидкостей. Обоснована актуальность разработки такой системы, а также рассмотрены основные области ее применения: коммунальное хозяйство, промышленность и задачи непрерывного мониторинга качества водных сред.

Показано, что стабильность оптического сигнала является ключевым фактором, определяющим точность измерений и достоверность экспериментальных данных. Проведен анализ преимуществ и недостатков существующих методов измерения мутности. Описана структура системы стабилизации оптического сигнала. Предложен вариант реализации ПИД-регулятора на программируемых аналоговых микросхемах.

турбидиметрия, стабилизация оптического сигнала, ПИД-регулятор, контроль мутности, микроконтроллер

В современных технических, измерительных и исследовательских системах важную роль играет автоматическая стабилизация физических параметров – температуры, давления, расхода, мощности излучения и др. Отклонение регулируемых величин от заданных значений снижает качество работы устройств, увеличивает погрешности измерений и ухудшает эксплуатационные характеристики. Особое значение задача стабилизации приобретает в оптико-электронных системах, где даже незначительные изменения мощности источника излучения способны существенно повлиять на достоверность результатов, например, в турбидиметрических исследованиях жидких и коллоидных сред [1].

Одновременно возрастает потребность в формальных подходах к проектированию систем автоматического регулирования, ориентированных на последующую программную реализацию на базе ПЛК. Традиционная разработка нередко требует больших временных затрат и сопровождается трудностями при согласовании модели и программного кода. Перспективным решением является метамоделирование – формальное описание со-

става системы, связей между компонентами, параметров элементов и правил их преобразования в исполняемое представление. Использование метамоделей создает основу для автоматизации проектирования и генерации прикладного кода.

Метамодельный подход к описанию систем стабилизации

Метамодель в контексте данной работы определяется как формализованное описание структуры и поведения устройства автоматической стабилизации, достаточное для автоматической генерации программного кода на языке ST стандарта IEC 61131-3. Метамодель включает [2]:

- состав функциональных блоков (датчик, регулятор, исполнительное устройство, объект);
- параметры блоков (коэффициенты регулятора, период дискретизации, диапазоны сигналов);
- связи между блоками (каналы передачи сигнала ошибки, управляющего воздействия);
- правила преобразования в код (шаблоны генерации для каждого типа блока).

Предлагаемый подход позволяет отделить логику системы от конкретной реализации и обеспечивает возможность повторного использования описания для разных объектов стабилизации.

Анализ систем стабилизации физических параметров

Наиболее распространенным подходом является использование замкнутых систем с отрицательной обратной связью, где ошибка регулирования $e(t) = r(t) - y(t)$, а управляющее воздействие формируется на основе выбранного закона. Сравнение классических законов регулирования показывает, что ПИД-регулятор обеспечивает наилучшее сочетание точности, быстродействия и помехоустойчивости, что делает его базовым вариантом для стабилизации мощности оптического излучения [3].

Выбор аппаратно-программных средств

ПЛК обладают высокой надежностью, развитыми средствами ввода-вывода и поддержкой языков IEC 61131-3, включая ST. Однако для высокоскоростной стабилизации с субмиллисекундным откликом традиционные

ПЛК могут быть недостаточно эффективны. В таких случаях целесообразно использовать гибридные архитектуры или программируемые микросхемы (ПЛИС, SoC FPGA). В рамках данной работы в качестве целевой платформы выбран ПЛК с поддержкой ST, что обеспечивает баланс между гибкостью разработки и промышленной применимостью [4].

Разработка метамодели ПИД-системы стабилизации мощности оптического излучения

Для выбранного примера метамодель описывает:

- объект – источник оптического излучения с передаточной функцией W(s);
- датчик – фотоприемник с коэффициентом преобразования Кф и аддитивным шумом n(t);
- регулятор – дискретный ПИД-закон:

$$u[k] = K_p e[k] + K_i \sum_{i=0}^{k} e[i]T + K_d \frac{e[k] - e[k-1]}{T},$$

где T – период дискретизации; исполнительный блок – цепь управления током накачки источника.

Метамодель формализуется в виде набора взаимосвязанных типов (Regulator, Sensor, Actuator, Plant) с заданными атрибутами (коэффициенты, пределы, период). Правила трансформации определяют, как каждый тип отображается в шаблон ST-кода с последующей подстановкой параметров.

Трансформация метамодели в программный код на ST

Разработан инструментальный прототип, который по описанию метамодели генерирует:

- объявление переменных (уставка, текущее значение, ошибка, управляющий сигнал, коэффициенты);
- реализацию ПИД-алгоритма в циклическом прерывании по таймеру;
- обработку аналоговых входов/выходов;
- защиту от насыщения интегратора (anti-windup).

Пример фрагмента кода:

```
VAR
 setpoint, pv, error, output, Kp, Ki, Kd, Ts: REAL;
 integral, prev_error: REAL;
END_VAR

// ПИД-алгоритм
error:= setpoint – pv;
integral:= integral + Ki * error * Ts;
output:= Kp * error + integral + Kd * (error – prev_error) / Ts;
prev_error:= error;
```

Генерация позволяет автоматически получать работоспособный код для ПЛК, сокращая ручную разработку и исключая ошибки согласования [5].

Альтернативной реализацией ПИД-регулятора может быть построена на базе дискретно программируемых аналоговых интегральных схем (ПАИС). Вариант реализации такого устройства в среде AnadigmDesigner2 показан на рисунке 1.

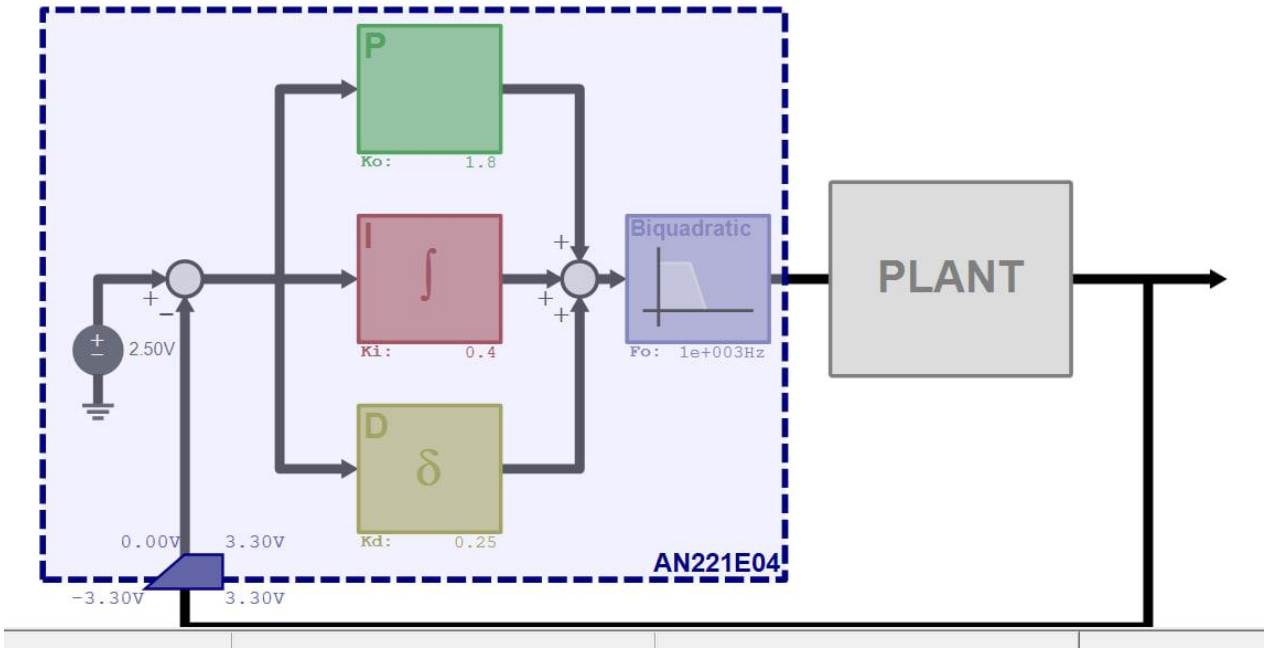


Рис. 1. ПИД-регулятор в среде AnadigmDesigner2

На рисунке представлена структурная схема системы автоматической стабилизации оптического сигнала, реализованной на базе программируемой аналоговой матрицы AN221E04 в среде AnadigmDesigner2.

Заключение

Предложенный метамодельный подход обеспечивает формализацию устройств автоматической стабилизации физических параметров и автоматизированную генерацию программного кода на языке ST. Разработанная метамодель ПИД-системы стабилизации мощности оптического излучения и инструментальный прототип позволяют сократить время проектирования, повысить надежность реализации и облегчить адаптацию системы к новым объектам. В дальнейшем планируется расширение метамодели для поддержки адаптивных и интеллектуальных регуляторов, а также интеграция с симуляционной средой для предварительной настройки параметров.

Список используемых источников

1. Карпов А. Г. Теория автоматического управления. Часть 1: учебное пособие – Томск: ТМЛ-Пресс, 2011, 212 с.

2. Шарапов В. М., Полищук Е. С., Кошевой Н. Д., Ишанин Г. Г., Минаев И. Г., Совлуков А. С. Датчики: Справочное пособие / под ред. В. М. Шарапова, Е. С. Полищука. М.: «Техносфера». 2012. 624 с.

3. Верхова Г. В. Языки программирования для автоматизированных производств. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. 64 с.

4. Что такое программируемые контроллеры (ПЛК) [Электронный ресурс] // Приборэнерго.рф. URL: https://xn--90aefk0afdbjdc7m.xn--p1ai/press/chto-takoe-programmiruemye-kontrollery-plk/ (дата обращения: 05.04.2026).

5. Актуаторы [Электронный ресурс] // БЕРГАБ URL: https://bergab.ru/lmaktuatory.shtml (дата обращения: 02.04.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры САР СПбГУТ А. В. Вагановым.

УДК 621.396.67

ВЛИЯНИЕ МАТЕРИАЛА КОРПУСА БПЛА НА ХАРАКТЕРИСТИКИ ИЗЛУЧЕНИЯ КОНФОРМНОЙ ПАТЧ-АНТЕННЫ

О. С. Воищев (студент группы РТ-11 СПбГУТ), voishchev.os@sut.ru
П. А. Межевов (старший преподаватель кафедры РТ СПбГУТ)

Статья посвящена влиянию конструкционных материалов корпуса БПЛА на характеристики излучения конформной патч-антенны. Показано, что экранирующий углепластик переотражает сигнал, повышая коэффициент усиления антенны. Стеклопластики, органопластики и термопластичные композиты, обладая низкой диэлектрической проницаемостью, обеспечивают радиопрозрачность и практически не изменяют форму диаграммы направленности. Приведены количественные оценки параметров излучения. Даны рекомендации по выбору материала и конструктивной компенсации влияния. Результаты работы могут быть использованы при проектировании конформных антенных систем для БПЛА гражданского и специального назначения, а также при оптимизации корпусных композитов с заданными электродинамическими свойствами.

БПЛА, конформная антенна, патч-антенна, материал корпуса

Беспилотные летательные аппараты (БПЛА) в последние годы получили широкое распространение как в гражданской, так и в военной сфере. Рост рынка БПЛА стимулирует развитие новых технологий, направленных на повышение их функциональности, автономности и скрытности. Одним из ключевых направлений совершенствования БПЛА является модернизация бортового радиоэлектронного оборудования, в частности антенных систем, которые обеспечивают связь, навигацию, радиолокацию и передачу данных. При этом традиционные выступающие антенны увеличивают аэродинамическое сопротивление и заметность аппарата, что особенно критично для высокоскоростных и малозаметных БПЛА.

Альтернативой выступающим антеннам являются конформные антенные системы, которые размещаются непосредственно на поверхности корпуса летательного аппарата или интегрируются в его несущие конструкции. Конформные антенны обладают малым профилем, что позволяет сохранить аэродинамику аппарата и не ухудшать его массогабаритные характеристики [1]. Особое место среди них занимают патч-антенны. Благодаря компактности, технологичности и возможности эффективной работы на изогнутых поверхностях, микрополосковые антенны широко используются в системах связи, навигации и радиолокации БПЛА [2].

Однако при интеграции конформных антенн в конструкцию планера может возникнуть проблема электромагнитной совместимости, связанная с материалом, из которого изготовлен корпус БПЛА, приводящая к искажению диаграммы направленности антенны. В настоящее время при производстве БПЛА широко применяются полимерные композитные материалы, некоторые из которых приведенные в табл. 1 [3].

ТАБЛИЦА 1. Материалы для корпусов БПЛА

Материал	Прочность на разрыв, МПа	Плотность, г/см3	Диэлектрическая проницаемость
Стеклотекстолит (FR-4, Rogers RT, СТЭФ)	200 – 400	1.7 – 2.2	2.2 – 10.2
Стеклопластики (GFRP, GF-PETG, GF-Nylon)	130 – 2300	1.4 – 2.1	3.5 – 5.5
Углепластики (XECARB® SL 17-C15-P3, Precimid1174Pro CF)	600 – 4000	1.4 – 1.8	Электропроводящий материал
Органопластики (ВКО-19Л, PP/PE-g-MA)	700 – 3300	1.0 – 1.5	2.5 – 4.0
Термопластичные композиты (ПА6-210-ДС, RTP 4087, АБС-пластик)	80 – 1500	1.0 – 1.9	2.0 – 6.0

Целью данной работы является анализ и количественная оценка влияния материала корпуса БПЛА на основные характеристики излучения конформной патч-антенны посредством моделирования в прикладном пакете ANSYS HFSS.

Патч-антенна (Рис. 1) была рассчитана по формулам представленным в книге [4].

В качестве диэлектрика был выбран стеклотекстолит FR-4 толщиной 2 мм, центральная частота равна 2.4ГГц. Тип питания – коаксиальный кабель. Полученные параметры представлены на рис. 2.

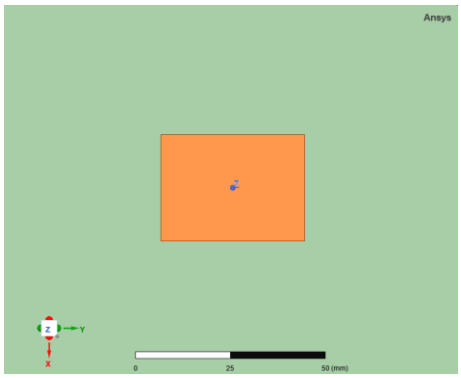


Рис. 1. Патч-антенна

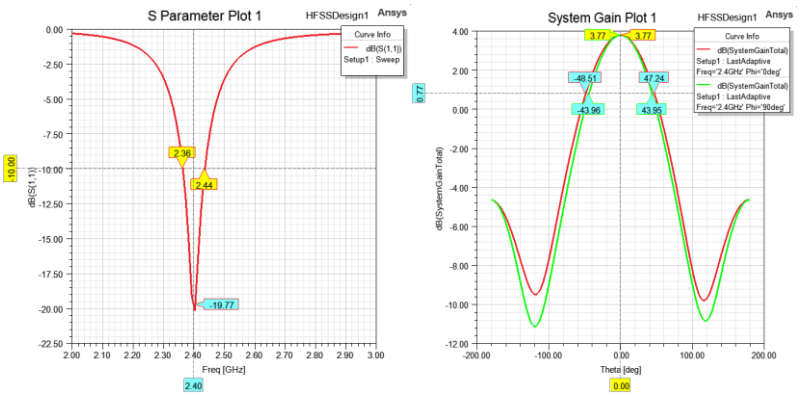


Рис. 2. График параметра S(1,1) и ДН в E (красн.) и H (зелен.) плоскостях для FR-4

В качестве материала стеклопластика выбран GF-Nylon. На рис. 3 представлены полученные результаты при моделировании. Рабочая полоса 80 МГц, резонансная частота 2.44 ГГц, КУ 4 дБ по мощности, ширина ДН в E и H плоскостях 91.8 и 89.5 град.

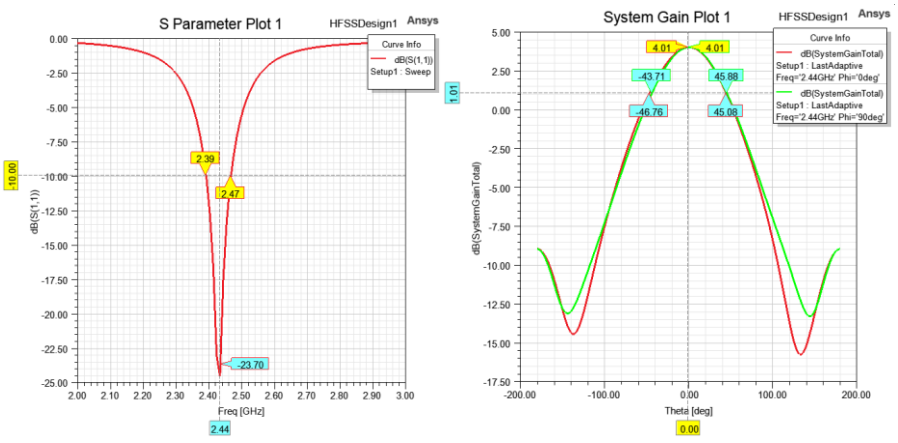


Рис. 3. График параметра S(1,1) и ДН в E (красн.) и H (зелен.) плоскостях для стеклопластика

В качестве углепластика выбран Precimid1174Pro CF. На рис. 4 представлены полученные результаты при моделировании. Рабочая полоса 70

МГц, резонансная частота 2.44 ГГц, КУ 5.24 дБ по мощности, ширирна ДН в Е и Н плоскостях 69 и 75 град.

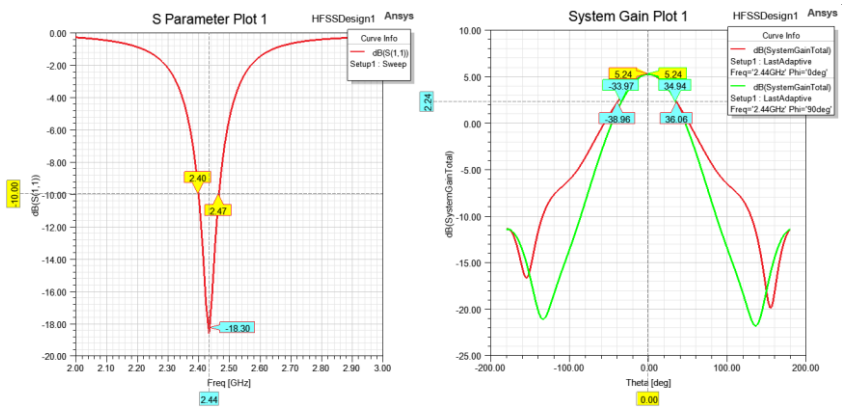


Рис. 4. График параметра S(1,1) и ДН в Е (красн.) и Н (зелен.) плоскостях для углепластика

В качестве органопластика выбран ВКО-19Л. На рис. 5 представлены полученные результаты при моделировании. Рабочая полоса 80 МГц, резонансная частота 2.44 ГГц, КУ 3.95 дБ по мощности, ширина ДН в Е и Н плоскостях 91.8 и 90.5 град.

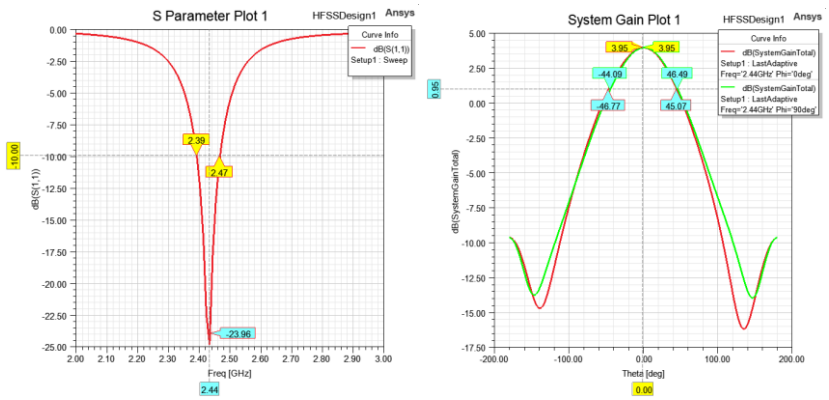


Рис. 5. График параметра S(1,1) и ДН в Е (красн.) и Н (зелен.) плоскостях для органопластика

В качестве термопластичного композита выбран ПВХ пластик. На рис. 6 представлены полученные результаты при моделировании. Рабочая полоса 80 МГц, резонансная частота 2.43 ГГц, КУ 4.11 дБ по мощности, ширина ДН в Е и Н плоскостях 91.7 и 87.7 град.

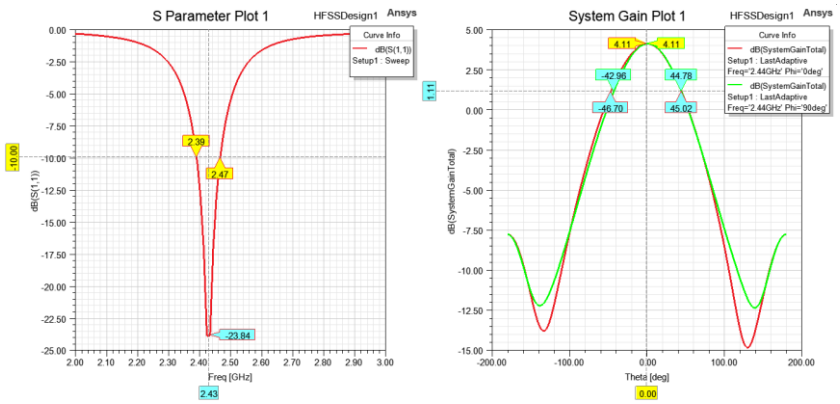


Рис. 6. График параметра S(1,1) и ДН в Е (красн.) и Н (зелен.) плоскостях для термопластичного композита

В результате выполнения работы по исследованию влияния материала корпуса БПЛА на характеристики излучения конформной патч-антенны были получены следующие основные выводы: применение современных материалов позволяет значительно увеличить прочность антенной системы, приводит к незначительному увеличению резонансной частоты и коэффициента усиления, в случае радиопрозрачных материалов и значительному росту КУ в случае экранирующих материалов, на примере угленаполненного композита Precimid1174Pro CF.

Металлические элементы внутри БПЛА (проводка, двигатели) также искажают поле антенны, поэтому конформные антенны требуют тщательной настройки в составе реальной конструкции [5].

Список используемых источников

1. Веревкина Е. В. Микрополосковая антенна для беспилотного летательного аппарата //Интерэкспо Гео-Сибирь. 2018. № 7. С. 191-196.

2. Ильин Е. М., Полубехин А. И., Черевко А. Г. Конформные антенные системы – перспективное направление развития бортовых РЛК для беспилотных летательных аппаратов. Вестник СибГУТИ. 2015;(2):149-155.

3. Гуртовник И. Г. и др. Радиопрозрачные изделия из стеклопластиков //Издательство «Мир». Москва. 2003.

4. James J. R., Hall P. S. (ed.). Handbook of microstrip antennas. IET, 1989. Т. 28. № 1.

5. Reis S. et al. General Overview of Antennas for Unmanned Aerial Vehicles: A Review // Electronics. 2025. Т. 14. № 16. С. 3205.

УДК 519.7

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОГО АНАЛИЗА ЛИЦЕВЫХ ЭКСПРЕССИЙ: МЕТОДЫ, ПРОБЛЕМЫ И НАПРАВЛЕНИЯ РАЗВИТИЯ

Е. А. Володина (студент группы ИСТ-262 СПбГУТ), volodina.ea@sut.ru
Л. М. Макаров (преподаватель кафедры САР СПбГУТ)

В статье рассматриваются концептуальные аспекты построения систем распознавания эмоциональных состояний через призму теории семантического позиционирования. Описывается метод гибридного анализа лицевых экспрессий, основанный на формировании информационных пакетов данных. Предложенный подход позволяет формализовать переход от численных метрик цифрового изображения к устойчивым семантическим категориям (эмоциям).

математика, компьютерный анализ изображений, кибернетика мышления

В условиях стремительного развития технологий искусственного интеллекта задачи автоматического анализа эмоциональных состояний человека приобретают особую актуальность. Лицевая экспрессия рассматривается как один из наиболее информативных каналов передачи невербальной информации, позволяющий интерпретировать внутреннее психоэмоциональное состояние субъекта [1, 2]. Несмотря на значительный прогресс в области машинного обучения и компьютерного зрения, проблема перехода от численных характеристик изображения к устойчивым семантическим категориям остается недостаточно формализованной, что обусловливает необходимость поиска новых теоретических подходов [3]. В данной работе предлагается рассмотреть процесс анализа лицевых экспрессий с позиций кибернетики мышления, интерпретируя его как задачу семантического позиционирования в пространстве смысловых состояний.

В рамках предлагаемого подхода анализ изображения трактуется как процесс формирования целостной информационной структуры, в которой исходные данные подвергаются последовательной иерархической трансформации. Переход от пиксельного представления к интерпретируемым категориям осуществляется через формирование информационных пакетов, обладающих определенной семантической нагрузкой. При этом различные уровни обработки соответствуют различным степеням абстракции, начиная от численных характеристик изображения и заканчивая интерпретацией

эмоциональных состояний. Итоговая категория рассматривается как эмерджентное свойство системы, возникающее в результате сложного взаимодействия множества признаков, что соответствует современным представлениям в области аффективных вычислений [8].

Начальный этап анализа связан с выделением однородных областей изображения, выступающих носителями первичной информации. Для решения данной задачи применяются методы кластеризации, позволяющие структурировать исходный массив данных и повысить его интерпретируемость. Использование алгоритма k-средних обеспечивает группировку пикселей по признаку цветового сходства и широко применяется в задачах компьютерного зрения в качестве предварительного этапа обработки данных [3]. В контексте анализа лицевых изображений целесообразно рассматривать разделение изображения на области, соответствующие основному тону кожи, теневым зонам и областям освещения. Соотношение указанных компонент может использоваться как количественный индикатор устойчивости визуального образа, поскольку преобладание основного тона, как правило, свидетельствует о снижении уровня шумов и характерно для нейтральных состояний.

Для повышения точности интерпретации необходимо учитывать микроструктурные особенности изображения, формируемые мимическими изменениями. Локальные деформации поверхности лица, включая морщины и складки, рассматриваются как значимые элементы, несущие дополнительную семантическую нагрузку. Подобный подход согласуется с принципами систем кодирования мимических движений, в частности FACS, где отдельные движения лицевых мышц выступают в качестве базовых единиц анализа [4]. Количественная оценка таких изменений может быть реализована посредством наложения дискретной матричной сетки и последующего анализа вариативности яркости внутри ее ячеек. Это позволяет отделять устойчивые текстурные признаки от случайных искажений, вызванных условиями освещения, и формировать систему информационных пакетов с различной степенью значимости.

Предлагаемый подход основан на интеграции цветовых и текстурных характеристик изображения в рамках единой модели анализа. Синтез данных признаков обеспечивает более устойчивую интерпретацию по сравнению с использованием каждого из них по отдельности. В ситуациях, когда между различными типами признаков возникает противоречие, приоритет отдается текстурным характеристикам, поскольку они в меньшей степени

подвержены влиянию внешних факторов. Эффективность подобных гибридных решений подтверждается современными исследованиями, посвященными распознаванию эмоций в условиях неконтролируемой среды [5, 6].

Несмотря на достигнутые результаты, существующие методы анализа лицевых экспрессий характеризуются рядом ограничений, связанных с зависимостью от качества исходных данных, чувствительностью к условиям освещения и сложности формализации субъективных эмоциональных состояний. Дополнительные трудности обусловлены ограниченностью доступных обучающих выборок и их неоднородностью [5]. Существенным аспектом также является необходимость соблюдения требований законодательства в области обработки персональных и биометрических данных, а также соответствие международным стандартам представления и защиты информации [7, 8]. В этой связи перспективными направлениями развития являются интеграция методов глубокого обучения с семантическими моделями, разработка адаптивных алгоритмов анализа и расширение использования мультимодальных данных.

Рассмотрение анализа лицевых экспрессий с позиций семантического позиционирования позволяет существенно расширить традиционные представления о процессе интерпретации визуальной информации. Предложенная модель, основанная на формировании информационных пакетов и интеграции различных типов признаков, обеспечивает повышение устойчивости и точности распознавания. Дальнейшее развитие данного направления связано с углублением междисциплинарных исследований и созданием интеллектуальных систем, способных к комплексному анализу невербального поведения человека.

Список используемых источников

1. Макаров Л. М., Поздняков А. В. Семантическое позиционирование кластеров информационных пакетов [Электронный ресурс] // Информационные технологии и телекоммуникации. 2023. Т. 11. № 3. С. 49–61. URL: https://itit.sut.ru/2023_3.pdf (дата обращения: 25.04.2026).

2. Прэтт У. Цифровая обработка изображений: в 2 т. М.: Мир, 1982. 790 с. (Фундаментальный труд по обработке сигналов)

3. Bishop C. M. Pattern Recognition and Machine Learning [Электронный ресурс] // Microsoft Research. 2006. URL: https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf.

4. Экман П., Фризен У. Система кодирования лицевых движений (FACS): Методика измерения движений лица. М.: Генезис, 2010. 200 с.

5. Goodfellow I. J. et al. Challenges in Representation Learning: A Report on Three Machine Learning Contests (FER2013) [Электронный ресурс] // ArXiv.org. 2013. URL: https://arxiv.org/abs/1307.0414 (дата обращения: 19.03.2026).

6. Федеральный закон № 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 31.03.2026).

7. Mollahosseini A. et al. AffectNet: A Database for Facial Expression, Valence, and Arousal Computing in the Wild [Электронный ресурс] // IEEE Xplore. 2017. URL: https://ieeexplore.ieee.org/document/8013717 (дата обращения: 25.04.2026).

8. ГОСТ Р ИСО/МЭК 19794-5-2013 Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200105315 (дата обращения: 25.04.2026).

УДК 535.245

АЛГОРИТМ ПОДБОРА ДЛИН ВОЛН ДЛЯ СОЗДАНИЯ СВЕТОФИЛЬТРОВ В ИК-ДИАПАЗОНЕ

Е. А. Гаврилова (студент гр. ИКФ-21 СПбГУТ), gavrilova.ea@sut.ru
И. Е. Скалецкая (к.т.н., доцент кафедры Ф СПбГУТ)

Методы инфракрасной спектроскопии широко применяются в химии, биологии, медицине, экологии и промышленности благодаря способности выявлять характерные спектральные признаки веществ. Светофильтры для ИК-диапазона выступают неотъемлемым элементом оптических систем, обеспечивая селективное пропускание излучения и минимизацию фоновых помех. Их корректное применение напрямую влияет на чувствительность и разрешающую способность измерительных установок.

светофильтр, длина волны, спектроскопия

Проблема монохроматизации света, т.е. выделение определенного спектрального интервала длин волн, имеет большое практическое значение. Одним из способов монохроматизации света является применение различного рода монохроматоров. При решении большинства задач практической спектроскопии сравнительно узкие спектральные области излучения можно выделить с помощью монохроматических светофильтров. В отличие от спектральных приборов – монохроматоров – монохроматические светофильтры обладают значительно большим сечением фильтруемого пучка и большей апертурой [1].

Светофильтрами, или просто фильтрами, называются устройства, меняющие спектральный состав или энергию падающей на них световой энергии без изменения формы ее фронта. Основные характеристики (параметры) светофильтров следующие.

1. Пропускание (прозрачность) в максимуме полосы пропускания.
2. Длина волны λ_{max}, соответствующая максимуму полосы пропускания.
3. Спектральная ширина полосы пропускания $2\delta\lambda$.
4. Крылья полосы пропускания.
5. Апертура светофильтра.

Светофильтры делятся на серые (нейтральные), у которых оптическая плотность не зависит от длины волны, и селективные – с зависимой плотностью. Селективные бывают узкополосными (монохроматическими) – для выделения узкой спектральной области.

Наиболее распространены абсорбционные светофильтры: ослабление света в них происходит за счет поглощения (по закону Бугера-Ламберта)

и частично – отражения. Отражательные светофильтры (металлические пленки и диэлектрические зеркала) ослабляют свет главным образом за счет отражения. Интерференционные светофильтры работают на основе многолучевой интерференции и состоят из подложки с чередующимися отражающими и диэлектрическими слоями [1].

Теоретический расчет интерференционного фильтра основан на анализе его многослойной структуры и направлен на определение ключевых параметров: максимального пропускания (T_{max}, до 70 %), длины волны максимума пропускания (λ_{max}), ширины полосы пропускания ($\Delta\lambda$) и фактора контраста – отношения максимального и минимального пропусканий. На итоговые характеристики существенно влияют толщина слоев, показатель преломления подложки и поглощение в слоях, особенно в металлических полупрозрачных элементах.

Для выполнения расчетов применяют несколько методов – матричный (через характеристическую матрицу), рекуррентный (с учетом многократных отражений и преломлений), адмиттансный, а также инструменты многопараметрического поиска для оптимизации конструкции под заданные требования.

Процесс начинается с задания исходных данных: центральной длины волны (λ_i), угла падения света (θ_{TF}) и показателей преломления используемых материалов (n_1 и n_2). Далее вычисляют период структуры (ΔTF) и оптимальную толщину (L_{TF}) для достижения максимального отражения. В ходе проверки оценивают ширину полосы пропускания ($\Delta\lambda$), коэффициент отражения и влияние разности показателей преломления ($\Delta n = |n_2 - n_1|$). При необходимости параметры корректируют – например, для сужения полосы пропускания уменьшают Δn и увеличивают L_{TF}. В результате получают фильтр с расчетными характеристиками, соответствующими техническим требованиям [2].

Экспериментальный подбор длин волн для выбора светофильтров под задачи ИК-спектроскопии, например полимеров, начинается с подготовки и регистрации спектральных характеристик исследуемых образцов. Последующее описание экспериментального метода будет рассмотрено на примере полимерного образца – полипропилена. Полученный спектр (зависимость коэффициента пропускания от волнового числа) необходимо сравнить с справочными материалами – рис. 1 [3].

Для сравнения необходимо учитывать ослабление ИК излучения при прохождении через образцы больших толщин. Чтобы сравнение оказалось корректным, необходимо нивелировать разницу толщин с помощью закона Бугера-Ламберта-Бера по формуле 1.

$$I = I_0 \exp(-k_\lambda l), \quad (1)$$

где I_0 – интенсивность излучения на входе, I – интенсивность излучения на выходе, k_λ – коэффициент поглощения, l – толщина образца.

Эталонная толщина должна быть выбрана под конкретные задачи, в данном случае была выбрана толщина в 10 мкм. Приведенный спектр к эталонной толщине представлен на рис. 2.

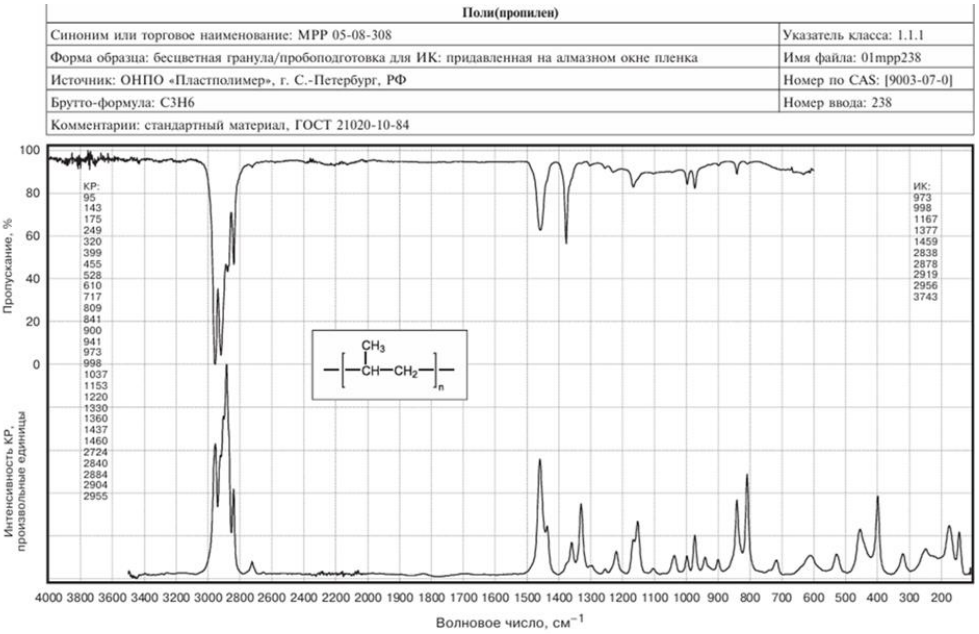


Рис. 1. Справочный ИК-спектр полипропилена

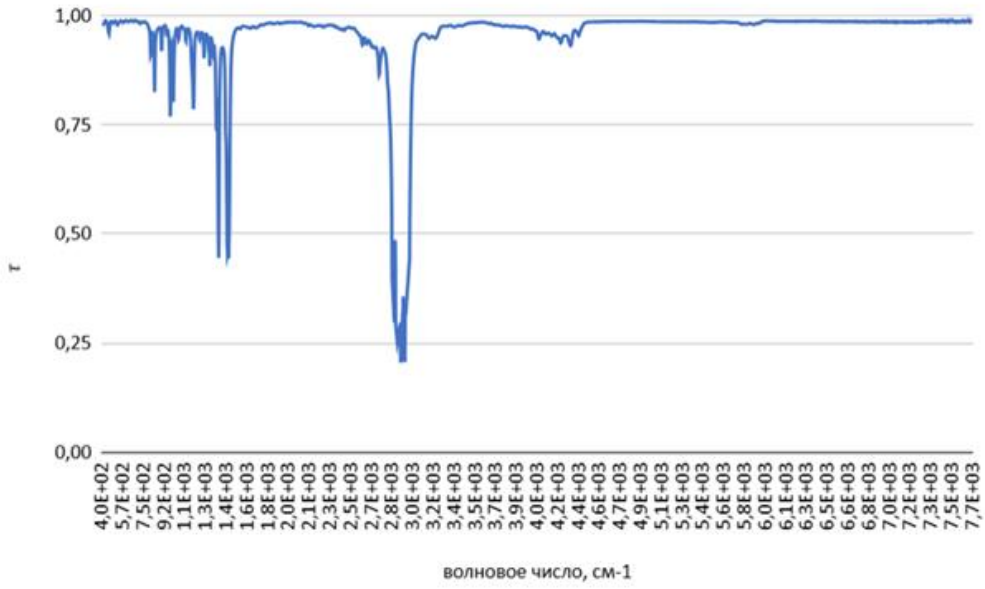


Рис. 2. Приведенный ИК-спектр полипропилена

Сравнив справочные и экспериментальные спектры необходимо оценить совпадение пиковых точек, что говорит о совпадении полимеров. После этого этапа можно переходить к подбору длин волн.

Для этого необходимо осуществить выборку пиковых значений τ (отношение интенсивностей на входе и выходе) с привязкой к длинам волн по всем образцам. В данном случае это образцы полиэтилена, полиэтилентерефталата, поливинилхлорида и полистирола. К каждому выбранному значению необходимо привести значение τ других образцов, соответствующее выбранной длине волны (рис. 3).

Длины волн, мкм	τ									
	Образец 3, PP		Образец 2, PE		Образец 8, PET		Образец 9, PVC		Образец 10, PS	
	d=10 мкм	d=100 мкм	d=10 мкм	d=100 мкм	d=10 мкм	d=100 мкм	d=10 мкм	d=100 мкм	d=10 мкм	d=100 мкм
5,659	0,9809457579	0,8249923743	0,89243335	0,3204482571	0,6810857854	0,0214792031	0,9788646199	0,8076558008	0,9394878793	0,535687873
5,766	0,9791251079	0,8098076485	0,87922597	0,2760610116	0,7405107128	0,0495807917	0,7967562369	0,1030990629	0,9377460635	0,5258386417
6,246	0,9750844459	0,7770022714	0,91175544	0,3969937158	0,8689885558	0,2455503571	0,9719869463	0,7526695114	0,5333681314	0,00186324786
6,322	0,9762865767	0,7866348462	0,92027801	0,4357028965	0,6358637089	0,01080538857	0,9800967767	0,8178800388	0,8046464144	0,1137760373
6,697	0,9382435077	0,5286347147	0,90741247	0,3784839191	0,8227335434	0,1420993338	0,9484103771	0,5887934526	0,2070743578	0,000000144965
6,829	0,4900131147	0,000798136251	0,36082235	0,000037405400	0,7444904076	0,05231076419	0,9051575283	0,3691829864	0,8609174588	0,2236738179
6,838	0,4435721178	0,000294878014	0,37389812	0,000053398961	0,7488294767	0,05544077786	0,9004126601	0,3502804724	0,8384989823	0,1718008856
6,884	0,4530352969	0,000364183613	0,7028231	0,02940764669	0,7322994646	0,04434934052	0,8504057529	0,1978162181	0,2318559723	0,000000448934
7,015	0,9043363577	0,365847351	0,8776564	0,2711722479	0,73217685	0,04427513886	0,6546918215	0,0144666894	0,9170265335	0,4205513372
7,26	0,4449622235	0,000304250581	0,81391054	0,1275753374	0,7375732812	0,04764877711	0,832073609	0,1590806938	0,8040866665	0,1129870335
7,491	0,9303133756	0,4856156234	0,85323876	0,2045058609	0,7543615028	0,05967537683	0,6297227335	0,009806041334	0,8504039141	0,197811941
7,938	0,9311603958	0,4900551554	0,87096328	0,2511877492	0,7700873577	0,07334996951	0,6464160989	0,0127385982	0,9284210925	0,4758279894
8,554	0,7999873193	0,1073571638	0,93421143	0,5063511089	0,7105799594	0,03281931772	0,827880887	0,1512441422	0,9139539341	0,4066708711
9,031	0,9566472335	0,6419751233	0,94536734	0,5701720769	0,6381270677	0,01119622626	0,7393773583	0,04882716085	0,9234979235	0,4511897579
9,708	0,9705500673	0,7416165972	0,90400696	0,3645169615	0,7345552505	0,04573457774	0,8324739759	0,1598477981	0,6588315184	0,01540790796
10,204	0,8954782579	0,3315510876	0,87499398	0,2630574771	0,7488909103	0,05548627802	0,6595487617	0,01557647179	0,8799110663	0,2782196479
10,623	0,9590798124	0,6584874415	0,86205703	0,2266522206	0,8689325231	0,2453920714	0,7412347961	0,05006773951	0,8799241541	0,2782610332
11,196	0,9620491257	0,6791606142	0,87134802	0,2522995563	0,6486959207	0,0131950691	0,8688016759	0,2450228009	0,9161321866	0,4164677874
11,889	0,8252028316	0,1464222565	0,90796113	0,3807786299	0,7443206364	0,05219159874	0,868585188	0,2444129375	0,8697873528	0,24781688
13,191	0,9860902157	0,8692936277	0,95225656	0,6131118803	0,9101808283	0,3901906286	0,9291168399	0,4794058352	0,2694641958	0,000002018415
13,897	0,9832272237	0,8443819644	0,59129107	0,005224120682	0,7757358481	0,07891119388	0,8553959094	0,2097353768	0,8875129996	0,3032125898
14,399	0,987203666	0,8791593407	0,95058328	0,6024232314	0,9411227134	0,5450828895	0,7452568752	0,05285181575	0,2293597126	0,000000402875
15,337	0,9878905206	0,8852953462	0,9218905	0,4433976595	0,9682074477	0,7239093573	0,5928415656	0,005362736465	0,9473612981	0,5823128691

Рис. 3. Таблица приведенных значений τ

Данная выборка позволяет вычленить лишь интересующие значения τ, по которым будет в последующем проводиться определение полимера.

Последним этапом является анализ полученной таблицы значений: нужно методом перебора выбрать длины волн, по которым будет определяться пиковое это значение τ или нет. В рассматриваемом примере выбраны следующие длины волн – 6,3; 6,8; 7,3; 8 и 9 мкм.

Список используемых источников

1. Чумак В. В. Лабораторный практикум по оптике: светофильтры [Электронный ресурс] / В. В. Чумак // Кафедра медицинской физики ИГУ, Иркутск. URL: https://www.medphysics-irk.ru/teaching/chumak/optics/chumak/ %20filters/literature/Opt-lab23.pdf (дата обращения: 12.04.2026).

2. Компьютерное исследование оптических демультиплексоров на основе интерференционных фильтров и фильтров фабри-перо / 2006г. // доцент каф. СВЧиКР С. Н. Шарангович, аспирант каф. СВЧиКР В. В. Кузнецов.

3. Купцов А. Х., Жижин Г. Н. Фурье-КР и Фурье-ИК спектры полимеров. 85 лет с открытия эффекта комбинационного рассеяния света / А. Х. Купцов, Г. Н. Жижин. Москва: Техносфера, 2013. С. 46.

УДК 621.396.2

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МОДУЛЯЦИИ В OFDM-СИСТЕМАХ СВЕРХШИРОКОПОЛОСНОЙ СВЯЗИ

А. Д. Гальцова (студент группы МРД-2521 СПбГУТ), galcova.ad@sut.ru

В статье представлены результаты исследования эффективности различных схем цифровой модуляции в системах сверхширокополосной (СШП) связи на основе технологии ортогонального частотного разделения каналов OFDM. Проведено моделирование в среде MATLAB для схем модуляции BPSK, QPSK и 16-QAM. Оценены ключевые параметры системы: вероятность битовой ошибки BER, спектральная эффективность и скорость передачи данных в зависимости от отношения сигнал/шум SNR. Результаты исследования позволяют сформулировать критерии выбора схемы модуляции для различных сценариев эксплуатации СШП-систем.

сверхширокополосные системы, OFDM, модуляция, BPSK, QPSK, 16-QAM, спектральная эффективность, помехоустойчивость

В эпоху стремительного развития телекоммуникаций особую значимость приобретают надежные методы передачи данных. Сверхширокополосные системы СШП отличаются высокой устойчивостью к внешним факторам и энерго-экономичностью. Исследования в этой сфере начались в СССР в конце 1980-х годов под руководством В. В. Крылова. После введения международных стандартов технологии СШП значительно продвинулись вперед и нашли широкое применение в мобильной связи и автономных системах. Регуляторные органы, включая FCC в США, ETSI в ЕС и ГКРЧ в России, устанавливают строгие нормы для спектральной плотности мощности СПМ сигналов сверхширокополосной связи. Например, решение ГКРЧ от 15 декабря 2009 года № 09-05-02 допускает работу в диапазоне частот 2,85–10,6 ГГц при СПМ не выше -47... -45 дБм/МГц [1,2,3]. Эти ограничения требуют применения технологий, которые максимально эффективно используют энергию сигнала. На рис. 1 представлен график ограничений СПМ сигнала.

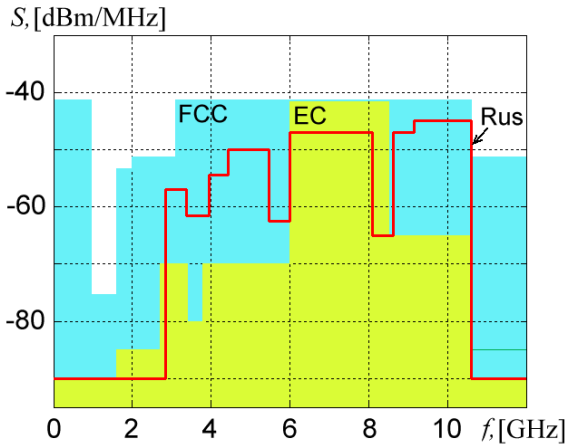


Рис. 1. Ограничения СПМ сигнала регуляторными органами: FCC в США, ETSI в ЕС и ГКРЧ в России

Одним из наиболее эффективных способов построения сверхширокополосных систем является технология ортогонального частотного мультиплексирования OFDM. Ее применение обеспечивает гибкое распределение частотного ресурса, устойчивость к многолучевому распространению и высокий уровень спектральной эффективности. При этом выбор метода модуляции поднесущих оказывает существенное влияние на соотношение между пропускной способностью и надежностью передачи информации [6, 7].

Цель исследования заключается в сравнении характеристик схем модуляций BPSK, QPSK и 16-QAM в составе OFDM-системы сверхширокополосной связи. Для достижения поставленной цели была разработана имитационная модель в MATLAB и проведена оценка показателей BER в канале с аддитивным белым гауссовским шумом. Кроме того, определялись параметры, обеспечивающие наилучшие результаты при различных сценариях использования.

Модель приемопередающего тракта создавалась на основе рекомендаций стандартов IEEE 802.15 и ECMA-368 с учетом российских нормативных требований. При моделировании использовалась полоса частот 550 МГц, размер FFT 128 поднесущих и 71 активная поднесущая. Для уменьшения внеполосных излучений были предусмотрены защитные интервалы по краям спектра. Длительность циклического префикса составляла 64 отсчета, что обеспечивало компенсацию многолучевых задержек до 60 нс. Интервал между соседними поднесущими был выбран равным 4,296 МГц.

Для повышения помехоустойчивости применялось сверточное кодирование со скоростью 1/2 и последующее перемежение данных. Такая обработка позволяет повысить вероятность исправления ошибок и обеспечить

более равномерное распределение энергии по спектру. В ходе экспериментов дополнительно анализировались различные скорости кодирования: 1/3, 1/2 и 5/8. Исследования проводились в канале AWGN при изменении SNR от −10 до 6 дБ.

Для сравнения были выбраны три схемы модуляции. BPSK использует два фазовых состояния и кодирует один бит на символ. QPSK обеспечивает передачу двух бит на символ за счет четырех фазовых состояний. Схема 16-QAM сочетает амплитудную и фазовую модуляцию, позволяя передавать четыре бита на символ. Для каждой конфигурации моделировалась передача пакета объемом один миллион бит, после чего вычислялась вероятность битовой ошибки.

На рис. 2 представлены результаты моделирования: графики спектра OFDM сигнала до и после канала связи при SNR = -10дБ с модуляцией: BPSK, QPSK, QAM-16. Спектр сигнала находится ниже -100дБ/МГц, следовательно, каждая система удовлетворяет маске ГКРЧ (-57дБ/МГц).

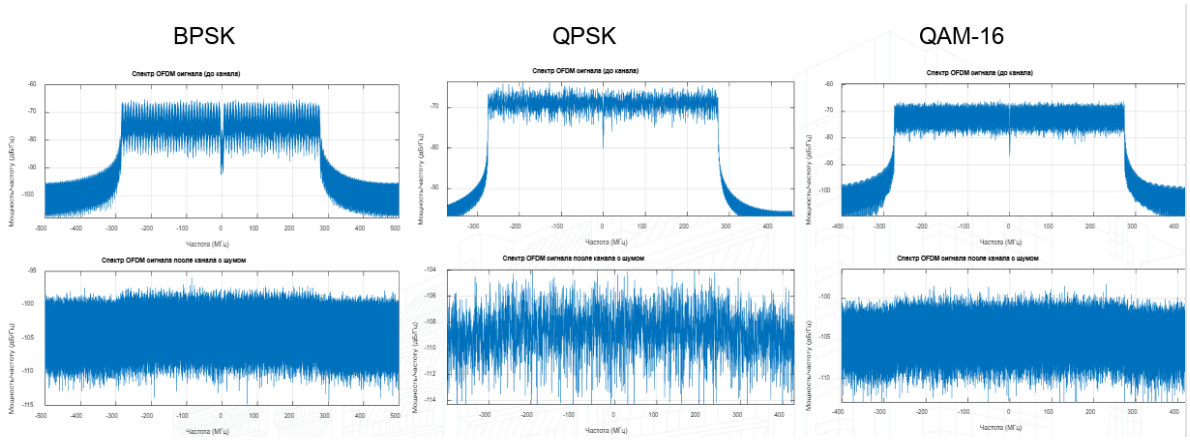


Рис. 2. Графики спектра OFDM сигнала до и после канала связи при SNR = -10дБ с модуляцией: BPSK, QPSK, QAM-16.

На рис. 3 показана зависимость BER от SNR. Ка видно из графика, BPSK обладает меньшим коэффициентом ошибок, даже при отрицательном SNR. Наибольший BER показывает система с использованием КАМ-16. QPSK является компромиссом, обеспечивая неплохие показатели коэффициента ошибок.

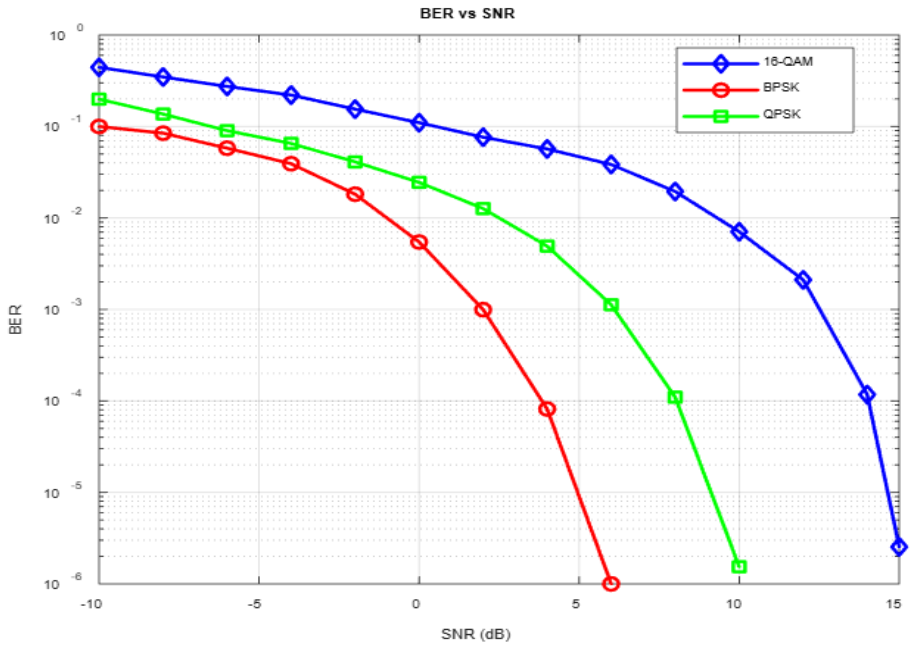


Рис. 3. График сравнения BER от SNR

Полученные результаты показали, что все рассмотренные варианты удовлетворяют требованиям спектральной маски ГКРЧ. Наиболее низкий уровень ошибок продемонстрировала схема BPSK, сохраняющая высокую надежность даже при неблагоприятных значениях SNR. Однако за повышенную устойчивость приходится платить снижением пропускной способности канала.

Модуляция QPSK обеспечивает компромисс между скоростью передачи и качеством связи. При сопоставимом уровне надежности она позволяет практически вдвое увеличить скорость обмена данными по сравнению с BPSK. Схема 16-QAM обеспечивает максимальную производительность и может достигать скорости порядка 400 Мбит/с, однако ее эффективное использование возможно только при достаточно высоком отношении сигнал/шум.

Сравнение показало, что время передачи одного мегабита информации существенно уменьшается при переходе к более сложным схемам модуляции. При этом требования к качеству радиоканала возрастают. Следовательно, выбор конкретного метода модуляции должен осуществляться с учетом условий эксплуатации и допустимого уровня ошибок.

Проведенное исследование подтвердило закономерность: увеличение порядка модуляции приводит к росту требований к параметрам канала связи. Экспериментальные данные позволили сформулировать практические рекомендации по выбору схемы модуляции для сверхширокополосных

OFDM-систем. BPSK целесообразно применять в энергоограниченных и шумных каналах, QPSK подходит для универсальных решений, а 16-QAM рекомендуется использовать в условиях высокого качества связи, где приоритетом является максимальная скорость передачи данных.

Список используемых источников

1. FCC 02-48. Решение Федеральной комиссии связи США (FCC) по регулированию UWB технологий (2002 г.).

2. ГКРЧ № 09-05-02. Решение Государственной комиссии по радиочастотам Российской Федерации от 15 декабря 2009 г.

3. ETSI EN 302 065. Европейский стандарт на сверхширокополосные устройства.

4. IEEE 802.15.4z. Enhanced Ultra Wideband (UWB) Physical Layer.

5. Бенедетто, М. Мир радиоэлектроники. Сверхширокополосная беспроводная связь / М. Бенедетто, Х. Арслан. Москва: Техносфера, 2008. 320 с.

6. Hadian, M. Multiband-OFDM MIMO for UWB Communication Systems / M. Hadian; advisor: Dr. M. J. Omidi. 2007.

7. Nayak, B. A Comparison Study of Pulsed and MB-OFDM UWB System of WPAN Using Matlab-VHDL Environment / B. Nayak. Independent Research, 2021.

Статья представлена научным руководителем, доцентом кафедры ЦТМ СПбГУТ, кандидатом технических наук А. А. Прасоловым.

УДК 004.05

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К ВЕРИФИКАЦИИ ТОКЕНОВ ДОСТУПА НА ОСНОВЕ ЛОКАЛЬНОЙ ВАЛИДАЦИИ И УДАЛЕННОЙ ИНТРОСПЕКЦИИ В МИКРОСЕРВИСНЫХ РЕШЕНИЯХ

К. Н. Гах (студент группы ИСТ-362 СПбГУТ), gakh.kn@sut.ru
Д. Г. Попугаев (студент группы ИСТ-261 СПбГУТ), popugaev.dg@sut.ru
А. П. Шабанов (старший преподаватель кафедры САР СПбГУТ)

В статье проведен сравнительный анализ подходов к верификации токенов доступа в микросервисных архитектурах, основанных на локальной валидации и удаленной интроспекции. Сравнение было выполнено по критериям качества систем и программ, в частности эффективности, надежности, возможности многократного использования, тестируемости, удобства использования, безопасности и совместимости. На основе проведенного анализа выявлены преимущества и ограничения рассматриваемых технологий, а также определены области их наиболее эффективного применения в микросервисных решениях.

микросервисы, аутентификация, авторизация, удаленная интроспекция, сравнительный анализ

В современных распределенных системах, основанных на принципах микросервисной архитектуры, особую значимость приобретает обеспечение безопасности передачи данных между отдельными компонентами. В отличие от монолитных приложений, где взаимодействие ограничено внутренними модулями, микросервисы обмениваются данными, используя сетевые каналы, что существенно увеличивает возможность атаки и требует применения механизмов защиты [1].

Современная разработка программного обеспечения характеризуется повсеместным внедрением технологий OAuth 2.0 и OpenID Connect для аутентификации и авторизации сервисов. В такой архитектуре сервисы взаимодействуют друг с другом путем обмена короткоживущими токенами доступа (access token), подтверждающие права пользователя или самого сервиса [2].

Условием успешной реализации такого взаимодействия является выбор подхода к верификации таких токенов. Среди множества доступных решений наибольшее распространение получили два подхода:

1) Локальная валидация, подразумевающая проверку токена на стороне ресурса;

2) Удаленная интроспекция, использующая обращение к сервису авторизации для проверки действительности токена.

Спецификация OAuth 2.0 не предписывает конкретный способ проверки токена на стороне сервиса. Ресурсный сервис может проверить токен локально по цифровой подписи и метаданным, содержащимся в токене, называемые клеймами, если токен имеет структурированный формат. При необходимости актуализации токена используется интроспекция, представляющая собой механизм проверки токена доступа на стороне сервиса авторизации для получения актуального статуса токена и его данных. Официальный стандарт RFC 7662, описывающий механизм интроспекции токенов, предписывает использование специального эндпоинта, на который ресурс отправляет токен для получения актуальной информации [3-4].

Локальная валидация подразумевает самостоятельность ресурсного сервиса, способного расшифровать полученный токен и проверить подпись и поля с помощью открытого ключа издателя. Проверки подлежат такие поля, как истечение срока, издатель, назначенная аудитория и права доступа. После успешной проверки токен считается валидным. Такой подход не требует дополнительных обращений к издателю токена после получения открытого ключа. Общая схема взаимодействия ресурсного сервиса и сервиса авторизации представлена на рисунке 1.

Локальная валидация является масштабируемым решением, поскольку ресурсы сервиса авторизации не нагружаются проверками токенов. Однако такой подход представляет собой угрозу безопасности, поскольку отсутствие механизма отзыва токена в реальном времени может привести к тому, что скомпрометированный токен доступа может оставаться актуальным до истечения срока действия. В связи с чем при локальной валидации используют короткоживущие токены, действующие от 10 до 15 минут, а также систему обновления посредством refresh-токенов.

При использовании подхода удаленной интроспекции проверка токена, полученного от ресурсного сервиса, происходит на стороне сервиса авторизации. Результатом проверки является ответ в виде JSON, содержащий поле active, представляющее собой значение логического типа, а также дополнительные данные о пользователе. Таким образом в реальном времени ресурс может узнать, является ли токен действительным. Достоинствами этого подхода являются гарантированная актуальность статуса токена и присутству-

ющий механизм мгновенного отзыва этого токена, активно использующийся в банковских и медицинских сервисах. На рисунке 2 представлено взаимодействие ресурсного сервиса и сервиса авторизации.

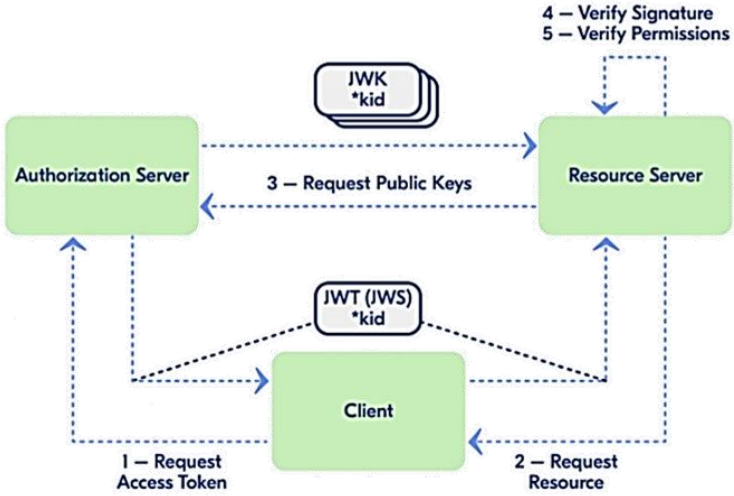


Рис. 1. Схема взаимодействия ресурсного сервиса и сервиса авторизации при локальной валидации.

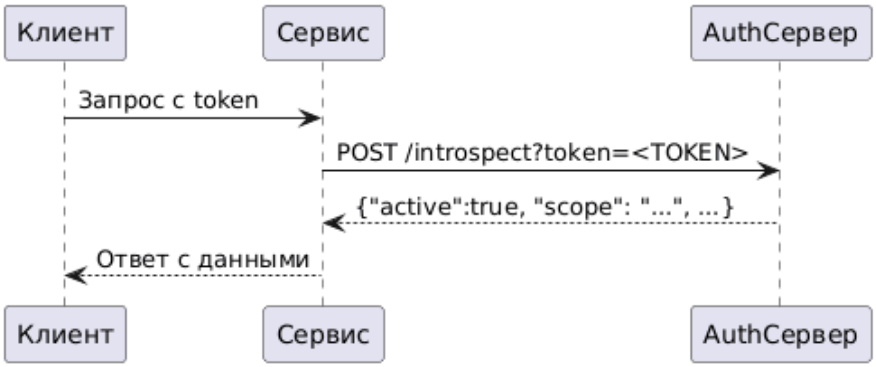


Рис. 2. Схема взаимодействия ресурсного сервиса и сервиса авторизации при удаленной интроспекции

Постоянные запросы к сервису авторизации увеличивают задержку проверки токена и увеличивают нагрузку на сеть и сервис авторизации, что в результате при высоком трафике приводит к лимиту запросов на сервис. Также главным недостатком такого подхода является сведение проверки всех токенов к одному сервису, что может нарушить процесс аутентификации и авторизации в случае его недоступности [5].

В ходе практического применения удаленной интроспекции для организации межсервисного взаимодействия замечено, что подход обеспечивает безопасный обмен данными между сервисами и высокую скорость реагирования на угрозы безопасности, в частности получение несанкционированного доступа с помощью скомпрометированного токена доступа. Вместе

с тем выявлены сложности в использовании, связанные с высокой нагрузкой на сервис авторизации и высокую задержку подтверждения актуальности информации о сервисе.

Для каждого из рассматриваемых подходов можно составить аналитическую модель, используя универсальные показатели качества, применяемые при выборе наиболее удобного решения обеспечения взаимодействия между различными источниками и приемниками (рис. 3).



Рис. 3. Универсальные показатели качества походов верификации токенов доступа

В качестве рассматриваемых параметров были взяты семь характеристик. «Эффективность» отражает способность подходов быстро обрабатывать запросы и рационально использовать вычислительные и сетевые ресурсы при различных уровнях нагрузки. «Надежность» показывает стабильность работы механизмов, их устойчивость к сбоям и способность корректно функционировать при отказах компонентов. «Возможность многократного использования» оценивает, насколько механизмы верификации можно повторно применять и масштабировать без изменения логики взаимодействия. «Тестируемость» описывает простоту проверки корректности работы механизмов и способность автоматизации тестов для разнообразных сценариев. «Удобство использования» отражает простоту внедрения подхода и понятность настройки. «Безопасность» показывает уровень защиты механизма, защиту передаваемых данных и устойчивость к угрозам. «Совместимость» оценивает способность технологии функционировать в разных системах.

Как видно из рисунка 3, обе технологии имеют как высокие, так и низкие значения по всем критериям. Тем не менее, среди них есть различия по

отдельным параметрам. В частности, выгоднее использовать локальную валидацию для решений, требующих удобства использования и высокой эффективности. В то же время, более подходящим выбором в безопасности и надежности будет удаленная интроспекция.

На основе проведенного анализа можно сделать вывод, что оба подхода справляются с основными задачами и находят разнообразное применение в современных микросервисных решениях. Локальная валидация проявляет явные преимущества в удобстве использования, эффективности и возможности многократного использования, что делает ее предпочтительным выбором для высоконагруженных внутренних сервисов, где важны низкая задержка и оптимальное использование ресурсов.

В то же время удаленная интроспекция выигрывает по надежности и безопасности, что делает ее более подходящей для информационных систем, требующих от технологий обеспечения безопасности передачи данных. В современных решениях оптимально использовать сочетание обоих подходов: локальную валидацию для взаимодействия внутренних высокопроизводительных сервисов и удаленную интроспекцию для внешнего взаимодействия с клиентами, что позволяет сочетать эффективность и удобство интеграции.

Список используемых источников

1. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2026. С. 12-19.

2. Token Introspection Endpoint [Электронный ресурс] URL: https://www.oauth.com/oauth2-servers/token-introspection-endpoint/ (дата обращения: 28.03.2026).

3. OAuth 2.0 Token Introspection [Электронный ресурс] URL: https://datatracker.ietf.org/doc/html/rfc7662 (дата обращения: 28.03.2026).

4. Validate Access Tokens | Okta Developer [Электронный ресурс] URL: https://developer.okta.com/docs/guides/validate-access-tokens/dotnet/main/ (дата обращения: 28.03.2026).

5. Remote vs local verification of access token – Questions – Okta Developer Community [Электронный ресурс] URL: https://devforum.okta.com/t/remote-vs-local-verification-of-access-token/17583 (дата обращения: 28.03.2026).

Статья представлена научным руководителем, и.о. заведующим кафедрой САР СПбГУТ, кандидатом технических наук, доцентом В. С. Уссом

УДК 612.087

СЕЛЕКТИВНЫЙ ФОТОТЕРМОЛИЗ СОСУДИСТЫХ ПАТОЛОГИЙ У ПАЦИЕНТОВ С ТЕМНОЙ КОЖЕЙ

О. С. Гвоздецкая (студент гр. РФ-42 СПбГУТ), gvozdetskaia.os@sut.ru
И. Е. Скалецкая (к.т.н., доцент кафедры физики СПбГУТ)
Т. И. Татаринов (студент гр. РФ-42 СПбГУТ), tatarinov.ti@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается принцип селективного фототермолиза и его роль в лазерной терапии. Описываются основные свойства лазерного излучения и особенности его взаимодействия с биологическими тканями. Рассмотрено, как различные компоненты тканей по-разному поглощают свет. Проанализирована физическая проблема конкуренции меланина и гемоглобина при лазерном лечении сосудистых патологий кожи. Рассмотрены современные технологические решения, выявлены их недостатки и предложены некоторые пути улучшения.

селективный фототермолиз, лазерное излучение, лазерная терапия, биологические ткани, хромофоры, гемоглобин, меланин, длина волны, импульсное излучение, поглощение света, темная кожа.

Лазер (от англ. Light Amplification by Stimulated Emission of Radiation) – это усиление направленного, когерентного и монохроматического света посредством вынужденного излучения. Его работа основана на уникальных физических процессах, которые можно разделить на несколько ключевых этапов [1].

1) Поглощение: работа лазера начинается с того, что энергия подается в активную среду, чтобы перевести атомы или молекулы на более высокие энергетические уровни.

2) Излучение: при воздействии фотона определенной энергии на возбужденный атом или молекулу происходит переход на более низкий энергетический уровень, при этом испускается еще один фотон с той же длиной волны, направлением и фазой.

3) Резонатор: активная среда помещена между двумя зеркалами. Одно зеркало полностью отражает свет, другое – частично пропускает его. Фотон

многократно отражается, стимулируя излучение новых фотонов. Свет многократно отражается внутри резонатора, проходя через активную среду

и усиливаясь за счет вынужденного излучения. Это процесс называется оптическим усилением.

4) Выход лазерного излучения: часть света, проходящего через полупрозрачное зеркало, выходит наружу, формируя лазерный луч. Этот луч отличается высокой интенсивностью, направленностью и монохроматичностью, что делает его уникальным инструментом для научных, медицинских и промышленных целей (рис. 1).

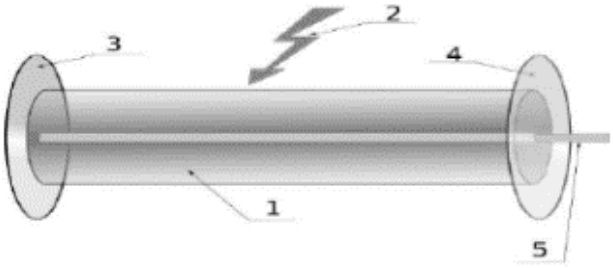


Рис. 1. Схема лазера
На схеме выделены: 1 – активная среда, 2 – энергия накачки лазера, 3 – непрозрачное зеркало, 4 – полупрозрачное зеркало, 5 – лазерный луч

Когда лазерный луч попадает на биологическую ткань, возможны несколько процессов [2]:

1) поглощение – энергия света поглощается хромофорами (водой, меланином, гемоглобином), вызывая нагрев и фотохимические реакции;

2) рассеяние – приводит к изменению направления света, снижая точность фокусировки и глубину воздействия;

3) отражение– часть энергии отражается, не вызывая эффекта.

Принцип селективного фототермолиза (рис. 2), сформулированный в 1983 году учеными Андерсоном и Парришем (Anderson & Parrish), стал основой для многих лазерных методик в медицине. Его суть заключается в точечном разрушении заданных мишеней – таких, как сосуды или пигментные клетки, – при сохранении целостности окружающих тканей [3].

Свет с различной длиной волны по-разному поглощается структурными элементами кожи, таким образом, для каждого из основных хромофоров кожи существует свой спектр поглощения. Выбирая световое излучение определенной длиной волны, можно целенаправленно воздействовать на определенные компоненты кожи, например:

- меланин, содержащийся в волосяных фолликулах и эпидермисе, интенсивно поглощает свет видимого спектра и практически не чувствителен к инфракрасной части спектра;

● гемоглобин, содержащийся в сосудах, в частности – в эритроцитах, имеет максимум поглощения в ультрафиолетовом спектре, а также интенсивно поглощает свет в желтом и фиолетовом диапазоне;

● вода, из которой на 70 % состоит кожа, поглощает свет инфракрасного спектра и практически не чувствительна к ультрафиолетовой части спектра.

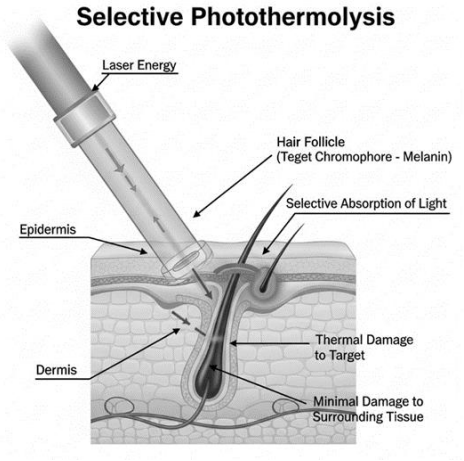


Рис. 2. Принцип селективного фототермолиза

Селективное воздействие на целевые элементы кожи достигается за счет правильного подбора характеристик лазерного излучения (его длины волны, продолжительности импульсов). Подбор указанных параметров излучения позволяет выборочно разрушать заданную мишень, избегая механической травмы или перегрева окружающих ее тканей, что может привести к нежелательным побочным эффектам в виде стойких косметических дефектов.

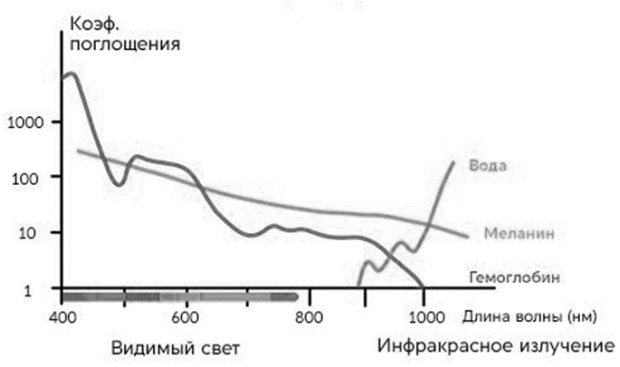


Рис. 3. Спектры поглощения основных хромофоров

Лазерная терапия широко применяется для лечения сосудистых заболеваний кожи: венозных озер, ангиокератом, мелазмы, купероза и других [4].

Однако у пациентов с темной кожей возникает серьезная физическая проблема – в кожном покрове содержится большое количество меланина, который также активно поглощает лазерный свет, как и гемоглобин. Чем темнее кожа у пациента, тем выше риск получения термических ожогов и стойких нарушений пигментации после лазерных процедур. Клинические исследования показывают, что осложнения при лазерном лечении возникают у 0,26 % пациентов со светлой кожей и у 33 % с темной. Стандартные протоколы были разработаны для лиц со светлой кожей. Поэтому врачи следуют базовым протоколам лечения с помощью лазерного воздействия, которые для темной кожи не подходят [5].

При лечении различных сосудистых патологий лазерное воздействие направлено на целевой хромофор – гемоглобин. Меланин выполняет защитную функцию в верхнем слое кожи, однако при медицинских манипуляциях этот природный пигмент становится конкурирующим веществом. Проблема заключается в перекрытии спектров поглощения этих биологических молекул в области 500–600 нм. В таком диапазоне коэффициент поглощения меланина в 5–10 раз превышает коэффициент поглощения гемоглобина.

У пациентов с фототипами IV–VI по шкале Фицпатрика концентрация меланина значительно выше, что приводит к побочному поглощению большей части лазерной энергии [6]. Следствием этого процесса является снижение эффективности лечения патологий и перегрев эпидермиса с развитием ожоговых поражений и пост воспалительных появлений гиперпигментации или гиперпигментации.

Преимущественным решением является использование Nd:YAG лазера с длиной волны 1064 нанометров [2]. Меланин на этом значении длины волны поглощает слабо. Энергия проходит сквозь кожу, почти не нагревая ее, и достигает сосуда. Во многих медицинских сводках такой лазер получил название «золотой стандарт» при указании лечения заболеваний у пациентов с темным кожным покровом.

Следующим способом минимизации рисков повреждения эпидермиса выделяют процесс увеличения длительности импульса [7]. Короткий импульс

сопоставим с высокой пиковой мощностью при подаче энергии лазерного излучения мгновенно. Меланин получает мощный удар теплом и не успевает остыть – температура резко подскакивает, возникает ожог. При использовании длинного импульса от 10 до 25 миллисекунд та же самая энергия распределяется на более долгое время, тем самым пиковая мощность

становится ниже– меланин успевает остывать во время импульса, температура не поднимается до опасного уровня, и риск повреждения кожи значительно снижается.

Для устранения недостатков ранее рассмотренных методов предлагается комплекс решений: необходимо в скором будущем внедрять системы, работающие с учетом индивидуальных особенностей каждого пациента. Чтобы преодолеть ограничение «золотого стандарта» необходимо найти способ разработки мультиволновых систем, которые будут способны автоматически переключаться между короткой длиной волны для поверхностных сосудов и длинной – для глубоких. Идет активное научное проектирование моделей, способных определять фототип кожи по фотографии лица с высокой точностью, что в перспективе позволит полностью автоматизировать выбор мощности, длительности импульса и интенсивности охлаждения. Также проводить больше исследований с фототипами IV–VI для усовершенствования технологий.

В данной работе были рассмотрены основные физические принципы лазерной терапии и изучен механизм селективного фототермолиза. Установлено, что взаимодействие лазера с тканями определяется процессами поглощения, рассеяния и отражения, при этом ключевую роль играют хромофоры – меланин, гемоглобин и вода. Правильный выбор длины волны и длительности импульса позволяет обеспечить избирательное воздействие на ткани и повысить безопасность процедур. Будущее лазерной терапии в персонализированном подходе, где происходит адаптация параметров под конкретного пациента с помощью искусственного интеллекта и роботизированных технологий.

Список используемых источников

1. Кожахметова А. М. Физика лазеров: типы, свойства, принципы работы и применение. 2024.

2. Treatment of purpura with Nd:YAG laser in skin types IV-VI // JAAD. 2018.

3. Общество с ограниченной ответственностью «Премиум Эстетикс». URL: https://www.premium-a.ru/tech/selektivnyj-fototermoliz/ (дата обращения: 10.04.2026).

4. Илларионов В.Е. Теория и практика лазерной терапии: учебное руководство. М.: URSS, 2024. 152 с.

5. Sheppard T.K., et al. Cosmetic Laser Procedures in Patients With Skin of Color // Cutis. – 2025. Vol. 116, N 2. P. 58-64.

6. Franco W., et al. Cryogen Spray Cooling Might Not Fully Protect Epidermis // Lasers in Surgery and Medicine. 2007.

7. Laser and Light Treatments for Hair Reduction in Fitzpatrick Skin Types IV-VI // JCAD. Spring 2023.

УДК 519.216

МОДЕЛИРОВАНИЕ ФИЛЬТРА КАЛМАНА В КАЧЕСТВЕ ИНТЕРПОЛЯТОРА

Е. И. Глушанков (д.т.н., профессор кафедры РТ СПбГУТ)
Г. С. Шевченко (студент гр. МРД-2521 СПбГУТ),
gsshevchenko@stud.etu.ru

Задача предсказания будущего и уточнения текущего местоположения воздушного судна набирает актуальность в свете применения средств РЭБ, подавляющих сигналы GNSS. Встает вопрос развития бортовых систем и алгоритмов, способных определять местоположение судна с высокой точностью, не опираясь на внешние сигналы и системы навигации. В данной статье рассматриваются результаты математического моделирования фильтра Калмана в качестве интерполятора в MATLAB в контексте измерения физических величин для различных моделируемых сценариев.

фильтр Калмана, интерполяция, моделирование

Фильтр Калмана, или фильтры Винера-Калмана – класс линейных последовательных алгоритмов оценивания состояния системы, обеспечивающих минимальную среднеквадратическую ошибку [1, с. 251]. Эти алгоритмы обеспечивают оптимальную оценку состояния системы на основе модели системы и прямых измерений [2, с. 87]. Фильтр Калмана можно применять для оптимальной оценки состояния системы в текущий момент времени (интерполяция) или для предсказания состояния системы в будущий момент времени (экстраполяция).

Работа фильтра Калмана основана на рекурсивной байесовской оценке. На рис. 1. представлена диаграмма байесовской оценки. Рекурсивная байесовская оценка смешивает предыдущий результат оценки с показаниями прямых измерений.

Работа фильтра-интерполятора была рассмотрена в MATLAB для следующих сценариев: измерение напряжения узла в схеме питания [2, с. 113] и измерение мгновенной высоты падающего объекта [2, с. 131].

На рис. 2. представлена зависимость значения напряжения узла схемы питания от времени, выраженного в итерациях фильтра Калмана. На графике темной линией отмечено истинное значение, пунктиром – измеренное значение, а светлой линией – обработанное фильтром Калмана значение напряжения.

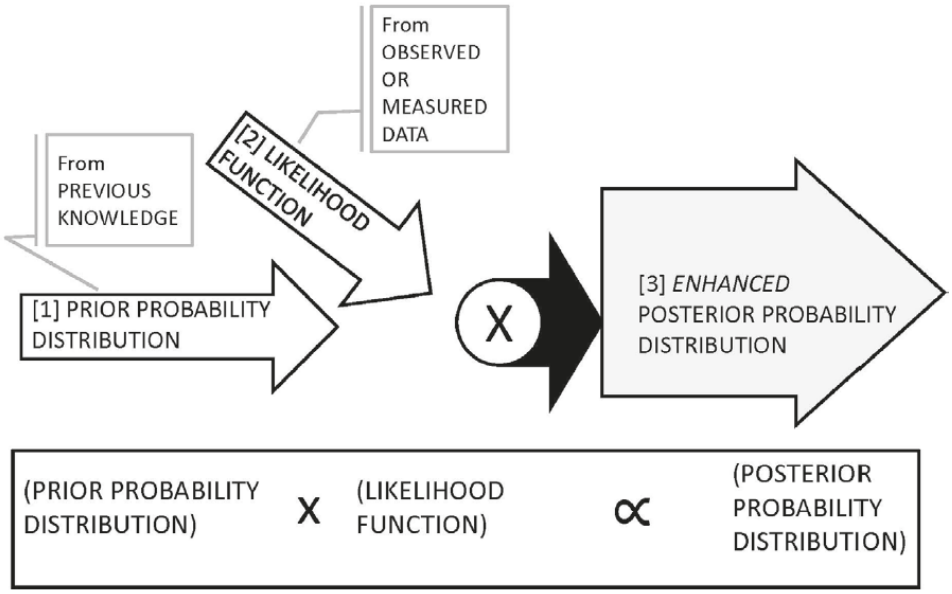


Рис. 1. Графическое представление принципа рекурсивной байесовской оценки [2, с. 52]

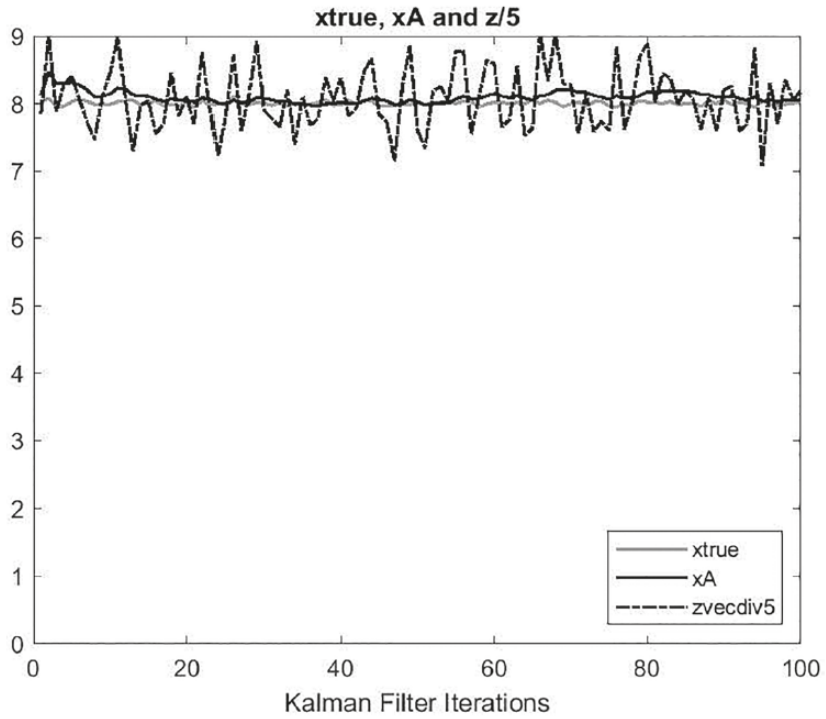


Рис. 2. Зависимость значения напряжения узла схемы питания от итераций фильтра [2, с. 122]

На рис. 3. представлена зависимость ошибки оценки напряжения от времени, выраженного в итерациях фильтра Калмана.

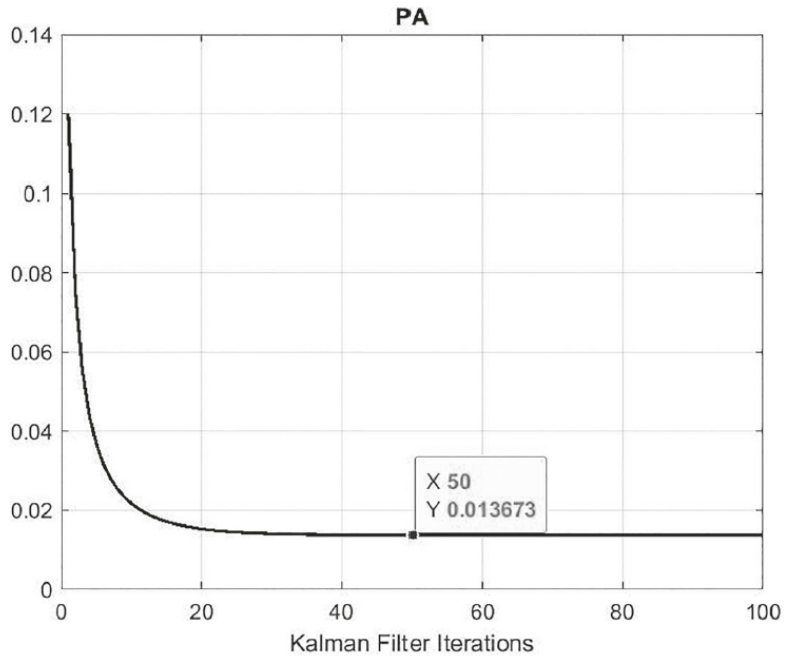


Рис. 3. Зависимость ошибки оценки напряжения от итераций фильтра [2, с. 122]

На рис. 4. представлена зависимость значения мгновенной высоты падающего объекта от времени, выраженного в итерациях фильтра Калмана. На графике светлой линией отмечено истинное значение, серой линией – измеренное значение, а темной линией – обработанное фильтром Калмана значение напряжения.

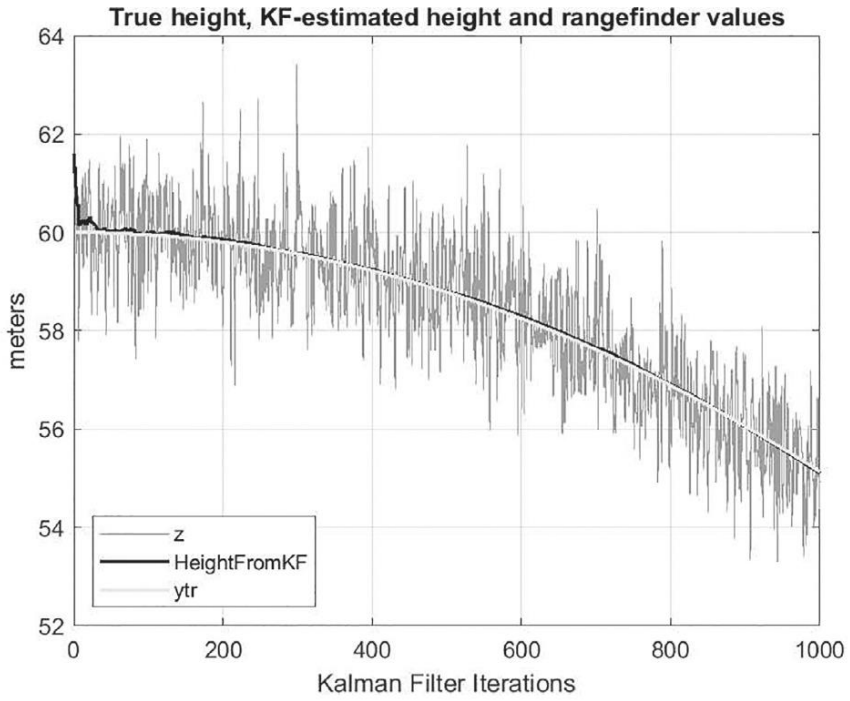


Рис. 4. Зависимость значения высоты падающего объекта от итераций фильтра [2, с. 141]

На рис. 5. представлена зависимость ошибки оценки высоты объекта от времени, выраженного в итерациях фильтра Калмана.

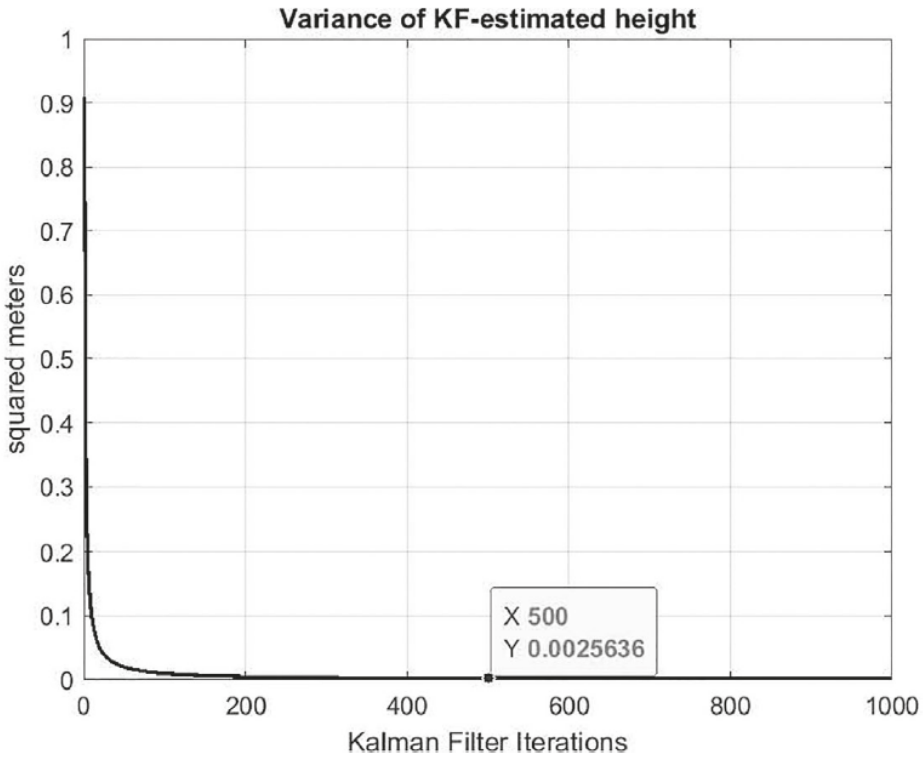


Рис. 5. Зависимость ошибки оценки высоты от итераций фильтра [2, с. 142]

Проанализировав Рис. 3. и Рис. 5., можно увидеть, что ошибки оценок минимизируются с течением времени наблюдений, или с увеличением итераций оценок фильтра Калмана. Сравнив кривые измеренных и оцененных фильтром Калмана значений на рис. 2 и Рис. 4, можно сделать вывод, что обработка результатов измерений фильтром Калмана дает более точную оценку измеряемой величины, чем прямое измерение без последующей обработки.

Список используемых источников

1. Сэйдж Э., Мелс Дж. Теория оценивания и ее применение в связи и управлении: пер. с англ. М.: Связь, 1976. 496 с.

2. Armando Barreto, Malek Adjouadi, Francisco R. Ortega, Nonnarit O-larnnithipong. Intuitive Understanding of Kalman Filtering with MATLAB. Boca Raton: CRC Press, 2021. 229 p.

УДК 621.373

ЛАБОРАТОРНЫЙ ГЕНЕРАТОР ТЕСТОВЫХ СИГНАЛОВ С ПРЯМЫМ ЦИФРОВЫМ СИНТЕЗОМ ЧАСТОТ

Д. А Денисов (студент группы ФП-31 СПбГУТ), denisov_da@sut.ru
Н. А. Костоломов (студент группы ФП-31 СПбГУТ), kostolomov_na@sut.ru
А. А. Пыркин (студент группы ФП-31 СПбГУТ), pyrkin_aa@sut.ru
А. А. Сапрыкин (студент группы ФП-31 СПбГУТ), saprykin_aa@sut.ru
П. П. Шумаков (к.т.н., заведующий кафедрой электроники СПбГУТ)
Е. Е. Шевченко (студент группы ФП-31 СПбГУТ), shevchenko_ee@sut.ru

Лабораторный генератор тестовых сигналов с прямым цифровым синтезом частот – проект, предназначенный для учебных и лабораторных работ по электронике, позволяет изучать свойства сигналов и настраивать электронные устройства. В ходе работы были разработаны электрическая схема, печатная плата, программное обеспечение и корпус устройства. Устройство реализовано на базе микроконтроллера Arduino Uno и модуля AD9833.

генератор частот, прямой цифровой синтез, генерация сигналов

Целью проекта являлась разработка программно-аппаратного комплекса, способного генерировать сигналы различной формы с заданной частотой и выводить результат на осциллограф. Основное назначение устройства – использование в учебных и лабораторных работах по электронике, схемотехнике и микроконтроллерной технике.

Разрабатываемое устройство позволяет формировать три основных типа сигналов: синусоидальный, прямоугольный и треугольный (см. рис. 1). Диапазон рабочих частот составляет от 1 Гц до 6 МГц. Пользователь может выбирать форму сигнала, изменять частоту и сбрасывать введенные данные без отключения питания. Управление осуществляется при помощи энкодера и кнопок, а текущие параметры отображаются на LCD-дисплее [1].

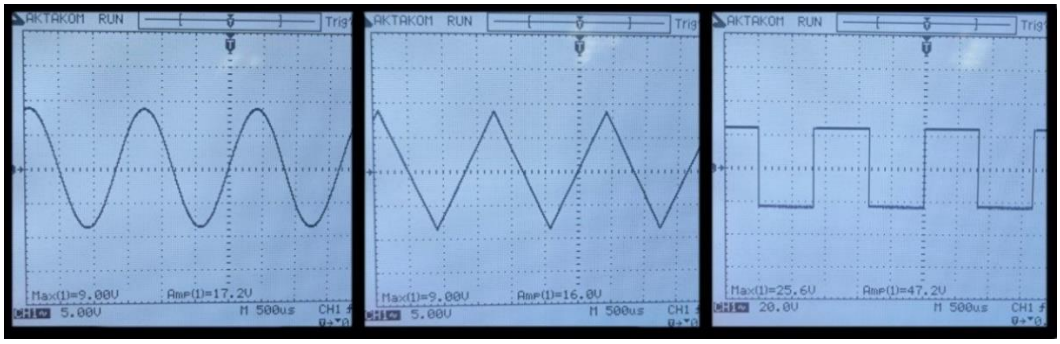


Рис. 1. Пример сигналов синусоидальной треугольной и прямоугольной форм

В качестве аппаратной основы был выбран микроконтроллер Arduino Uno. Он обеспечивает обработку пользовательских команд, взаимодействие с дисплеем и модулем генерации сигнала. Для генерации частоты использован модуль AD9833 DDS Function Generator, который реализует прямой цифровой синтез частот. В качестве средства отображения выбран LCD-дисплей RUICHI RH1602D-TFH со встроенным модулем I2C, а для изменения параметров используется энкодер KY-040. Питание устройства осуществляется от внешнего источника питания, что делает устройство автономным и удобным в использовании.

При выборе элементной базы учитывались несколько факторов: соответствие электрическим параметрам, совместимость с Arduino IDE, доступность компонентов и экономическая целесообразность.

Разработка проекта выполнялась поэтапно. Сначала было подготовлено техническое задание и проведен анализ доступной элементной базы. Затем была разработана схема устройства, включающая питание, интерфейсы SPI и I2C, а также подключение периферийных модулей. После этого была проведена проверка ключевых узлов на макетной плате (см. рис. 2). На этапе макетирования были протестированы вывод информации на дисплей, взаимодействие микроконтроллера с периферией и генерация сигналов различной формы. Результаты испытаний показали, что устройство работает корректно, а программная часть успешно управляет аппаратной частью проекта.

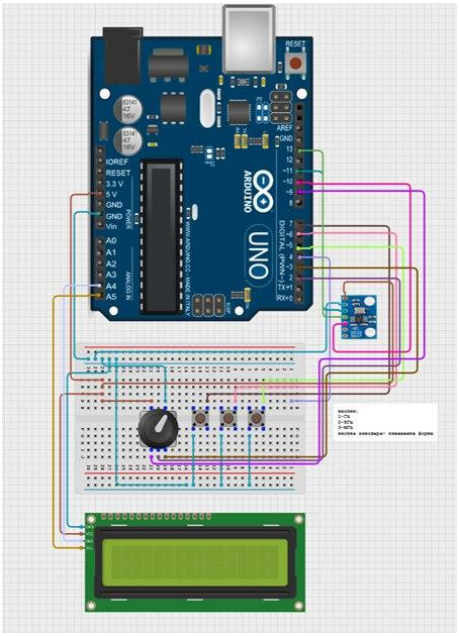


Рис. 2. Цифровое макетирование платы проекта

После завершения макетирования была выполнена разработка печатной платы. Размер платы составил 57 на 73 миллиметра, материал – двусторонний фольгированный гетинакс толщиной 1,5 миллиметра. Разводка печатной платы была выполнена в Altium Designer с учетом требований к трассировке сигналов, питания и заземления (см. рис. 3). Также был разработан корпус устройства с использованием программ 3ds Max и Fusion 360. (см. рис. 4)

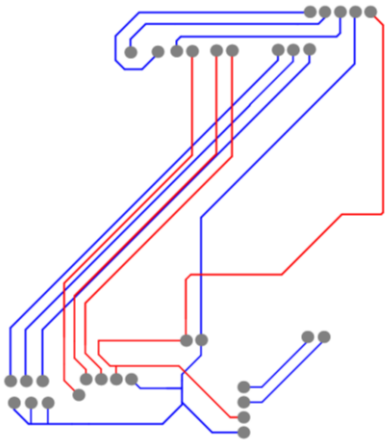


Рис. 3. Вид платы с верхними и нижними дорожками



Рис. 4. 3Д-визуадизация корпуса в сборке

Программная часть проекта была реализована на языке C++ в среде Arduino IDE. Программой предусмотрено, что частота может изменяться по разрядам, что позволяет точно задавать требуемое значение [2]. Необходимо выбрать разрядную декаду и затем провести более точную настройку. Например, указывается декада «десятки килогерц», после чего, энкодером можно выставить значение от 0 до 9. Дополнительно реализована защита от установки частоты выше допустимого значения [3].

Практическая значимость проекта заключается в том, что устройство может использоваться в лабораторных работах для изучения свойств сигналов, настройки электронных схем, проверки работы фильтров, усилителей и других электронных устройств. По сравнению с промышленными генераторами проект имеет более низкую стоимость и простую конструкцию, при этом полностью выполняет основные учебные функции.

Таким образом, в ходе выполнения проекта было успешно разработано устройство с функцией генерации тестовых сигналов с прямым цифровым синтезом частот. Устройство соответствует требованиям технического задания, обладает удобным интерфейсом управления и может быть использовано как учебный лабораторный прибор.

Список использованных источников

1. Никитин Ю. А. Математическая модель формирования колебаний с использованием методов пассивного цифрового синтеза// Российский технологический журнал – «Известия высших учебных заведений. Приборостроение» 2011, (том 54, номер 9, страницы 52–57).

2. Никитин Ю. А Моделирование цифро-аналогового преобразования частоты в нониусном тракте приведения умножающего кольца ифап: Учебное пособие. 2008. 216 с.

3. Гуревич И. Н., Никитин Ю. А. Синтез сетки частот с произвольным шагом // Радиотехника. 1992. № 4.

УДК 537.67

ЦИФРОВИЗАЦИЯ ЛАБОРАТОРНОЙ РАБОТЫ «ОПРЕДЕЛЕНИЕ ГОРИЗОНТАЛЬНОЙ СОСТАВЛЯЮЩЕЙ МАГНИТНОГО ПОЛЯ ЗЕМЛИ» И ИЗУЧЕНИЕ СФЕР ПРИМЕНЕНИЯ ПОЛУЧЕННЫХ ДАННЫХ

В. М. Деткова (к.ф.-м.н., доцент кафедры физики, СПБГУТ)
Л. Б. Пургин (студент гр. ИКТ-2512, СПБГУТ), purgin.lb@sut.ru

В ходе работы, при помощи языка программирования Python, была проведена автоматизация обработки экспериментальных данных, полученных при измерении горизонтальной составляющей напряженности магнитного поля Земли с помощью тангенс-гальванометра, включая детальный расчет погрешностей и визуализацию результатов. Также было проведено исследование по практическому применению полученных в результате обработки данных.

Python, тангенс-гальванометр, напряженности магнитного поля Земли

В настоящее время данные о магнитном поле Земли применяются во многих сферах. Они необходимы для ориентирования на местности, наблюдений за космосом, сбора данных о структуре земной коры и т.д.

Расчет величины и направления магнитного поля выполняет созданный программный модуль. Для определения экспериментальных данных была использована лабораторная работа «Определение горизонтальной составляющей магнитного поля Земли» из курса физики (электричество и магнетизм [1-2]).

Для создания программного модуля был выбран язык программирования Python. Выбор был обусловлен таким факторами как: Простота восприятия, универсальность и широкая область применения, мощность экосистемы, высокая скорость разработки, большое сообщество пользователей.

Алгоритм работы программы

1. Программа получает от пользователя входные данные (рис. 1-2) – параметры приборов, погрешности приборов, угол магнитного наклонения в точке измерения, географическую широту, данные опытов и доверительную вероятность для расчета погрешностей [3].

```
Лабораторная работа 4.3
Определение горизонтальной составляющей магнитного поля Земли
--------------------------------------------------

--- Ввод параметров установки ---
Введите радиус катушки R (в метрах): 0.203
Введите число витков N: 162

Параметры установки:
  Радиус катушки R = 0.203 м
  Число витков N = 162

--- Ввод параметров погрешностей ---
Введите абсолютную погрешность радиуса ΔR (в метрах): 0.002
Введите абсолютную погрешность измерения тока ΔI (в миллиамперах): 0.3

Параметры погрешностей:
  ΔR = 0.002 м
  ΔI = 0.3 мА
  Δβ = 0.5° (фиксированная)

--- Ввод угла наклонения ---
Введите угол магнитного наклонения i (в градусах): 71.9

--- Ввод географической широты (опционально) ---
Введите географическую широту точки наблюдения (градусы, северная положительная)
(Enter - пропустить, будет оценена по углу наклонения): 59.9

Угол наклонения i = 71.9°
Географическая широта = 59.9°
```

Рис. 1. Входные данные

```
--- Ввод экспериментальных данных ---
Введите количество измерений: 4

--- Измерение №1 ---
  Введите I (мА): 13
  Введите β1 (град): 32
  Введите β2 (град): 32

--- Измерение №2 ---
  Введите I (мА): 20
  Введите β1 (град): 41.5
  Введите β2 (град): 41.5

--- Измерение №3 ---
  Введите I (мА): 29
  Введите β1 (град): 52
  Введите β2 (град): 52

--- Измерение №4 ---
  Введите I (мА): 42
  Введите β1 (град): 61.5
  Введите β2 (град): 61.5

--- Ввод лучшего опыта ---
(Измерение с углом β, наиболее близким к 45°)
Введите номер измерения из списка выше, которое будет использовано
для расчёта погрешностей (рекомендуется β ≈ 45°):
Номер лучшего измерения: 2

Выбрано измерение №2:
  I = 20.0 мА
  β = 41.50°
  C = 22.6059 мА

--- Ввод доверительной вероятности ---
Доступные значения: 0.7, 0.8, 0.9, 0.95, 0.98, 0.99
Введите доверительную вероятность α: 0.7
```

Рис. 2. Входные данные

2. Программа производит расчеты и выводит пользователь детальный отчет (рис. 3-5).

```
================================================================================
Сводная таблица экспериментальных данных
================================================================================
№    I, мА      β1, град     β2, град     β, град      C = I/tg(β), мА
--------------------------------------------------------------------------------
1    13.00      32.00        32.00        32.00        20.8043
2    20.00      41.50        41.50        41.50        22.6059           *
3    29.00      52.00        52.00        52.00        22.6573
4    42.00      61.50        61.50        61.50        22.8041

1. Расчёт случайной погрешности ΔCα:
   Формула: ΔCα = t(α, n) · √[ Σ(Ci - C⁻)² / (n·(n-1)) ]
   n = 4
   t(0.7, 4) = 1.25
   C⁻ = (20.8043 + 22.6059 + 22.6573 + 22.8041) / 4 = 22.2179 мА
   C1 - C⁻ = 20.8043 - 22.2179 = -1.4136
   C2 - C⁻ = 22.6059 - 22.2179 = 0.3880
   C3 - C⁻ = 22.6573 - 22.2179 = 0.4394
   C4 - C⁻ = 22.8041 - 22.2179 = 0.5862
   Σ(Ci - C⁻)² = (-1.4136)² + (0.3880)² + (0.4394)² + (0.5862)²
                = 2.6854
   Σ(Ci - C⁻)² / (n·(n-1)) = 2.6854 / (4·3) = 0.2238
   √ = 0.4731
   ΔCα = 1.25 × 0.4731 = 0.5913 мА

2. Расчёт относительной погрешности δC (для лучшего опыта):
   Формула: δC = √[ (ΔI/I)² + (2Δβ/sin2β)² ]
   I = 20.00 мА
   ΔI = 0.3 мА
   ΔI/I = 0.3/20.00 = 0.015000
   (ΔI/I)² = 0.00022500
   β = 41.50° = 0.7243 рад
   Δβ = 0.5° = 0.0087 рад
   2β = 83.00°
   sin(2β) = sin(83.00°) = 0.992546
   2Δβ/sin2β = (2·0.0087)/0.992546 = 0.017584
   (2Δβ/sin2β)² = 0.00030921
   δC = √(0.00022500 + 0.00030921) = 0.023113
   δC = 2.3113%

3. Расчёт полной погрешности ΔC:
   Формула: ΔC = √(ΔCα² + (δC·C⁻)²)
   ΔCα = 0.5913 мА
   ΔCα² = 0.34966086
   δC·C⁻ = 0.023113 × 22.2179 = 0.5135 мА
   (δC·C⁻)² = 0.26370507
   ΔC = √(0.34966086 + 0.26370507) = 0.7832 мА
```

Рис. 3. Выходные данные

```
================================================================================
РАСЧЁТ ГОРИЗОНТАЛЬНОЙ СОСТАВЛЯЮЩЕЙ МАГНИТНОГО ПОЛЯ ЗЕМЛИ H0
================================================================================

4. Расчёт H0:
   Формула: H0 = (N / (2R)) · C
   N = 162
   R = 0.203 м
   2R = 0.406 м
   N/(2R) = 162/0.406 = 399.014778 м⁻¹
   C⁻ = 22.2179 мА = 0.022218 А
   H0 = 399.014778 × 0.022218 = 8.865276 А/м

5. Расчёт погрешности H0:
   Формула: δH0 = √[ (ΔI/I)² + (ΔR/R)² + (2Δβ/sin2β)² ]
   ΔI/I = 0.015000
   (ΔI/I)² = 0.00022500
   ΔR/R = 0.002/0.203 = 0.009852
   (ΔR/R)² = 0.00009707
   2Δβ/sin2β = 0.017584
   (2Δβ/sin2β)² = 0.00030921
   δH0 = √(0.00022500 + 0.00009707 + 0.00030921)
        = √(0.00063128) = 0.025125
   ΔH0 = H0 · δH0 = 8.865276 × 0.025125 = 0.222742 А/м
```

Рис. 4. Выходные данные

```
================================================================================
РАСЧЁТ ВЕРТИКАЛЬНОЙ И ПОЛНОЙ НАПРЯЖЁННОСТИ МАГНИТНОГО ПОЛЯ ЗЕМЛИ
================================================================================

6. Расчёт вертикальной составляющей H_z:
   Формула: H_z = H0 · tg(i)
   H0 = 8.865276 А/м
   i = 71.9°
   tg(i) = tan(71.9°) = 3.059504
   H_z = 8.865276 × 3.059504 = 27.123347 А/м
   ΔH_z = H_z · δH0 = 27.123347 × 0.025125 = 0.681480 А/м

7. Расчёт полной напряжённости H_full:
   Формула: H_full = H0 / cos(i)
   H0 = 8.865276 А/м
   cos(i) = cos(71.9°) = 0.310676
   H_full = 8.865276 / 0.310676 = 28.535400 А/м
   ΔH_full = H_full · δH0 = 28.535400 × 0.025125 = 0.716958 А/м

* - лучший опыт (используется для расчёта погрешностей)

РЕЗУЛЬТАТЫ:
  Угол наклонения i = 71.9°
  Географическая широта = 59.9°
  Постоянная тангенс-гальванометра: C = 22.2179 ± 0.7832 мА (α = 0.7)
  Горизонтальная составляющая H0 = 8.865276 ± 0.222742 А/м
  Вертикальная составляющая H_z = 27.123347 ± 0.681480 А/м
  Полная напряжённость H = 28.535400 ± 0.716958 А/м

Окончательный результат:
  H0 = (8.8653 ± 0.2227) А/м
  H_z = (27.1233 ± 0.6815) А/м
  H = (28.5354 ± 0.7170) А/м
  δH0 = 2.51%
```

Рис. 5. Выходные данные

3. По полученным данным программа строит раскладку вектора полной напряженности магнитного поля Земли на составляющие и схематические изображение земли с точкой наблюдения (рис. 6).

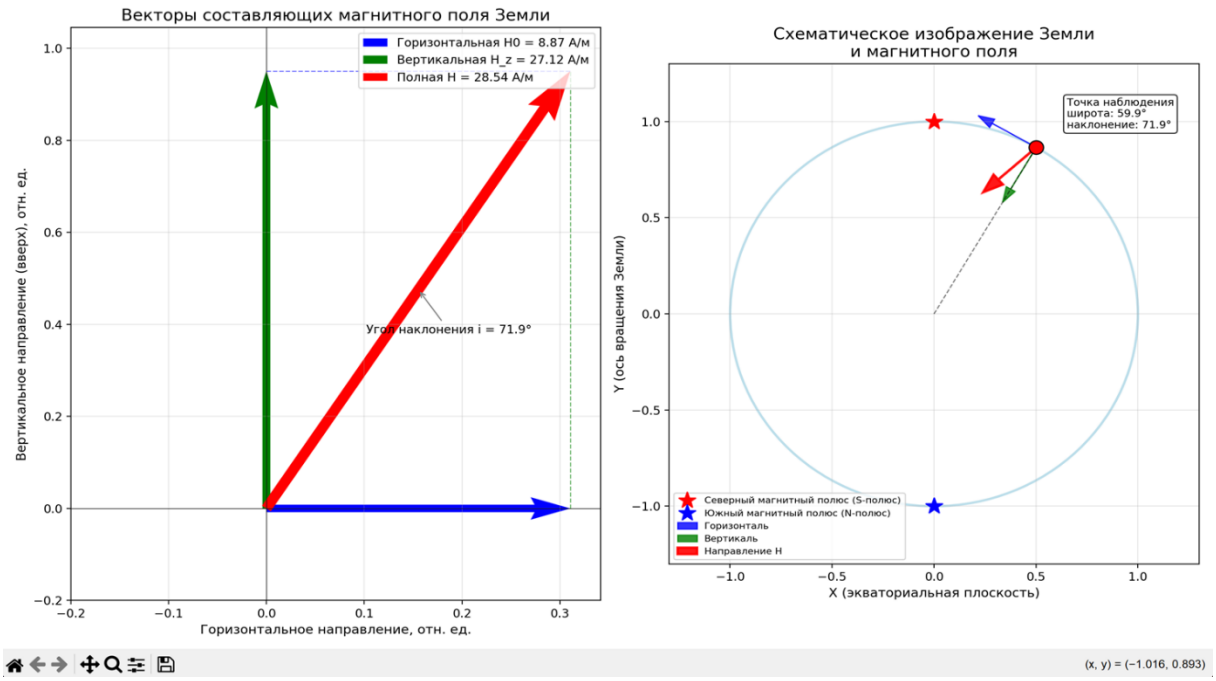


Рис. 6. Построение раскладки вектора напряженности магнитного поля на вертикальную и горизонтальную составляющие

Сферы применения

Разработанная программа может быть использована для построения карт магнитных аномалий и магниторазведочных карт, а также для долгосрочных исследований магнитного поля Земли и влияний внешних факторов на магнитное поле Земли в определенной точке наблюдения.

Список используемых источников

1. Андреев А. Д., Черных Л. М.. Физика. Магнетизм. Конспект лекций. Изд. ГУТ, СПб. 2009 г.

2. Методические указания к лабораторному практикуму по физике. Раздел «Электричество и магнетизм» / сост. Коллектив кафедры физики СПбГУТ. Санкт-Петербург: Изд-во СПбГУТ, 2022. 48 с.

3. Данные геомагнитной активности и параметров солнечного ветра [Электронный ресурс] / Институт земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова (ИЗМИРАН), отделение в Санкт-Петербурге. URL: https://www.izmiran.ru (дата обращения: 07.04.2026)

4. Магнитное поле Земли: структура, вариации, методы измерений / под ред. В. Н. Ораевского. Москва: Наука, 2015. 312 с. ISBN: 978-5-02-036548-5.

УДК 004.2

СИСТЕМНЫЙ АНАЛИЗ ПРЕДЕЛНЫХ ФАКТОРОВ РОСТА ПРОИЗВОДИТЕЛЬНОСТИ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

В. М. Деткова (к.ф.-м.н., доцент кафедры физики СПбГУТ
А. Д. Сидоров (студент гр. ИКТБ-43 СПбГУТ), sidorov.ad@sut.ru

В работе представлен системный анализ факторов, ограничивающих рост производительности современных вычислительных систем на уровне архитектуры и физики. Цель исследования – формализация совокупности ограничений, определяющих достижимую производительность процессоров. Рассматриваются три архитектурных ограничения (пропускная способность памяти, вычислительные ресурсы, параллелизм) и два физических (тепловыделение и конечность скорости распространения сигналов). Предложена упрощенная аналитическая модель, учитывающая их совместное влияние. Показано, что в современных условиях доминирующим физическим ограничением является тепловыделение, тогда как ограничение скорости распространения сигналов носит потенциальный характер. Результаты применимы для анализа и оптимизации высокопроизводительных вычислительных систем.

производительность процессоров; memory wall; parallelism wall; закон Амдала; вычислительные системы; тепловые ограничения; архитектура ЭВМ; аналитическая модель

Рост производительности современных вычислительных систем на текущем этапе определяется не столько увеличением аппаратных ресурсов, сколько системой ограничений, возникающих при их использовании. Увеличение числа ядер и тактовой частоты приводит к насыщению прироста производительности, что указывает на наличие предельных факторов, ограничивающих эффективность вычислений [1]. В этой связи задача анализа сводится к выявлению доминирующих ограничений и их формализации.

На архитектурном уровне производительность определяется тремя ключевыми факторами:

- ограничение пропускной способностью памяти (memory wall);
- ограничение вычислительными ресурсами (compute wall);
- ограничение степенью параллелизма (parallelism wall).

Эти ограничения действуют совместно, формируя верхнюю границу достижимой производительности [2].

В обобщенном виде архитектурное ограничение может быть представлено следующим выражением:

$$P_{arch} = min\left(B_{peak} \cdot I,\ N_{cores} \cdot f \cdot \text{FLOP/цикл} \cdot \frac{1}{1 - p + \frac{p}{N_{cores}}}\right)$$

где P_{arch} – предельная производительность, ограниченная архитектурой (FLOPS);

B_{peak} – пиковая пропускная способность памяти (байт/с);

I – арифметическая интенсивность (FLOP/байт);

N_{cores} – число вычислительных ядер;

f – тактовая частота (Гц);

FLOP/цикл – число операций на ядро за такт;

p– доля параллелизуемого кода.

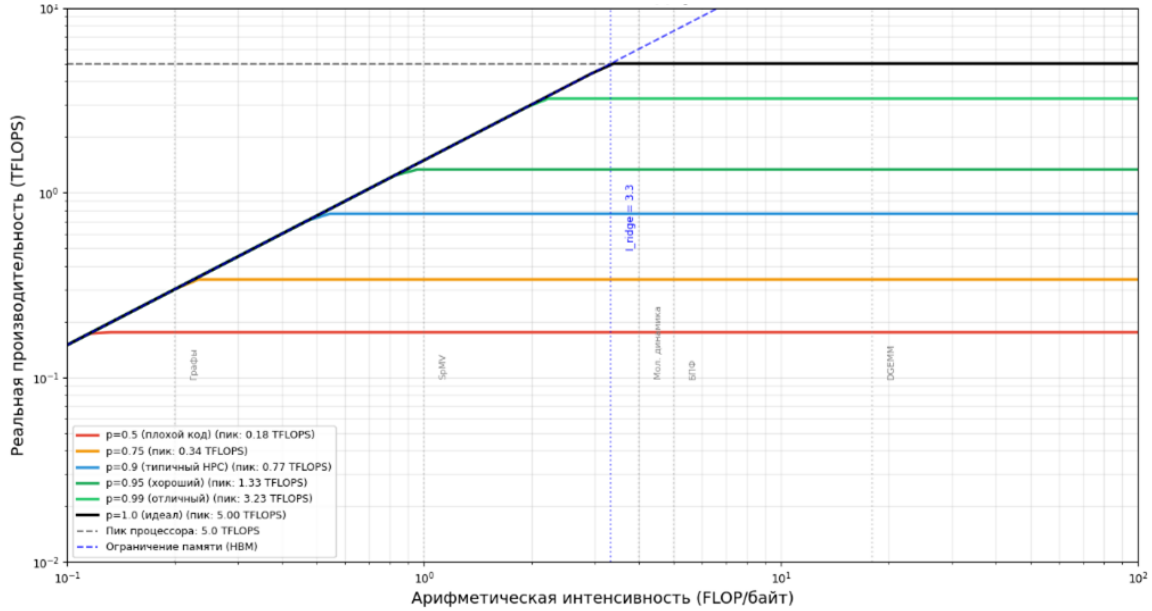


Рис. 1. График предельной производительности, ограниченной архитектурой

Из графика следует (рис. 1), что при малых значениях арифметической интенсивности производительность ограничивается пропускной способностью памяти (memory-bound режим). По мере ее роста система переходит в область, где доминируют вычислительные ресурсы и степень параллелизма, что соответствует compute/parallel-bound режиму [3].

Однако архитектурные ограничения не реализуются в полной мере из-за действия физических факторов, среди которых можно выделить тепловыделение, утечки тока, задержки межсоединений и ограничения технологического процесса, при этом доминирующим фактором в современных условиях является тепловыделение, определяющее допустимые режимы работы процессора [4].

Мощность тепловыделения может быть аппроксимирована зависимостью:

$$TDP = \beta \cdot f^3 \cdot N_{cores} \cdot p.$$

Здесь под p понимается средняя доля одновременно активных ядер, которая в первом приближении определяется степенью распараллеливания алгоритма;

TDP– тепловая мощность (Вт);

β– коэффициент, учитывающий параметры технологического процесса, напряжение питания и паразитные емкости;

f– тактовая частота (Гц);

N_{cores}– число ядер.

При фиксированном тепловом бюджете допустимая частота ограничивается следующим образом:

$$f_{max} = \left(\frac{TDP}{\beta \cdot N_{cores} \cdot p}\right)^{1/3},$$

где f_{max} – максимально допустимая тактовая частота (Гц).

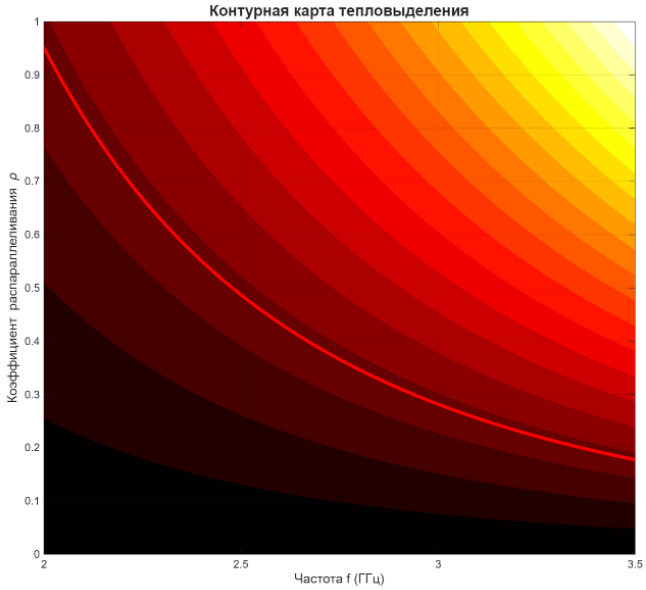


Рис. 2. Ограничение частоты процессора тепловыми условиями

Представленная зависимость (рис. 2) показывает, что допустимая тактовая частота убывает с ростом числа активных ядер и степени параллелизма при фиксированном тепловом бюджете [3]. Это подтверждает, что тепловыделение выступает доминирующим фактором, ограничивающим масштабирование частоты.

Объединение архитектурных и физических факторов позволяет получить итоговую аналитическую модель производительности:

$$P = \left(\frac{TDP}{\beta \cdot N_{cores} \cdot p}\right)^{1/3} \cdot N_{cores} \cdot \text{FLOP/цикл} \cdot \frac{1}{1 - p + \frac{p}{N_{cores}}},$$

где P– достижимая производительность (FLOPS).

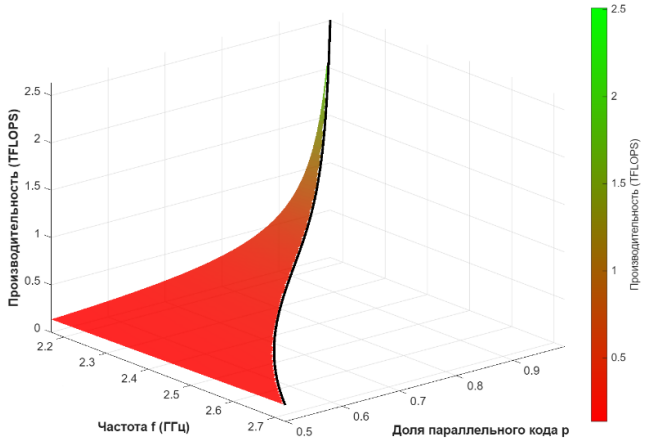


Рис. 3. График итоговой модели производительности

Из графика на рис. 3 видно, что производительность достигает максимума при некотором сочетании числа ядер, тактовой частоты и степени параллелизма. Объясняется это тем, что при фиксированном тепловом бюджете рост числа ядер обычно требует снижения частоты. В результате выигрыш от параллельной обработки не всегда компенсирует потерю производительности каждого отдельного ядра.

Значение параметра p определяет, насколько эффективно программа может задействовать имеющиеся ядра [5]. При невысокой степени параллелизма увеличение их количества дает сравнительно небольшой прирост, тогда как падение частоты остается заметным. Поэтому оптимальный режим работы системы зависит не только от архитектуры процессора, но и от характера решаемой задачи.

Уменьшение техпроцесса повышает плотность транзисторов и снижает энергопотребление, однако в рамках рассмотренной модели главным фактором роста производительности оно не является. Более существенны допустимое тепловыделение и способность программного обеспечения эффективно распределять вычисления между ядрами.

При фиксированном TDP производительность, таким образом, не растет линейно с увеличением числа ядер. Чтобы выйти на максимум, необходимо искать компромисс между частотой, количеством вычислительных ядер и уровнем параллелизма конкретной задачи. Предложенная модель позволяет оценить этот компромисс количественно – то есть подобрать параметры под конкретные условия, а не наугад.

Список используемых источников

1. Хеннесси Дж., Паттерсон Д. Архитектура вычислительных систем. СПб.: Питер, 2019. 1440 с.

2. Williams S., Waterman A., Patterson D. Roofline: An Insightful Visual Performance Model for Multicore Architectures // Communications of the ACM. 2009. Vol. 52. № 4. PP. 65–76.

3. Vetter J. S., DeBenedictis E. P., Conte T. M. Architectures for the Post-Moore Era // IEEE Micro. 2017. Vol. 37. № 4. PP. 6–8.

4. Sutter H. The Free Lunch Is Over: A Fundamental Turn Toward Concurrency // Dr. Dobb's Journal. 2005. № 3. PP. 202–210.

5. Kim N. S. et al. Heterogeneous Computing Meets Near-Memory Acceleration and High-Level Synthesis in the Post-Moore Era // IEEE Micro. 2017. Vol. 37. № 4. PP. 10–18.

УДК 621.362:533.9

ЭФФЕКТИВНОСТЬ МГД-ПРЕОБРАЗОВАНИЯ ЭНЕРГИИ: СРАВНЕНИЕ КОНСТРУКЦИЙ И МАТЕРИАЛОВ

О. А. Долматова (к.ф.-м.н., доцент СПбГУТ)
В. А. Пирогов (студент гр. РК-2512 СПбГУТ), pirogov.va@sut.ru

В статье рассматриваются факторы, определяющие эффективность магнитогидродинамического (МГД) преобразования энергии. Проводится сравнительный анализ трех основных типов МГД-генераторов: фарадеевского, холловского и дискового с точки зрения их энергетической эффективности, показывается влияние электродных, изоляционных и конструкционных материалов на ресурс и коэффициент полезного действия установок. На основе проведенных сравнений делаются выводы о наиболее перспективных решениях для повышения эффективности МГД-генераторов в разных областях применения.

МГД-генератор, эффективность преобразования энергии, сравнительный анализ, материалы, перспективные решения, области применения

Рост интереса к прямым методам преобразования энергии и появление новых материалов актуализируют выбор оптимальных схем и материалов МГД-генераторов [1]. Цель работы определить оптимальное их сочетания для разных сфер применения. В процессе решения необходимо выполнить следующие четыре задачи: выявить факторы эффективности, сравнить три типа МГД-генератора, оценить влияние материалов, сформулировать оптимальные сочетания.

Рассмотрим принцип работы генератора (рис. 1). Топливо и окислитель в камере создают плазму. В магнитном поле канала под действием силы Лоренса происходит разделение зарядов [2] положительные ионы идут к одному электроду, отрицательные к другому. Между ними возникает разность потенциалов, при замыкании внешней цепи которой через нагрузку идет ток. Таким образом тепловая энергия сгорания преобразуется в электрическую. Это общий принцип всех МГД-генераторов. На практике есть три их типа, различающихся только способом съема тока. Рассмотрим их.

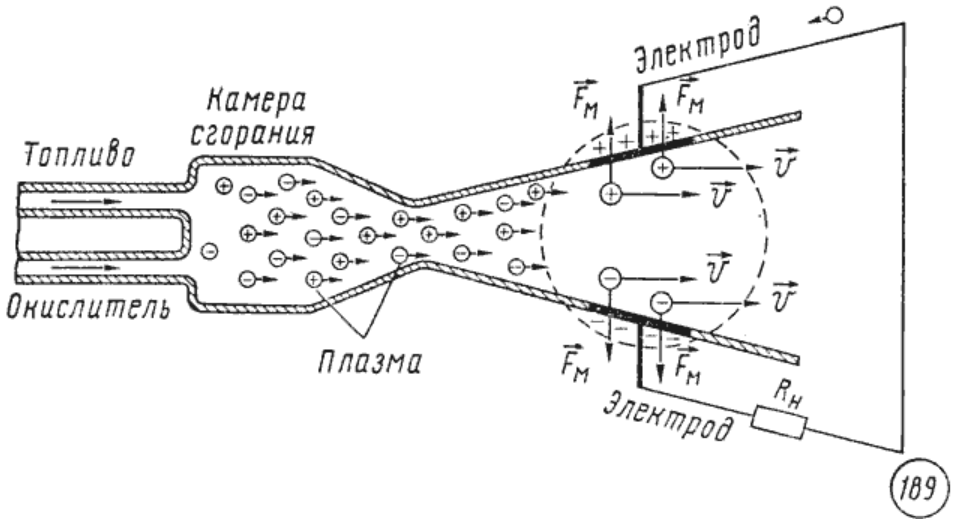


Рис. 1. Схема конструкции МГД-генератора

В фарадеевском типе (рис. 2) электроды расположены на противоположных стенках канала, перпендикулярно направлению потока плазмы и магнитного поля, а ток снимается поперек канала.

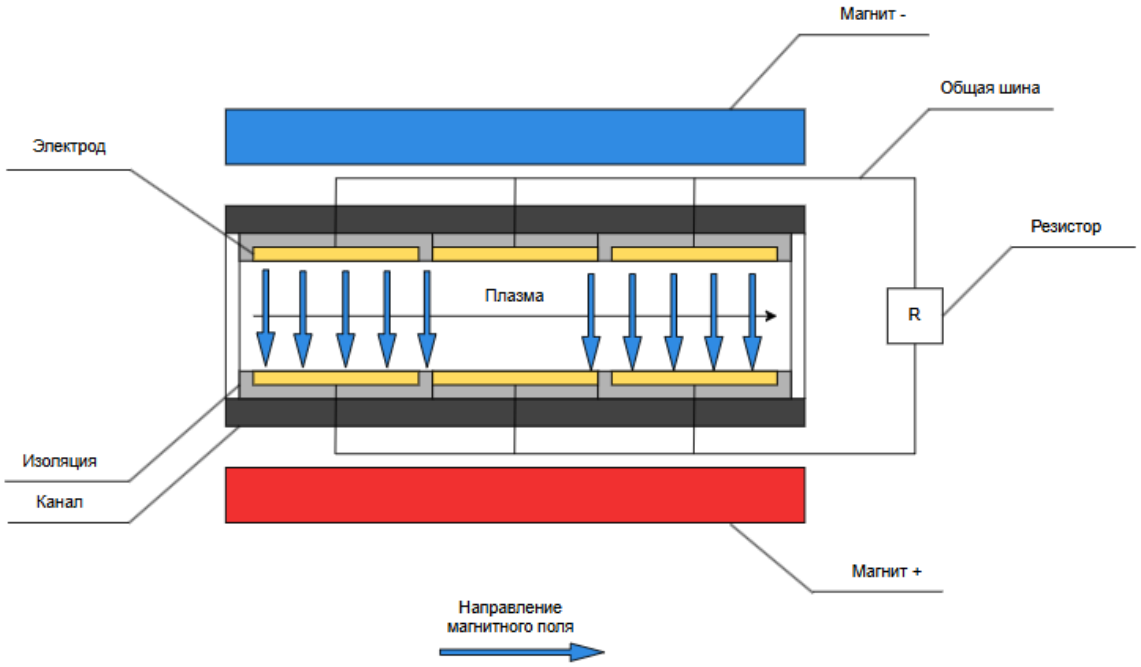


Рис. 2. Фарадеевский тип МГД-генератора

В холловском (рис. 3) электроды расположены вдоль канала, а ток снимается продольно, то есть в направлении движения плазмы. Конструкция значительно проще, чем у фарадеевского, однако из-за холловских токи снижают общий КПД.

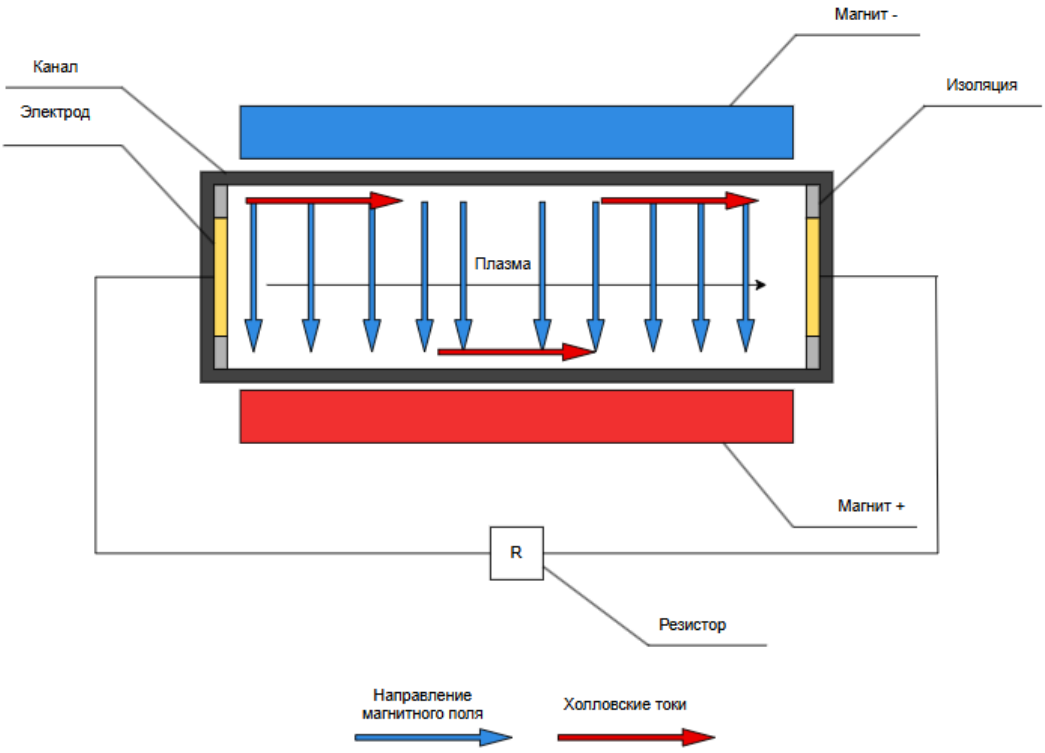


Рис. 3. Холловский тип МГД-генератора

Дисковой тип (рис. 4) является разновидность холловского, но с принципиальным отличием в строении. Канал выполнен в виде кольца, ток снимается с кольцевых электродов, что дает очень высокую удельную мощность. Сравним характеристики трех типов МГД-генераторов.

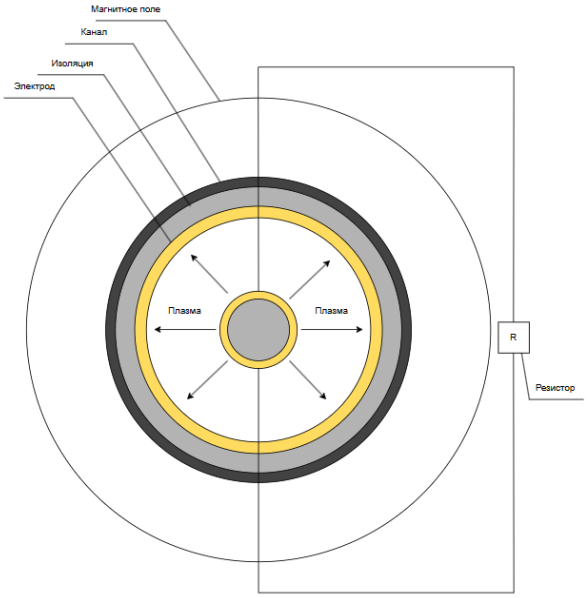


Рис. 4. Дисковой тип МГД-генератора

По КПД в стационаре лидирует фарадеевский до 25 % за счет поперечного съема тока, а холловский до 18 % из-за возникновения паразитных холловских токов. В импульсе дисковый эффективнее. Его кольцевая система лучше приспособлена к высоким скоростям потока.

По удельной мощности в стационаре дисковый впереди выдавая до 20 кВт/кг благодаря кольцевой системе. Фарадеевский проигрывает до 8 кВт/кг из-за сложного соединения электродов [3]. В импульсе дисковый лидирует до 100 кВт/кг за счет кольцевой системе минимизирующей потери.

По ресурсу в стационаре фарадеевский работает дольше всех до 5000 ч за счет более равномерного распределения нагрузок. Дисковый до 800 ч из-за высоких тепловых потоков. В импульсном режиме фарадеевский и холловский выдерживают десятки импульсов, в то время как дисковый от 1 до 20. Но за эти импульсы он выдает до 100 кВт/кг.

По температуре плазмы фарадеевский и холловский работают при 2500–3000 К, дисковый требует 3000–3500 К так как для высокой удельной мощности необходима большая проводимость плазмы.

По магнитному полю фарадеевский требует 3–5 Тл, холловский от 4–6 Тл, дисковый от 5–10 Тл. Дисковому нужно самое сильное поле для максимального взаимодействия плазмы с полем и компенсации потерь [4].

Сравнение характеристик фарадеевского, холловского и дискового МГД-генератора дано в таблице 1.

ТАБЛИЦА 1. Характеристики фарадеевского, холловского и дискового МГД-генератора

Параметр	Режим работы	Фарадеевский	Холловский	Дисковой
КПД, %	Стационарный	20 – 25	12 – 18	18 – 22
	Импульсный	8 – 12	6 – 10	10 – 15
Удельная мощность, кВт/кг	Стационарный	3 – 8	5 – 12	10 – 20
	Импульсный	10 – 20	20 – 40	50 – 100
Ресурс, часов / импульсов	Стационарный	1000 – 5000	500 – 2000	200 – 800
	Импульсный	10 – 50	20 – 100	1 – 20
Температура плазмы, К	Оба режима	2500 – 3000	2500 – 3000	3000 – 3500
Магнитное поле, Тл	Оба режима	3 – 5	4 – 6	5 – 10

Перейдем ко второму фактору эффективности – материалам. Они делятся на три группы.

Первыми являются электродные материалы (вольфрам, молибден, графит). От них зависят ресурс и съем тока. Вольфрам самый тугоплавкий его температура плавления более 3400°С, что дает более высокий ресурс, но делает его слишком дорогим. Молибден дешевле, но уступает в стойкости. Графит самый дешевый и легко обрабатывается, но быстро разрушается. Он подходит для импульсных режимов.

Вторые – это изоляционные материалы (оксид циркония, оксид алюминия). Они защищают стенки от пробоев. Так оксид циркония выдерживает 2500 °С и химически инертен, что делает его лучшим выбором для стационара. Оксид алюминия дешевле, но его предел 2000 °С.

Последние конструкционные материалы (углеродные композиты и жаростойкие сплавы). Композиты легкие, выдерживают до 3000 °С, позволяют МГД-генератору работать в импульсных режимах без разрушения. Сплавы дешевле, но применяются в менее горячих зонах. Теперь перейдем к областям применения.

Фарадеевский тип с вольфрамовыми электродами и изоляцией из оксида циркония лучше всего подходит для стационарной энергетики. Его можно использовать как надстройку на ТЭС для повышения КПД, а также в гибридных установках

Холловский тип благодаря простоте конструкции и обслуживания отлично подойдет для автономных электростанций или резервных источников питания. Лучше всего для них подойдут молибденовые электроды и изоляция из оксида алюминия.

Дисковый тип с графитовыми электродами и высокотемпературными углеродными композитами лучше использовать в импульсных системах для мощных кратковременных разрядов.

Список используемых источников

1. Панченко В. П. Физико-технические основы магнитогидродинамического преобразования энергии: учеб. пособие. М.: Изд-во МГТУ им. Н. Э. Баумана, 2015. 80 с. ISBN 978-5-7038-4140-2.

2. Ватажин А. Б., Любимов Г. А., Регирер С. А. Магнитогидродинамические течения в каналах. М.: Наука, 1970. 572 с.

3. Бреев В. В., Губарев А. В., Панченко В. П. Сверхзвуковые МГД-генераторы. М.: Энергоатомиздат, 1988. 240 с.

4. Том Р., Тарр Дж. Магнитные системы МГД-генераторов и термоядерных установок: Основы расчета магнитных полей и сил: пер. с англ. М.: Энергоатомиздат, 1985. 272 с.

УДК 621.372.542.21

СРАВНЕНИЕ ЭНЕРГЕТИЧЕСКИХ ПОКАЗАТЕЛЕЙ ФИЛЬТРОВ С РАЗНЫМИ ВИДАМИ ФИЛЬТРУЮЩИХ ФУНКЦИЙ

З. В. Зайцева (к.т.н., доцент кафедры электроники СПбГУТ)
А. А. Кузьменков (студент гр. РЭ-41 СПбГУТ), kuzmenkov.aa@sut.ru
В. М. Мантуров (студент гр. РЭ-41 СПбГУТ), manturov.vm@sut.ru

При проектировании фильтров для мощных радиотехнических и преобразовательных устройств технико-экономические показатели такие как вес, габаритные размеры, стоимость, КПД и стабильность частотных характеристик имеют определяющее значение. Все эти показатели напрямую связаны с энергетическими функциями фильтра, то есть с энергией, накапливаемой в его реактивных элементах – конденсаторах и катушках индуктивности.

фильтры низких частот, аппроксимирующие функции, энергетические показатели

При проектировании фильтров, предназначенных для работы в мощных радиотехнических и преобразовательных устройствах, на первый план выходят не только электрические параметры, но и технические-экономические, которые в значительной степени определяются энергетическими функциями фильтра – количеством энергии, накапливаемой в реактивных элементах. Чем меньше запасенная энергия, тем легче, компактнее и экономичнее, может быть, устройство при заданных требованиях к избирательности [1-3].

Целью данной работы является сравнительный анализ фильтров по энергетическим показателям при изменении допустимой неравномерности затухания в полосе пропускания Δa. Для анализа были выбраны фильтры нижних частот (ФНЧ) со следующими видами аппроксимирующих функций: максимально плоская (Баттерворта), равноволновая (Чебышева) и эллиптическая (Золотарева – Кауэра). Выражение для ослабления ФНЧ в общем виде можно записать следующим образом:

$$a(\Omega) = 10 \cdot \lg\left(1 + \varepsilon^2 {\Psi_n}^2(\Omega)\right),$$

где $\Psi_n(\Omega)$ – фильтрующая функция; $\Omega = f/f_0$ – нормированная частота, f_0 – граничная частота полосы пропускания (ПП); $\varepsilon = \sqrt{10^{0.1*\Delta a} - 1}$ – коэффициент неравномерности; n – порядок фильтра.

Для корректного сравнения фильтров с различными аппроксимирующими функциями были заданы следующие требования к характеристике затухания: гарантированное ослабление в полосе задерживания (ПЗ) a_0 = 40 дБ; граничная частота полосы пропускания (ПП) f_0 =17 кГц; нормированная частота, равная отношению граничных частот полосы задерживания и пропускания, $\Omega_k = f_k / f_0 = 2$; максимальная мощность в нагрузке равна 2 кВт.

В качестве критерия эффективности рассматривалось максимальное значение относительной суммарной реактивной энергии в полосе пропускания. Также рассчитывалось групповое время задержки (ГВЗ), которое в LC-фильтре пропорционально запасенной энергии.

Энергетические функции были рассчитаны для фильтров с разными аппроксимирующими функциями при следующих значениях Δa: 0.0109 дБ, 0.0988 дБ, 0.2803 дБ и 1.2494 дБ. Схемы фильтров и их параметры были рассчитаны с использованием справочника Зааля Р. по расчету фильтров [4].

Рассмотрим особенности фильтров с разными фильтрующими функциями:

1. Фильтр с максимально плоской характеристикой – фильтр Баттерворта.

Фильтрующая функция имеет вид:

$$\Psi_n(\Omega) = \Omega^{2n}$$

К особенностям данного фильтра можно отнести: максимально плоскую АЧХ в ПП, из-за чего отсутствуют локальные пики напряжения и тока на реактивных элементах; самое малое влияние допусков емкости и индуктивности на изменение из всех фильтров АЧХ; для заданной крутизны среза фильтр Баттерворта требует более высокого порядка или больших номиналов L и C, что повышает вес и объем конструкции. Также у данного фильтра отсутствуют резонансные всплески энергии в ПЗ [1, с. 16-21].

2. Фильтр с равноволновой характеристикой – фильтра Чебышева.

Фильтрующая функция имеет вид:

$$\Psi_n(\Omega) = P_n(\Omega),$$

где $P_n(\Omega)$ – полином Чебышева:

$$P_n(\Omega) = \begin{cases} \cos(n \cdot \arccos(\Omega)) \text{ при } |\Omega| \le 1 \\ ch\big(n \cdot arcch(\Omega)\big) \text{ при } |\Omega| > 1 \end{cases}.$$

К особенностям данного фильтра относят: более высокая, чем у фильтра Баттерворта, крутизна среза, при одинаковом значении n; на резонансных частотах в ПП возникают локальные пики ослабления, что приводит к повышенным напряжениям и токам на реактивных элементах; данный фильтр имеет наибольшие фазовые искажения из всех фильтров и занимает промежуточное положение по чувствительности АЧХ к изменению параметров [1, с. 16-21].

3. Фильтр с эллиптической характеристикой – фильтр. Золотарева – Кауэра

Фильтрующая функция имеет вид:

$$\Psi_n(\Omega) = R_n(\Omega),$$

где $R_n(\Omega)$ – дробь Золотарева:

Для четных n: $R_n(\Omega) = H_1 * \prod_{v=1}^{0.5*n} \frac{\frac{1}{k^2\Omega^2_{ov}} - \Omega^2}{\Omega^2_{ov} - \Omega^2}$,

Для нечетных n: $R(\Omega)_n = H_1 * \Omega * \prod_{v=1}^{0.5*(n-1)} \frac{\frac{1}{k^2\Omega^2_{ov}} - \Omega^2}{\Omega^2_{ov} - \Omega^2}$,

где H_1 – нормируемый коэффициент, Ω_{ov} – частота всплесков затухания, k=1/Ω_k.

Основные особенности эллиптического фильтра: наличие всплесков в ПЗ позволяет обеспечить максимальную крутизну среза, меньше всего реактивных элементов и меньшие номиналы L и C, а также очень большая чувствительность к допускам на изменение параметров емкостей и индуктивностей среди всех трех типов фильтров [1, с. 16-21].

В процессе выполнения работы были получены схемы ФНЧ для трех видов аппроксимирующих функций и четырех значений Δa. Для каждого из фильтров были рассчитаны энергетические характеристики: энергия, запасенная на индуктивностях и емкостях; суммарная энергия в реактивных элементах фильтра и ГВЗ фильтра.

В табл. 1-4 представлены полученные значения энергетических характеристик фильтров на граничной частоте полосы пропускания, а также групповое время задержки (ГВЗ).

ТАБЛИЦА 1. Энергетические характеристики и ГВЗ при $\Delta a = 0.0109$ дБ

Название фильтра (ФНЧ)	Порядок	Суммарная индуктивность, мГн	Суммарная емкость, нФ	Энергия, запасенная в индуктивности, мДж	Энергия, запасенная в емкости, мДж	Суммарная энергия в реактивных элементах, мДж	Групповое время задержки, мкс
Баттерворт	11	30.0640	83.5110	67.9305	67.0855	135.0160	33.7540
Чебышев	7	24.8701	80.0198	82.6385	81.9195	164.5580	41.1395
Золотарев-Кауэр	5	12.9749	47.3639	44.5209	37.1591	81.6780	20.42

ТАБЛИЦА 2. Энергетические характеристики и ГВЗ при $\Delta a = 0.0988$ дБ

Название фильтра (ФНЧ)	Порядок	Суммарная индуктивность, мГн	Суммарная емкость, нФ	Энергия, запасенная в индуктивности, мДж	Энергия, запасенная в емкости, мДж	Суммарная энергия в реактивных элементах, мДж	Групповое время задержки, мкс
Баттерворт	10	29.7367	82.6021	75.1769	74.1705	149.3474	37.3368
Чебышев	6	24.3792	67.7201	90.5350	88.0395	178.5744	44.6436
Золотарев-Кауэр	4	11.7423	35.6315	40.6591	39.0475	79.7065	19.9266

ТАБЛИЦА 3. Энергетические характеристики и ГВЗ при $\Delta a = 0.2803$ дБ

Название фильтра (ФНЧ)	Порядок	Суммарная индуктивность, мГн	Суммарная емкость, нФ	Энергия, запасенная в индуктивности, мДж	Энергия, запасенная в емкости, мДж	Суммарная энергия в реактивных элементах, мДж	Групповое время задержки, мкс
Баттерворт	9	27.8300	77.3056	72.9222	76.6558	149.5780	37.3945
Чебышев	6	26.3039	73.0665	117.4616	115.1848	232.6464	58.1616
Золотарев-Кауэр	4	13.5312	40.2246	53.0404	52.3846	105.4250	26.3563

ТАБЛИЦА 4. Энергетические характеристики и ГВЗ при $\Delta a = 1.2494$ дБ

Название фильтра (ФНЧ)	Порядок	Суммарная индуктивность, мГн	Суммарная емкость, нФ	Энергия, запасенная в индуктивности, мДж	Энергия, запасенная в емкости, мДж	Суммарная энергия в реактивных элементах, мДж	Групповое время задержки, мкс
Баттерворт	8	26.8823	74.6731	77.4930	82.8772	160.3702	40.0925
Чебышев	5	11.6292	122.3899	119.5213	126.4196	245.9409	61.4852
Золотарев-Кауэр	4	16.9289	49.0959	72.5876	78.7033	151.2909	37.8227

Как видно из табл.1 фильтр Баттерворта имеет самый большой порядок и самые большие значения величин C и L, а фильтр Золотарева – Кауэра – самые минимальные. При этом во всем диапазоне значений Δa суммарная энергия эллиптического фильтра наименьшая: выигрыш по энергии относительно фильтра Баттерворта достигает 5–40 %, относительно фильтра Чебышева – 40–55 %. Отсюда следует, что фильтр Чебышев имеет самую большую суммарную энергию, а фильтр Баттерворта занимает промежуточное положение. При этом при увеличении Δa фильтр Чебышева имеет самое большое из всех ГВЗ, а фильтра Золотарев – Кауэра – минимальное.

Если сравнить энергетические показатели фильтров с одинаковыми фильтрующими функциями при изменении Δa от 0.109 дБ до 1.2494 дБ, то можно сделать следующий вывод: влияние величины Δa на суммарную энергию, накапливаемую в индуктивностях и емкостях, имеет следующую зависимость:

- у фильтра Баттерворта суммарная энергия растет незначительно (+19 %);
- у фильтра Чебышева суммарная энергия растет умеренно (+50 %);
- у фильтра Золотарева-Кауэра суммарная энергия увеличивается существеннее всего (+85 %) при изменении Δa от минимального значения 0.109 дБ до максимального значения1.2494 дБ. Это показывает, что наиболее чувствительным фильтром к изменение допустимого ослабления в ПП Δa является эллиптический фильтр Золотарева-Кауэра. Это обусловлено смещением нулей передачи и увеличением всплесков запасаемой энергии.

Наиболее устойчивым к изменению Δa из всех является фильтр Баттерворта. Это связано с тем, что он имеет максимально плоскую характеристику в ПП.

Пересчитаем вес и объем фильтров основываясь на энергии реактивных элементов по формулам:

$$G = \frac{W_L}{{\gamma_L}^G} + \frac{W_C}{{\gamma_C}^G}, \qquad V = \frac{W_L}{{\gamma_L}^V} + \frac{W_C}{{\gamma_C}^V}$$

где ${\gamma_L}^G = 0.15$ Дж/кг и ${\gamma_L}^V = 30$ Дж/м3 – удельные энергоемкости катушек индуктивности, а ${\gamma_C}^G = 0.3$ Дж/кг и ${\gamma_C}^V = 700$ Дж/м3 – удельные энергоемкости конденсаторов.

ТАБЛИЦА 5. Объем и вес при разных допустимых ослаблениях в ПП

Название фильтра	$\Delta a = 0.0109$ дБ		$\Delta a = 0.0988$ дБ		$\Delta a = 0.2803$ дБ		$\Delta a = 1.2494$ дБ	
	Вес, кг	Объем, м^3	Вес, кг	Объем, м^3	Вес, кг	Объем, м^3	Вес, кг	Объем, м^3
Баттерворт	0,6763	0,002359	0,7498	0,002617	0,7414	0,002617	0,7927	0,002701
Чебышев	0,8234	0,002869	0,8962	0,003141	1,1657	0,004198	1,227	0,004198
Золотарев-Кауэр	0,4203	0,001536	0,4009	0,00141	0,5279	0,001842	0,7467	0,002534

Их анализа полученных результатов из табл.5 можно сделать вывод, что фильтр Чебышева имеет наибольшие массо-габаритные параметры, а фильтр Золотарева – Кауэра –самый компактный и легкий. Фильтр Баттерворта занимает промежуточное положение.

Список используемых источников

1. Дмитриков В. Ф., Сергеев В. В., Самылин И. Н. Повышение эффективности преобразовательных и радиотехнических устройств. М.: Радио и связь, 2005. 424 с.

2. А. А. Аль-Номан, В. В. Сергеев Энергетические характеристики нагруженных реактивных четырехполюсников // Автомат. и телемех., 1999. № 1. 180–186.

3. Сергеев В. В. Показатели эффективности LC-фильтров с различными аппроксимирующими функциями // Труды учебных заведений связи. 2016. Т. 2. № 3. С. 98–103.

4. Зааль Р. Справочник по расчету фильтров / пер. с нем. под ред. Н. Н. Слепова. М.: Радио и связь, 1983. 94–753 с.

УДК 621.317.757:378.147(075.8)

РАЗРАБОТКА ПОРТАТИВНОГО ДВУХКАНАЛЬНОГО ОСЦИЛЛОГРАФА ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ «КОМПОНЕНТЫ ЭЛЕКТРОННОЙ ТЕХНИКИ»

В. А. Зелинский (студент гр. РК-21 СПбГУТ), zelinskii.va@sut.ru
В. Н. Мордовин (к.п.н., доцент, доцент кафедры КПРЭС СПбГУТ)

В статье представлено обоснование основных этапов разработки специализированного портативного двухканального осциллографа, предназначенного для использования в лабораторных работах по дисциплине «Компоненты электронной техники». Прибор должен обладать повышенной устойчивостью к механическим воздействиям, оптимизированным набором функций и возможностью адаптации программного обеспечения. Детально описаны принятые технические решения, конструктивные особенности, результаты экспериментальной проверки макетного образца. Приведены данные об экономической эффективности прибора.

лабораторный осциллограф, двухканальный осциллограф, портативный осциллограф, устойчивость к механическим воздействиям, адаптивное программное обеспечение, экспериментальная проверка

Дисциплина «Компоненты электронной техники» является базовой для подготовки бакалавров по направлениям: 11.03.01 «Радиотехнические системы»; 11.03.02 «Инфокоммуникационные технологии и системы связи»; 11.03.03 «Конструирование и технология электронных средств»; 11.03.04 «Электроника и наноэлектроника».

В рамках лабораторных работ студенты исследуют пассивные и активные компоненты, усилители, цифровые схемы. Анализ учебно-методического пособия [1] показал необходимость создания измерительного прибора, сочетающего достаточную функциональность, низкую стоимость и высокую механическую надежность. Коммерческие аналоги либо избыточны по функциям, либо не адаптированы к интенсивной эксплуатации в условиях учебного процесса.

Технические требования и принятые решения

На основе анализа лабораторных работ определены следующие параметры.

Технические характеристики:

- количество каналов измерения: 2;
- полоса пропускания: 30 кГц;
- максимальная частота дискретизации: 250 *MS/s*;
- разрядность АЦП: 12 бит;
- диапазон входных напряжений: ±36 В;
- возможность автономной работы на протяжении 2-х часов.

Функциональные возможности:

- измерение амплитуды, частоты, периода электрического сигнала;
- триггерные режимы: по фронту, по уровню измеряемого сигнала.

Для реализации прибора выбран микроконтроллер ATSAM3X8E [2] (Arduino Due) со встроенным 12-битным АЦП. Входные цепи построены на операционных усилителях AD8066 с защитными диодами и делителями. Питание осуществляется от литий-полимерного аккумулятора 12,6 В с контроллером заряда TP4056 и низкошумящими стабилизаторами. Предусмотрена возможность питания от сети.

Конструктивное исполнение

Корпус спроектирован в САПР SolidWorks и изготовлен методом 3D-печати [3] из ABS-пластика толщиной 3 мм. Углы корпуса усилены резиновыми накладками. Дисплей (3,2” TFT) защищен закаленным стеклом. Органы управления – энкодеры с тактовой кнопкой, устойчивые к многократным нажатиям. Предусмотрена цветовая индикация каналов, разъемы BNC с защитой от короткого замыкания.

Экспериментальная проверка

Макетный образец испытан в лабораторных условиях [4]. Проверка полосы пропускания проводилась с помощью генератора сигналов АКIP-3409. Полоса по уровню –3 дБ составила 32 кГц. Погрешность измерения амплитуды при подаче синусоидального сигнала частотой 1 кГц не превысила 3 % в диапазоне 0,1…30 В. Частота дискретизации в двухканальном режиме подтверждена при регистрации импульсных сигналов длительностью 10 нс. Время автономной работы при непрерывном измерении и активной подсветке дисплея составило 2 часа 15 минут, что соответствует заявленным требованиям. Программное обеспечение модульное, позволяет обновлять прошивку через USB порт.

На рис. 1 представлена структурная схема разработанного осциллографа. Она включает микроконтроллер, аналоговую часть (входные цепи, коммутатор, АЦП), блок управления, дисплей и органы управления.

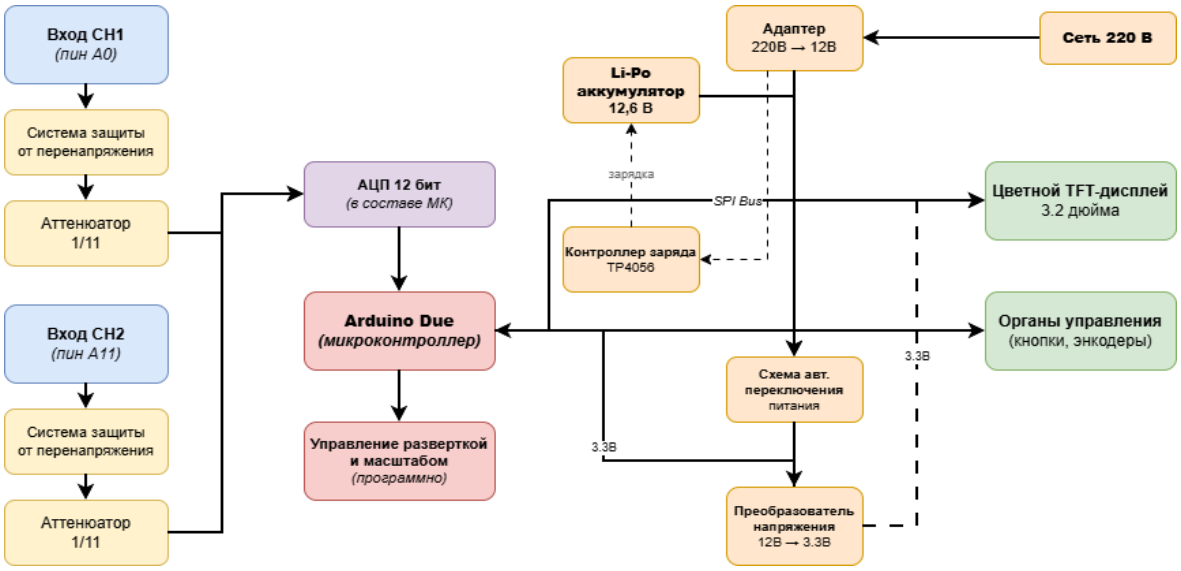


Рис. 1. Структурная схема разрабатываемого осциллографа.

Структурная схема портативного двухканального осциллографа (рис. 1) включает следующие основные функциональные блоки. Входные сигналы поступают на каналы CH1 (пин A0) и CH2 (пин A11) микроконтроллерной платформы Arduino Due. Каждый канал содержит систему защиты от перенапряжения, предотвращающую выход из строя входных цепей при превышении допустимого уровня сигнала, и аттенюатор с коэффициентом деления 1/11, позволяющий увеличить диапазон измерения входных напряжений. Аналоговые сигналы с выходов аттенюаторов подаются на 12-битный аналого-цифровой преобразователь (АЦП), встроенный в микроконтроллер ATSAM3X8E (Arduino Due). Оцифрованные данные обрабатываются микроконтроллером, который реализует функции управления разверткой и масштабом программными средствами. Отображение информации осуществляется на цветном TFT-дисплее с диагональю 3,2 дюйма, подключенном по интерфейсу SPI. Управление прибором производится с помощью кнопок и энкодеров, подключенных к цифровым входам микроконтроллера. Питание дисплея обеспечивается отдельным преобразователем напряжения, снижающим входное напряжение 12 В до необходимого уровня 3,3 В.

Экономический аспект разработки

Себестоимость осциллографа составляет 7000 руб. (с учетом печати корпуса и сборки). Для сравнения: Tektronix TBS1052B-EDU – 150000 руб., Rigol DS1054Z – 90000 руб. [5, 6]. При оснащении лаборатории на 15 рабочих мест экономия превышает 1 000 000 руб.

Заключение

Разработанный осциллограф полностью соответствует требованиям учебного процесса в рамках дисциплины «Компоненты электронной техники». Проведенные экспериментальные исследования подтвердили корректность выбранных технических решений.

Список используемых источников

1. Кирик Д. И., Мордовин В. Н., Горобцов И. А. Компоненты электронной техники: учебно-методическое пособие. СПб.: СПбГУТ, 2023. 112 с.

2. Техническая документация на микроконтроллер ATSAM3X8E. 1459 с. URL: https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-11057-32-bit-Cortex-M3-Microcontroller-SAM3X-SAM3A_Datasheet.pdf (дата обращения: 20.04.2026).

3. ГОСТ Р 57558-2025. Аддитивные технологические процессы. Базовые принципы. М.: Стандартинформ, 2025. 36 с.

4. Зелинский В. А., Мордовин В. Н. Результаты экспериментальных испытаний макетного образца: протокол № 1 от 10.03.2026. СПб.: СПбГУТ, 2026. 4 с.

5. Tektronix TBS1000B Series Oscilloscopes: официальный флаер характеристик прибора. 1 с. URL: https://assets.testequity.com/te1/Documents/pdf/TBS1000B-flyer.pdf. (дата обращения: 20.04.2026).

6. Rigol DS1054Z Digital Oscilloscope: официальный сайт производителя. URL: https://www.rigolna.com/products/digital-oscilloscopes/1000z/ (дата обращения: 20.03.2026).

УДК 621.396

ВЛИЯНИЕ ГЛУБИНЫ ОБУЧЕНИЯ НА ЭФФЕКТИВНОСТЬ ДЕМОДУЛЯТОРОВ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ В КОРОТКОВОЛНОВОМ КАНАЛЕ РАДИОСВЯЗИ

М. В. Исаков (студент гр. РТ-42м СПбГУТ), isakov.mv@sut.ru

В настоящее время методы машинного обучения и искусственный интеллект стремительно развиваются и применяются в области цифровой обработки сигналов, поэтому появляется возможность реализации и проведения обучения демодуляторов на основе нейронных сетей в коротковолновом канале радиосвязи. Результаты моделирования показывают, что с увеличением глубины обучения системы адаптируются к изменяющимся условиям ионосферы, при этом качество связи улучшается на 1,7 дБ при 700 итерациях обучения относительно метода корреляции.

машинное обучение, нейронные сети, короткие волны, радиосвязь, ионосфера, демодуляция

В настоящее время наблюдается стремительное развитие и применение искусственного интеллекта в области радиосвязи и цифровой обработки сигналов. Одной из приоритетных задач является улучшение качества и надежности связи в коротковолновом канале радиосвязи, который подвергается различным ионосферным возмущениям, влияющим на радиосигнал и приводящим к возникновению битовых ошибок при передаче данных.

Применение методов машинного обучения для демодуляции радиосигнала позволяет системе сохранять в памяти предыдущие параметры демодуляции и адаптироваться к различным факторам, которые вызывают искажения радиосигнала, например, к импульсным помехам, доплеровскому сдвигу и замираниям сигнала. С увеличением итераций обучения демодуляторы на основе нейронных сетей способны выявить различные закономерности возникновения негативно влияющих на радиосигнал факторов и временные корреляции шумов. Это позволяет системе адаптировать параметры демодуляции сигнала к различным характеристикам радиоканала для достижения наилучшего качества связи [1]. В качестве методов машинного обучения при моделировании коротковолнового радиоканала были выбраны MLP (Multi-Layer Perceptron – многослойный перцептрон) и CNN (Convolution Neural Network – сверточная нейронная сеть), т.к. принцип их работы соответствует структуре входных данных, а также требованиям к вычислительной эффективности в конкретных подзадачах.

MLP представляет собой полносвязную нейронную сеть, которая наиболее эффективно подходит для прогнозирования на основе ранее полученных данных о параметрах ионосферы, например, об индексе солнечной активности, максимально применимой частоте, времени суток и времени года, а также о геомагнитных возмущениях. Во время обучения система с MLP определяет временные корреляции полученных данных, чтобы на их основе составить прогноз и адаптировать параметры демодуляции [2].

Системы с CNN позволяют работать не только с табличными данными, которые используются для обучения MLP, но и с спектрограммами радиосигналов в реальном времени, а также учитывает наличие межсимвольной интерференции, доплеровский сдвиг и замирания сигнала [3]. Преимуществом демодуляторов на основе сверточных нейронных сетей является также возможность обнаружения локальных корреляций в спектре сигнала, например, наличие схожих искажений в нескольких соседних поднесущих OFDM-сигнала (Orthogonal Frequency-Division Multiplexing – ортогональное мультиплексирования с частотным разделением канала) [4].

Для демонстрации эффективности выбранных методов машинного обучения было проведено моделирование коротковолнового радиоканала в среде MATLAB. Моделирование включает несколько этапов, в каждом из которых проведено различное количество итераций обучения для демодуляторов на основе MLP и CNN. На каждом этапе моделирования параметры передаваемого радиосигнала остаются неизменными. Для обучения систем необходимо наличие целевых показателей качества связи, поэтому при моделировании используется канал, в котором отсутствуют шумы и замирания, т.е. соблюдаются «идеальные» условия передачи радиосигнала. Помимо методов с искусственным интеллектом был рассмотрен корреляционный метод, который наиболее часто используется в коротковолновых системах связи при демодуляции радиосигнала. В каждой итерации обучения на радиосигнал воздействуют помехи различной мощности, а также замирания и доплеровский сдвиг от 0,1 до 30 Гц. Наличие негативно влияющих факторов приближает моделирование к реальным условиям ионосферного распространения радиосигнала и позволяет системам с MLP и CNN адаптироваться к ним. На рис. 1 показаны графики зависимости BER (Bit Error Rate – вероятность битовой ошибки) от SNR (Signal/Noise Ratio – отношение сигнал/шум) для корреляционного метода и демодуляторов на основе нейронных сетей при 100 итерациях обучения.

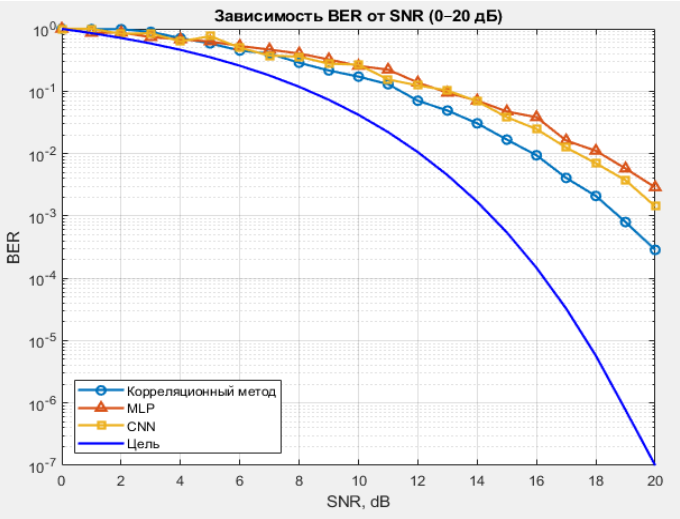


Рис. 1. График зависимости BER от SNR для корреляционного метода и демодуляторов на основе нейронных сетей при 100 итерациях обучения

Анализ графиков показывает, что при 100 итерациях обучения эффективность систем с CNN и MLP меньше, чем у метода корреляции. Корреляционный метод не требует обучения и подбирает параметры демодуляции по заранее известным шаблонам для каждого из полученных сигналов. На рис. 2 представлены графики зависимости BER от SNR для корреляционного метода и демодуляторов на основе нейронных сетей при 300 итерациях обучения.

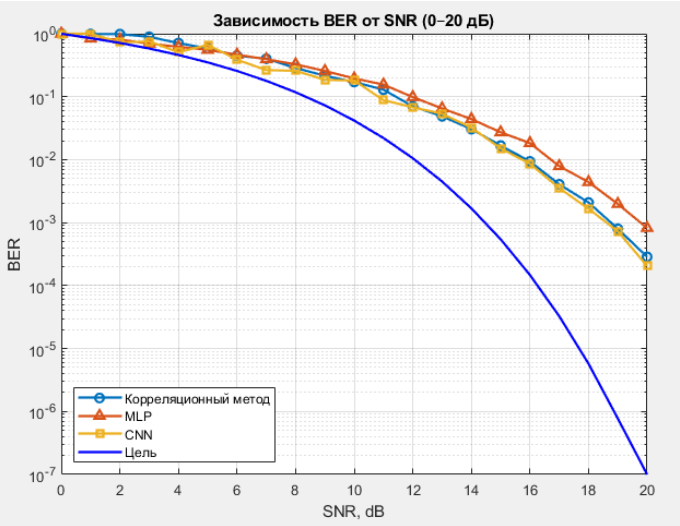


Рис. 2. График зависимости BER от SNR для корреляционного метода и демодуляторов на основе нейронных сетей при 300 итерациях обучения

Графики показывают, что при 300 итерациях обучения эффективность системы с CNN и метода корреляции приблизительно равна. Производительность демодулятора на основе MLP при BER = 10^{-3} меньше на 1,2 дБ относительно CNN. На рис. 3 показаны графики зависимости BER от SNR

для корреляционного метода и демодуляторов на основе нейронных сетей при 500 итерациях обучения.

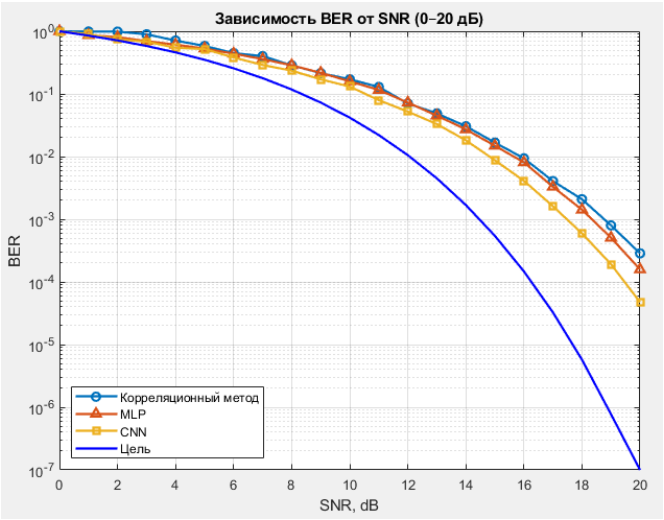


Рис. 3. График зависимости BER от SNR для корреляционного метода и демодуляторов на основе нейронных сетей при 500 итерациях обучения

При 500 циклах обучения демодуляторы на основе MLP и CNN показывают лучшую производительность относительно корреляционного метода при BER = 10^{-3} на 0,5 дБ и 1,3 дБ соответственно. На рис. 4 представлены графики зависимости BER от SNR для корреляционного метода и демодуляторов на основе нейронных сетей при 700 итерациях обучения.

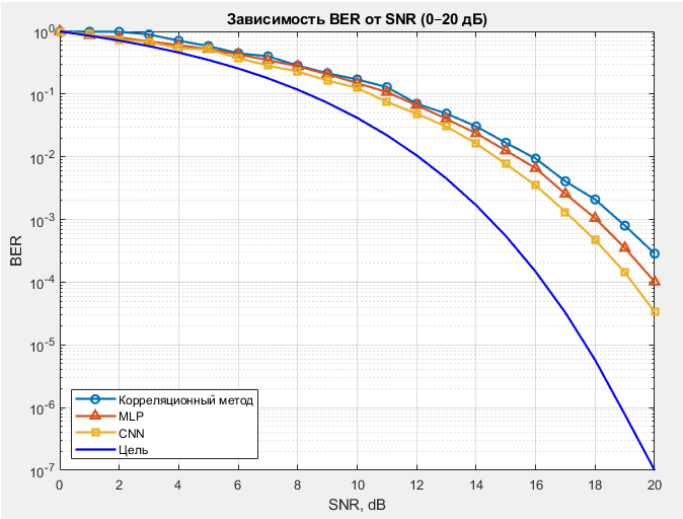


Рис. 4. График зависимости BER от SNR для корреляционного метода и демодуляторов на основе нейронных сетей при 700 итерациях обучения

Из графиков следует, что при 700 итерациях обучения обе системы с применением искусственного интеллекта показывают лучшую производительность, чем метод корреляции, при BER = 10^{-3} демодуляторы на основе CNN эффективнее на 1,7 дБ, а на основе MLP – на 0,8 дБ. Стоит отметить,

что при дальнейшем увеличении количества итераций будет достигнут предел обучаемости, т.е. вероятность ошибки перестанет уменьшаться [5]. В таблице 1 приведены результаты моделирования.

ТАБЛИЦА 1. Результаты моделирования

Количество итераций	SNR, дБ при BER = 10^{-3}		
	Метод корреляции	MLP-демодулятор	CNN-демодулятор
100	18,8	>20	>20
300	18,8	19,8	18,6
500	18,8	18,3	17,5
700	18,8	18,0	17,1

Таким образом, в результате моделирования было установлено, что увеличение глубины обучения повышает эффективность демодуляторов на основе нейронных сетей MLP и CNN. При 100 циклах обучения нейросетевые демодуляторы уступают корреляционному методу, однако при 300 итерациях CNN-демодулятор достигает сопоставимого качества. При 500 и 700 циклах обучения демодуляторы MLP и CNN показывают меньшую вероятность ошибки, чем метод корреляции. Наибольший выигрыш в 1,7 дБ при BER = 10^{-3} демонстрирует сверточная нейронная сеть при 700 итерациях. Рассмотренные методы машинного обучения и полученные данные способны усовершенствовать системы в коротковолновом канале радиосвязи, повысив надежность и качество связи.

Список используемых источников

1. Чихачев А. В., Будко П. А., Шмидт А. А. Применение алгоритмов машинного обучения для решения задач прогнозирования технического состояния средств радиосвязи // Телекоммуникации и связь. 2024. № 3 (3). С. 33–40.

2. Maranhão J. P. A., da Costa J. P. C. L., de Freitaset E. P., Javidial E. Noise-Robust Multilayer Perceptron Architecture for Distributed Denial of Ser-vice Attack Detection // IEEE Communications Letters. 2020. Vol. 25. Iss. 2. PP. 402–406.

3. Евстратько В. В., Коноваленко А. И., Мишуров А. В., Юхманов А. Д. Цифровой радиоприемник на основе нейронной сети. // Журнал радиоэлектроники. 2024. № 1

4. Егоров В. В., Мингалев А. Н., Щеглова Е. Ф. Многопараметрическая адаптация в коротковолновых системах передачи данных сигналами OFDM // Техника средств связи. 2021. № 3 (155). С. 18-28.

5. Чепцов М. Н., Сонина С. Д. Анализ методов оптимизация скорости обучения нейронной сети // Сборник научных трудов ДОНИЖТ. 2022. № 65. С. 27-31.

Статья представлена научным руководителем, доцентом кафедры РТ СПбГУТ, кандидатом технических наук О. А. Симониной.

УДК 614.8; 629.7

ИСПОЛЬЗОВАНИЕ БПЛА ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

В. А. Копычко (студент гр.РТ-41, СПБГУТ), kopychko.va@sut.ru
М. А. Межевова (ассистент кафедры РТ факультета РСР СПбГУТ), mezhevova.ma@sut.ru

В современном мире беспилотные летательные аппараты (БПЛА) имеют множество возможностей эксплуатации в различных сферах. В связи с растущими запросами общества расширяются возможности использования БПЛА как при мониторинге опасных объектов, так и при ликвидации последствий ЧС. Актуальность работы обусловлена стремительным развитием технологий в этой области. Так, за последний десяток лет БПЛА превратились из «инженерных игрушек» в полноценные автономные летательные аппараты, способные улетать от оператора на многие километры. Данные особенности открывают уникальную возможность применения при ликвидации ЧС: возможность существенно сократить угрозу для жизни при ликвидации последствий ЧС и возможность их предотвращения путем дистанционного мониторинга опасных районов без непосредственного участия человека в районах потенциальной опасности.

беспилотный летательный аппарат (БПЛА), чрезвычайная ситуация (ЧС), мониторинг, ретрансляция, пожаротушение

В век колоссального развития технологий человек медленно и старательно улучшает свои разработки и внедряет их в сферы жизни, например, как можно использовать достижения в технологической сфере актуальнее и безопаснее. Как отмечают авторы работы [1], «за несколько лет БПЛА из инженерных игрушек перешли в разряд полезных технических средств». Беспилотные летательные аппараты не стали исключением, они стремительно развиваются и внедряются в нашу жизнь.

Целью данной работы является проведение анализа научной литературы для обоснования перспектив применения БПЛА в условиях ЧС и выявления приоритетных направлений разработки радиотехнического оборудования на них.

Функциональные направления применения БПЛА при ЧС:

1. Поиск и спасение.

С помощью БПЛА осуществляется поиск людей в зонах стихийных бедствий, доставка медикаментов и гуманитарной помощи, а также сброс спасательного обмундирования.

Известен пример спасения человека с крыши затопленного дома в Китае с помощью беспилотника. Во время наводнения оператор эвакуировал пострадавшего с помощью каната, закрепленного за коптер. Спасательная операция была случайной: Лай Чжунсинь помогал жителям затопленной деревни в регионе Гуанси, а беспилотник применялся для распыления удобрений и перевозки стройматериалов [1].

2. Обеспечение связи.

БПЛА используются для развертывания временных сетей связи в условиях отсутствия или неполного радиопокрытия необходимой территории. Такие сети применяются для обеспечения связью зон ликвидации последствий ЧС.

Существуют три сценария использования:

1) ретрансляция между наземными объектами;

2) цепь ретрансляции между воздушными объектами;

3) использование БПЛА в качестве оконечная нагрузки.

Прогресс в области спутниковых систем связи предоставляет возможность передачи целевой информации с БПЛА по спутниковым каналам в любую точку земного шара.

3. Мониторинг и разведка.

БПЛА позволяют получать руководителям тушения пожара информацию и о виде и размерах пожара, и о рельефе местности, и о скорости, и о направлении распространения огня, ожидаемом развитии пожара за период его тушения, и об участках, где возможно наиболее интенсивное развитие пожара. Использование тепловизоров и камер наблюдения помогает находить людей в условиях ограниченной видимости и сильной задымленности [2]. Теплолокаторы микроволнового диапазона способны обнаруживать скрытые очаги горения при подземных пожарах на торфяниках [3].

4. Пожаротушение.

Тяжелые БПЛА способны осуществлять подбор воды из водоемов и сброс ее на очаг возгорания. Беспилотные аппараты вертолетного типа могут иметь взлетную массу до 1360 кг и грузоподъемность до 770 кг. Российский беспилотный аппарат «Ворон-700» оснащен противопожарными «бомбами» и оборудованием для порошкового тушения [4].

Технические характеристики БПЛА

Классификация БПЛА по типу включает самолетные аппараты (скорость до 400 км/ч, время полета от 30 мин до 8 ч), вертолетные аппараты

(время полета до 3 ч, вертикальный взлет) [5] и аэростаты (наблюдение на высоте до 400 м) [6].

Среди отечественных разработок выделяются:

- **БАС-200** (КумАПП, Башкортостан): взлетная масса 200 кг, полезный груз до 50 кг, скорость до 160 км/ч, время полета до 4 ч, дальность управления до 100 км (до 400 км с ретрансляцией) [1];
- **«Гектор» S-80** (компания «Транспорт будущего»): грузоподъемность до 40 кг, время полета до 20 мин, распыление на площади до 18 га за час [1];
- **«Ворон-700»**: оснащен противопожарными «бомбами» и оборудованием для порошкового тушения [4];
- **Hi-Fly Taxi** (Инновационный центр «Бирюч»): грузоподъемность 170 кг, дальность 20 км, скорость 100 км/ч [1].

Приоритетные направления разработки радиотехнического оборудования

Анализ технических ограничений показал, что большинство антенных систем БПЛА являются ненаправленными и обладают малыми коэффициентами усиления, что «приводит к увеличению количества промежуточных БПЛА в цепи ретрансляции, а соответственно и к усложнению сети» [6].

В качестве приоритетных направлений выделены:

1. Антенные системы с управляемой диаграммой направленности.

Предлагаются два варианта: кольцевая антенная решетка (КУ 7 дБ, ширина полосы 1200 МГц), а также переключаемая секторная антенная система (КУ 7.1 дБ, ширина ДН 50°), которая не требует сложного диаграммообразующего устройства [6].

2. Системы ретрансляции.

Использование цепочек БПЛА-ретрансляторов и стационарных ретрансляторов (на мачтах сотовой связи) позволяет увеличить дальность связи до 400 км.

3. Спутниковые каналы связи.

Спутниковая система «Иридиум» приходит на замену устаревшей «Инмарсат-С» для обеспечения безопасности в море. В отличие от предшественника, у которого задержка сообщений до двух часов, «Иридиум» обеспечивает 100 % покрытия планеты, в том числе полюса, и позволяет передавать данные в реальном времени через спутники «Iridium Next» [7].

4. Лидарные комплексы.

Оснащение БПЛА лидарами позволяет решать задачи определения источника аварийного загрязнения, измерения концентрации загрязняющих веществ и порогового обнаружения загрязнения в зоне до 50 км.

В результате анализа научной литературы были систематизированы основные функциональные направления применения БПЛА при чрезвычайных ситуациях: это поиск и спасение людей, обеспечение временной связи, мониторинг и разведка, а также пожаротушение. Изучение технических характеристик существующих отечественных образцов (БАС-200, «Ворон-700» и др.) подтвердило их способность решать широкий круг задач – от мониторинга труднодоступных территорий до транспортировки грузов. Определены приоритетные направления разработки радиотехнического оборудования для БПЛА: антенные системы с управляемой диаграммой направленности, цепочки ретрансляции, интеграция спутниковых каналов связи и оснащение лидарными комплексами. Таким образом, развитие и внедрение БПЛА в условиях ЧС является перспективным, оно позволяет перейти от пассивного наблюдения к активному вмешательству в ликвидацию последствий ЧС и спасение людей.

Список используемых источников

1. Дымов С. М., Вищекин М. В., Александров А. М., Коренкова О. А. Беспилотные летательные аппараты как средство спасения людей с высоты при пожаре // Актуальные вопросы пожарной безопасности. 2026. Т. 1 (27). С. 21–30.

2. Авелина М. А. К вопросу о применении беспилотных летательных аппаратов в различных сферах жизнедеятельности общества // Право и управление. 2024. № 4. С. 501–504.

3. Янников И. М., Фомин П. М., Габричидзе Т. Г., Захаров А. В. Применение беспилотных летательных аппаратов при разведке труднодоступных и масштабных зон чрезвычайных ситуаций. Ижевск, 2012. 5 с.

4. Мартемьянов С. И., Маторина О. С., Стрельцов О. В., Нестерова С. В. Применение беспилотных летательных аппаратов для поддержки управления противопожарными действиями в условиях чрезвычайных ситуаций // Международный научно-исследовательский журнал. 2024. № 1 (139). С. 1–8.

5. Вытовтов А. В., Калач А. В., Разиньков С. Ю. Современные беспилотные летательные аппараты // Вестник Белгородского государственного технологического университета им. В. Г. Шухова. 2015. № 4. С. 70–74.

6. Коровин К. О., Межевов П. А. Разработка антенных систем БПЛА для развертывания временных сетей связи // Военная связь будущего. Квантовый скачок как неизбежность: материалы международной научно-практической конф., СПб, 10–11 нояб. 2023 г. СПб.: ФГКВОУ ВО «ВАС» МО РФ, 2023. С. 200–204. EDN: GATAAX.

7. Саранча А. М. Предстоящая замена спутниковой системы «Инмарсат-С» на систему «Иридиум» // Modern Science. 2020. № 3-1. С. 408-411. EDN: QLOARI.

Статья представлена заведующим кафедрой РТ, кандидатом физико-математических наук, доцентом К. О. Коровиным.

УДК 654.739

АНАЛИЗ ВАРИАНТОВ ПОСТРОЕНИЯ АНТЕНН ДЛЯ ИЗЛУЧЕНИЯ СВЕРХКОРОТКИХ СВЕРХШИРОКОПОЛОСНЫХ ИМПУЛЬСОВ

К. О. Коровин (к.ф-м.н., доцент, доцент зав. кафедрой РТ СПбГУТ)
Г. В. Чернов (студент гр. МВТ-2511 СПбГУТ), chernov.gv@sut.ru

Актуальность исследования связана с потребностью в повышении эффективности генерации и передачи коротких импульсов, в частности для оценки помехоустойчивости электронных устройств в условиях сложной электромагнитной обстановки. Проанализированы требования к выбранному импульсному генератору, позволяющие сохранить длительность фронта и амплитуду сигнала. Исследованы три типа излучателей: на основе экспоненциального рупора, антенны Вивальди и диск-конусной антенны. Для ТЕМ-рупора исследована оптимизация геометрических параметров. Результаты анализа демонстрируют значительное повышение эффективности излучения ТЕМ-рупора по сравнению с рассмотренными аналогами.

сверхкороткие сверхширокополосные (СШП) импульсы, ТЕМ-рупор, антенна Вивальди, диск-конусная антенна, эффективность излучения

Автоматизированные и роботизированные производственные линии, а также системы с дистанционным или автономным радиоуправлением, могут сталкиваться с воздействием интенсивных ненамеренных (EMI) и намеренных (IEMI) электромагнитных помех. Поэтому оценка устойчивости к EMI и IEMI важна. Для таких испытаний в качестве источников IEMI рассмотрены генераторы мощных сверхкоротких электромагнитных импульсов длительностью менее 2нс, фронтом импульса около 150-200пс, и амплитудой не менее 10кВ. На вход антенн подается двойной экспоненциальный импульс, который очень близок к выходным сигналам высоковольтных генераторов, рис. 1.

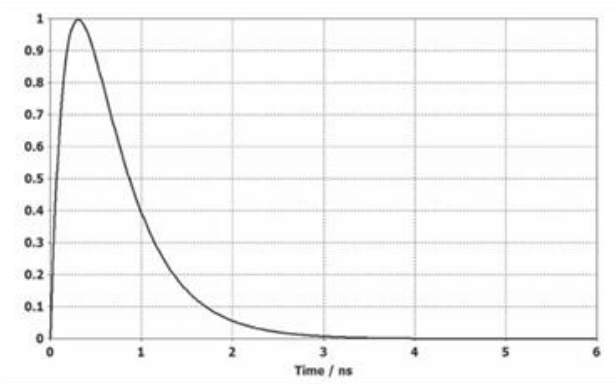


Рис. 1. Двойной экспоненциальный импульс

При разработке необходимо учитывать требования к хорошему согласованию в предельно широкой полосе частот, включая ее низкочастотную область, где поперечные размеры излучателя могут оказаться значительно меньше половины длины волны и требования к габаритам антенны, которая должна эффективно работать как самостоятельно, так и в составе антенной решетки. Классические решения не отвечают этим условиям из-за значительных размеров и особенностей конструкции используемого генератора импульсов.

К перспективным можно отнести различные варианты исполнения антенн типа ТЕМ-рупоров, антенн Вивальди и диск-конусных антенн.

ТЕМ-рупоры не имеют ограничений на минимальные размеры питающего волновода. Самый простой вариант состоит из двух металлических пластин треугольной формы и показан на рис. 2.

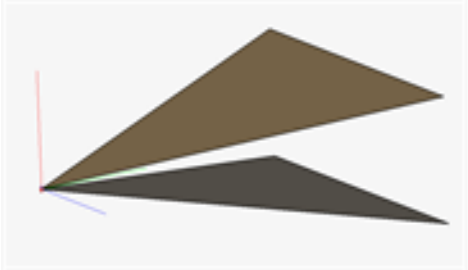


Рис. 2. ТЕМ-рупор с плоским раскрывом

Питание подведено через двухпроводную линию, в основании треугольных пластин. ТЕМ-рупор характеризуется высокой направленностью, однако его коэффициент использования поверхности (КИП), особенно в верхней части рабочего диапазона частот, остается невысоким. Один из недостатков ТЕМ-рупоров, заключается в значительной разнице между углами α и β, что приводит к нерациональному использованию пространства. Тем не менее, подобные рупоры успешно применяются для генерации сверхкоротких импульсов. Так, в [1] была разработана и исследована система, состоящая из сверхширокополосной решетки, включающей четыре S-ТЕМ-рупора, с дополнительными экранирующими прямоугольными пластинами, обеспечивающими путь для обратного тока. Рупоры соединены с двухпроводной линией передачи, а все четыре линии объединены с общим фидером антенны. Этот фидер подключен к полупроводниковому генератору с 50-омным разъемом, формирующему высоковольтные униполярные импульсы амплитудой до 100 кВ, с временем нарастания около 100 пс, длительностью примерно 1000–1500 нс и частотой повторения 1–100 кГц. Для лучшего эффекта была применена решетка 2×2 из S-ТЕМ-рупоров. Оценка

эффективности излучения проводилась как путем расчета поля во временной области, так и с помощью экспериментальных измерений. Частотный спектр импульса на выходе генератора принимался равным 0,1–6 ГГц.

Часть недостатков плоского рупора может быть устранена за счет использования экспоненциального раскрыва, что, например, улучшает согласование со свободным пространством в широкой полосе частот. Пример такого экспоненциального ТЕМ-рупора показан на рис. 3.

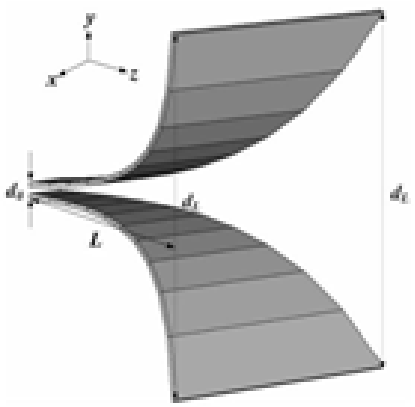


Рис. 3. ТЕМ-рупор с экспоненциальным раскрывом

В ТЕМ-рупоре на рис. 3, волновое сопротивление изменяется по экспоненциальному закону: от 50 Ом – фидера до 377 Ом – волнового сопротивления свободного пространства. Однако, данное упрощение не принимает во внимание излучение электромагнитных волн с боковых поверхностей антенны, а также краевые эффекты.

Основной недостаток ТЕМ-рупоров – их значительные размеры. Поэтому для уменьшения габаритов при сохранении широкой полосы частот применяются комбинированные антенны (КА). Простейший пример КА приведен на рис 4.

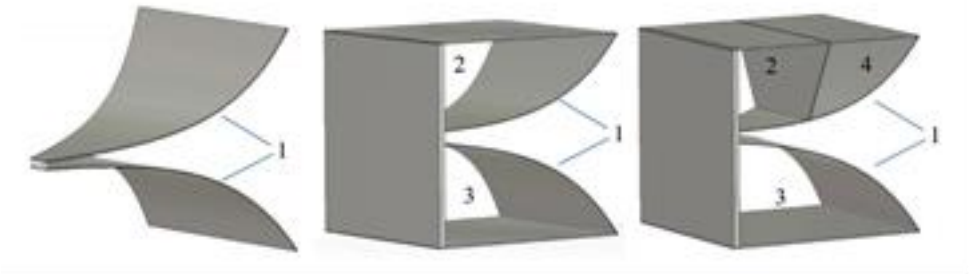


Рис. 4. Экспоненциальный ТЕМ-рупор и варианты с использованием комбинированной системы из электрического монополя 1 и магнитных диполей. 2 – активный магнитный диполь, 3 и 4 – пассивный магнитный диполь

Для настройки КА в ее верхней части предусмотрена пластина, разделяющая магнитный диполь на активную и пассивную области. В активном магнитном диполе ток от источника проходит по верхней пластине и замыкается на заднюю. Пассивные же магнитные диполи возбуждаются за счет полей, создаваемых токами, протекающими по пластинам (электрический монополь). Входной зазор между пластинами ТЕМ-рупора имеет малую величину, что приводит к риску электрического пробоя. Применение комбинированных возбуждающих элементов позволяет повысить коэффициент защитного действия (отношение прямой мощности к обратной) и расширить рабочий диапазон частот рупора [2].

Антенны на основе искрового разрядника очень компактны и просты по конструкции. Будь то коническая антенна или диполь, они хорошо подходят для работы при очень высоких напряжениях, и с их помощью можно достичь высоких излучаемых электрических полей при увеличении входного напряжения [3]. Способность выдерживать напряжение можно увеличить, поместив зазор в среду с высокой диэлектрической прочностью и более высоким давлением, но это усложняет конструкцию. Второй вариант – увеличить зазор между электродами, но чем больше зазор, тем хуже время нарастания. Большой коэффициент качества (показатель качества) достигается за счет использования антенны в больших параболических отражателях, где их эффективность увеличивается в несколько раз. Одна из таких конструкций была предложена Барышевским [4], с отражателем длиной 1,6 м. Хорошо известно, что диск-конусная антенна, со схемой на рисунке 5(а), широко используется для сверхширокополосных свойств. Она применяется в пассивных радарах, радарах проникновения в грунт и т. д., однако ее использование в высоковольтных приложениях является новшеством. У экспериментальной антенны на рисунке 5(б) искровой зазор помещен в трансформаторное масло и предусмотрен механизм для регулировки зазора между электродами. Излучаемый сигнал, согласно [4], составляет около 4 $кВм^{-1}$ на расстоянии 30 м при входном напряжении 300 кВ (не указано явно), поэтому показатель качества будет равен 0,4. Однако исследуемая антенна, рисунок 5(в), показала лучшие результаты с отражателем 60 см и входным напряжением 200 кВ. Здесь диск помещен в контейнер из ацетального сополимера с маслом. Переходный излучаемый сигнал, измеренный на расстоянии 4 м, показан на рисунке 5(г), а коэффициент качества составляет 1,2.



а) б) в) г)

Рис. 5. а) Элементы антенны: 1 – конус; 2 – диск; 3 – зазор; 4 – масло, б) конструкция, в) в сборке с отражателем, г) измеренная переходная характеристика излучения отражателя с диск-конусным питанием по сравнению с излучением только от диск-конуса

В качестве одного из вариантов направленного сверхширокополосного излучателя можно рассматривать антенну Вивальди, которая выполнена на базе расширяющейся щелевой линии. Ее рабочий диапазон частот, в зависимости от конкретных размеров и конструктивных особенностей, обычно составляет от 0,3–0,8 до 10–17 ГГц. Данная конструкция, впервые предложенная в 1978 году, нашла широкое применение в самых разных областях: от ближнепольной микроволновой визуализации в медицине, исследования материалов и конструкций до использования в радарах, космических аппаратах и системах дистанционного зондирования. К числу основных достоинств антенн Вивальди относятся сверхширокополосность, направленность и малые габариты. Подробный обзор различных исполнений и характеристик таких антенн приведен в работе [5]. Из нее видно, что антенны, предварительно удовлетворяющие требованиям по частоте, обеспечивают коэффициент усиления 7–10 дБ в рабочей полосе от 0,4 ГГц до 3,2–3,8 ГГц и выше. Однако существенным недостатком является конструктивное ограничение по входному напряжению, поэтому для мощных сверхкоротких сверхширокополосных импульсов антенна Вивальди не подходит.

Список используемых источников

1. Fedorov V. M., Efanov M. V., Ostashev V. Y., Tarakanov V. P., Ul'yanov A. V. Antenna Array with TEM-Horn for Radiation of High-Power Ultra Short Electromagnetic Pulses // Electronics 2021, 10, 1011.

2. Плиско В. В. Излучение мощных сврехширокополосных импульсов решетками комбинированных антенн: автореф. дис.... канд. техн. наук: 31.05.22 / Плиско Вячеслав Владимирович. СПб., 2022. 20 с.

3. Ratan S. D., Syed A., A comprehensive review of high voltage wideband and ultra-wide band antennas for IEMI applications // Engineering Research Express 2021-03-01, DOI: 10.1088/2631-8695/abd873.

4. Baryshevsky V. G., Borisevich A. E., Gurinovich A. A., Drobyshev G.Y., Molchanov P. V. Senko A.V. A compact high power microwave (HPM) source // IET Europian Pulsed Power Conf. 2009.

5. Cadilhon B., Cassany B., Modin P., Diot J-C., Bertrand V., Pecastaing L. Ultra wide-band antennas for high pulsed power applications // Ultra Wideband Commun. Nov. Trends – Antennas and Propag. 2014. 277–306.

Статья представлена научным руководителем, заведующим кафедры РТ СПбГУТ, кандидатом физико-математических наук, доцентом К. О. Коровиным.

УДК 004.658

АВТОМАТИЗИРОВАННЫЙ УЧЕТ ЗАЩИЩЕННЫХ РАБОТ

В. А. Крючков (студент группы ИСТ-261 СПбГУТ), kruchkov.va@sut.ru

Внедрение цифровых технологий в учебный процесс начального, среднего и высшего образования предполагает совершенствование стандартных методик работы, связанных с преподаванием, учетом и оценкой знаний, навыков и умений обучающихся. Одним из важных этапов при подготовке к оценке знаний, например, при сдаче зачетов и экзаменов является наличие сведений о сдаче и защите лабораторных и практических занятий. Внедрение специальных программно-аппаратных решений позволит обеспечить защиту от утраты, снизит вероятность подмены и введения в заблуждение. В статье представлен обзор существующих решения и предложен подход к автоматизированному учету защищенных лабораторных и практических работ.

автоматизация, мониторинг, цифровизация, база данных, система электронного обучения

Важной частью процесса промежуточной аттестации является выполнение учебного плана, в которое входит посещение лекций, сдача лабораторных и практических работ и другие формы деятельности [1]. Традиционный метод контроля количества сданных лабораторных и практических работ студентов, предполагающий «бумажную запись» в журнале или на листочке является неэффективным, в связи со множеством факторов, среди которых утрата, повреждения, как случайные, так и намеренные, ручное заполнение, ошибки и др. [2]. Наличие программно-аппаратного обеспечения позволяет преподавателю и сотрудникам деканата получать доступ к успеваемости в режиме реального времени, что исключает необходимость прямого обращения для запроса текущих сведений, тем самым оптимизируя рабочее время сотрудников и минимизируя административные барьеры [2, 3].

Для мониторинга успеваемости активно применяются системы управления обучением (Learning Management Systems, LMS). В ряде учебных заведений внедряются специализированные системы, интегрирующие данные о результатах защиты работ в общую ведомость, но требуют достаточно сложной настройки при первичной установке, в результате чего популярным инструментом остаются облачные сервисы и электронные таблицы, хотя они не гарантируют целостность данных и защищенности от ошибок ручного ввода.

Интеграция специализированных инструментов учета в общую цифровую образовательную экосистему обеспечивает синергетический эффект между сбором первичных данных и их глубоким стратегическим анализом. Создание единого цифрового профиля студента в рамках такой системы позволяет не только исключить дублирование информации, но и применять методы предиктивного мониторинга для выявления академических рисков на ранних стадиях выполнения учебного плана [4].

Внедрение подобных комплексных решений трансформирует систему из инструмента пассивной фиксации оценок в активный механизм управления качеством образования, что способствует формированию прозрачной информационной инфраструктуры вуза, позволяя администрации оперативно корректировать образовательные траектории и значительно повышать общую операционную эффективность учебного процесса [5].

В таблице представлен краткий сравнительный анализ существующих систем, реализующих необходимый функционал.

ТАБЛИЦА 1. Сравнительная таблица готовых решений

Критерий	iSpring Learn	Moodle	Unicraft
Целевая аудитория	Корпоративный сектор.	Вузы, школы, академическая среда.	Малый и средний бизнес, HR-автоматизация.
Модель владения	SaaS (облако), подписка за пользователя.	Open Source (бесплатно) или платное облако.	SaaS, модульная система оплаты.
Основное преимущество	Скорость внедрения; мощный встроенный конструктор курсов.	Гибкость. Неограниченные возможности кастомизации и тысячи плагинов.	Простота. Интуитивный интерфейс, заточенный под базу знаний компании.
Основной недостаток	Высокая стоимость при масштабировании; слабая кастомизация.	Сложность настройки; устаревший интерфейс.	Ограниченный функционал для глубоких академических задач.
Инструменты аналитики	Развитые графики, автоматические отчеты.	Базовые ведомости (требуют настройки плагинов для аналитики).	Настраиваемые отчеты и визуализация прогресса сотрудников.

Приведенные инструменты, помимо основной задачи – обеспечения цифровой образовательной среды, позволяют решать и задачу учета защищенных работ, но форма отчета и процесс авторизации в системе представляется достаточно сложными.

В качестве средства решения задачи автоматизированного учета сдачи работ предлагается использование системы, построенный по клиент-серверному принципу, в которой в задачу сервера входит хранение базы данных и генерация динамических страниц интерфейса пользователя. Общий алгоритм работы системы учета представляет собой следующую последовательность действий:

1. Преподаватель с помощью пары «имя пользователя» – «пароль» регистрируется в системе. После успешного входа в систему отображается интерфейс, в котором преподавателю требуется выбрать дисциплину, группу и вид занятия (лабораторная работа или практическое занятие). Тематика занятий может быть заполнена вручную или автоматически подтянута из рабочей программы дисциплины.

2. После выбора сведений, указанных в п. 1, открывается список группы, в котором напротив ФИО каждого студента отображается флажок и выпадающий список с отметками 2…5, позволяющий обеспечить более адекватную систему оценивания, чем классическая оценка по системе «зачет» – «незачет».

3. Преподаватель после приема работы проставляет отметки, после чего выполняется выход из системы.

4. В конце семестра он будет иметь полную картину по группам и дисциплинам.

При необходимости в системе можно настроить разбивку студентов по бригадам.

В качестве средств создания программного кода можно использовать практически любой язык программирования, поддерживающий возможность написания приложений для сетей интранет/Интернет в связке с базой данных. Например, в прототипе разработанного приложения используется язык PHP и СУБД Maria DB.

Концепт пользовательского интерфейса представлен на рис. 1 и 2. Схема БД – на рис. 3.

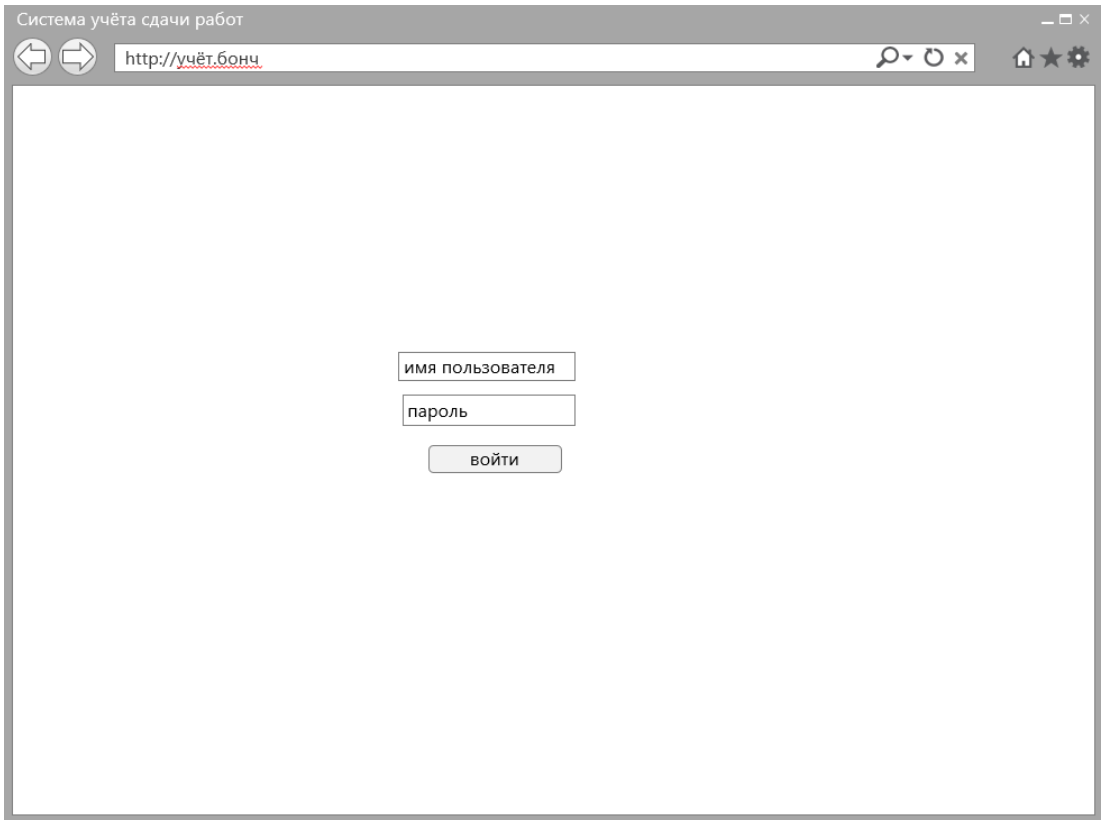


Рис. 1. Регистрационное поле



Журнал защит лабораторных и практических работ группы «Тестовая»

Дисциплина «Программирование встраиваемых систем»

Преподаватель: Иванов Иван Иванович, к.т.н., доцент

ФИО	Лабораторная работа1	Лабораторная работа 2	Практическая работа 1	Практическая работа 2
Алисов Антон	☑ зачтено 5	☐ не зачтено 5	☑ зачтено 5	☐ не зачтено 2...5
Баранов Дмитрий	☑ зачтено 4	☑ зачтено 4	☐ не зачтено 2...5	☐ не зачтено 2...5
Васюков Олег	☐ не зачтено 2...5	☐ не зачтено 2...5	☐ не зачтено 2...5	☐ не зачтено 2...5
Гиров Кирилл	☑ зачтено 5	☑ зачтено 5	☐ не зачтено 2...5	☐ не зачтено 2...5
Демидов Стас	☑ зачтено 4	☐ не зачтено 4	☐ не зачтено 2...5	☐ не зачтено 2...5
Жирафов Евгений	☑ зачтено 2...5	☐ не зачтено 2...5	☐ не зачтено 2...5	☐ не зачтено 2...5
Зайкова Ольга	☑ зачтено 4	☐ не зачтено 2...5	☐ не зачтено 2...5	☐ не зачтено 2...5
Кириллова Ксения	☐ не зачтено 2...5	☑ зачтено 4	☑ зачтено 2...5	☐ не зачтено 2...5

Рис. 2. Журнал сдачи работ

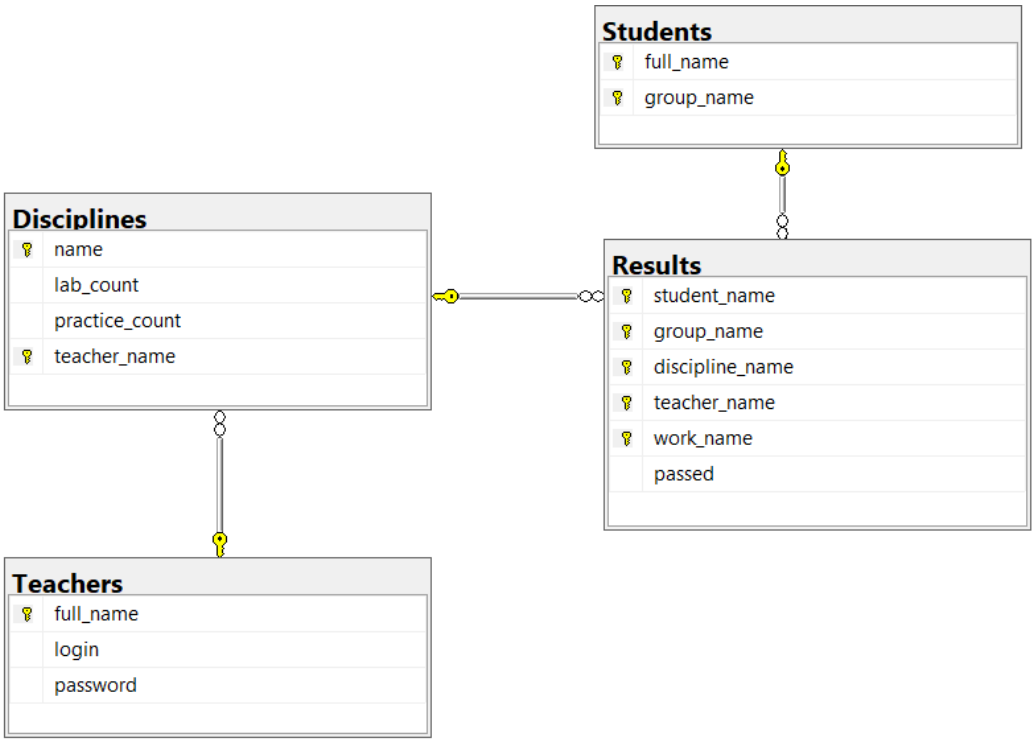


Рис. 3. Диаграмма базы данных

На рис. 3 предоставлена диаграмма БД, показывающая связь между ними. Основной сущностью, управляющей учебным процессом, является сущность Teachers (Преподаватели). Он хранит данные о преподавателях: полное имя, логин и пароль. Связь этой сущности с учебными курсами позволяет определить, какой преподаватель отвечает за конкретную дисциплину.

С сущность Teachers связана с сущность Disciplines (Дисциплины) один ко многим. Он описывает учебные предметы и содержит их уникальное название, а также количество лабораторных и практических работ. Данная сущность используется для формирования учебных заданий и последующего учета их выполнения.

Обучающиеся представлены сущностью Students (Студенты). Он содержит полное имя студента и код его академической группы. Эти данные позволяют системе однозначно идентифицировать каждого обучающегося и использовать информацию для отслеживания его успеваемости.

Центральной частью структуры является сущность Results (Результаты). Он объединяет данные из всех остальных таблиц. В данной сущности фиксируется выполнение конкретной работы определенным студентом по выбранной дисциплине и под руководством соответствующего преподавателя. Логический атрибут «passed» показывает, выполнена ли работа.

Список используемых источников

1. Белоус К. В., Давыдова Е. В. О комплексном подходе к оценке качества знаний студентов с использованием информационных технологий / VII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018)». Санкт- Петербург, 2018. С. 494-498.

2. Here’s How Paperwork is Slowing Down Your Institution in 2025 [Электронный ресурс] // Academia ERP. 2025. URL: https://www.academiaerp.com/blog/heres-how-paperwork-is-slowing-down-your-institution-in-2025/ (дата обращения: 25.03.2026).

3. Design and Development of a Student Record System [Электронный ресурс] // Scientific Journal of Engineering, and Technology. 2025. Vol. 2. № 1. P. 40–54. DOI: 10.69739/sjet.v2i1.424. URL: https://journals.stecab.com/sjet/article/view/424 (дата обращения: 02.04.2026).

4. Аствацаров Г. О., Кочегарова Л. В. Эффективный урок в мультимедийной образовательной среде (практическое пособие). М.: Национальный книжный центр, ИФ «Сентябрь», 2015. 176 с.

5. Осин А. В. Открытые образовательные модульные мультимедиа системы / А. В. Осин. М.: Агентство «Издательский сервис», 2010. 325 с.: ил.

Статья представлена научным руководителем, доцентом кафедры САР СПБГУТ, кандидатом технических наук, доцентом К. В. Белоусом

УДК 004.89

МЕТОД АВТОМАТИЧЕСКОЙ ГЕНЕРАЦИИ КЛАССОВ DTO И МАППЕРОВ НА ОСНОВЕ LLM

В. А. Крючков (студент группы ИСТ-261 СПбГУТ), kruchkov.va@sut.ru
В. А. Кузичев (студент группы ИСТ-261 СПбГУТ), valentin.kuzichev@yandex.ru

В статье рассматривается метод автоматической генерации классов DTO и маппперов на основе больших языковых моделей (LLM). Анализируются противоречивые данные исследований о влиянии LLM на продуктивность разработчиков. Особое внимание уделено промпт-инжинирингу: назначению роли, формату ответа, положительным инструкциям. Для реализации метода выбрана локально развернутая модель Qwen2.5-coder (Ollama). Описывается разработанное расширение для Visual Studio Code, формирующее HTTP-запросы и создающее файлы DTO и маппперов на C#. Приводятся сравнение скорости ручной и автоматизированной генерации, а также оценка вероятности ошибок.

LLM, генерация кода, DTO, Mapper, промпт-инжиниринг, C#, Ollama, автоматизация разработки

Значимость DTO в разработке заключается в создании различных представлений на основе моделей, что позволяет создавать новые представления с помощью уже готовой области, оптимизируя их под нужны клиента. Такая гибкость является мощным инструментом в решении задач.

Ручное создание DTO и соответствующих маппперов является высокозатратной и рутинной операцией. Изменение даже одной модели многократно увеличивает риск внесения ошибок (пропущенных полей, несоответствия типов данных). Особенно остро проблема проявляется в проектах с десятками и сотнями сущностей, где поддержка DTO в актуальном состоянии отнимает значительную часть времени разработки.

Для ускорения разработки DTO и еще большего ускорения всего процесса можно использовать LLM, которая ускоряет процесс закрытия простых задач, как показывают внутренние исследования Google на 21 %, а исследование Metr показывает, что для опытных разработчиков наоборот замедляет на -19 %. Из-за того, что Senior-разработчики тратят больше времени на написание промтов и уточнение контекста, чем если сами будут писать этот код. В свою очередь исследование Faros Ai демонстрирует такие

показатели, что само закрытие простых задач возрастает на 47 %, но при этом само ревью становится больше на 91 % и багов на 9 % больше в сгенерированном коде [1].

Существуют некоторые рекомендации для написания качественных промптов. Задача заключается в конструировании такого промпта, который направляет модель к более корректному ответу и релевантной последовательности токенов. Промпт-инжиниринг представляет собой систематическую практику разработки и оптимизации промптов, включает в себя:

- эксперименты с семантическими формулировками, добавление или изменение ключевых слов;
- калибровку длины и детализации контекста, что позволяет ограничивать ошибочную генерацию;
- оценку стилистических и структурных особенностей промпта применительно к целевой задаче.

В контексте обработки естественного языка промпт выступает структурированным входным сигналом, на основе которого модель производит требуемое прогностическое или генеративное действие.

Оптимизированные промпты позволяют применять LLM для решения широкого спектра задач обработки текста, включая: суммаризацию текста, извлечение информации, вопросно-ответные системы, классификацию текста, перевод языков или кода, генерацию кода, документирование кода или логические рассуждения.

С назначенной ролью модель сужает область поиска информации до специфической ниши, используя профессиональный лексикон и проверенные методики [2].

Использование инструкций предоставляет явные указания о желаемом формате, стиле или содержании ответа. Акцент направляется на то, что нужно делать или производить. Набор ограничений или границ для ответа содержит то, что нельзя делать или нужно избегать [3].

Фокусирование на положительных инструкциях в промпте может быть более эффективным, чем сильная опора на ограничения [4].

Создан системный промпт в соответствии с основными правилами, для генерации DTO и DTO Mapper. Ниже представлена таблица 1, которая описывает структуру.

ТАБЛИЦА 1. Структура правил системного промпта

Правило	Пример реализации	Эффект и значимость
Назначение роли	«Ты – генератор DTO и MAPPER-ов для C#. Твоя задача: анализировать входной код (Entity классы) и создавать соответствующие DTO и Mapper классы»	Модель использует профессиональный лексикон и проверенные методики
Формат ответа	Весь вывод модели должен быть JSON без пояснений до/после. {«dto»: [{«file»:»UserDto.cs»,»code»:»...»}], «dtomapper»: [{«file»:»UserMapper.cs»,»code»:»...»}]}	Гарантирует машинную читаемость, упрощает парсинг и автоматическую обработку результата. Четко разделяет DTO и мапперы, позволяет возвращать несколько файлов для разных сущностей
Использование инструкций	Именование {Entity}Dto авто-свойства{ get; set; } Mapper класс: статические методы ToDto / ToEntity с примерами. Отношения One-to-One, One-to-Many / Many-to-One Использование List<…Dto>	Предоставляет явные указания конкретной структуры кода. Единообразие, стандартизация
Положительное направление	«Используй паттерн статического класса для Mapper», «Используй C# 10+». Добавлять XML комментарии для публичных методов и свойств	Повышает качество генерируемого кода, его соответствие стандартам
Специфические указания	Ограничение глубины вложенности (3 уровня). Циклические ссылки. Обработка ошибок: некорректный вход. Неподдерживаемые типы	Инструкция снижает риск ошибок

Использована LLM Qwen2.5-coder, распространяемая в open-source и предназначенная для написания, анализа и оптимизации программного кода, развернутая с помощью инструмента Ollama [5]. Из рис. 1 видно, что модель с количеством 32 млрд параметров по исследованиям не уступает флагманам.

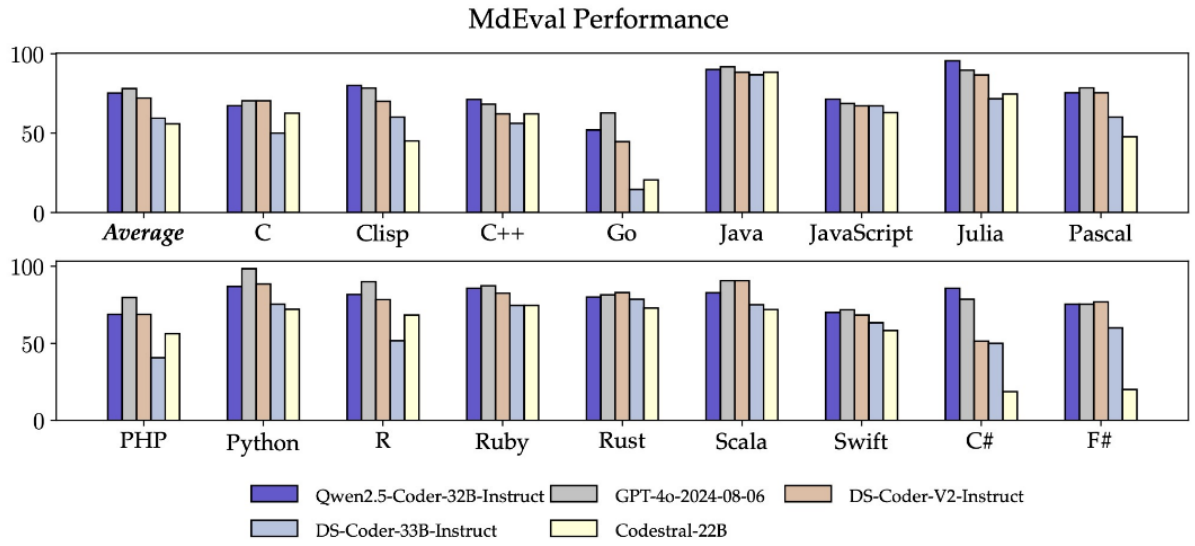


Рис. 1. Показатели исследования LLM на разных языках

Для обеспечения взаимодействия с языковой моделью разработан программный модуль-расширение (плагин) для интегрированной среды разработки Visual Studio Code. В локальной вычислительной среде развернута языковая модель Qwen2.5-coder:7b. Расширение формирует HTTP-запрос к сервису Ollama, в теле которого передается промпт, содержащий код выбранных пользователем файлов, реализующих классы-сущности. На основе системного промпта и предоставленных сущностей модель генерирует код классов Data Transfer Object (DTO) и соответствующих мапперов (DTOMapper). Результат возвращается в структурированном формате JSON, после чего осуществляется его парсинг и создание файлов с сгенерированным кодом в целевой файловой системе.

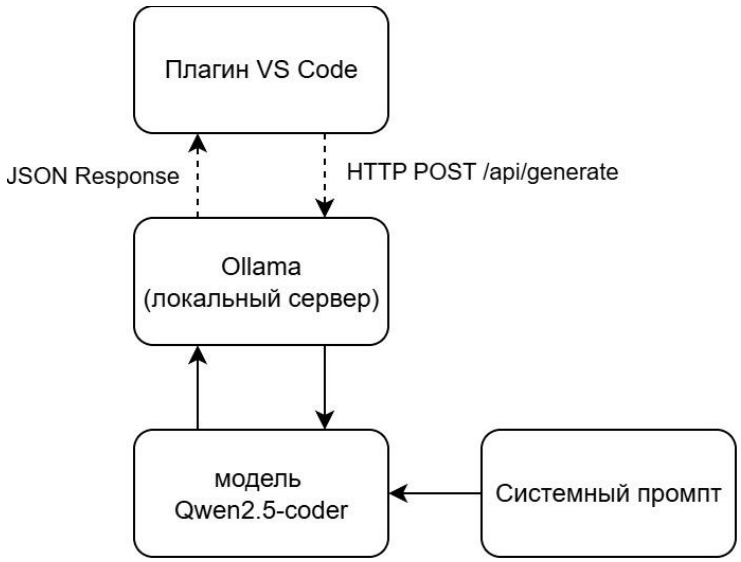


Рис. 2. Структура программы

Код расширения работает в специальном окружении Extension Host, который является изолированным Node.js процессом. Разработанный плагин базируется на официальной технологии VS Code Extension API, открывающей доступ к ключевым функциям редактора кода. Также имеется функционал публикации расширения в открытый доступ для всеобщего пользования.

Пользователь активирует команду, выбирает исходные данные, директории назначения и отправляет запрос. По завершении генерации в указанных пользователем директориях создаются файлы:

- для каждой сущности «EntityName» формируется «EntityNameDto.cs» с классом DTO;
- формируется «EntityNameMapper.cs» со статическим классом маппера, содержащим методы преобразования между сущность и DTO.

Процесс генерации, несмотря на требуемые временные затраты, обеспечивает существенное сокращение времени разработки классов DTO и соответствующих мапперов. Данный подход позволяет автоматизировать рутинные операции по созданию типовых структур, минимизируя вероятность ошибок, связанных с человеческим фактором. В результате достигается повышение производительности труда разработчика за счет делегирования генерации шаблонного кода вычислительной системе.

Список используемых источников

1. Как ИИ действительно влияет на продуктивность разработчика: неожиданные выводы из исследований [Электронный ресурс]. URL: https://ibs-training.ru/about/news/Kak_II_deystvitelno_vliyaet_na_produktivnost_razrabotchika_neozhidannye_vyvody_iz_issledovaniy/ (дата обращения: 20.03.2026).

2. Руководство Google по промпт-инжинирингу. Часть 1: основы и базовые техники [Электронный ресурс]. URL: https://habr.com/ru/articles/901426/ (дата обращения: 20.03.2026).

3. Руководство Google по промпт-инжинирингу. Часть 2: продвинутый промптинг и работа с кодом [Электронный ресурс]. URL: https://habr.com/ru/articles/901920/.

4. Пособие по промт-инжинирингу для программистов [Электронный ресурс]. URL: https://habr.com/ru/companies/sravni/articles/928604/ (дата посещения 20.03.2026).

5. The latest series of Code-Specific Qwen models [Электронный ресурс]. URL: https://ollama.com/library/qwen2.5-coder (дата посещения 20.03.2026).

6. Qwen2.5 Technical Report [Электронные ресурс]. URL: https://arxiv.org/abs/2412.15115 (дата обращения: 20.03.2026).

Статья представлена научным руководителем, доцентом кафедры САР СПбГУТ, кандидатом технических наук, доцентом С. В. Акимовым.

УДК 621.391

ПОВЫШЕНИЕ ТОЧНОСТИ ПОЗИЦИОНИРОВАНИЯ МАНЕВРИРУЮЩИХ ЦЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕРАКТИВНОГО МНОГОМОДЕЛЬНОГО АЛГОРИТМА

П. А. Куприянов (студент гр. РТ-31 СПбГУТ), kupriianov.pa@sut.ru
Д. Р. Сидоркович (ассистент кафедры РТ СПбГУТ), sidorkovich.dr@sut.ru

В работе рассматривается задача фильтрации координат маневрирующей цели при наличии шумов измерений и возможных выбросов. Предложен интерактивный многомодельный (ИММ) алгоритм, основанный на банке фильтров Калмана с различными моделями движения: прямолинейное (CV) и постоянный разворот (CT). Переключение между моделями осуществляется с помощью цепи Маркова, вероятности переходов которой заданы априорно. Обновление вероятностей моделей выполняется по байесовскому правилу с использованием правдоподобия невязок. Алгоритм реализован в среде MATLAB. Результаты моделирования показывают снижение среднеквадратической ошибки оценки координат с 4 м (при использовании только измерений) до 2.7 м, что соответствует увеличению точности более чем на 35 %. Полученные результаты подтверждают эффективность предложенного подхода.

фильтр Калмана, интерактивный многомодельный фильтр (ИММ), цепь Маркова, байесовское оценивание, траекторная обработка, маневрирующая цель

Постановка задачи

В силу неточности измерений координат цели, а также возможности экстремальных значений необходим алгоритм фильтрации данных, дающий оптимальную оценку истинных координат цели.

Введение

В контексте вторичной обработки локационных данных и рассматриваемого ниже алгоритма, понятию траектория может быть дано немного иное определение: Траектория – случайная комбинация детерминированных функций, соответствующих определенным кинематическим моделям.

Всего существует несколько паттернов движения: поворот, прямолинейное, равноускоренное.

Стоит заметить, что сущность случайности имеет ряд ограничений, связанных с физикой движения, авионикой и особенностями строения фюзеляжа летательного аппарата. Например, прямолинейное движение не может резко перейти в крутое пике, без переходного состояния в виде появления минимального углового ускорения. Данные особенности будут

в последствии учтены при составлении переходной матрицы Цепи Маркова. На уровне идеи рассмотренный алгоритм подставляет собой усовершенствованный банк фильтров Калмана.

1. Анализ задачи

В каждый момент времени ОЛ характеризуется вектором состояния

$$x = [x_0\ v_x\ y_0\ v_y\ \omega].$$

Эволюция системы описывается линейным разносным стохастическим уравнением (РСУ) [1]:

$$\hat{x}_n = Fx_{n-1} + Gw,$$

где F – матрица сноса k-ой модели, G – матрица диффузии k-ой модели, w – случайный вектор ускорений.

Уравнение наблюдения имеет вид:

$$Z_n = H\ y_n + q,$$

где H – матрица наблюдения, y_n- измерение с датчика, q – вектор шума измерения.

Следующим этапом работы является синтез оптимального алгоритма оценки координат ОЛ в n-ый момент времени. Исходя из критерия минимума среднеквадратической ошибки оптимальным фильтром для систем с линейной эволюцией и шумовой составляющей, распределенной по нормальному закону, является линейный фильтр Калмана (ЛФК). Ниже приведены его основные уравнениях [2]:

1. Уравнения предсказания

1.1 Экстраполяция состояния k-ой модели

$$\hat{x}_n = F\ x_{n-1}. \quad (1)$$

1.2 Экстраполяция ковариации ошибок k-ой модели

$$P_n^- = FP_{n-1}F^T + Q, \quad (2)$$

где P_{n-1}^k – ковариация k-ой модели с предыдущего шага, а Q – матрица шума процесса, $Q = G * cov(x, y) * G^T$

2. Уравнения коррекции предсказания

2.1 Вычисления коэффициента Калмана

$$K_{\text{n}} = P_{\text{n}}^{-} H^T (H P_{\text{n}}^{-} H^T + R)^{-1}. \quad (3)$$

2.2 Обновление оценки с учетом

$$\widehat{x_{\text{n}}} = \widehat{x_{\text{n}}^{-}} + K_{\text{n}}(Z_{\text{n}} - H\widehat{x_{\text{n}}^{-}}). \quad (4)$$

2.3 Обновление ковариации

$$P_k = (I - K_k H) P_k^{-}. \quad (5)$$

На данный момент полученный алгоритм является банком фильтров и на достигнутом результате можно остановиться, приняв за окончательную оценку результат работы фильтра с наименьшей ошибкой предсказания. Однако этот метод имеет ряд недостатков [1, 3]. Последующая модификация методики оценивания будет выстроенная вокруг понятий: Цепь Маркова и байесовский подход.

2. Описание работы Интерактивного Многомодельного (ИММ) алгоритма

Цепь Маркова необходима для задания вероятности эволюции одного состояния в другое. Марковский прогресс задается переходной матрицей:

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1j} \\ \vdots & \ddots & \vdots \\ p_{i1} & \cdots & p_{ij} \end{pmatrix},$$

где p_{ij} – вероятность перехода от $i-$ой модели к $j-$ой.

На данном этапе необходимо совместить составные части и получить усовершенствованный подход.

Полное описание работы можно разделить на два этапа [3]:

1. Инициализация начальных состояний фильтров

1.1 Вычисление априорных вероятностей перехода

$$\mu_{n|n-1^{j|i}} = \frac{\pi_{ij}\mu_{n-1}^{i}}{\sum_{i=1}^{N} \pi_{ij}\mu_{n-1}^{i}}.$$

1.2 Вычисление начальных состояний каждого фильтра:

$$\widehat{x_{n-1}^{0j}} = \sum_{i=1}^{N} \widehat{x_{n-1}^{i}}\, \mu_{n|n-1^{j|i}},$$

$$P_n^{0j} = \sum_{i=1}^{N} \mu_{n|n-1^{j|i}} \left[P_{n-1}^{i} + \left(\widehat{x_{n-1}^{i}} - \widehat{x_{n-1}^{0J}} \right) \left(\widehat{x_{n-1}^{i}} - \widehat{x_{n-1}^{0J}} \right)^T \right].$$

1.3 Экстраполяция и корректировка. Выполняется по формулам (1-7)

1.4 Вычисление отношения правдоподобия и обновление априорных данных.

2. Основная петля ИММ

2.2 Вычисление априорных вероятностей перехода

$$\mu_{n|n-1^{j|i}} = \frac{\pi_{ij}\mu_{n-1}^{i}}{\sum_{i=1}^{N} \pi_{ij}\mu_{n-1}^{i}}.$$

2.3 Смешивание

$$\widehat{x_{n-1}^{ij}} = \sum_{i=1}^{N} \widehat{x_{n-1}^{i}}\, \mu_{n|n-1^{j|i}},$$

$$P_n^{ij} = \sum_{i=1}^{N} \mu_{n|n-1^{j|i}} \left[P_{n-1}^{i} + \left(\widehat{x_{n-1}^{i}} - \widehat{x_{n-1}^{ij}} \right) \left(\widehat{x_{n-1}^{i}} - \widehat{x_{n-1}^{ij}} \right)^T \right].$$

2.3 Каждый фильтр осуществляет предсказание и коррекцию по формулам (1-7).

2.4 Вычисление правдоподобия каждой из моделей

$$\Lambda_n^j = \frac{1}{\sqrt{(2\pi)^m \left| \mathrm{S_n^j} \right|}} \exp\left(-\frac{1}{2} \left(\mathrm{v_n^j} \right)^T \left(\mathrm{S_n^j} \right)^{-1} \left(\mathrm{v_n^j} \right) \right),$$

где $\mathrm{v_n^j}$ – невязка j-ой модели, $\mathrm{S_n^j} = HP_{\mathrm{n}}^{-}H^T + R$ – ковариация предсказания.

2.5 Вычисление апостериорной вероятности

$$\mu_n^j = \frac{\Lambda_n^j \sum_{i=1}^{N} \pi_{ij}\mu_{n-1}^{i}}{\sum_{j=1}^{N} \Lambda_n^j \sum_{i=1}^{N} \pi_{ij}\mu_{n-1}^{i}}.$$

2.6 Вычисление итоговой оценки

$$\widehat{x_n} = \sum_{j=1}^{N} \widehat{x_n^j}\, \mu_n^j.$$

Стоит отметить, что полученная оценка не используется для последующих вычислений, а только отображается потребителю.

После выполнения п. 2.6 «блок 2» начинается с начала.

3. Синтез частного случая алгоритма (практическая часть)

В целях упрощения модель CV был заменена на CT с малой угловой скоростью, что дает право использовать одинаковую матрицу сноса и диффузии для всех моделей [4].

$$F = \begin{pmatrix} 1 & \frac{\sin(\omega T)}{\omega} & 0 & \frac{1-\cos(\omega T)}{\omega} & 0 \\ 0 & \cos(\omega T) & 0 & -\sin(\omega T) & 0 \\ 0 & \frac{1-\cos(\omega T)}{\omega} & 1 & \frac{\sin(\omega T)}{\omega} & 0 \\ 0 & \sin(\omega T) & 0 & \cos(\omega T) & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$G = \begin{pmatrix} 0 & 1 \\ \frac{1-\cos(\omega T)}{\omega} & \frac{\sin(\omega T)}{\omega} \\ 1 & 0 \\ \frac{\sin(\omega T)}{\omega} & -\frac{1-\cos(\omega T)}{\omega} \end{pmatrix}.$$

Угловые скорости: [0.2 0.1 0.000001]

При необходимости множество скоростей дополняемо значениями обратного знака. В моделировании использован однополярный набор для повышения информативности эпюров, подтверждающих адекватную работу алгоритма.

В качестве случайных ускорений, отвечающих за турбулентность и рысканье, взяты некоррелированные СВ $w = [w_x\ w_y] \sim N(0, q)$, где $q =$ 2 м/с.

Шум датчика является покоординатно независимым и подчиняется нормальному закону распределения с нулевым математическим ожиданием и среднеквадратическими отклонениями $\sigma_x = \sigma_y = 4$ м.

Вероятности переходов позаимствованы из [5] и равны:

$$\Pi = \begin{pmatrix} 0.99 & 0.0075 & 0.0025 \\ 0.005 & 0.99 & 0.005 \\ 0.00025 & 0.00975 & 0.99 \end{pmatrix}.$$

4. Результаты моделирования

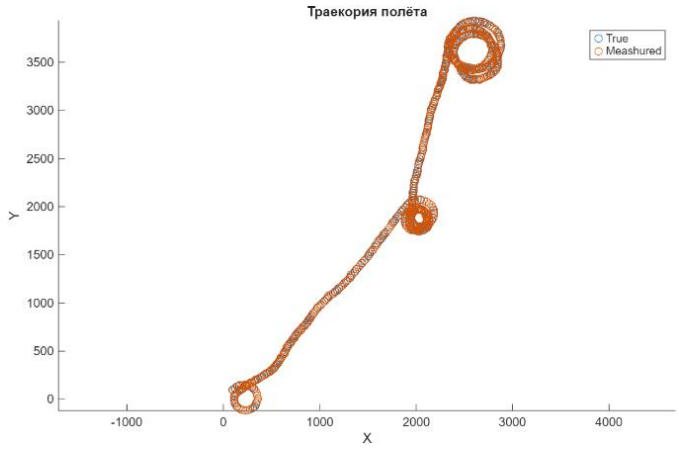


Рис. 1. Полная траектория

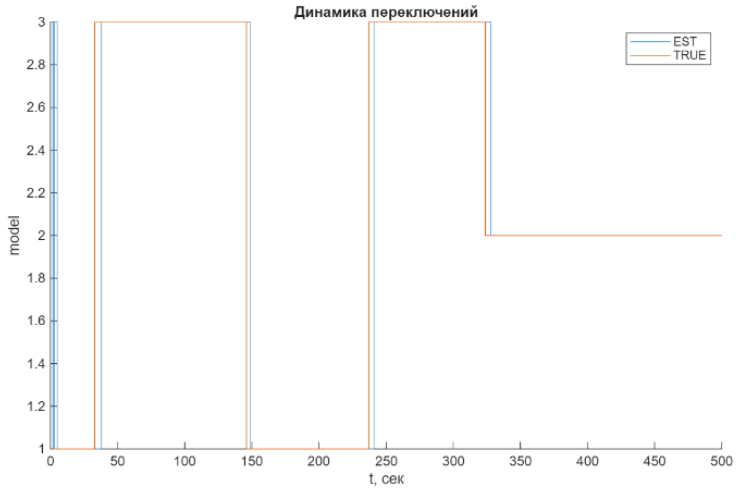


Рис. 2. Динамика переключения состояний ИММ

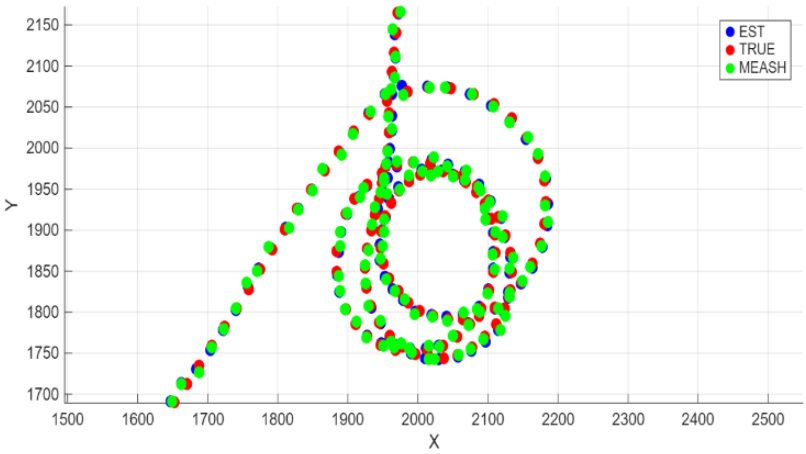


Рис. 3. Участок сопровожденной траектории

На рис. 1 приводится полная траектория ОЛ. Диаграмма динамики переключений моделей представлен на рис. 2. Из-за большого кол-ва точек, график сопровождения представлен только частично (рис. 3).

Выводы

Результаты моделирования показали унижение СКО с 4 м, как если бы задача позиционирования решалась только по измерениям датчика, до 2.7 м. Это соответствует увеличению точности более чем на 35 %. Полученный результат решает поставленную в начале исследования задачу.

Список используемых источников

1. Коновалов А. А. Основы траекторной обработки радиолокационной информации: в 2 ч. СПб.: Изд-во СПбГЭТУ. 2014. Ч. 2. 180 с.

2. Балакришнан А. В. Теория фильтрации Калмана. М.: Мир, 1988

3. Коновалов А. А. Основы траекторной обработки радиолокационной информации: в 2 ч. – СПб.: Изд-во СПбГЭТУ. 2013. Ч. 1. 164 с.

4. Фарина А. Студер Ф. Цифровая обработка радиолокационной информации. Сопровождение целей: Пер. с англ. М.: Радио и связь, 1993. 320 с.: ил.

5. Chui C. K., Chen G. Kalman filtering with real time applications // Applied Optics. 1989. Т. 28. № 10. С. 1841. Ramachandra K. V. Kalman filtering techniques for radar tracking. CRC Press, 2018.

Статья представлена заведующим кафедрой РТ, кандидатом физико-математических наук, доцентом К. О. Коровиным.

УДК 004.896

ИНТЕЛЛЕКТУАЛЬНЫЕ МАТРИЧНЫЕ СХЕМЫ УПРАВЛЕНИЯ ПРОМЫШЛЕННОЙ РОБОТИЗИРОВАННОЙ ЯЧЕЙКОЙ: КЕЙС СБОРКИ «ВТУЛКА-ВАЛ»

Л. М. Макаров (к.т.н., доцент, доцент кафедры САР)
К. А. Чаузов (студент гр.МАП-2512 СПбГУТ), kchauzov.ka@sut.ru

В статье рассматривается задача автоматизации сборочной операции типа «втулка-вал» с использованием промышленного робота. Показано, что классические развязанные ПИД-регуляторы не обеспечивают требуемой точности при малых зазорах из-за перекрестных связей в динамике манипулятора. Предложена интеллектуальная матричная схема управления, в которой матрица коэффициентов адаптируется нейронной сетью в реальном времени. Описана архитектура системы, приведены математическая модель объекта управления, результаты моделирования и фрагменты реализации.

матричные схемы управления, промышленный робот, сборка «втулка-вал», нейросетевой регулятор, адаптивное управление, MIMO-система

Операция сборки цилиндрической пары «втулка-вал» – одна из наиболее распространенных в машиностроении. При ее автоматизации промышленными роботами возникает противоречие: технологические зазоры составляют 20–50 мкм, тогда как погрешность позиционирования деталей на конвейере достигает сотен микрон. Классические системы управления строятся по принципу декомпозиции: для каждого сочленения синтезируется независимый ПИД-регулятор [1]. Однако динамика 6-степенного манипулятора описывается системой сильно связанных нелинейных уравнений [2]. При взаимодействии с внешней средой перекрестные связи становятся значимыми, что приводит к росту ошибки и повышенным усилиям в момент касания. При перекосе втулки относительно вала возникают заклинивающие усилия, способные повредить детали и оборудование.

В последние годы активно развиваются методы матричного управления многомерными системами с законом $\boldsymbol{\tau} = \mathbf{K} \cdot \mathbf{e}$, где $\mathbf{e}$ – вектор ошибки, $\mathbf{K}$ – матрица усилений [3]. Однако постоянная матрица $\mathbf{K}$ не позволяет адаптироваться к изменению геометрии деталей, трения и жесткости контакта. Цель работы – разработка и экспериментальная проверка интеллектуальной матричной схемы управления, в которой матрица $\mathbf{K}(t)$

пересчитывается нейронной сетью в реальном времени на основе текущей ошибки и измеряемых сил.

Рассматривается роботизированная ячейка на базе промышленного манипулятора с шестью степенями свободы (аналог UR10e: радиус 1300 мм, грузоподъемность до 10 кг, повторяемость ±0,1 мм). Подачу вала осуществляет конвейер с погрешностью остановки ±0,5 мм. Втулка закреплена в пневматическом схвате, оснащенном шестикомпонентным датчиком силы (аналог ATI Gamma, измеряет F_x,F_y,F_z,M_x,M_y,M_z). Зазор соединения составляет 20–50 мкм – величина, сопоставимая с точностью робота и значительно меньшая погрешности конвейера. Управление реализуется промышленным контроллером реального времени (Beckhoff TwinCAT 3 с модулем нейросетей или National Instruments с поддержкой Python), обеспечивающим выполнение нейросетевых вычислений за время менее 1 мс [4].

Динамика манипулятора описывается уравнением [2]:

$$M(q)\ddot{q} + C(q,\dot{q})\dot{q} + g(q) = \tau + \tau_{ext}$$

где $\mathbf{q} \in \mathbb{R}^6$ – углы сочленений, $\mathbf{M}(\mathbf{q})$ – матрица масс (6×6), $\mathbf{C}$ – матрица кориолисовых сил, $\mathbf{g}$ – гравитационные моменты, $\boldsymbol{\tau}$ – управляющие моменты, $\boldsymbol{\tau}_{ext}$ – моменты от контакта.

В окрестности рабочей точки выполнена линеаризация:

$$\dot{x}(t) = Ax(t) + Bu(t)$$

$$y(t) = Cx(t)$$

где $\mathbf{x} = [\Delta\mathbf{q}^T, \Delta\dot{\mathbf{q}}^T]^T$ – 12-мерный вектор состояния, $\mathbf{u} = \Delta\boldsymbol{\tau}$ – управление. Ключевая сложность: матрица масс $\mathbf{M}(\mathbf{q})$ имеет существенные недиагональные элементы. Ускорение в одном сочленении зависит от моментов, приложенных к другим сочленениям. Каналы управления перекрестно связаны, что делает неприменимой классическую стратегию независимой настройки регуляторов [3].

Для решения сформулированной задачи предлагается двухуровневая интеллектуальная матричная схема управления. Нижний уровень образует базовый матричный ПИД-регулятор с постоянной матрицей усилений $\mathbf{K}_0$, обеспечивающий устойчивость в номинальном режиме.

Верхний адаптивный уровень реализован в виде нейронной сети прямого распространения, вычисляющей поправочную матрицу $\Delta\mathbf{K}(t)$ на основе текущей ошибки, ее производной и измеренных сил контакта. Итоговый закон управления:

$$\tau(t) = \mathbf{K}_0\mathbf{e}(t) + \mathbf{N}(\mathbf{e}(t), \dot{\mathbf{e}}(t), f_{ext}) \cdot \mathbf{e}(t)$$

где $\mathbf{e}(t) = \mathbf{q}_{des}(t) – \mathbf{q}(t)$ – вектор ошибки, $\mathbf{f}_{ext}$ – вектор сил, $\mathbf{N}(\cdot)$ – выход нейросети, формирующий $\Delta\mathbf{K}(t)$. Сеть выдает полную матрицу 6×6, позволяя корректировать как диагональные, так и недиагональные связи [5].

Архитектура сети: входной слой (15 сигналов: $\mathbf{e}$, $\dot{\mathbf{e}}$, три компоненты силы), два скрытых слоя с 32 и 16 нейронами (ReLU), выходной слой (36 нейронов, линейная активация). Число обучаемых параметров – около 1500, что обеспечивает время прямого прохода менее 1 мс [4]. Обучение производится с составной функцией потерь, включающей квадрат ошибки, квадрат силы контакта и регуляризатор $|\Delta\mathbf{K}|_2^2$.

Особенность схемы – автоматическая перестройка структуры связей в зависимости от этапа операции. На этапе сближения сеть удерживает недиагональные элементы близкими к нулю (диагональный регулятор). В момент касания увеличивает диагональные элементы для компенсации перекоса и активирует отдельные недиагональные связи [5].

Моделирование выполнено в Simulink. Модель включала нелинейную динамику манипулятора класса UR10e, контакт с зазором 20 мкм, начальный перекос 0,5°, погрешность позиционирования вала 0,4 мм. Частота управления – 1 кГц. Сравнивались три регулятора: классический развязанный ПИД, матричный ПИД с постоянной полной матрицей $\mathbf{K}$, и предложенный интеллектуальный матричный регулятор.

Классический ПИД показал максимальную ошибку 0,32 мм, силу соударения 85 Н, время стабилизации 2,4 с, успешность сборки 78 %. Постоянный матричный регулятор улучшил показатели: ошибка 0,21 мм, сила 62 Н, время 1,9 с, успешность 86 %. Предложенный интелгоритмический регулятор обеспечил ошибку 0,12 мм (снижение на 38 %), силу 38 Н (в 1,9 раза), время 1,5 с, успешность 97 %.

Анализ динамики $K_{1,1}$ показал: на этапе сближения снижение со 120 до 95, в момент касания рост до 140, на этапе запрессовки возврат к 110. Аналогичная адаптация наблюдалась для недиагональных элементов [6].

Основное преимущество – адаптация матрицы $\mathbf{K}(t) $ к фазе процесса, недостижимая для постоянной матрицы, и обобщающая способность нейросети, обеспечивающая робастность к вариациям параметров [5].

Ограничения: отсутствие формальных гарантий устойчивости [2] (компенсируется ограничением нормы $|\Delta\mathbf{K}|$ и сигнатурными алгоритмами), вычислительная нагрузка (онлайн-дообучение исключено, выполняется в фоне), риск нештатных значений (аппаратные ограничители). Перспективы: обучение с подкреплением [6], интеграция технического зрения, распространение на мультироботные ячейки с блочно-матричной структурой.

Предложена интеллектуальная матричная схема управления промышленным роботом для сборки «втулка-вал». Показано, что классические развязанные ПИД-регуляторы неэффективны из-за перекрестных связей, обусловленных недиагональными элементами матрицы масс. Разработан двухуровневый регулятор: базовый с постоянной матрицей $\mathbf{K}_0$ и нейросетевой адаптивный модуль, вычисляющий $\Delta\mathbf{K}(t)$ на основе ошибки и силы контакта. Моделирование подтвердило эффективность: ошибка позиционирования снижена на 38 %, сила соударения – в 1,9 раза, успешность сборки повышена с 86 % до 97 %. Основные ограничения: отсутствие формальных гарантий устойчивости и вычислительная нагрузка. Перспективы связаны с обучением с подкреплением и интеграцией технического зрения.

Список используемых источников

1. Åström K.J., Hägglund T. PID Controllers: Theory, Design, and Tuning. 2nd ed. ISA, 1995. 343 p. URL: https://www.ucg.ac.me/skladiste/blog_2146/objava_92847/fajlovi/Astrom.pdf (дата обращения 10.03.2026).

2. Siciliano B., Khatib O. Springer Handbook of Robotics. 2nd ed. Springer, 2016. 2259 p. ISBN 978-3-319-32552-1. URL: https://www.academia.edu/26665877/Handbook_Springer_of_Robotics (дата обращения 10.03.2026).

3. Khalil H. K. Nonlinear Systems. 3rd ed. Prentice Hall, 2002. 750 p. ISBN 0-13-067389-7. URL: https://www.researchgate.net/profile/Muhammad_Ahsan23/post/What_is_the_general_principle_of_designing_the_switching_control_in_sliding_mode_control/attachment/59d62f0dc49f478072e9f5e3/AS%3A272534484783104%401441988692243/ download/ H-K-Khalil-Nonlinear-Systems-3rd-Edition-2002.pdf (дата обращения 10.03.2026).

3. Beckhoff Automation. TwinCAT 3 Neural Network Integration. Technical Documentation. 2023. 45 p. URL: https://download.beckhoff.com/download/document/ automation/twincat3/TF38x0_TC3_ML_NN_Inference_Engine_EN.pdf (дата обращения 10.03.2026).

4. Lewis F.L., Jagannathan S., Yesildirak A. Neural Network Control of Robot Manipulators and Nonlinear Systems. Taylor & Francis, 1999. 486 p. ISBN 0-7484-0597-X. URL: https://dl.acm.org/doi/10.5555/552206 (доступ ограничен, источник указан по данным публикации).

5. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. 2nd ed. MIT Press, 2018. 552 p. ISBN 978-0-262-03924-6. URL: https://web.stanford.edu/class/psych209/ Readings/SuttonBartoIPRLBook2ndEd.pdf (дата обращения 10.03.2026).

УДК 621.396.67

АНАЛИТИЧЕСКАЯ МОДЕЛЬ ДИАГРАММЫ НАПРАВЛЕННОСТИ ПАТЧ-АНТЕННЫ

П. А. Межевов (старший преподаватель СПбГУТ), mezhevov.pa@sut.ru
Е. Г. Яловицын (студент гр. МВТ-2511 СПбГУТ), yalovicyn.eg@sut.ru

Актуальность разработки аналитической модели диаграммы направленности патч -антенны связана с потребностью быстрого расчета и оценки диаграмм направленности антенных систем без применения численного моделирования. В статье рассмотрены основные этапы получения выражения для диаграммы направленности прямоугольной патч-антенны, проведено сравнение с моделью в программе HFSS Ansys electronics desktop. Результат: получена аналитическая модель патч антенны на основе двухщелевого приближения.

патч-антенна, двухщелевое приближение, диаграмма направленности, антенная решетка

При проектировании антенных систем, в частности из патч-антенн, возникает необходимость быстрой оценки диаграммы направленности антенной системы. Подобные модели могут стать хорошим первым приближением для дальнейшего, более подробного рассмотрения в программах численного моделирования. Рассмотрена модель на основе двухщелевого приближения.

На рисунке 1 изображена геометрия исследуемого объекта и указаны обозначения, используемые при вычислениях.

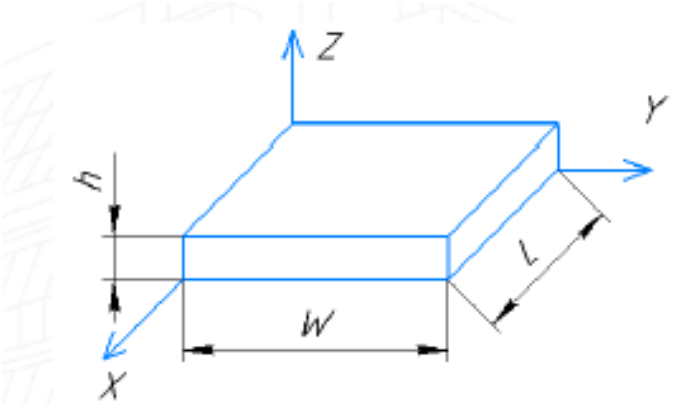


Рис. 1. Геометрия патч-антенны

Рассмотрим решения уравнения Гельмгольца для одиночного патча. Так как в рассматриваемом случае возбуждение поля происходит вдоль оси Z решение будем искать для соответствующей составляющей поля:

$$\nabla E_Z + k^2 E_z = 0 \rightarrow \frac{d^2 E_z}{dx^2} + \frac{d^2 E_z}{dy^2} + k^2 E_z = 0 \text{ при } \lambda << h \rightarrow \frac{d^2 E_z}{dz^2} = 0,$$

Также применим граничные условия для тангенциальных составляющих напряженности магнитного поля.

$$x = 0, x = L$$

$$y = 0, y = W \qquad \frac{dE_z}{dx} = H_y = 0$$

$$\frac{dE_z}{dy} = H_x = 0.$$

Данные условия формируются исходя из соображений, что поверхностные токи на краях патча отсутствуют. Таким образом, получим итоговые выражения для составляющих E_z и H_y для моды TM_{10}:

$$E_z(x) = E_0 \cdot cos\left(\frac{m \cdot \pi}{L} \cdot x\right)$$

$$H_y(x) = j \cdot \frac{E_0 \cdot \pi \cdot sin\left(\frac{\pi \cdot x}{L}\right)}{2 \cdot \pi \cdot f \cdot \mu}.$$

Их графики изображены на рисунке 2:

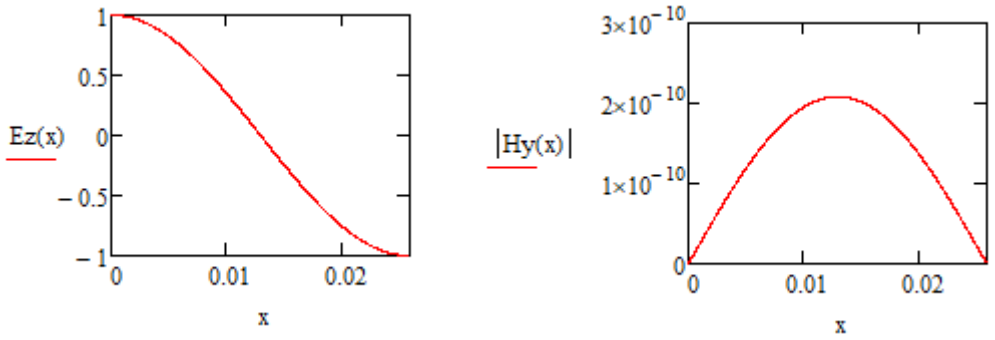


Рис. 2. Графики $E_z(x)$ и $H_y(x)$

Так как составляющая $E_z(x)$ при выходе за границы патча испытывает скачкообразное изменение, согласно теореме эквивалентности, в малом приграничном объеме dVдолжны протекать фиктивные магнитные токи $\vec{J}_м = [\vec{n} \times \vec{E}_z]$. Запишем уравнение векторного потенциала магнитных токов в объеме V [1, с. 75]:

$$\dot{A} = \frac{\tilde{\varepsilon}_a}{4\pi} \int_V \frac{\delta_{ст.м} \cdot e^{-jkR}}{R} dV,$$

учтем, что $\lambda << h$, следовательно $\delta_{ст.м}$ постоянно вдоль оси z. Для упрощения вычислений будем полагать, что фиктивный магнитный ток распределен в малом δ – слое на границе патча. Таким образом в силу нормировки δ – функции и постоянства $\delta_{ст.м}$ можем заменить интеграл по dV на dlа $\delta_{ст.м}$ на $\vec{J} = [\vec{n} \times \vec{E}_z]$. Получим:

$$\dot{A} = \frac{\tilde{\varepsilon}_a}{4\pi} \int_L J_м \cdot \frac{e^{-jk(r-\hat{r}\cdot\dot{r})}}{r-\hat{r}\cdot\dot{r}} dl,$$

где $\hat{r}$– единичный вектор, направленный в сторону точки наблюдения, $\dot{r}$– радиус-вектор фиктивного магнитного тока, r – радиус-вектор точки наблюдения.

Для дальней зоны можем пренебречь слагаемым $\hat{r} \cdot \dot{r}$ в знаменателе, так как он не влияет на фазовые соотношения, а $\hat{r} \cdot \dot{r}$ в фазовом множителе представим как функцию от y (так как фиктивный магнитный ток протекает вдоль оси y): $\hat{r} \cdot \dot{r} = y \cdot sin\,\theta \cdot sin\,\phi$. Таким образом, формула векторного потенциала преобразуется в следующее уравнение:

$$\dot{A} = \frac{\tilde{\varepsilon}_a}{4\pi} \int_L J \cdot \frac{e^{-jk(r-\hat{r}\cdot\dot{r})}}{r-\hat{r}\cdot\dot{r}} dl \rightarrow \frac{\tilde{\varepsilon}_a}{4\pi} e^{-jkr} \int_{-\frac{W}{2}}^{\frac{W}{2}} J_м \cdot e^{-jk\cdot y\cdot sin\,\theta\cdot sin\,\phi} dy$$

$$\rightarrow \frac{\tilde{\varepsilon}_a}{4\pi} e^{-jkr} J_м \cdot sinc\left(\frac{k \cdot W \cdot sin\,\theta \cdot sin\,\phi}{2}\right) \cdot W$$

Из векторного потенциала вычислим значения векторов электрического поля,

$$\dot{E} = -\frac{1}{\tilde{\varepsilon}} rot \dot{A}_м.$$

Перейдем к сферической системе координат, пренебрегая слагаемыми второго порядка малости (для дальней зоны). Получим следующие выражения для $\dot{E}_\theta$ и $\dot{E}_\phi$:

$$\dot{E}_\theta = jk \cdot cos\,\phi \cdot \frac{J_м \cdot e^{-jkr}}{4\pi r} \cdot sinc\left(\frac{k\cdot W}{2} \cdot sin\,\theta \cdot sin\,\phi\right) \cdot W \;\; \dot{E}_\theta = -jk \cdot$$

$$cos\,\theta \cdot sin\,\phi \cdot \frac{J_м \cdot e^{-jkr}}{4\pi r} \cdot sinc\left(\frac{k\cdot W}{2} \cdot sin\,\theta \cdot sin\,\phi\right) \cdot W.$$

Так как абсолютные значения амплитуды поля не представляют особого интереса, в дальнейших расчетах не будем учитывать множители, не

зависящие от углов ϕ и θ. Сложим составляющие вектора напряженности и получим выражение для ДН одного диполя:

$$Fslot(\theta, \phi) = \sqrt{1 - sin(\theta)^2\, sin(\phi)^2} \cdot sinc\left(\frac{k \cdot W}{2} \cdot sin\,\theta \cdot sin\,\phi\right) \cdot W.$$

Далее вычислим разность хода Δ между двумя диполями на расстоянии L до точки наблюдения M (рис. 3).

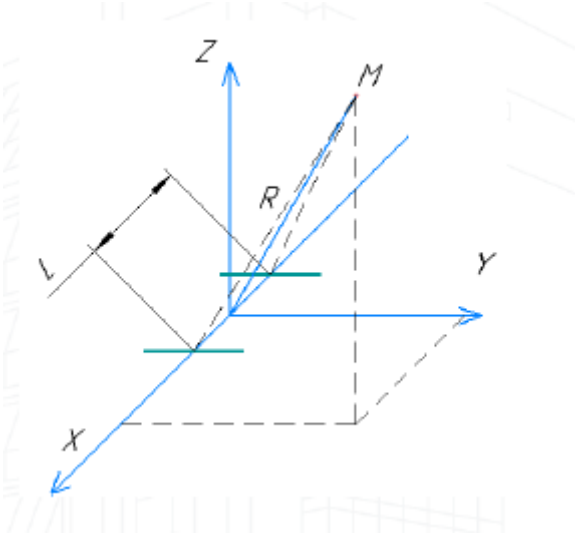


Рис. 3. Схема расположения диполей

$$\Delta = L\, sin\,\theta \cdot cos\,\phi.$$

Подставим в фазовый множитель и найдем множитель решетки [2, с. 287]:

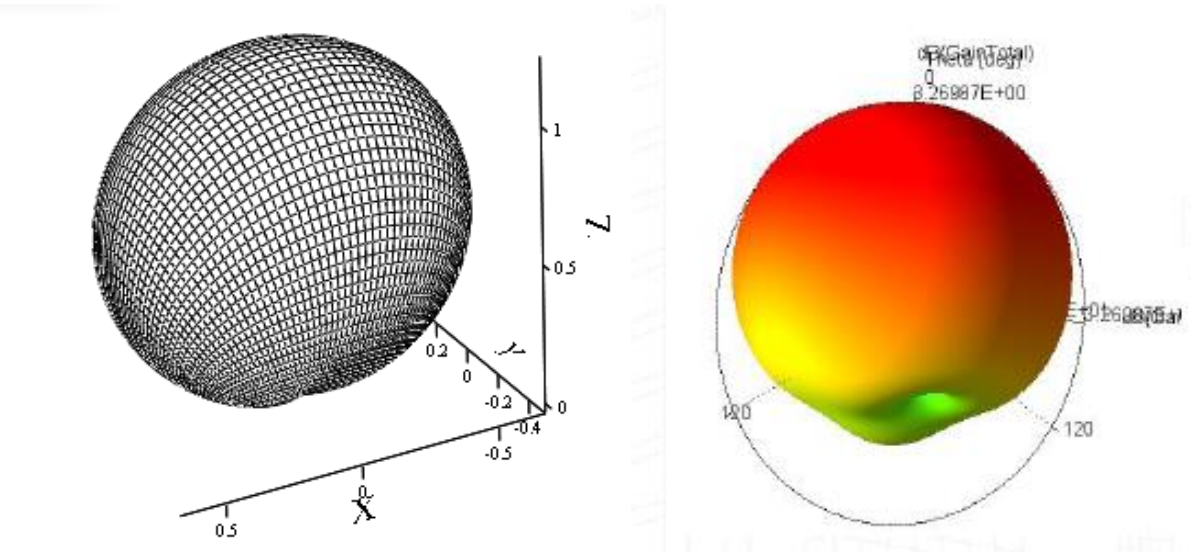
$$Farray(\theta, \phi) = e^{\frac{jk\Delta}{2}} - e^{-\frac{jk\Delta}{2}} = 2\, sin\left(\frac{k \cdot L \cdot sin(\theta) \cdot cos(\phi)}{2}\right).$$

Итоговое выражения для диаграммы направленности патча:

$$Fpatch(\theta, \phi) = Farray(\theta, \phi) \cdot Fslot(\theta, \phi).$$

Объемное представление ДН видно на рис. 4.

Для более детального сравнения полученных результатов, рассмотрим декартовы графики для угломестной плоскости рис. 5).



А – расчетная ДН Б – ДН в Ansys HFSS

Рис. 4. Объемное представление ДН

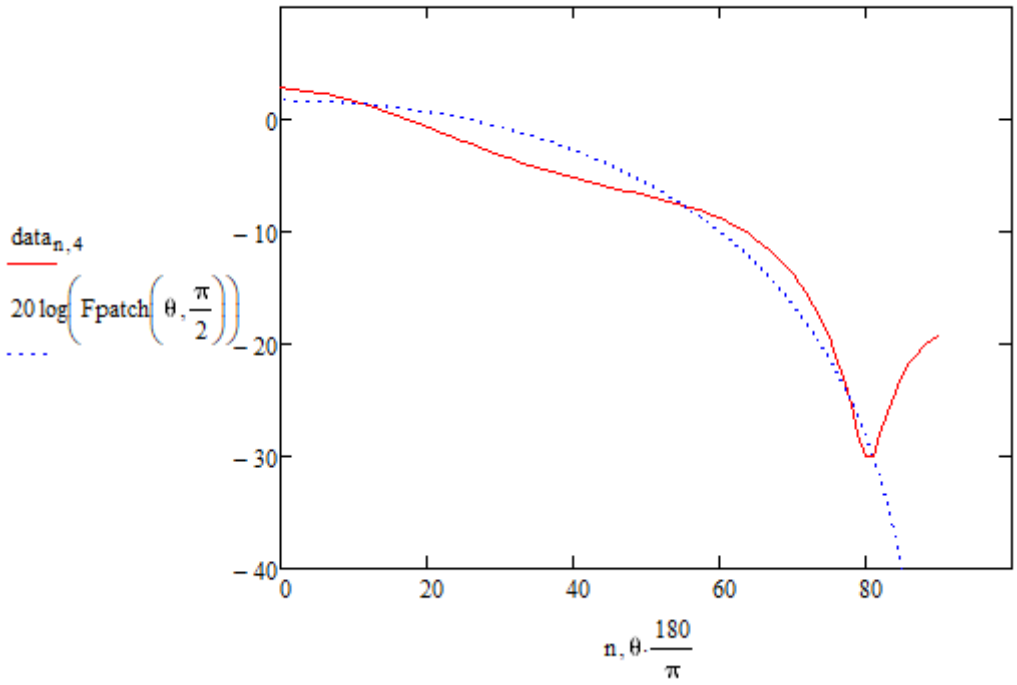


Рис. 5. Сравнение ДН

Двухщелевая модель не учитывает наличие экрана, поэтому у расчетной ДН присутствует 2 равных лепестка. На рисунках 4, 5 изображены верхние полпространства для более удобного сравнения. Как видно из графика 5, модель достаточно хорошо описывает общую картину излучения, что не-

плохо подходит для оценки характеристик антенны. Однако, при экстремальных углах расчетная модель перестает коррелировать с численным моделированием.

Данные расхождения обусловлены эффектами, возникающими на краях экрана. Поверхностные токи, индуцируемые полем под патчем распространяются на поверхности экрана. На краях экрана из-за разрыва тока возникают вторичные источники излучения, которые объясняют наличие заднего лепестка у реальной антенны.

Для дальнейшего развития модели необходимо проанализировать влияние геометрических параметров экрана на диаграмму направленности.

Список используемых источников

1. Фальковский О. И. Техническая электродинамика: учебник. 2-е изд., стер. Санкт-Петербург: Лань, 2022. 432 с. ISBN: 978-5-8114-0980-8.

2. Balanis C. A. Antenna Theory: Analysis and Design. 4th ed. Hoboken, New Jersey: John Wiley & Sons, 2016. 1072 p. ISBN: 978-1-118-64206-1.

УДК 681.7.08

ДАТЧИК ДВИЖЕНИЯ С ПРЕДВАРИТЕЛЬНЫМ СКАНИРОВАНИЕМ

Г. К. Меньшиков (студент группы РК-41м СПбГУТ), menshikov.gk@sut.ru
Д. А. Харьков (студент группы МТП-2511 СПбГУТ), harkov.da@sut.ru

В статье рассматривается разработка датчика движения с предварительным сканированием зоны наблюдения. Актуальность темы обусловлена использованием датчиков движения в системах автоматического освещения, охраны и бытовой автоматизации, где требуется стабильное обнаружение присутствия человека. Отмечается ключевой недостаток пассивных инфракрасных датчиков, связанный с преждевременным отключением нагрузки при временном отсутствии движения. Предлагается алгоритм работы, в котором после основного интервала удержания выполняется дополнительная проверка наличия сигнала с инфракрасного сенсора. Описаны функциональные блоки устройства, включающие PIR-сенсор, микроконтроллерный блок управления, блок питания и модуль реле для коммутации устройства.

датчик движения. Предварительное сканирование. PIR-сенсор. Инфракрасный сенсор. Arduino Nano. AM312

Датчики движения являются одним из основных элементов современных систем автоматизации и безопасности. Они используются для автоматического управления освещением, активации сигнализации, запуска вентиляции и других исполнительных устройств. В общем виде датчик представляет собой техническое средство, преобразующее изменение физического параметра внешней среды в электрический сигнал, пригодный для последующей обработки [1]. Для обнаружения присутствия движения человека наиболее широко применяются пассивные инфракрасные датчики, поскольку, они имеют малое энергопотребление и относительно простую реализацию.

Пассивный инфракрасный датчик движения работает за счет регистрации изменения ИК-излучения в зоне наблюдения. Человек или другой теплый объект отличается по температуре от окружающего фона, поэтому при перемещении через чувствительные зоны датчика изменяется поток инфракрасного излучения, попадающий на пироэлектрический чувствительный элемент. В работах, посвященных PIR-детекторам для автоматического управления освещением, отмечается, что такая технология хорошо подходит для энергоэффективного управления нагрузкой в зданиях [2]. При этом

качество работы датчика определяется не только чувствительным элементом, но и оптической системой, схемой обработки и алгоритмом принятия решения.

Несмотря на распространенность PIR-датчиков, в большинстве случаев, логика их работы имеет существенное ограничение. После обнаружения движения нагрузка включается на заранее заданный интервал времени, а затем отключается, если новое изменение сигнала не обнаружено. Такая схема проста, но она не учитывает ситуацию, когда человек остается в помещении, однако некоторое время не совершает выраженных движений. В результате возможны ложные отключения света или другого управляемого устройства. Исследования пироэлектрических инфракрасных сенсоров также показывают, что обработка динамики сигнала и логика интерпретации событий являются важными факторами при определении движения и положения объекта [3].

Для снижения вероятности ложного отключения в разрабатываемом устройстве используется алгоритм предварительного сканирования. Его основная идея состоит в том, что перед отключением нагрузки датчик выполняет дополнительную проверку зоны обнаружения. Если в этот момент фиксируется повторный сигнал от инфракрасного сенсора, устройство не отключает коммутационное устройство, а возвращается к основному интервалу работы. Алгоритм работы представлен на рис. 1.

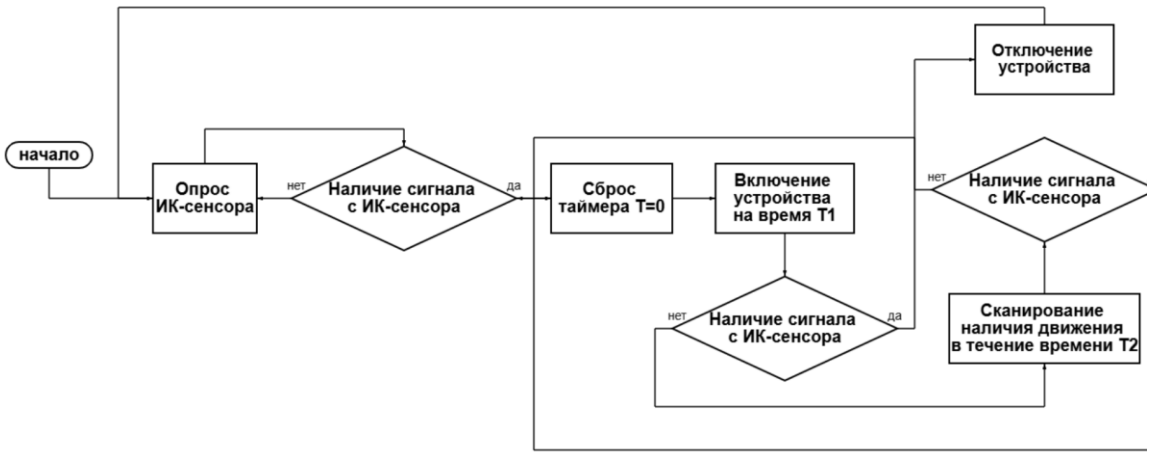


Рис. 1. Алгоритм работы датчика движения с предварительным сканированием

После подачи питания микроконтроллер переходит к циклическому опросу инфракрасного сенсора. Если сигнал отсутствует, устройство продолжает находиться в режиме ожидания. При появлении логического сиг-

нала с сенсора микроконтроллер включает реле и запускает основной временной интервал T1. Данный интервал определяет время удержания нагрузки после обнаружения движения.

В течение интервала T1 устройство продолжает контролировать состояние сенсора. Если за это время движение фиксируется повторно, таймер сбрасывается, и нагрузка остается включенной. Такой режим соответствует обычной работе датчика движения при нахождении человека в зоне наблюдения. Если же в течение времени T1 новый сигнал не появляется, устройство не отключается сразу, а переходит ко второму этапу – предварительному сканированию.

Этап предварительного сканирования соответствует временному интервалу T2. В течение этого интервала микроконтроллер продолжает опрашивать сенсор и проверять, не появился ли повторный сигнал. Если сигнал появляется, устройство возвращается к основному режиму и снова запускает интервал T1. Если за время T2 сигнал не фиксируется, делается вывод об отсутствии движения, после чего реле отключает нагрузку. Такая логика позволяет отделить действительное отсутствие человека от кратковременного отсутствия движения.

Структура устройства построена по модульному принципу. В его состав входят блок сенсора, блок управления и обработки, блок питания и исполнительное реле. Блок сенсора отвечает за обнаружение изменения инфракрасного излучения. Блок управления выполняет обработку сигнала, настройку временных параметров T1 и T2 и управление коммутационным устройством. Структурная схема устройства приведена на рис. 2.

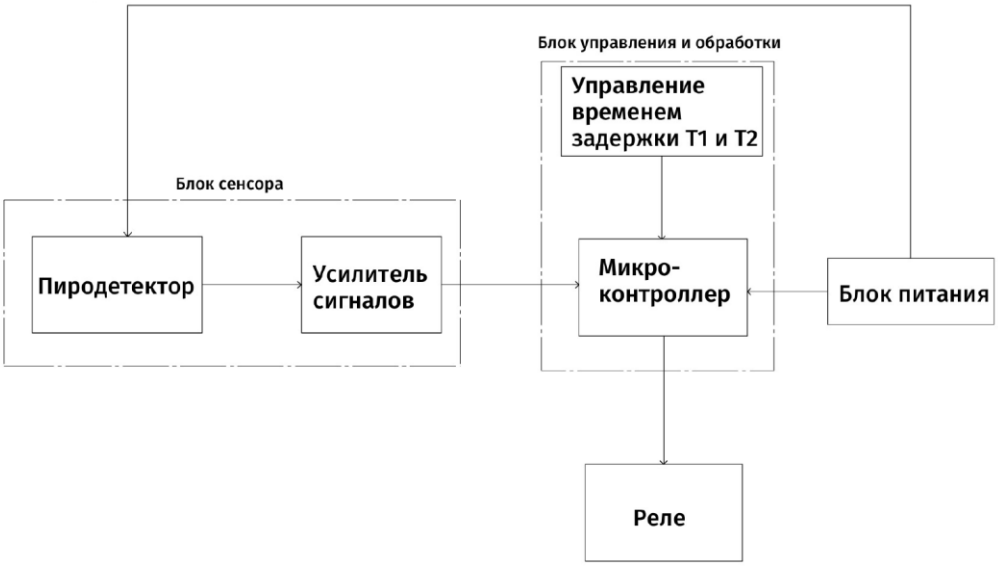


Рис. 2. Структурная схема датчика движения с предварительным сканированием

В качестве блока управления выбран микроконтроллерный модуль Arduino Nano. Его применение обусловлено малыми габаритами, наличием цифровых и аналоговых входов, возможностью программирования через среду Arduino IDE и достаточной производительностью для реализации алгоритма опроса сенсора и управления реле. Согласно техническому описанию, плата Arduino Nano построена на базе микроконтроллера ATmega328P и предназначена для компактных встраиваемых устройств [4]. В разрабатываемом датчике цифровой вход используется для приема сигнала от PIR-модуля, а аналоговые входы могут применяться для считывания положений подстроечных резисторов, задающих временные интервалы T1 и T2.

Чувствительным элементом устройства является модуль AM312. Это компактный пассивный инфракрасный датчик движения с цифровым выходом, что упрощает его подключение к микроконтроллеру. В техническом описании AM312 указывается диапазон питающего напряжения, малое энергопотребление, конус обнаружения до 100 градусов и дальность обнаружения порядка 3-5 м [5]. Для разрабатываемого прототипа такой модуль является рациональным выбором, поскольку позволяет реализовать обнаружение движения без дополнительного аналогового усилителя и сложной схемы предварительной обработки.

Исполнительная часть устройства реализуется на базе модуля реле. Микроконтроллер формирует управляющий сигнал, а реле коммутирует внешнюю нагрузку, например осветительный прибор. AC/DC преобразователь обеспечивает преобразование сетевого напряжения в низковольтное питание, необходимое для работы микроконтроллера, сенсора и релейного модуля. Разделение устройства на функциональные блоки упрощает отладку, замену компонентов и последующее развитие конструкции.

Основное улучшение достигается за счет изменения логики принятия решения: перед отключением нагрузки устройство дополнительно проверяет наличие движения. Это особенно важно для систем освещения, где пользователь может находиться в помещении, но не перемещаться в течение некоторого времени. В таком случае предварительное сканирование снижает вероятность преждевременного отключения и повышает комфорт эксплуатации.

Таким образом, датчик движения с предварительным сканированием представляет собой устройство, в котором классическая PIR-детекция дополнена этапом предварительного сканирования. Основной интервал T1

обеспечивает удержание нагрузки после обнаружения движения, а дополнительный интервал T2 используется для подтверждения отсутствия активности перед отключением. Разработанная логика может быть применена в системах автоматического освещения, бытовой автоматизации и охранных устройствах, где требуется простое, недорогое и более устойчивое к ложным отключениям решение.

Список используемых источников

1. Фрайден Дж. Современные датчики. Справочник. М.: Техносфера, 2005. 592 с.

2. Волков А. А. Принцип действия PIR-детекторов для автоматического энергоэффективного управления освещением в зданиях [Электронный ресурс] // Интернет-журнал «Науковедение». 2013. № 6. URL: https://cyberleninka.ru/article/n/printsip-deystviya-pir-detektorov-dlya-avtomaticheskogo-energoeffektivnogo-upravleniya-osvescheniem-v-zdaniyah-1 (дата обращения: 28.04.2026).

3. Zappi P., Farella E., Benini L. Tracking Motion Direction and Distance With Pyroelectric IR Sensors // IEEE Sensors Journal. 2010. Vol. 10, N 9. P. 1486-1494. DOI: 10.1109/JSEN.2010.2044861.

4. Arduino Nano. Техническое описание платы на базе микроконтроллера ATmega328P [Электронный ресурс]. URL: https://docs.arduino.cc/hardware/nano (дата обращения: 28.04.2026).

5. AM312 Mini PIR Motion Sensor. Техническое описание инфракрасного модуля движения [Электронный ресурс]. URL: https://www.image.micros.com.pl/ _dane_ techniczne_auto/cz %20am312.pdf (дата обращения: 28.04.2026).

Статья представлена научным руководителем, доцентом кафедры КПРЭС СПбГУТ А. Г. Колосько.

УДК 681.2.083

ЛАБОРАТОРНАЯ УСТАНОВКА ИЗМЕРЕНИЯ ВОЛЬТАМПЕРНЫХ ХАРАКТЕРИСТИК ТУННЕЛЬНЫХ ПРИБОРОВ

Г. К. Меньшиков (студент группы РК-41м СПбГУТ), menshikov.gk@sut.ru
Д. А. Харьков (студент группы МТП-2511 СПбГУТ), harkov.da@sut.ru

В статье рассматривается разработка лабораторной установки измерения вольтамперных характеристик туннельных приборов. Актуальность темы обусловлена необходимостью внедрения в учебный процесс средств автоматизации исследования характеристик полупроводниковых приборов.

В работе предложена возможная реализация установки, а также структурная схема. Кроме того, приведены ее преимущества в сравнении с существующими методами измерения туннельных приборов.

ВАХ, туннельный диод, LabVIEW, микроконтроллер

На сегодняшний день активно применяются различные компоненты микро- и наноэлектроники. Среди них одну из ключевых ролей в конструировании электроаппаратуры играет туннельный диод. Его широко применяют в области генерирования незатухающих колебаний и конструировании усилителей. За счет своего уникального свойства – участка вольтамперной характеристики (ВАХ) с отрицательным дифференциальным сопротивлением, он способен компенсировать положительное активное сопротивление участка электрической цепи и обеспечить либо усиление сигнала, либо генерацию колебаний [1]. Для корректной работы туннельного диода в электрической цепи необходимо располагать данными о его ВАХ. Очевидно, что действительные параметры устройства будут отличаться от тех, что указаны в документации или справочной литературе, за счет допусков и погрешностей, возникающих в процессе производства. Чтобы точно определить ВАХ туннельного диода, необходимо ее измерить при помощи специальных приборов [2]. Такие измерительные устройства должны уметь достаточно точно определять ток и напряжение, проходящие через диод, а также строить графики ВАХ и визуализировать их для дальнейшего анализа. Несмотря на распространенность туннельных приборов и значимость изучения их характеристик, во многих высших учебных заведениях, на кафедрах в учебной программе которых присутствуют дисци-

плины по изучению микро- и наноэлектроники, отсутствует соответствующее лабораторное оснащение. Разработка лабораторного стенда для измерения ВАХ туннельных приборов с возможностью передачи данных в ПО «LabVIEW» может выступить в качестве инструмента для устранения вышеуказанных проблем.

Существуют готовые решения задач измерения ВАХ не только туннельных диодов, но и любых электронных компонентов. Одно из таких решений – использование двухканального осциллографа по нижеприведенной схеме (рис. 1).

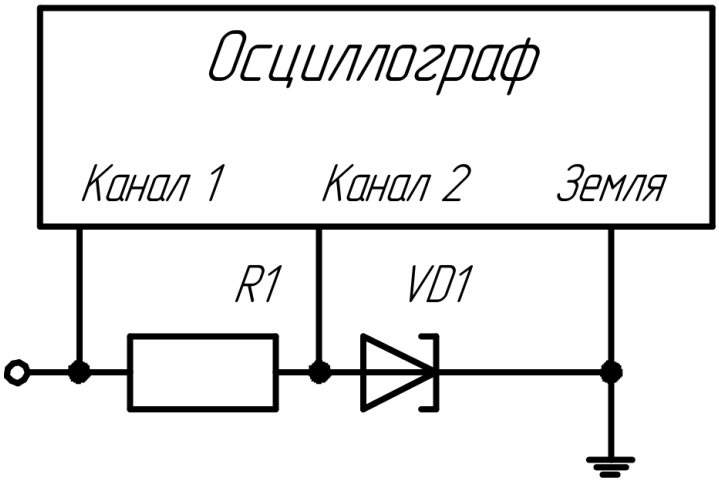


Рис. 1. Схема измерения свойств туннельного диода при помощи двухканального осциллографа

В таком случае, после получения осциллограмм и отправки их на персональный компьютер в виде файлов, можно получить ВАХ диода VD1. Для этого достаточно знать напряжение на диоде (измеряется каналом 2), а также ток, проходящий через него. Поскольку ток через резистор и диод течет одинаковый, достаточно вычислить ток на пассивном компоненте. Ток вычисляется по закону Ома для участка цепи (1):

$$I\partial = \frac{U_1 - U_2}{R_1} \quad (1)$$

где $I\partial$ – ток, протекающий через туннельный диод;

U_1 – напряжение на первом канале осциллографа (суммарное напряжение на резисторе и диоде);

U_2 – напряжение на втором канале осциллографа (напряжение на диоде);

R_1 – сопротивление резистора.

Полученные данные позволяют исследовать ВАХ используемого в измерительной схеме туннельного диода (а также прочих двухполюсных электронных компонентов).

Однако такая схема обладает рядом недостатков для использования в университетах. Во-первых, отсутствие генератора в схеме. Его нужно подключать отдельно и согласовывать с диодом. Даже если использовать сторонний генератор сигнала и усилить его по току, установка будет сильно громоздкой. Во-вторых, приобретение самого осциллографа и генератора может быть достаточно дорогим, чтобы использовать их для лабораторных работ по исследованию ВАХ.

Именно поэтому оптимальным решением будет создание прибора, нацеленного под конкретную задачу – измерение ВАХ.

В соответствии с целью использования проектируемое устройство должно соответствовать перечню критериев, а именно:

- регистрация ВАХ;
- компактность;
- подключение к персональному компьютеру;
- ремонтопригодность;
- обработка данных при помощи LabVIEW;
- низкая стоимость изготовления.

Устройство измерения ВАХ может функционировать по простейшей схеме, представленной на рис. 2.

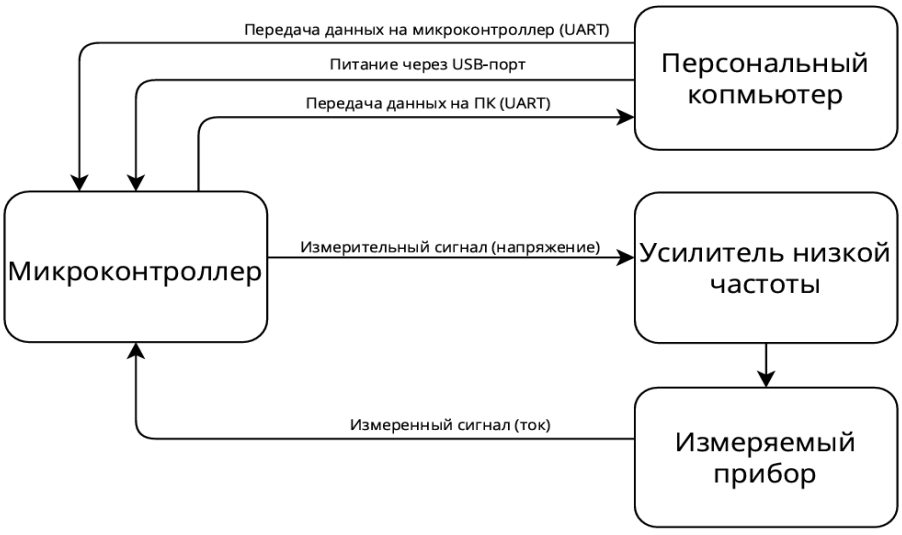


Рис. 2. Структурная схема устройства измерения ВАХ

Существует подобное запатентованное решение [3] для ВАХ-анализатора туннельных диодов, однако оно не раскрывает подробностей управления микроконтроллером процесса, передачи данных, а также подразумевает использование пилообразного генератора сигнала без возможности создавать программируемые измерительные сигналы.

В качестве микроконтроллера для устройства измерения требуется любой программируемый чип, который имеет в своей структуре аналого-цифровой преобразователь (АЦП), а также регистры для работы с протоколами UART и SPI. Наличие АЦП необходимо из-за того, что это основной инструмент микроконтроллера для измерения напряжения и тока с исследуемого туннельного диода. Регистры управления интерфейсом UART необходимы для передачи данных на ПК. Кроме того, по этому интерфейсу возможен и прием данных. На компьютере через программу при необходимости возможно задать определенное поведение измерителя. Необходимость наличия регистров управления интерфейсом SPI уже менее очевидна. Измерение ВАХ любого компонента должно производиться в пределах определенного диапазона напряжения, при этом само напряжение будет изменятся по заданному закону. Поэтому в устройстве должен быть своего рода встроенный генератор сигнала нужной формы. Микроконтроллер, чьи порты настроены только на цифровой вывод информации, не способен «сходу» сгенерировать аналоговый сигнал какой бы то ни было формы (кроме прямоугольной). Для решения этой проблемы можно использовать принцип резистивного делителя напряжения (рис. 3).

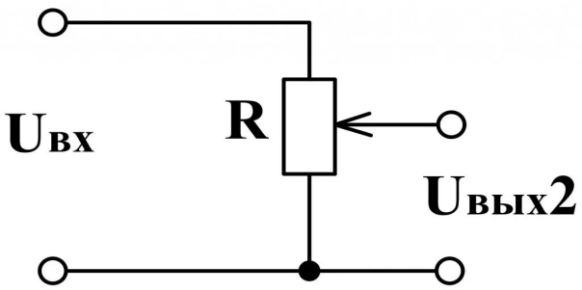


Рис. 3. Схема переменного резистивного делителя напряжения

Напряжение $U_{вх}$ может быть постоянным – микроконтроллер спокойно может это обеспечить. $U_{вых2}$ в свою очередь будет изменяться в зависимости от положения среднего вывода переменного резистора. В качестве такого резистора отлично подойдет чип серии MCP41xxx/42xxx. Этот чип является переменным резистором со встроенным обработчиком протокола SPI [4]. Использование такого цифрового резистора также имеет дополнительное преимущество, а именно возможность настроить генерацию сигналов любой формы, будь то «пила», «треугольник», «синус» и т.д.

Сигнал, полученный со встроенного генератора, будет иметь достаточно высокое входное сопротивление, поскольку он изначально проходит через резистор, значение сопротивления которого измеряется в десятках ки-

лоом. Такой сигнал нельзя использовать для измерения электронных компонентов – из-за высокого сопротивления, значения тока будут очень малы. Для усиления сигнала по сопротивлению можно использовать транзисторный усилительный каскад по схеме с общим коллектором. Его особенность заключается в том, что он усиливает не напряжение сигнала, а ток и мощность [5]. Кроме того, выходное напряжение такого усилителя совпадает по фазе с входным. Временную диаграмму работы усилительного каскада можно построить в симуляторе электрических цепей Proteus 8 (рис. 4).

На диаграмме видно, что сигнал имеет ступенчатый вид из-за применения цифрового потенциометра. Также можно отметить, что из-за превышения допустимого напряжения на коллекторе транзистора у усиленного сигнала «усекается» верхушка, однако это некритично. Поскольку верхнее значение напряжения получается около 2,3 В этого будет достаточно для измерения ВАХ многих диодов, особенно туннельных.

При подаче такого сигнала на измеряемом приборе формируется свое напряжение (реакция на сигнал). Значение этого напряжения передается на микроконтроллер для дальнейшей обработки. А для того, чтобы получить значение тока, проходящего через диод, достаточно это напряжение поделить на сопротивление цепи по закону Ома для участка цепи (1).

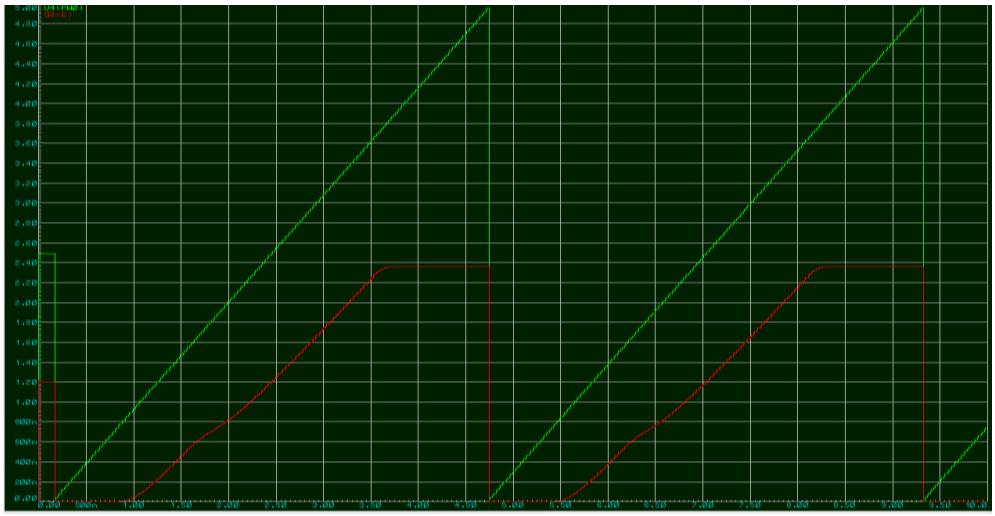


Рис. 4. Временная диаграмма пилообразного сигнала в Proteus 8. Зеленым цветом обозначен сигнал, идущий напрямую с цифрового потенциометра, а красным, прошедший через усилительный каскад

Микроконтроллер получает данные, обрабатывает их и отправляет на персональный компьютер.

Таким образом, получается прибор с простой конструкцией и оптимальной стоимостью, который способен измерять как туннельные, так

и обычные выпрямительные диоды. Данное устройство сможет найти широкое применение в качестве учебных лабораторных установок.

Список используемых источников

1. Поляков А. М. Разгаданный полупроводник: Кн. для внеклас. чтения. VIII-X кл. М.: Просвещение, 1981. 160 с., ил. (Мир знаний).

2. Елкин С. А. Туннельный диод: оценка, отбор и практическое применение // Радиоаматор. 2006. № 4. С. 26-29.

3. Патент № 172271 Российская Федерация, МПК G01R 31/26 (2014.01). Установка для динамического измерения вольтамперной характеристики туннельных диодов: № 2016145141: заявл. 18.11.2016: опубл. 03.07.2017 / Ким Дин Чер, Саяпин Сергей Григорьевич, Татаринов Павел Семенович, Томский Кирилл Олегович. 5 с.

4. Microchip MCP41XXX/42XXX Single/Dual Digital Potentiometer with SPI Interface: [электронный ресурс]. 2025 URL: https://static.chipdip.ru/lib/303/DOC012303841.pdf (дата обращения: 28.09.2025).

5. Степаненко И. П. основы теории транзисторов и транзисторных схем. Изд. 4, перераб. И доп. М., «Энергия», 1977 г. 672 с.

Статья представлена научным руководителем, доцентом кафедры КПРЭС СПбГУТ, кандидатом физико-математических наук А. Г. Колосько.

УДК 621.396

МОДЕЛИРОВАНИЕ И ОЦЕНКА ТОЧНОСТИ ПОЗИЦИОНИРОВАНИЯ В ПОМЕЩЕНИИ НА ОСНОВЕ АНАЛИЗА RSSI WI-FI УСТРОЙСТВ С УЧЕТОМ ВЛИЯНИЯ СТЕН

А. В. Михайлов (студент группы РТ-42м СПбГУТ), mikhailov.av@sut.ru

В статье рассчитана оценка точности позиционирования мобильного устройства внутри помещения с использованием существующей Wi-Fi инфраструктуры. В отличие от подходов на основе BLE-маяков, требующих установки дополнительного оборудования, предлагаемый метод использует сигналы от обычных бытовых устройств (телевизоров, компьютеров, смартфонов), которые постоянно присутствуют в сети. Разработана модель, позволяющая моделировать распространение сигнала с учетом затухания в стенах, выполнять трилатерацию по трем ближайшим устройствам и вычислять коэффициент точности позиционирования.

Wi-Fi, позиционирование, RSSI, трилатерация, карта стен

Современные системы позиционирования в помещениях активно используют сигналы беспроводных сетей благодаря повсеместному распространению Wi-Fi и Bluetooth-устройств [1]. Однако точность определения местоположения сильно зависит от затухания сигнала, которое искажает зависимость RSSI от расстояния.

В последние годы активно развиваются системы позиционирования на основе технологии Bluetooth Low Energy (BLE). Его суть заключается в анализе уровня сигнала маячка, с устройства приемника, находящегося у человека. Маячок передают информацию о силе излучаемого сигнала на приемники, установленные в помещении, далее уровень полученного сигнала конвертируется в расстояние, что позволяет определить удаленность человека от контролируемой зоны, а также судить о том, находится человек в данной зоне или покинул ее [2]. Однако основной недостаток BLE-подходов заключается в необходимости развертывания специализированной инфраструктуры, дополнительных BLE-меток.

В отличие от этого, предлагаемая методика использует существующую Wi-Fi инфраструктуру и обычные пользовательские устройства – телевизоры, компьютеры, смартфоны, ноутбуки и другую бытовую технику, поддерживающую подключение к беспроводной сети. Технически это реализуется следующим образом: мобильное устройство (например, смартфон) сканирует радиоэфир и измеряет уровень сигнала (RSSI) от всех доступных Wi-Fi устройств в сети. Эти устройства постоянно излучают радиосигналы в процессе работы (кадры данных, управления, служебные beacon-кадры), поэтому

не требуется установка дополнительных маяков. Собранные измерения RSSI вместе с известными координатами стационарных устройств позволяют вычислить текущее местоположение мобильного объекта [3]. Такой подход может применяться, например, в «умном доме», где телевизоры, компьютеры и другие гаджеты образуют естественную сеть опорных станций.

В основе разработанной модели лежит предположение, что координаты всех стационарных Wi-Fi устройств (телевизоров, компьютеров и т.п.) известны. Это реалистично, так как их положение можно определить один раз при установке или с помощью предварительной калибровки. Мобильное устройство (например, смартфон) периодически измеряет уровень сигнала (RSSI) от этих опорных устройств. Используя модель затухания, можно оценить расстояния до них, а затем вычислить собственные координаты методом трилатерации.

Модель затухания сигнала в свободном пространстве с добавлением ослабления от стен:

$$RSSI = P_0 - 10 * n * \log_{10}\left(\frac{d}{d_0}\right) - \sum L_{walls,} \quad (1)$$

где P_0 – мощность сигнала на опорном расстоянии d_0 (обычно 1 м, P_0 = –40 дБм); n – коэффициент потерь в среде (для офисных помещений n = 2); d – истинное расстояние между устройствами; L_{walls} – затухание каждой пересекаемой прямой стены (в модели принято 15 дБ).

Для оценки расстояния по измеренному RSSI (без знания карты стен) используется обратная формула:

$$d = d_0 * 10^{\frac{P_0 - RSSI}{10*n}}, \quad (2)$$

Трилатерация выполняется по трем устройствам с наибольшей мощностью сигнала. Координаты определяются методом наименьших квадратов решением системы линейных уравнений, полученной вычитанием уравнений окружностей для опорных станций, в модели эту задачу выполняет функция numpy.linalg.lstsq [4]:

$$\begin{cases} (x - x_1)^2 + & (y - y_1)^2 = d_1^2 \\ (x - x_2)^2 + & (y - y_2)^2 = d_2^2 \\ (x - x_3)^2 + & (y - y_3)^2 = d_3^2 \end{cases}, \quad (3)$$

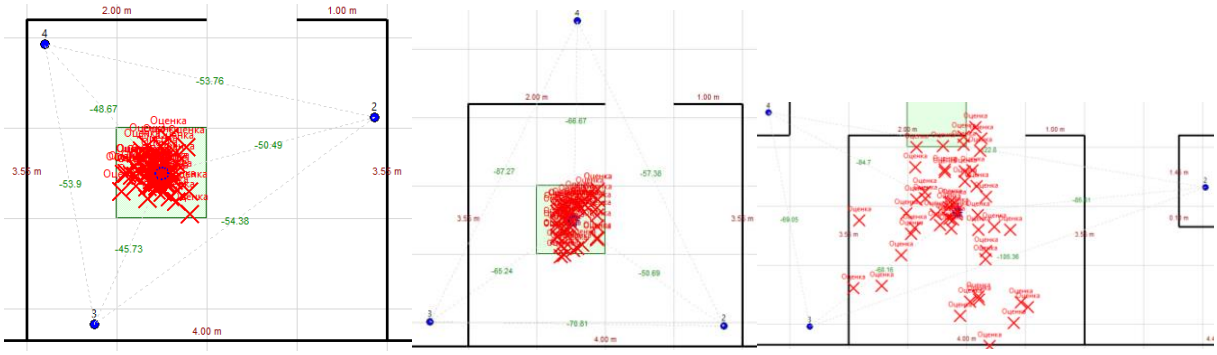
Модель системы определения местоположения была спроектирована на языке программирования Python.

Для приближения к реальным условиям предусмотрены:

● Шум измерения RSSI – к рассчитанному по формуле (1) значению RSSI добавляется случайная величина, распределенная по нормальному закону с нулевым средним и стандартным отклонением σ (по умолчанию 2 дБ). Это имитирует дрожание сигнала, вызванное временными изменениями среды, интерференцией и погрешностями приемника.

● Затухание стен – для каждой стены, пересекаемой лучом, фактическое ослабление является фиксированным (15 дБ).

Результат моделирования при различных условиях распространения показан на рисунке 1:



а) б) в)

Рис. 1. Результат трилатерации а) без учета стены; б) с учетом прохождения сигнала через 1 стену; в) с учетом прохождения сигнала через 2 стены

ТАБЛИЦА 1. Отклонение от истинного значения

	Измерение							
	№ 1-7	№ 8-14	№ 15-21	№ 22-28	№ 29-35	№ 36-42	№ 43-49	среднее значение
Отклонение от истинного значения, см	8	15	15	50	12	21	55	22
	5	32	31	11	14	28	11	
	35	16	19	13	4	10	36	
	2	16	15	13	35	11	26	
	15	40	25	32	9	34	20	
	16	8	39	16	22	29	42	
	32	39	30	20	13	13	16	
Отклонение от истинного значения при наличии 1 стены, см	25	58	34	16	35	35	43	30
	21	24	33	29	32	30	24	
	27	46	42	14	11	41	58	
	35	55	16	41	20	51	6	
	14	37	29	6	42	27	25	
	16	22	14	13	10	29	35	
	46	13	41	27	39	27	28	
	22	77	87	4	233	29	37	93

	Измерение							
	№ 1-7	№ 8-14	№ 15-21	№ 22-28	№ 29-35	№ 36-42	№ 43-49	среднее значение
Отклонение от истинного значения при наличии 2 стен, см	151	210	55	199	168	71	72	
	17	87	131	77	46	81	147	
	73	175	116	218	17	37	152	
	59	17	19	54	112	120	66	
	94	76	3	34	106	186	179	
	149	14	92	132	130	66	55	

Рост ошибки обусловлен двумя основными факторами. Во-первых, в системе присутствует шум измерения RSSI (стандартное отклонение 2 дБ), который вносит случайные флуктуации. Во-вторых, каждая стена дает дополнительное затухание, которое в реальных условиях невозможно точно предсказать. В модели оно принимается равным 15 ± 4 дБ, что отражает неопределенность характеристик материалов. С увеличением числа стен неопределенность накапливается, и ошибка растет непропорционально – уже при двух стенах средняя ошибка превышает 0.9 м.

Далее был произведен расчет точности попадания в определенную область (20,50,100 см) по формуле (4), результаты занесены в таблицу 2 и продемонстрированы на рисунке 2.

$$P = \frac{n_{\text{количество измерений попадающих в область}}}{N_{\text{Общее число измерений}}}. \quad (4)$$

ТАБЛИЦА 2. Точность попадания в область

Набор данных	Количество измерений	Область до 20 см	Область до 50 см	Область до 100 см
0 стен	49	57,14 %	97,96 %	100 %
1 стена	49	26,53 %	91,84 %	100 %
2 стены	49	14,29 %	26,53 %	61,22 %

Проведенный анализ наглядно демонстрирует, что точность Wi-Fi позиционирования критически зависит от условий распространения сигнала. При малом количестве препятствий система способна обеспечивать ошибку менее 20 см в половине случаев и менее 50 см – практически всегда. Однако с ростом числа стен точность резко падает, и при двух и более стенах более трети измерений дают ошибку свыше метра.

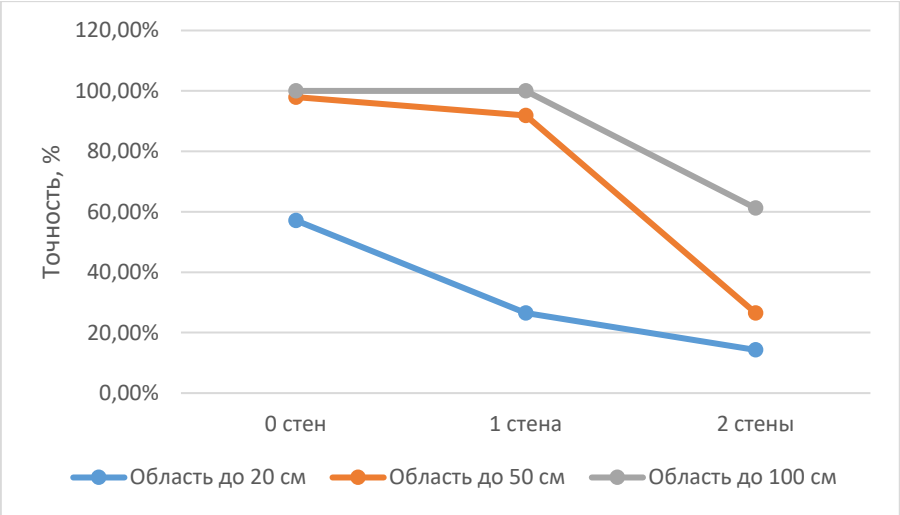


Рис. 2. График зависимости точности от количества стен

При одной стене система обеспечивает определение местоположения с точностью до 1 метра в 100 % случаев, что достаточно для большинства навигационных задач. При двух стенах точность до 1 метра снижается до 61 % можно лишь констатировать факт присутствия человека в комнате без точной позиции.

Таким образом, точность позиционирования критически зависит от количества препятствий и точности их моделирования. Для повышения надежности необходимо либо использовать более детальные карты стен, либо обеспечить прямую видимость хотя бы для одной опорной точки.

Список используемых источников

1. Хоров Е., Кирьянов А., Ляхов А., Бьянки Д. A Tutorial on IEEE 802.11ax High Efficiency WLANs // IEEE Communications Surveys & Tutorials. 20 September 2018. 21. С. 197-216.

2. Халин А. А., Зрюмова А. Г., Зрюмов П. А. Анализ возможностей Bluetooth low energy датчиков для проектирования систем контроля местоположения человека // сборник трудов конференции. Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2019. С. 172-176.

3. Kotaru M., Joshi K., Bharadia D., Katti S. SpotFi: Decimeter Level Localization Using Wi-Fi // ACM SIGCOMM Computer Communication Review. 2015. Vol. 45. № 4. P. 269-282.

4. Разбираемся в тонкостях проектирования Wi-Fi сетей в помещениях // Hubr URL: https://habr.com/ru/specials/456918/ (дата обращения: 08.03.2026).

УДК 621.371.31

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОПТИМИЗАЦИИ ПОКРЫТИЯ ТРЕХМЕРНЫХ WI-FI СЕТЕЙ В УСЛОВИЯХ БОЛЬШИХ ПОМЕЩЕНИЙ С ПРЕПЯТСТВИЯМИ

Р. Ф. Мустаев (студент гр. РТ-42м СПбГУТ), mustaev.rf@sut.ru

В эпоху Индустрии 4.0 и повсеместной автоматизации складских комплексов, надежное беспроводное покрытие становится критически важным фактором эффективности логистических операций. Современные склады представляют собой сложные трехмерные пространства с металлическими стеллажами, бетонными колоннами и другими препятствиями, создающими значительные помехи для распространения радиосигнала. При оптимизации покрытия на складских помещениях лучше использовать генетический алгоритм оптимизации.

Wi-Fi, планирование сети, генетический алгоритм, оптимизация размещения, трехмерное моделирование, COST 231 Multi-Wall, изоповерхностная визуализация, складское помещение

При развертывании Wi-Fi на складах и других подобных помещениях есть несколько вызовов. Сложная электромагнитная обстановка, большие площади, множество препятствий, интерференция, высокие требования к качеству связи. Неправильное планирование покрытия Wi-Fi сети на складских объектах приводит к значительным ошибкам позиционирования логистического оборудования, что в условиях современной автоматизации является критическим фактором [1-5].

Для сравнения было выбрано три метода оптимизации размещения точек доступа в трехмерной среде: равномерный, случайный поиск и генетический алгоритм. Равномерный метод показывает то, какое покрытие можно получить без оптимизации, тут точки доступа равноудалены и формируют «сетку». Метод остается востребованным в научной среде как контрольная группа в экспериментах по оптимизации. Без сравнения с простым методом невозможно объективно оценить выигрыш от применения сложного алгоритма. Случайный поиск основан на том, что он генерирует случайные места расположения точек доступа и запоминает лучший. Он хорош тем, что равномерно исследует все пространство и каждая итерация независима. Этот метод используют как быстрый способ оценки пространства решений. Генетический алгоритм имитирует процессы естественного отбора и генетического наследования в природе. Он последовательно улучшает решения,

адаптируется к препятствиям и находит глобальный оптимум. [3] В качестве целевой метрики используется процент площади склада, покрытый сигналом от -35 дБм до -45 дБм.

Исследования [2] показывают, что модели, основанные на учете затухания при прохождении через стены и перегородки, обеспечивают наилучшую точность прогноза, что подтверждает выбор модели COST 231 Multi-Wall [5] в настоящей работе.

В отличие от простых моделей свободного пространства (1), данная модель учитывает затухание при прохождении через препятствия различной природы, что критически важно для складских помещений с металлическими стеллажами и бетонными колоннами. Модель COST 231 Multi-Wall (2) обеспечивает наилучшую точность среди эмпирических моделей для indoor-среды за счет учета материалов внутренних конструкций. [4]

$$L_{FS} = 20log_{10}(d) + 20log_{10}(f) - 147{,}55, \quad (1)$$

где d – расстояние, f – частота, на которой работает точка доступа.

$$L_{total} = L_{FS} + L_{walls} + L_{floors}, \quad (2)$$

где L_{walls} – потери при прохождении сигнала через стены, L_{floors} – потери при прохождении сигнала между этажами

Для моделирования использовалась точка доступа Huawei AirEngine 5761-11. Ее характеристики можно увидеть в таблице 1.

ТАБЛИЦА 1. Характеристики точки доступа Huawei AirEngine 5761-11

Характеристики	Численное значение
Мощность передачи	23 дБм
Рабочие диапазоны частот	2,4 и 5 ГГц
Чувствительность	-100 дБм

Для оценки эффективности методов был разработан код, который создает трехмерное пространство склада с препятствиями размером 100x200x8. В этом пространстве по трем алгоритмам происходит расстановка точек доступа в диапазонах 2.4 ГГц и 5 ГГц и выводятся карты с точечной диаграммой и сравнительная диаграмма, показывающая какой алгоритм покрыл больше площади сигналом от -35 дБм до -45 дБм. На рисунке 1 можно увидеть одну из смоделированных карт.

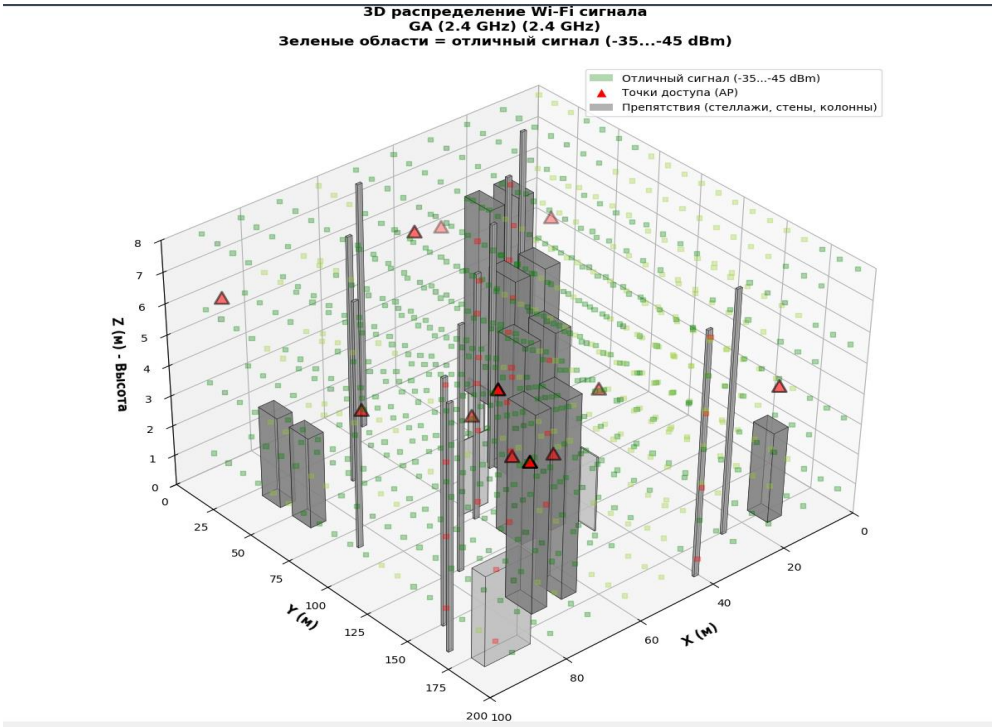


Рис. 1. Точечная диаграмма силы сигнала в диапазоне 2.4 ГГц

Из рис. 2 видно, что эффективность генетического алгоритма на складских помещениях выше в обоих диапазонах частот, чем у случайного расположения на 9 процентов и метода равномерной сетки на 7,3 процента.

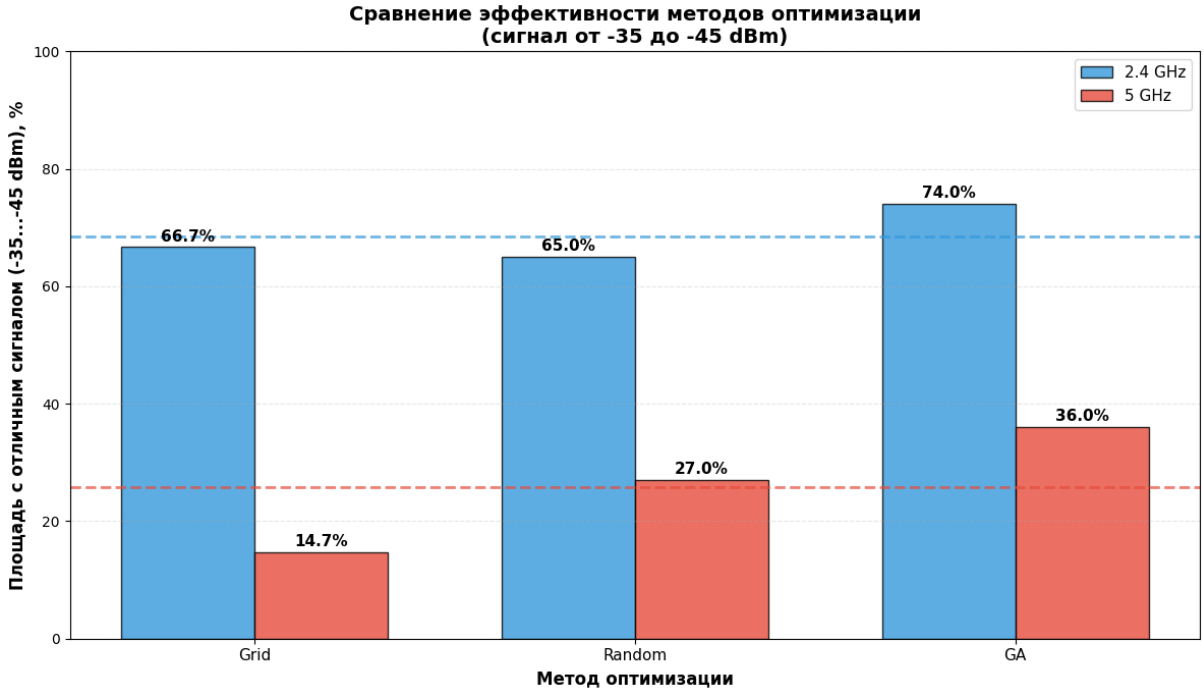


Рис. 2. Зависимость площади покрытого сигнала от метода оптимизации

В работе решена актуальная научно-практическая задача оптимизации размещения точек доступа Wi-Fi в трехмерной среде складского помещения. Предложенный подход, основанный на применении генетического алгоритма в сочетании с моделью распространения сигнала COST 231 Multi-Wall, позволяет увеличить площадь с отличным качеством сигнала (-35…-45 dBm) на 7.3 % по сравнению с традиционным методом равномерной сетки в диапазоне 2.4 ГГц и на 21,3 % в диапазоне 5 ГГц. Разработанный программный комплекс и полученные результаты могут быть использованы при проектировании беспроводных сетей на промышленных складах, логистических центрах и других indoor-объектах со сложной электромагнитной обстановкой.

Список используемых источников

1. Кокорева Е., Шурыгина К., Брагин А. Влияние планирования покрытия Wi-Fi сети на точность позиционирования объектов логистики // E3S Web of Conferences. 2022. Т. 363. С. 01041. DOI: 10.1051/e3sconf/202236301041.

2. Прогнозирование покрытия и алгоритмы оптимизации для внутренних помещений // EURASIP Journal on Wireless Communications and Networking. 2012. Т. 2012. Статья 123. DOI: 10.1186/1687-1499-2012-123.

3. Cheng C.P., Li C.T. Разработка BIM-ассистированного алгоритма оптимизации трехмерного размещения точек доступа для улучшения Wi-Fi позиционирования по отпечаткам сигнала // Computing in Civil Engineering 2019. ASCE, 2019. С. 232-240. DOI: 10.1061/9780784482421.030.

4. Обейдат Х.А., Алабдулла А.А.С., Эльхазми Э.А. и др. Обзор распространения сигнала в помещении // Обзор компьютерных наук. 2020. Том 37. С. 100272. DOI: 10.1016/j.cosrev.2020.100272.

5. ITU-R P.1238-13. Данные о распространении и методы прогнозирования для планирования систем внутренней радиосвязи и локальных радиосетей в диапазоне частот от 300 МГц до 450 ГГц. Женева: Международный союз электросвязи, 2025. 33 с.

Статья представлена научным руководителем, профессором кафедры РТ СПбГУТ, доктором технических наук, профессором О. А. Симониной.

УДК 621.396

АЛГОРИТМ УПРАВЛЕНИЯ МНОГОКАНАЛЬНОЙ BLUETOOTH-СИСТЕМОЙ С ДИНАМИЧЕСКИМ РАСПРЕДЕЛЕНИЕМ УСТРОЙСТВ И АДАПТИВНЫМ РЕГУЛИРОВАНИЕМ МОЩНОСТИ

П. А. Нестерчук (студент гр. РТ-42м СПбГУТ), nesterchuk.pa@sut.ru

В статье представлен комплексный подход к управлению беспроводными сетями Bluetooth в перегруженном ISM-диапазоне. Предложен алгоритм, объединяющий динамическое распределение устройств между несколькими пикосетями и адаптивное регулирование мощности передачи на основе оценки текущего уровня помех. В отличие от традиционных методов, рассматривающих эти задачи раздельно, разработанная модель учитывает взаимное влияние распределения нагрузки и энергопотребления на общую помехоустойчивость системы. Математическая модель включает расчет внутриканальных, межканальных и внешних помех, функцию стабилизации переключений. Разработана программная реализация в среде MATLAB, позволяющая проводить численные эксперименты для различных сценариев эксплуатации. Результаты моделирования демонстрируют снижение энергопотребления и улучшение надежности связи при высокой плотности устройств по сравнению со статическими схемами распределения и фиксированной мощностью передачи.

Bluetooth, многоканальная архитектура, управление мощностью, динамическое распределение, помехоустойчивость, математическое моделирование, энергоэффективность, алгоритм адаптации

Современные беспроводные технологии сталкиваются с проблемой стремительного роста плотности устройств в ограниченном частотном спектре. Диапазон 2,4 ГГц, используемый технологией Bluetooth, является глобально нелицензируемым ISM-диапазоном, что обуславливает его высокую популярность, но одновременно создает сложную электромагнитную обстановку [1]. В этом диапазоне одновременно работают сети Wi-Fi, устройства ZigBee, беспроводная периферия, бытовая техника и промышленное оборудование. Такое соседство формирует нестационарную интерференционную картину, где уровень помех существенно варьируется в зависимости от времени суток, расположения и плотности узлов в зоне покрытия.

Классическая архитектура Bluetooth-сети строится на основе пикосети, где одно мастер-устройство координирует работу до семи активных ведомых устройств [2]. Все устройства в пикосети синхронизированы и используют единую псевдослучайную последовательность частотных скачков. Однако при увеличении количества подключений возникают внутриканальные

помехи, снижающие помехоустойчивость системы. Кроме того, классические алгоритмы часто используют фиксированную мощность передачи, что приводит к избыточному энергопотреблению в благоприятных условиях и недостаточному качеству связи при ухудшении обстановки [3].

Раздельная оптимизация этих параметров не позволяет достичь глобальной эффективности. Например, переключение устройства на менее загруженный канал может потребовать увеличения мощности из-за большего расстояния до нового мастера, что нивелирует выигрыш от снижения внутрисетевых помех.

Цель работы – разработать комплексный алгоритм, одновременно решающий задачи распределения устройств между пикосетями для минимизации помех и регулировки мощности передачи в реальном времени для снижения энергопотребления и обеспечения устойчивой связи.

Процесс подключения включает сканирование эфира ведомым устройством, получение списка доступных пикосетей, уровня сигнала и класса устройства. Устройство оценивает качество канала, помеховую обстановку и требуемую мощность передачи, оценивая расстояние по затуханию сигнала. Затем на основе интегральной функции стоимости (качество канала, мощность, загруженность пикосети) выбирается мастер устройство с минимальным значением.

Для корректного управления мощностью и распределением устройств необходимо детально моделировать природу помех. Полный уровень интерференции I_{total} на канале k в момент времени t складывается из трех основных компонентов [4]:

$$I_{total,k}(t) = I_{intra,k}(t) + I_{inter,k}(t) + I_{ext,k}(t)\,,$$

где: $I_{intra,k}(t)$ – внутриканальные помехи, создаваемые другими устройствами той же пикосети, работающими на канале k; $I_{inter,k}(t)$ – межканальные помехи, возникающие от соседних пикосетей той же системы из-за неидеальной фильтрации сигналов; $I_{ext,k}(t)$ – внешние помехи от сторонних источников (Wi-Fi, бытовые приборы, фоновый тепловой шум).

Внутриканальные помехи зависят от числа активных устройств N_kв пикосети и средней мощности их передатчиков. Поскольку устройства в пикосети используют синхронные частотные скачки, их сигналы могут коллизировать при одновременной передаче. Модель внутриканальных помех описывается следующим выражением:

$$I_{intra,k} = P_{tx,avg} \cdot (N_k - 1) \cdot \eta_{orth},$$

где $P_{tx,avg}$ – средняя мощность передатчиков в пикосети, η_{orth} – коэффициент ортогональности кодов, учитывающий степень взаимного влияния устройств внутри одной сети. Чем больше устройств в пикосети, тем выше уровень внутренних помех, что подтверждается исследованиями зависимости качества связи от количества подключений.

Внешние помехи моделируются как фоновый шум (−110 дБм, нормальное распределение) и импульсные воздействия (например, от микроволновых печей или Wi-Fi), при которых уровень шума на каналах кратковременно возрастает до −70 дБм и выше.

Мощность передачи устройства i в пикосети k не должна быть фиксированной. Она должна определяться исходя из требования к минимальному отношению сигнал/шум SNR_{target}, необходимому для обеспечения заданной вероятности битовой ошибки (BER). Используя модель канала с затуханием, требуемая мощность рассчитывается по формуле [5]:

$$P_{tx,i} = \min\left(P_{max}, \max\left(P_{min}, \frac{SNR_{target}\cdot(N_0+I_{total,k})\cdot L(d_i)}{G_{ant}}\right)\right),$$

где P_{max} – максимальная допустимая мощность устройства (Вт); P_{min} – минимальная мощность, поддерживаемая радиомодулем (дБм); N_0 – уровень теплового шума; $L(d_i)$ – функция потерь на пути распространения сигнала, зависящая от расстояния d_iмежду устройством и мастером пикосети; G_{ant}-коэффициент усиления антенны.

Функция потерь $L(d)$обычно моделируется по закону затухания:

$$L(d) = L_0 \cdot \left(\frac{d}{d_0}\right)^{\gamma},$$

где γ – показатель потерь на пути (для помещений обычно 3…4), d_0 – расстояние.

Данная формула обеспечивает принцип «минимально необходимой мощности»: устройство увеличивает мощность только тогда, когда рост помех или расстояния угрожает качеству связи. Это позволяет экономить энергию батареи и снижать общий уровень интерференции в эфире.

Для принятия решения о распределении устройств вводится функция стоимости $C_{i,k}$, которая объединяет несколько критериев качества. Устройство выбирает пикосеть с минимальным значением стоимости:

$$C_{i,k} = \alpha \cdot \frac{1}{Q_k} + \beta \cdot \frac{P_{tx,i}}{P_{max}} + \gamma \cdot \frac{N_k}{N_{max}},$$

где Q_k – интегральный показатель качества канала k, учитывающий отношение сигнал/шум и уровень внешних помех; $P_{tx,i}$ – требуемая мощность для устройства i на канале k, рассчитанная по модели управления мощностью; N_k – текущая загрузка пикосети (количество подключенных устройств); N_{max} – максимальное количество устройств в пикосети (по стандарту 7); α, β, γ – весовые коэффициенты, сумма которых равна 1.

Настройка весовых коэффициентов позволяет адаптировать алгоритм под различные сценарии. Например, для энергоэффективных IoT-устройств увеличивается β, чтобы приоритизировать каналы с меньшим энергопотреблением [6]. Для систем реального времени увеличивается α, чтобы выбирать каналы с наилучшим качеством сигнала и минимальной задержкой.

Одной из проблем динамического распределения заключается в том, что устройство часто переключается между пикосетями при незначительных колебаниях параметров канала. Чтобы избежать этого, вводится условие: переход устройства из пикосети k_1 в k_2 разрешен только если выигрыш в функции стоимости превышает пороговое значение:

$$C_{i,k_1} - C_{i,k_2} > \Delta_{hyst},$$

где Δ_{hyst} – порог гистерезиса. Это правило обеспечивает устойчивость работы алгоритма: переключение происходит только при существенном улучшении условий, превышающем уровень случайных флуктуаций.

Для оценки качества связи используется модель вероятности битовой ошибки для модуляции DQPSK, используемой в режиме EDR (Enhanced Data Rate) Bluetooth:

$$BER \approx \frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{SNR}{2}}\right),$$

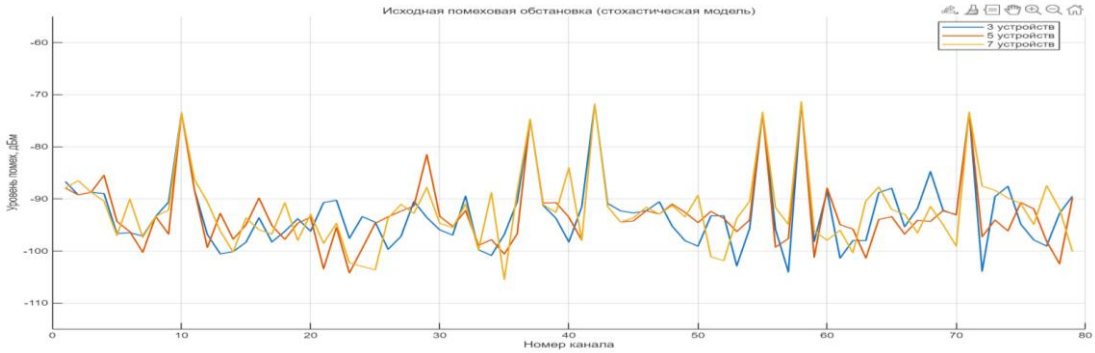


Рис. 1. Исходная помеховая обстановка в многоканальной Bluetooth-архитектуре

На рис. 1 исходная помеховая обстановка в многоканальной Bluetooth-архитектуре неудовлетворительна на каналах 11, 37, 42, 58, 68 и 71 из-за помех и отсутствия адаптивного регулирования мощности (превышение пороговых значений).



Рис. 2. Помеховая обстановка после применения адаптивного регулирования мощности

Согласно рисунку 2 – применение адаптивного регулирования мощности снижает уровень собственных помех пикосетей за счет реализации принципа «минимально необходимой мощности»: устройство уменьшает P_{tx} в благоприятных условиях, что линейно снижает вклад в интерференцию согласно формуле. Интегральная функция стоимости согласует управление мощностью с балансировкой нагрузки, а правило гистерезиса обеспечивает устойчивость переключений. В результате совокупный уровень внутриканальных и межканальных помех снижается на 2,5–7 дБ без ухудшения качества связи, что подтверждает эффективность предложенного подхода для работы в перегруженном ISM-диапазоне.

Список использованных источников

1. Bluetooth Core Specification v5.3 / Bluetooth SIG. URL: https://www. bluetooth.com/specifications/ (дата обращения 10.03.2026).

2. Haartsen J. The Bluetooth radio system // IEEE Personal Communications. 2000. Vol. 7. № 1. P. 28–36.

3. Rappaport T. S. Wireless Communications: Principles and Practice. 2nd ed. Prentice Hall, 2002.

4. Goldsmith A. Wireless Communications. Cambridge University Press, 2005.

5. Chiang M., Tan C. W., Palomar D. P., O'Neill D., Julian D. Power control by geometric programming // IEEE Transactions on Wireless Communications. 2007. Vol. 6. № 7. P. 2640–2651.

6. Palattella M. R., Dohler M., Grieco A., Rizzo G., Torsner J., Engel T., Ladid L. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models // IEEE Journal on Selected Areas in Communications. 2016. Vol. 34. № 3. P. 510–527.

Статья представлена научным руководителем, доцентом кафедры РТ СПбГУТ, кандидатом технических наук О. А. Симониной.

УДК 621.396.946

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ РАСПОЛОЖЕНИЯ БАЗОВЫХ СТАНЦИЙ МОБИЛЬНЫХ СЕТЕЙ 4G В УСЛОВИЯХ БОЛЬШИХ ГОРОДОВ

А. М. Ниязгулыева (заведующий кафедрой радиосвязи и радиотехнических систем ИТиИТ)
А. Ч. Чарыярова (студентка гр. ПЭ-1, ИТиИТ),
charyyarovaayjemal@gmail.com

При проектировании сетей сотовой связи необходимо учитывать архитектурно-географический рельеф города, чтобы обеспечить оптимальное размещение их базовых станций. В данной работе проведены измерения характеристик распространения радиосигналов базовых станций стандарта четвертого поколения в 9, 10 и 11-ом микрорайонах города Ашхабад. Исследование выполнено с использованием программного приложения Netmonitor. Также представлены расчеты потерь мощности в радиоканалах на основе модели Уолфиша-Икегамы. Полученные результаты позволяют сопоставить теоретические модели с реальными данными в условиях плотной городской застройки.

мобильная связь, 4G LTE, базовая станция, модель Уолфиша-Икегамы, распространение радиоволн, Netmonitor, городская застройка, качество сигнала

В настоящее время в Туркменистане реализуются масштабные проекты по расширению сетей мобильной связи и внедрению современных коммуникационных сервисов. Внедрение услуг 4G основывается на передовом мировом опыте и требует постоянного совершенствования инфраструктуры. При строительстве сетей в условиях мегаполиса критически важно учитывать архитектурно-географические характеристики города [1, 2].

Изучение влияния радиопомех и замираний сигналов в плотно застроенных районах необходимо для обеспечения высокого качества обслуживания и оптимизации затрат на базовые станции.

В микрорайонах 9, 10 и 11 столицы Ашхабада проводится исследование расположения базовых станций мобильных сетей 4G, а также моделирование характеристик распространения радиосигналов в зонах их обслуживания на основе модели Уолфиша-Икегамы. Измерительные исследования средней мощности радиосигналов проводятся с использованием программного комплекса «Netmonitor» на мобильных телефонах на платформе Android (таблица 1).

ТАБЛИЦА 1. Основные энергетические свойства радиосигналов в сетях сотовой связи 4G

		Энергетические свойства сигналов в радиоканалах сети 4G			
		RSSI (dBm)	RSRQ (dB)	RSRP (dBm)	SINR (dB)
Качество сигналов	Очень хороший	> – 65	> – 5	> – 84	> 12,5
	Хороший	- 66... – 75	- 6, – 7, – 8	- 85... – 102	10... 12,4
	Удовлетворяющий	- 76... – 85	- 9, – 10	- 103... – 111	7... 9
	Низкий	< – 86	< – 11	< – 112	< 6

Программное обеспечение «Netmonitor» предназначено для поиска базовых станций мобильных релейных станций, определения и измерения их технических характеристик и параметров. Основные цели программы «Netmonitor», используемой для технического мониторинга мобильных релейных станций, включают в себя создание базы данных о базовых станциях мобильных операторов и поддержание ее в активном состоянии [3, 4].

RSRP (Reference Signal Received Power) – Мощность принимаемого пилотного сигнала.

RSSI (Received Signal Strength Indicator) – Индикатор мощности принимаемого сигнала.

RSRQ (Reference Signal Received Quality) – Качество мощности принимаемого пилотного сигнала. Его значение рассчитывается по следующей формуле:

$$RSRQ = \frac{RSRP}{RSSI/_N}, \quad (1)$$

где N – количество блоков, из которых измерен RSSI.

SINR (RSSRN) (Signal Interference + Noise Ratio) – соотношение сигналов, интерференция + Радиошум.

С помощью программы «Netmonitor» были проведены измерения средней мощности радиосигналов 4G мобильных сетей в пределах 9-го, 10-го и 11-го микрорайонов, расположенных на восточной стороне города Ашхабад.

ТАБЛИЦА 2. Сравнительные результаты измерений, проведенных с помощью программы «Netmonitor», и расчетов, выполненных на основе модели Уолфиша-Икегамы

Интервал, m	Средние потери радиосигналов dB	Средняя мощность радиосигналов, dBm (по модели Уолфиша-Икегамы)	Средняя мощность радиосигналов, dBm (на основании результатов измерений)	Средняя мощность радиосигналов, dBm (на основании результатов измерений) (RSSI)
20	62,82	– 2,52	-62	-42
40	74,3	– 14	-58	-38
60	81,16	– 20,86	-69	-49
80	85,78	– 25,48	-68	-48
100	89,4	– 29,1	-68	-48
120	92,4	– 32,1	-70	-50
140	94,9	– 34,5	-74	-54
160	97,16	– 36,86	-71	-51
180	99,16	– 38,86	-64	-44
200	100,9	– 40,6	-75	-55
220	102,46	– 42,16	-76	-56
240	103,9	– 43,6	-73	-53
260	105,1	– 44,8	-76	-56
280	106,4	– 46,1	-72	-52
300	107,5	– 47,2	-72	-52
320	108,5	– 48,2	-80	-60
340	109,5	– 49,2	-72	-52
360	110,4	– 50,1	-79	-59
380	111,4	– 51,1	-83	-63
385	111,7	– 51,4	-77	-57

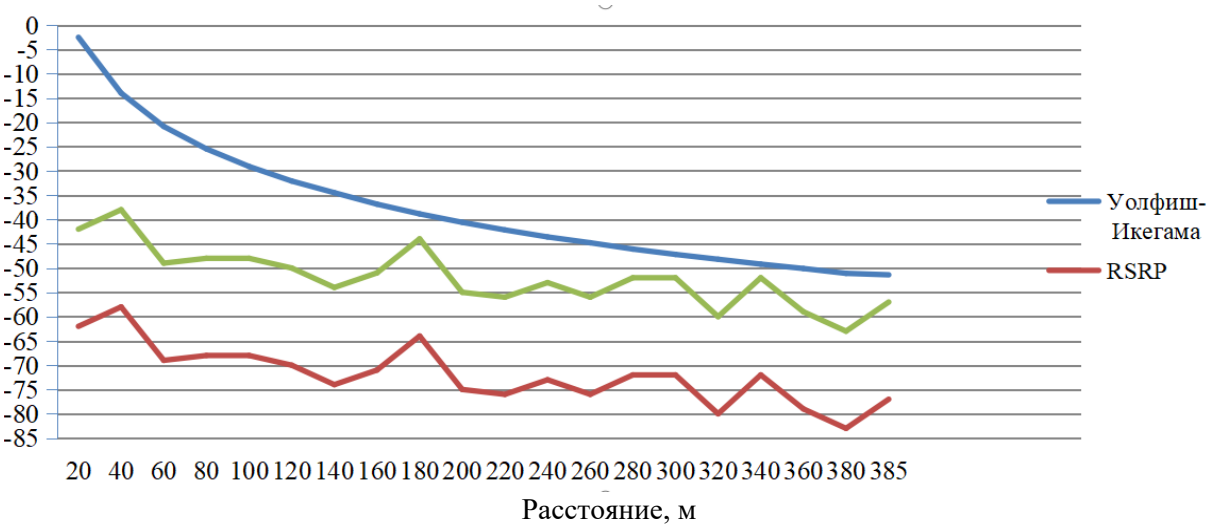


Рис. 1. График, сравнительных результатов измерений, проведенных с помощью программы «Netmonitor», и расчетов, выполненных на основе модели Уолфиша-Икегамы

Таким образом, краткие результаты состоят из следующего:

1. По результатам расчетов модели Уолфиша-Икегамы мощность принимаемых сигналов изменяется в диапазоне от -2,52 dBm до -51,4 dBm. С помощью программы «Netmonitor» были проведены измерения мощности радиосигнала в пределах зоны обслуживания базовой станции с номером 10068, расположенной в 10-м микрорайоне, где мощность радиосигнала изменяется от -38 dBm до -63 dBm (RSSI). Мощность пилотных сигналов колеблется в пределах от -58 dBm до -83 dBm.

2. В пределах зоны обслуживания базовой станции с номером 10068, расположенной в 10-м микрорайоне города Ашхабад, были определены характеристики качества радиосигналов. По результатам измерений качества сигнала в зоне обслуживания базовой станции было установлено, что уровень сигнала изменяется от -6 dB до -14 dB, а отношение сигнал/шум – от 27 dB до 0 dB.

Список используемых источников

1. Веселовский К. Системы подвижной радиосвязи. М.: Горячая линия Телеком, 2006.

2. Вишневский В., Портной С., Шахнович И. Энциклопедия Wi-Max путь к 4G. М.: Техносфера, 2009.

3. Мониторинг сетей мобильной связи XXI века [Электронный ресурс]. URL: http://xinit.ru (дата обращения: 23.05.2024).

4. Справочные данные по параметрам NetMonitor [Электронный ресурс] // Википедия: свободная энциклопедия. URL: https://ru.wikipedia.org (дата обращения: 27.12.2025).

УДК 621.396.99

ПРОЦЕСС ХЭНДОВЕРА В СПУТНИКОВЫХ СИСТЕМАХ СВЯЗИ VLEO

Г. С. Рябчун (студент группы РМ-02), ryabchun.gs@sut.ru

Рассматривается процесс хэндовера в спутниковых системах связи на сверхнизких околоземных орбитах. Анализируется влияние малой высоты орбиты на время радиовидимости спутника, размеры зоны обслуживания и частоту переключений между спутниками. Представлена упрощенная математическая модель, связывающая параметры орбитальной геометрии с параметрами линии связи, включая угол места, наклонную дальность, мощность принимаемого сигнала, доплеровский сдвиг и задержку распространения. В среде MATLAB реализована имитационная модель, в которой рассчитываются момент инициирования хэндовера, выбор целевого спутника и число переключений за сеанс связи. Результаты моделирования показали, что для систем наибольшую устойчивость обеспечивает многокритериальный выбор целевого спутника, учитывающий геометрические и энергетические параметры канала.

VLEO, спутниковая связь, хэндовер, зона обслуживания, угол места, доплеровский сдвиг, имитационное моделирование, MATLAB

Спутниковая система VLEO рассматривается как совокупность наземного терминала и спутников, последовательно входящих в зону радиовидимости. Диапазон VLEO в литературе обычно ограничивается высотами ниже 200-450 км [1, 5]. Малая высота орбиты сокращает время обслуживания каждым спутником и вызывает частые процедуры хэндовера [1, 2].

В упрощенной геометрической модели время радиовидимости определяется максимальным центральным углом ψ_{max} между наземным терминалом и подспутниковой точкой при заданном минимальном угле места θ_{min} (1.1):

$$\psi_{max} = \arccos\left(\frac{R_3}{R_3 + h} cos\theta_{min}\right) - \theta_{min} \quad (1.1)$$

где $R_3 -$ радиус Земли; $h -$ высота орбиты спутника.

Тогда для пролета, близкого к зенитному, время радиовидимости оценивается как (1.2):

$$T_v = \frac{2\psi_{max}}{n}, n = \sqrt{\frac{\mu}{(R_3 + h)^3}} \quad (1.2)$$

где $n -$ средняя угловая скорость спутника; μ – гравитационный параметр Земли.

При входных условиях $R_З = 6371$ км, $\theta_{min} = 10$ град и $h = 300$ км время видимости спутника T_v составляет около 5 мин. В сравнении с системами LEO разница составляет порядка 41 %. На рисунке 1 представлена зависимость времени видимости от угла места и высоты спутника.

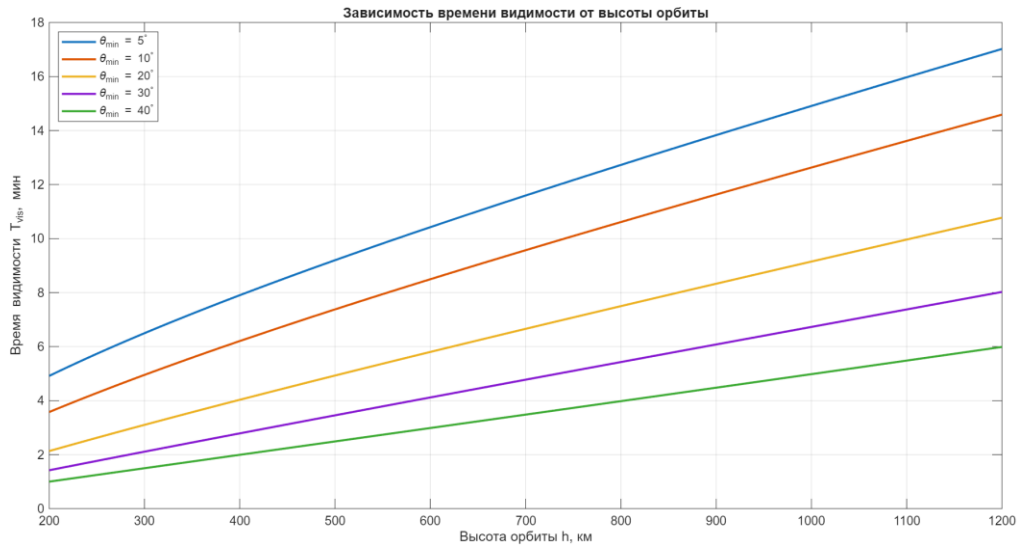


Рис. 1. Зависимость времени видимости от угла места и высоты спутника

Сокращение времени видимости при уменьшении высоты орбиты связано с уменьшением центрального угла радиовидимости, а уменьшение фактической зоны обслуживания связано с ограничением области покрытия луча условием по уровню половинной мощности *P(t)* (1.3):

$$P(t) \geq P_{\text{3дБ}} \tag{1.3}$$

Для системы VLEO при $h = 300$ км, $\theta_{min} = 10$ град и ширине луча по уровню половинной мощности, $\theta_{0.5} = 24$ град фактическая зона определяется зоной покрытия луча антенны. Радиус зоны радиовидимости составляет около 1120 км, тогда как радиус пятна обслуживания – около 64 км.

Параметры состояния линии связи описывают текущее положение спутника относительно наземного терминала и текущее состояние радиоканала Инициирование хэндовера в системе VLEO выполняется при ухудшении параметров текущей линии связи или при прогнозируемом выходе спутника из зоны обслуживания [3, 4, 6]. В модели процесса хэндовера вектор состояния линии связи задается в виде (1.4):

$$x(t) = [\theta(t), d(t), P_r(t), f_D(t), \tau(t)\,] \tag{1.4}$$

где $\theta(t)$ – функция времени угла места; $d(t)$ – функция времени наклонной дальности; $P_r(t)$ – функция времени мощности принимаемого сигнала; $f_D(t)$ – функция времени доплеровского сдвига; $\tau(t)$ – функция времени задержки распространения сигнала.

Инициирование хэндовера в системе VLEO выполняется при ухудшении параметров текущей линии связи или при прогнозируемом выходе спутника из зоны обслуживания. Момент хэндовера t_{HO} задается по пороговому условию на один или несколько параметров состояния (1.5):

$$t_{HO} = \min\{t: F\big(x(t)\big) \leq \Gamma\} \tag{1.5}$$

где Г – порог инициирования хэндовера.

В качестве частного случая используется критерий по углу места (1.6):

$$t_{HO} = \min\{t: \theta(t) \leq \theta_{HO}\}, \theta < \theta_{HO}. \tag{1.6}$$

Такая постановка обеспечивает временной запас для завершения процедуры переключения до выхода спутника из зоны обслуживания [3, 4]. Для повышения устойчивости решения используется комбинированный критерий (1.7):

$$P_r^{(j)}(t) \geq P_r^{(i)}(t), \theta^{(i)} \leq \theta_{HO} \tag{1.7}$$

где i – текущий спутник, j – спутник-кандидат [3].

После инициирования хэндовера выбирается целевой спутник из множества доступных кандидатов. В множество кандидатов включаются спутники, для которых одновременно выполняются условия радиовидимости и допустимого качества приема. Дальнейший выбор выполняется по одному из критериев или по их комбинации. Для систем NTN такой подход согласуется с зависимостью процедуры переключения от геометрии трассы, уровня сигнала, доплеровского сдвига и времени доступности канала [3, 4]. Критерии:

- по уровню принимаемого сигнала, основанный на выборе спутника, обеспечивающего максимальную мощность сигнала;
- по углу места, в котором выбирается спутник с наибольшим значением угла места;
- по ожидаемому времени удержания канала, ориентированный на выборе спутника, для которого ожидаемое оставшееся время обслуживания максимально;

● комбинированный критерий выбора, учитывающий несколько параметров [3, 4, 5].

В имитационной модели MATLAB выбор целевого спутника выполняется по одному из приведенных критериев, что позволяет сравнить момент хэндовера, число переключений и длительность удержания канала для разных правил принятия решения. В каждый момент времени вычисляются параметры состояния линии связи x(t), формируется множество доступных спутников-кандидатов и принимается решение о сохранении текущего соединения либо о его переключении на новый спутник (рисунок 2).

В модели использовались следующие входные данные: радиус Земли 6371 км, высота орбиты 300 км, минимальный угол места 10 град, порог инициирования хэндовера 18 град, рабочая частота 2 ГГц, мощность передатчика 30 дБм, усиление антенны спутника 12 дБи, усиление антенны терминала 5 дБи, дополнительные потери 2 дБ, порог принимаемой мощности -120 дБм. Орбитальная группировка задавалась как многоплоскостная конфигурация из трех орбитальных плоскостей по четыре спутника в каждой. Шаг моделирования – 1 с.

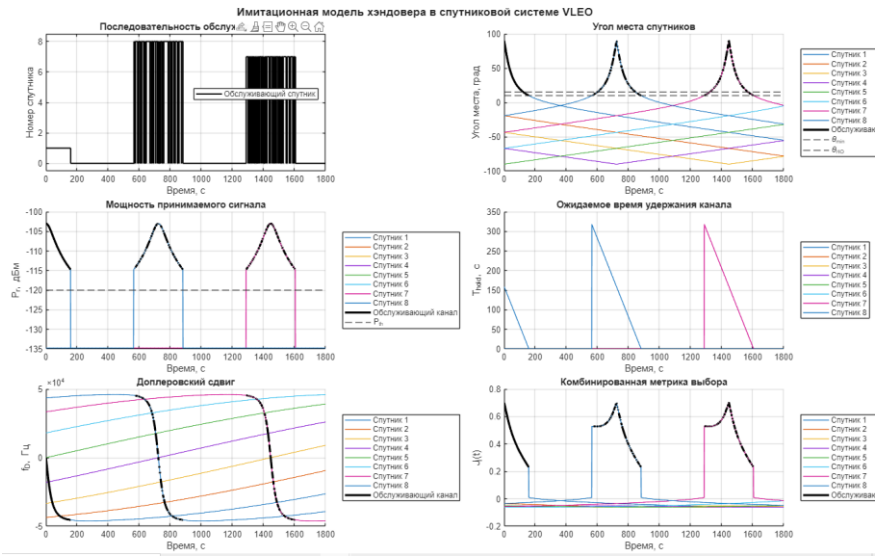


Рис. 2. Результаты выполнения моделирования

Выходными параметрами модели являются момент инициирования хэндовера, число переключений за сеанс связи, длительность удержания канала и интервалы обслуживания каждым спутником. Результаты моделирования показали, что для систем VLEO наибольшую устойчивость обеспечивает многокритериальный выбор целевого спутника. Такой подход снижает частоту неэффективных переключений и лучше соответствует условиям работы негеостационарных спутниковых сетей.

Список используемых источников

1. Crisp N. H., Roberts P. C. E., Livadiotti S. [et al.]. The benefits of very low earth orbit for earth observation missions // Progress in Aerospace Sciences. 2020. Vol. 117. Art. 100619. DOI: 10.1016/j.paerosci.2020.100619.

2. Crisp N. H., Roberts P. C. E., Romano F., Smith K. L., Oiko V. T. A., Sulliotti-Linner V., Hanessian V., Herdrich G. H., García-Almiñana D., Kataria D., Seminari S. System modelling of very low Earth orbit satellites for Earth observation // Acta Astronautica. 2021. Vol. 187. P. 475–491.

3. 3rd Generation Partnership Project (3GPP). Technical Report TR 38.811 V15.1.0 (2019-06). Study on New Radio (NR) to support non-terrestrial networks (Release 15). Sophia Antipolis: 3GPP, 2019.

4. Kodheli O., Lagunas E., Maturo N., Sharma S. K., Shankar B., Montoya J. F. M., Duncan J. C. M., Spano D., Chatzinotas S., Kisseleff S., Querol J., Lei L., Vu T. X., Goussetis G. Satellite Communications in the New Space Era: A Survey and Future Challenges // IEEE Communications Surveys & Tutorials. 2021. Vol. 23/ N 1. P. 70–109. DOI: 10.1109/COMST.2020.3028247.

5. Lee C., Kim T., Jung C., Yoon Z. IoT-NTN with VLEO and LEO Satellite Constellations and LPWAN: A Comparative Study of LoRa, NB-IoT, and Mioty // Electronics. 2025. Vol. 14. N 9. Art. 1798. DOI: 10.3390/electronics14091798.

6. Международный союз электросвязи. Рекомендация МСЭ-R P.531-15. Данные об ионосферном распространении радиоволн и методы прогнозирования, необходимые для проектирования спутниковых сетей и систем. Женева: МСЭ, 2024.

7. Международный союз электросвязи. Рекомендация МСЭ-R P.835-7. Эталонные атмосферы. Женева: МСЭ, 2025. 9 с.

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры БТС СПбГУТ А. А. Прасоловым.

УДК 621.396.96

РОЛЬ МАТЕРИНСКОГО ВЕЙВЛЕТА В ЗАДАЧАХ ОБНАРУЖЕНИЯ ЦЕЛЕЙ В ГИДРОАКУСТИКЕ: ВЫБОР ОПТИМАЛЬНОГО БАЗИСА

Д. Р. Сидоркович (ассистент кафедры РТ СПбГУТ)
С. А. Скобкин (студент гр. РТ-31 СПбГУТ), skobkin.sa@sut.ru

В работе рассматривается проблема выбора материнского вейвлета при решении задач обнаружения целей в гидроакустике. Вейвлет-преобразование, благодаря свойству многомасштабного анализа, является эффективным инструментом для обработки нестационарных гидроакустических сигналов, осложненных шумами, реверберацией и многолучевым распространением. Особое внимание уделяется сравнительному анализу различных вейвлет-базисов (Хаара, Добеши, Symlets, Coiflets, Морле) и критериям их выбора. На основе анализа современных отечественных исследований обосновывается, что оптимальный выбор материнского вейвлета позволяет повысить эффективность обнаружения целей, при этом универсального решения не существует.

материнский вейвлет, гидроакустика, обнаружение целей, вейвлет-преобразование, выбор базиса, интегральный вейвлет-спектр

Введение

Гидроакустические системы сталкиваются с рядом серьезных проблем, влияющих на качество обнаружения целей: шумы различной природы, реверберация, неоднородность водной среды, многолучевое распространение сигналов и переменные профили скорости звука. Как отмечается в [1], итоговый шум движущегося в воде объекта (подводной лодки или надводного судна) состоит из двух компонент: широкополосного шума с непрерывным спектром частот и узкополосного шума, имеющего прерывистый (линейчатый) спектр. В задаче обнаружения вторую составляющую гидроакустического шума считают полезным сигналом на фоне аддитивной помехи [2].

Традиционные методы спектрального анализа, такие как преобразование Фурье, оказываются недостаточно эффективными при обработке нестационарных сигналов, характерных для гидроакустики. Как подчеркивается в [3], «подчеркивается актуальность вейвлет анализа над анализом с применением преобразований Фурье». Вейвлет-преобразование, называемое «математическим микроскопом», позволяет осуществлять многомасштабный анализ сигнала, одновременно отслеживая его временные и частотные характеристики [4].

Ключевую роль в этом преобразовании играет **материнский вейвлет** – базисная функция, путем масштабирования и сдвига которой строится весь базис пространства сигналов [4]. Выбор оптимального материнского вейвлета является критически важным этапом, поскольку различные вейвлеты обладают разными свойствами: симметричностью, гладкостью, длиной носителя, количеством исчезающих моментов.

Теоретические основы вейвлет-анализа гидроакустических сигналов

Непрерывное вейвлет-преобразование (НВП) сигнала x(t) определяется следующим образом [5]:

$$W_x(a,b) = \int_{-\infty}^{\infty} x(t) \frac{1}{\sqrt{|a|}} \psi^* \left(\frac{t-b}{a}\right) dt$$

где a – параметр масштаба, b – параметр сдвига, ψ(t) – материнский вейвлет. Как отмечается в [1], в задаче обнаружения шумовых гидроакустических сигналов на основе интегрального вейвлет-спектра (ИВС) вычисление НВП требует больших вычислительных затрат:

$$K(a_j) = \sum_{k=1}^{N} |W_k(a_j, b_k)| \Delta t$$

где a_j – масштаб, b_k – сдвиг по времени [1].

Для гидроакустики особенно ценными являются следующие свойства вейвлет-преобразования:

1. Локализация в пространстве-масштабе – возможность выделять как кратковременные импульсные помехи, так и протяженные узкополосные сигналы.

2. Устойчивость к шумам – вейвлет-коэффициенты обладают свойством разрежения сигнала, что позволяет эффективно отделять полезную составляющую от шума.

3. Способность выделять дискретные составляющие (ДС) спектра шума – частоты и амплитуды ДС, обусловленные работой энергетической установки и гребных винтов, изменяются со скоростью движения объекта, что важно для идентификации [1].

Сравнительный анализ материнских вейвлетов

Классификация и свойства

В учебном пособии В. Н. Малоземова и С. М. Машарского [6] подробно рассматриваются различные базисы, включая быстрое преобразование Хаара и вейвлетные базисы. В таблице 1 представлены основные типы вейвлетов и их характеристики применительно к гидроакустическим задачам.

Таблица 1. Сравнительная характеристика материнских вейвлетов

Тип вейвлета	Ключевые свойства	Преимущества	Недостатки
Хаар	Простейший, ступенчатый	Максимальная скорость вычислений, обнаружение резких перепадов	Низкая частотная разрешающая способность
Добеши (dbN)	Ортогональный, компактный носитель	Энергия сохраняется, хорошо выделяет гладкие сигнатуры	Асимметрия, возможны фазовые искажения
Symlets (symN)	Улучшенная симметрия	Меньше фазовых искажений, ортогональность	Более высокая вычислительная сложность
Coiflets (coifN)	Высокая симметрия	Высокая точность, хорош для осциллирующих сигналов	Длинные фильтры
Морле	Комплексный, модулированный гауссиан	Выделяет амплитуду и фазу, идеален для анализа гармоник	Неортогональный

Критерии выбора оптимального базиса

Выбор оптимального вейвлета должен основываться на следующих критериях [1; 3]:

1. Соответствие форме сигнала. Вейвлет должен визуально и по свойствам напоминать характерные особенности ожидаемого сигнала цели.

2. Требования к вычислительной эффективности. Как отмечается в [1], «вычисление интегрального вейвлет-спектра... требует больших вычислительных затрат». В реальных системах обработки предпочтение может отдаваться вейвлету Хаара.

3. Характер решаемой задачи. Для обнаружения резких фронтов – Хаар или Добеши; для анализа узкополосных сигналов – Морле; для классификации сложных портретов – Coiflets или Symlets.

Эмпирические результаты и рекомендации

В работе А. А. Хамухина [1] рассматривается применение непрерывного вейвлет-преобразования для обнаружения шумовых гидроакустических сигналов. Отмечается, что основными источниками шумовых гидроакустических сигналов являются: энергетическая установка, гребные винты, вспомогательные механизмы, гидродинамические эффекты [1].

В работе Н. Ю. Гришина [3] рассмотрен алгоритм обработки гидроакустических сигналов в частотной области с использованием вейвлетов. Представлен способ жесткого порога сглаживания коэффициентов и показаны преимущества такого подхода над мягким порогом.

Рекомендации по выбору:

- для быстрых алгоритмов обнаружения в реальном времени – Хаар;
- для общей обработки с балансом качества и скорости – Добеши;
- для высокоточного спектрального анализа и классификации – Symlets или Coiflets;
- для анализа нестационарных колебаний и ЧМ-сигналов – Морле.

Заключение

Роль материнского вейвлета в гидроакустических задачах обнаружения целей является определяющей для успеха последующего анализа. В работе показано, что универсального «лучшего» вейвлета не существует. Выбор оптимального базиса представляет собой задачу, решаемую с учетом типа целевых сигналов (широкополосный шум, дискретные составляющие), уровня шумов, требуемой вычислительной производительности и специфики конечной задачи. Перспективным направлением является разработка адаптивных методов автоматического подбора оптимального материнского вейвлета.

Список используемых источников

1. Хамухин А. А. Применение ячеек однородной структуры в задаче обнаружения шумовых гидроакустических сигналов на основе интегрального вейвлет-спектра // Известия Томского политехнического университета. 2013. Т. 322. № 5. С. 68–72. EDN: QAPYFZ.

2. Хамухин А. А. Применение итерационного алгоритма вейвлет-преобразования для обнаружения узкополосных сигналов // Вестник компьютерных и информационных технологий. 2014. № 8 (122). С. 17–22. DOI: 10.14489/vkit.2014.08. PP.017-022.

3. Гришин Н. Ю. Обработка гидроакустических сигналов с помощью вейвлетов // Инженерный вестник Дона. 2023. № 10. EDN: VOCDHL.

4. Добеши И. Десять лекций по вейвлетам: пер. с англ. М.: РХД, 2004. 464 с. ISBN: 5-93972-285-6.

5. Хамухин А. А. Применение ячеек однородной структуры для вычисления непрерывного вейвлет-преобразования // Известия Томского политехнического университета. 2010. Т. 317. № 5. С. 149–153. EDN: MTFZHJ.

6. Малоземов В. Н., Машарский С. М. Основы дискретного гармонического анализа: учебное пособие. СПб.: Лань, 2021. 301 с. ISBN 978-5-8114-0963-7.

7. Красильников В. А. Звуковые и ультразвуковые волны. М.: Физматгиз, 1960. 572 с.

8. Новиков Л. В. Основы вейвлет-анализа сигналов: учебное пособие. М.: Бином, 2003. 128 с. ISBN: 5-94774-187-8.

9. Шамаев В. Г., Шамаев Н. В. Новые книги по акустике и смежным дисциплинам, изданные в 2008 году на русском языке // Акустический журнал. 2010. Т. 56. № 3. С. 398–428.

Статья представлена заведующим кафедрой РТ, кандидатом физико-математических наук, доцентом К. О. Коровиным.

УДК 621.372.54

ВЛИЯНИЕ ПРЕДЫСКАЖЕНИЯ НА СИГНАЛЫ ПЕРЕДАТЧИКОВ В РАЗЛИЧНЫХ СИСТЕМАХ СВЯЗИ

Д. П. Смирнов (студент гр. РТ-42м СПбГУТ), smirnov.dp@sut.ru

В наше время в радиосвязи активно применяются усилители мощности. Вместе с ними применяются устройства предыскажения (predistortion) как метода линейризации трактов передачи сигналов. В этой статье анализируется влияние цифровых и аналоговых схем предыскажения на энергетическую эффективность, спектральную чистоту и качество обработки сигналов в системах радиосвязи и спутниковой связи.

усилители мощности, аналоговое предыскажение, цифровое предыскажение

Современные системы связи предъявляют противоречивые требования к передатчикам: высокая скорость передачи данных требует использования сложных видов модуляции (OFDM, QAM-256/1024) с высоким пик-фактором (PAPR), в то время как требования к энергоэффективности заставляют использовать усилители мощности (УМ) в режимах, близких к насыщению.

В этой зоне работы усилители проявляют сильные нелинейные свойства, что приводит к следующим негативным эффектам:

1. Спектральная регенерация (спектральное разрастание) – возникновение интермодуляционных искажений, создающих помехи соседним каналам (ACPR).

2. Искажение сигнального созвездия – рост ошибки вектора ошибки (EVM), увеличение коэффициента битовых ошибок (BER).

3. Снижение эффективности – при откате (back-off) мощности КПД усилителя падает с 50 – 70 % до 10 – 20 %.

Предыскажение (Predistortion) является наиболее эффективным методом компенсации этих искажений, позволяя сохранить высокий КПД при обеспечении требований к линейности. Метод основан на внесении в тракт тракта передачи искусственной, «анти-нелинейной» характеристики. Каскад «предыскажитель – усилитель» должен вести себя как линейная система. Существуют 2 вида предыскажения:

1. Аналоговое предыскажение (RF Predistortion) используется в старых системах или в сверхширокополосных каналах, где цифровые методы ограничены скоростью АЦП/ЦАП. Заключается в использовании диодных схем

или транзисторных каскадов, формирующих нелинейность, обратную нелинейности УМ [1, 2].

Преимущества*:* широкая полоса, низкая задержка.

Недостатки*:* низкая точность компенсации, невозможность адаптации к старению компонентов и температурному дрейфу.

2. Цифровое предыскажение (DPD) стандартно для современных систем (4G/5G, Wi-Fi 6/7). Реализуется в цифровой области (обычно в FPGA или ASIC) до ЦАП. Включает нелинейную модель УМ (ряды Вольтерра, GMP, нейросеть), адаптивный алгоритм идентификации (LMS, RLS) и тракт обратной связи (наблюдательный приемник) [3, 4].

Ключевым ограничением DPD является то, что полоса наблюдательного тракта должна в 3–5 раз превышать полосу сигнала (для учета интермодуляционных продуктов 3-го и 5-го порядка).

В наше время активно применяется цифровое предыскажение.

В сотовой связи (4G/5G/6G) в базовых станциях используются архитектуры с широкополосным DPD (до 400 МГц для 5G мм-диапазона).

Главная проблема – память усилителя (memory effects). Из-за квадратурной модуляции и широкой полосы искажения носят частотно-зависимый характер. Используются модели обобщенная полиномиальная модель (GMP), позволяющие учитывать тепловую память и эффекты в цепях смещения.

В спутниковой связи используются специфические типы усилителей: лампа бегущей волны и твердотельные усилители. TWTA имеет фазо-амплитудную конверсию, которая значительно более выражена, чем AM/AM. У твердотельных усилителей при работе с широкополосными сигналами проявляются «эффекты памяти», для борьбы с которыми используются полиномиальные модели DPD Влияние DPD критически важно для спутниковых каналов с одноканальной передачей, где используется модуляция APSK. DPD позволяет увеличить пропускную способность транспондера, работая в точке максимальной выходной мощности (Saturation), что критично для спутников с ограниченным энергетическим бюджетом. DPD используется для компенсации искажений в ретрансляционных системах навигации и связи, включая обработку сигналов в реальном времени на ПЛИС (FPGA).

Проведено моделирование для оценки влияния цифрового предыскажения на сигнал. Проведено сравнение спектров, созвездий и метрик (EVM, ACPR, PAPR) до и после применения цифрового предыскажения (рис 1).

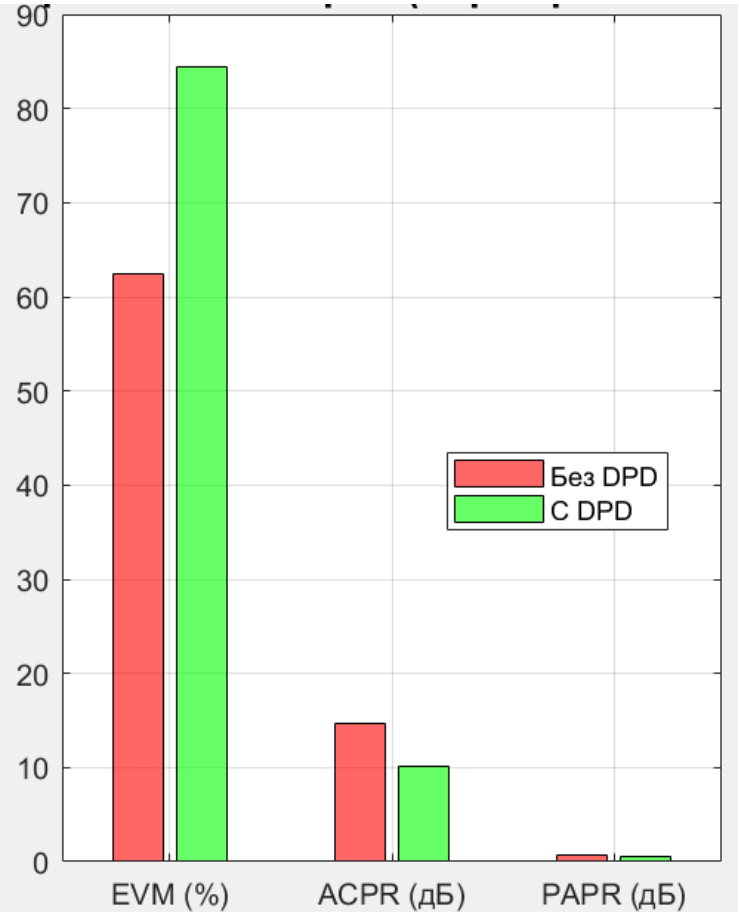


Рис. 1. Зависимость времени передачи от ширины полосы и уровня сигнала

Анализ таблицы 1 подтверждает, что применение DPD улучшает.

ТАБЛИЦА 1. Результаты моделирования

	EVM, %	ACPR, дБ	PAPR, дБ
До DPD	62,5	-14,6	0,66
После DPD	84,38	-10,2	0,60
Улучшение	-21,9	4,4	-0,06

Аналоговое предыскажение сохраняет актуальность для сверхширокополосных (UWB) и аналоговых радиолиний с жесткими ограничениями по задержке и простоте реализации. Цифровое DPD с адаптивными моделями является доминирующим решением для сотовой и спутниковой связи, обеспечивая наилучший компромисс между линейностью, энергоэффективно-

стью и гибкостью. Основным ограничением DPD остается полоса наблюдательного тракта и рост вычислительной сложности при учете эффектов памяти.

Список используемых источников

1. Tikhonov, V. Yu. Comparison of nonlinear distortion compensation methods in power amplifiers / V. Yu. Tikhonov, A. R. Abdipour // Synchroinfo Journal. 2023. Vol. 9. N 5. P. 2-8. DOI 10.36724/2664-066x-2023-9-5-2-8. EDN: FLXEDN.

2. Caoyu Li, Songbai He, Fei You, Jun Peng. Analog Predistorter Averaged Digital Predistortion for Power Amplifiers in Hybrid Beam-Forming Multi-Input Multi-Output Transmitter // IEEE Access DOI 10.1109/ACCESS.2020.3013965.

3. Digital predistortion for RF power amplifiers: State of the art and advanced approaches [Электронный ресурс]. URL: https://www.researchgate.net/publication/261310345_Digital_predistortion_for_RF_power_amplifiers_State_of_the_art_and_advanced_approaches (дата обращения: 13.11.2024).

4. A Generalized Memory Polynomial Model for Digital Predistortion of RF Power Amplifiers [Электронный ресурс]. URL: https://www.researchgate.net/publication/3319867_A_Generalized_Memory_Polynomial_Model_for_Digital_Predistortion_of_RF_Power_Amplifiers (дата обращения 10.03.2026).

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, кандидатом технических наук, доцент А. А. Прасоловым.

УДК 621.396

РАЗРАБОТКА НЕЙРОСЕТЕВОЙ СИСТЕМЫ ПРОГНОЗИРОВАНИЯ ПАРАМЕТРОВ РАСПРОСТРАНЕНИЯ РАДИОСИГНАЛА В УСЛОВИЯХ ПЛОТНОЙ ГОРОДСКОЙ ЗАСТРОЙКИ

А. М. Стрижкина (студент группы РТ-42м СПбГУТ), strizhkina.am@sut.ru

Разработка точных методов прогнозирования распространения радиосигнала в условиях плотной городской застройки является актуальной задачей для развертывания IoT-сетей. В работе проведена разработка и исследование нейросетевой модели на основе полносвязной глубокой нейронной сети прямого распространения для прогнозирования RSSI, Delay Spread и SINR. Предложенная модель демонстрирует высокую точность, средняя абсолютная ошибка составляет 2–3 дБм для RSSI, не более 15 нс для Delay Spread и 2–3 дБ для SINR.

нейросетевое прогнозирование, распространение радиоволн, городская застройка, RSSI, SINR, Delay Spread, полносвязная нейронная сеть

Повышение плотности городской застройки создает значительные трудности при прогнозировании распространения радиоволн, что требует разработки новых подходов. В работе предлагается подход, основанный на использовании глубокой нейронной сети прямого распространения [1], которая обучается на синтетических данных [2], генерируемых с учетом физических закономерностей распространения радиоволн [3, 4], что позволяет прогнозировать уровень принимаемого сигнала (RSSI), разнос задержек (Delay Spread) и отношение сигнал-помеха-шум (SINR) на основе параметров городской застройки.

Входные данные, представленные в таблице 1, представляют собой фиксированный набор из десяти параметров, количественно описывающих городскую среду вокруг точки приема сигнала.

ТАБЛИЦА 1. Параметры моделирования

Параметр	Единицы измерения	Описание
Расстояние 2D	м	дистанция между передатчиком и приемником в горизонтальной плоскости
Расстояние 3D	м	полная пространственная дистанция с учетом разницы высот
Угол места	град.	угол между горизонталью и направлением на приемник

Параметр	Единицы измерения	Описание
Наличие прямой видимости (LoS)	бинарный параметр	наличие беспрепятственного пути
Количество препятствий	шт.	число зданий, пересекающих линию прямой видимости
Плотность застройки в радиусе 50 м	-	отношение площади, занятой зданиями, к общей площади
Плотность застройки в радиусе 100 м	-	
Средняя высота зданий	м	средняя высота сооружений в радиусе 100 метров
Максимальная высота зданий	м	высота самого высокого здания в радиусе 150 м
Разница высот	м	перепад высот между передатчиком и приемником

Для конкретной точки в городе с координатами (x, y, z) относительно базовой станции система автоматически вычисляет все 10 параметров на основе цифровой модели местности (рисунок 1) и передает их на вход нейронной сети для получения прогноза трех ключевых параметров сигнала.

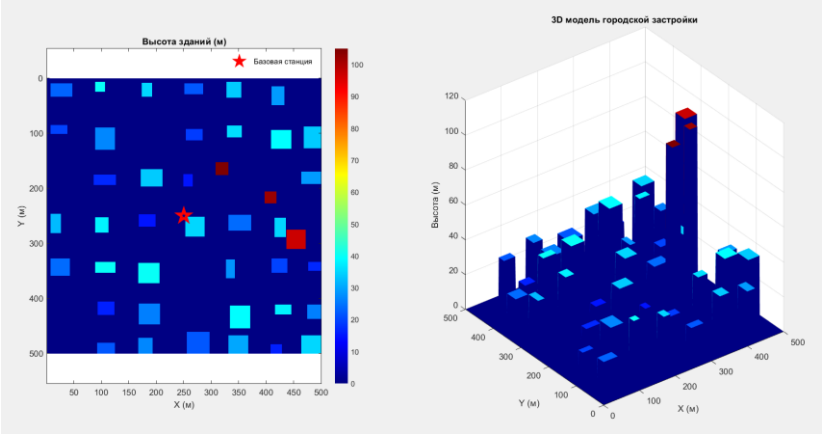


Рис. 1. Цифровая модель местности

В ходе моделирования была проведена серия экспериментов по прогнозированию параметров радиосигнала на частотах 2,4 ГГц и 868 МГц в городской среде с использованием разработанной нейросетевой модели.

Обучение нейронной сети проводилось в течение 100 эпох. На рисунке 2 представлен график изменения функции потерь в процессе обучения.

На начальном этапе, в течение первых 2-3 эпох, наблюдается резкое и практически линейное снижение функции потерь, что свидетельствует о быстром усвоении моделью основных закономерностей в данных. После 5-й эпохи кривая потерь переходит в фазу плавного экспоненциального зату-

хания, где скорость снижения ошибки постепенно уменьшается. К 40 эпохам функция потерь стабилизируется, достигая условного минимума, что указывает на достижение моделью максимально возможной точности при заданной архитектуре и параметрах обучения.

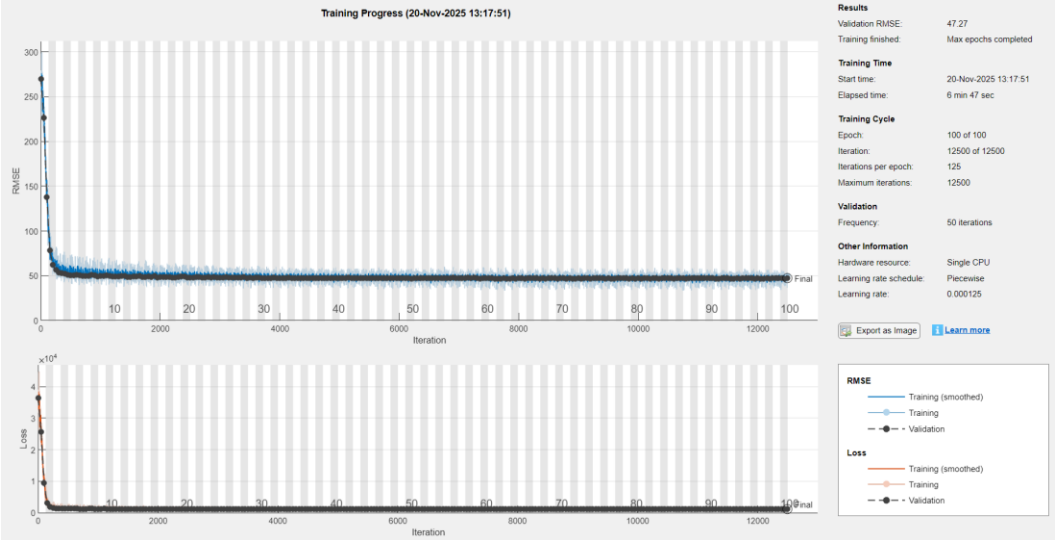


Рис. 2. График изменения функции потерь

Результаты прогнозирования параметров сигнала на рабочей частоте 2,4 ГГц и 868 МГц представлены на рисунках 3 и 4 соответственно.

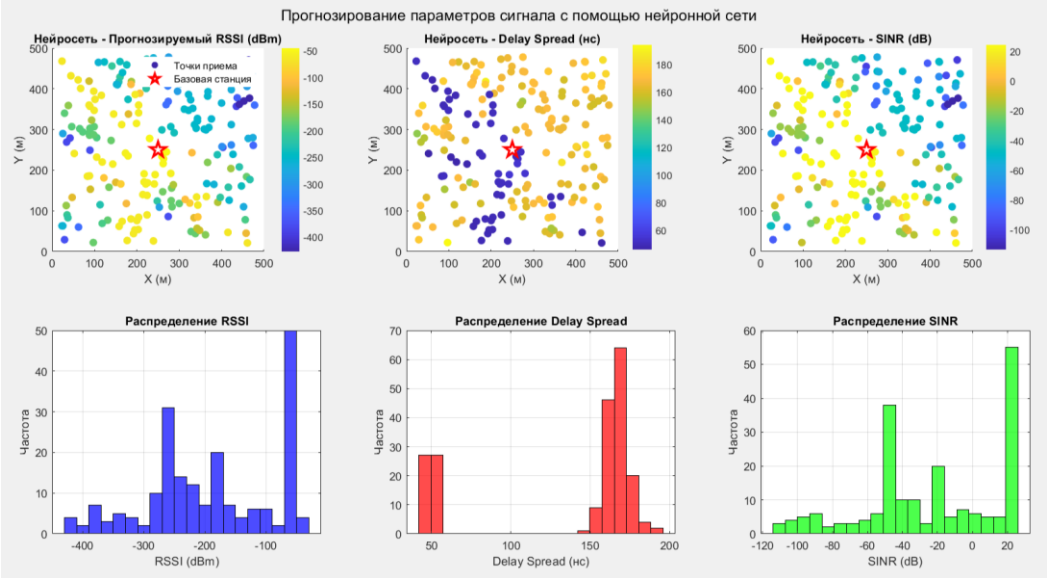


Рис. 3. Прогнозирование параметров сигнала на частоте 2,4 ГГц

Уровень принимаемого сигнала (RSSI) прогнозируется со средней абсолютной ошибкой 2–3 дБм. Вблизи базовой станции (до 100 м) значения составляют от –65 до –75 дБм, на расстоянии 300–400 м в плотной застройке снижаются до –200 дБм. Модель точно предсказывает резкие перепады сигнала из-за затенения высотными зданиями.

Разнос задержек (Delay Spread) прогнозируется с ошибкой не более 15 нс. В районах с плотной многоэтажной застройкой значения достигают около 180 нс, при прямой видимости и малоэтажной застройке составляют 50 – 80 нс.

Отношение сигнал-помеха-шум (SINR) прогнозируется с точностью 2–3 дБ. В центральных районах с высокой интерференцией от 8 до 12 дБ, в периферийных зонах от 20 до 25 дБ.

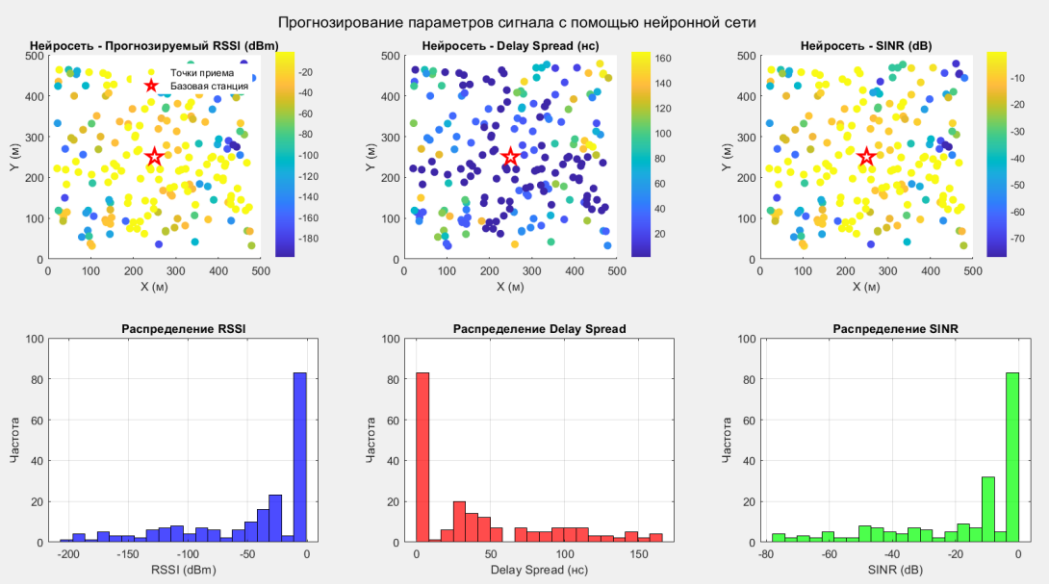


Рис. 4. Прогнозирование параметров сигнала на частоте 868 МГц

При переходе на частоту 868 МГц средние значения RSSI составляют от –20 до –50 дБм, зона уверенного приема расширяется на 40–60 %, а градиент изменения сигнала становится менее резким по сравнению с диапазоном 2,4 ГГц. Значения SINR для большинства точек находятся в диапазоне от 10 до 20 дБ, а Delay Spread снижается до 60 – 90 нс.

Статистические данные по результатам работы модели на частотах 2,4 ГГц и 868 МГц представлены в таблице 2.

ТАБЛИЦА 2. Статистические данные прогнозирования параметров сигнала

Параметр	2,4 ГГц	868 МГц
Средний RSSI, дБм	-190,49	-39,44
Средний Delay Spread, нс	135,55	17,48
Средний SINR, дБ	-23,19	-3,92

Для диапазона 2,4 ГГц характерны крайне низкие показатели: средний RSSI составляет –190,49 дБм, что свидетельствует о критическом затухании сигнала на значительных удалениях от базовой станции. Значение Delay

Spread 135,55 нс указывает на интенсивное многолучевое распространение, а SINR –23,19 дБ отражает высокий уровень интерференции, обусловленный перегруженностью данного частотного диапазона.

Переход на частоту 868 МГц позволяет достичь значительного улучшения всех параметров. Средний RSSI повышается до –39,44 дБм, что является оптимальным показателем для обеспечения устойчивого покрытия. Delay Spread снижается до 17,48 нс, что свидетельствует о минимальном влиянии многолучевости. SINR улучшается до –3,92 дБ, приближаясь к пороговому значению, достаточному для надежного декодирования сигнала.

Результаты экспериментов показали, что предложенная модель демонстрирует высокую точность прогнозирования: средняя абсолютная ошибка для RSSI составляет 2–3 дБм, для Delay Spread – не более 15 нс, для SINR – 2–3 дБ. Нейросетевая система успешно выявляет зоны с различным уровнем сигнала, точно предсказывает резкие перепады, связанные с затенением от высотных зданий, и адекватно оценивает влияние многолучевого распространения и интерференции.

Таким образом, разработанная нейросетевая модель может быть эффективно применена для оптимизации развертывания и управления беспроводными сетями в условиях сложной городской инфраструктуры, а полученные результаты подтверждают целесообразность выбора более низких частот для обеспечения качественного покрытия больших площадей.

Список используемых источников

1. Хайкин С. Нейронные сети: полный курс. М.: Вильямс, 2016. 1104 с.

2. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение. М.: ДМК Пресс, 2018. 652 с.

3. Васудэван М., Юксель М. Машинное обучение для моделирования распространения радиоволн: всесторонний обзор // IEEE Open Journal of the Communications Society. 2024. Т. 5. № 99. С. 5123–5153.

4. ITU-R P.1411-11. Рекомендация МСЭ-R P.1411-11: Прогнозирование распространения радиоволн для систем наземной связи на малых расстояниях. Женева: Международный союз электросвязи, 2021.

Статья представлена научным руководителем, доцентом кафедры РТ СПбГУТ, кандидатом технических наук, доцентом О. А. Симониной.

УДК 621.39

АДАПТИВНОЕ УПРАВЛЕНИЕ ВЫСОКОПЛОТНЫМИ СЕТЯМИ WI-FI НА ОСНОВЕ СЕТЕЙ ПЕТРИ

М. И. Хечуев (студент гр. РТ-42м СПбГУТ), hechuev.mi@sut.ru

Предложен метод адаптивного управления высокоплотными сетями Wi-Fi на основе математического аппарата сетей Петри. Формализованы параметры сети, учитывающие внешние воздействия и ограничения для минимизации интерференции. Проведено моделирование высокоплотной сети Wi-Fi на языке программирования Python, в котором продемонстрировано увеличение пропускной способности сети в часы пиковой нагрузки на 52 % для наиболее загруженных точек доступа и на 35 % для точек доступа средней загруженности.

адаптивное управление, Wi-Fi, сети Петри

В целях развития возможностей сетей Wi-Fi, происходит регулярное внедрение новых технологий в современные версии стандарта IEEE 802.11, нацеленных на улучшение качественных показателей, таких как: увеличение пропускной способности, совершенствование методов доступа к среде, улучшение параметров физического уровня. На основе новейших версий стандарта выпускается новое сетевое оборудование, которое, теоретически, необходимо регулярно обновлять, в целях достижения наилучших показателей работы сети, но это не всегда представляется возможным. В качестве препятствующих факторов можно выделить экономический и юридический. Исходя из этого, следует уделять внимание совершенствованию методов планирования и управления сетями, в рамках доступного оборудования.

В области планирования сетей Wi-Fi основным является статичное планирование, с фиксированными параметрами. Такой подход сохраняет свою эффективность для зон с легкопрогнозируемой пользовательской нагрузкой, но может быть неэффективен в динамических средах. В связи с этим возникает необходимость перехода к адаптивным методам управления, способным реагировать на изменение условий работы сети.

В рамках данной статьи предложен подход к адаптивному управлению структурой высокоплотных сетей Wi-Fi на основе математического аппарата сетей Петри, позволяющий повысить эффективность утилизации ресурсов сети в условиях неопределенности и переменной нагрузки.

Сети Петри представляют собой математический аппарат, предназначенный для моделирования систем с большим количеством параметров, это

наглядная и хорошо формализованная модель поведения параллельных систем с асинхронным воздействием [1]. За основу предложенного механизма адаптивного управления параметрами сетей Wi-Fi высокой плотности была взята интерпретация алгоритма сетей Петри из работы [2]. Любая сеть Wi-Fi может быть интерпретирована как система взаимодействующих сущностей, таких как точки доступа, клиентов и среда распространения сигнала.

Для математического описания алгоритма адаптивного управления высокоплотными сетями Wi-Fi, был сформулирован набор параметров, характеризующий статические и динамические свойства сети. Модель работы такой сети описывается выражением

$$C = (M, US),$$

где *M* – это маркированная стохастическая сеть Петри с событийными дугами, а *US* – управляющий вектор. Маркированная сеть Петри *M* задается как

$$M = (T, P, G, O, MB, MVT, VZS, PIG, \mu).$$

Множество переходов *T* представляет собой множество стохастических подсистем моделируемой сети Wi-Fi. В представленной интерпретации переходы условно разделены на три подмножества: переходы, соответствующие точкам доступа $T_{\text{тд}}$ и переходы $T_{\text{ку}}$, соответствующие клиентским устройствам.

Точка доступа характеризуется пропускной способностью *C*, количеством подключенных клиентов n, загрузкой p. Эти параметры позволяют сформулировать множество моделей *MB,* описывающее поведение каждой точки доступа в сети как системы массового обслуживания:

$$MB = f(C_i, p_i, n_i).$$

Множество позиций *P* представляет собой множество наборов элементов системы, соответствующих качественным показателям системы

$$P = \{p_1, p_2, \dots, p_n\},$$

которые можно интерпретировать как состояние частотных каналов и статус подключения клиентов. Значение маркера $\mu(p_n)$ в позиции p_n кодирует количественную характеристику состояния.

Входная функция *G* определяет множество наборов входов элементов системы из переходов *T в* комплекты позиций *P.* В свою очередь, выходная

функция *O* определяет множество наборов выходов, это необходимо для обновления состояния системы. Таким образом, представленные функции можно выразить как

$$G: T \to 2^P$$
$$O: T \to 2^P.$$

Матрица значений координат MVT (Matrix of values of phase coordinates) подразумевается, как информация о состоянии элементов сети за итерацию моделирования. Для каждой точки доступа фиксируется нагрузка, количество подключенных клиентов, а для клиента фиксируется пропускная способность. Использование этой матрицы позволяет сформировать «оценку» состояния системы, которая может быть использована для прогнозирования и планирования дальнейшей работы. На основе *MVT* вычисляются величины средних квадратических отклонений

$$\sigma(Y,t) = \sqrt{\frac{1}{\tau}\sum_{k=1}^{\tau}\left(Y_i(t_k) - Y_i(t)\right)^2},$$

которые используются в качестве критериев оптимальности, при формировании следующего состояния системы.

Вектор внешних сигналов VZS (Vector of External Signals) задает группу воздействий, которые не контролируются системой управления. Применительно к сетям Wi-Fi высокой плотности можно выделить следующие неконтролируемые воздействия: уровень фонового шума *N* и количество активных клиентов сети. Количество клиентов определяется суточной активностью и напрямую зависит от специфики местности, на которой развернута сеть *Wi-Fi*. В представленном варианте адаптивного управления используется регрессионная модель с учетом суточной периодичности

$$V(t_1) = Acos\left(\frac{2\pi}{T}\right) + Bcos\left(\frac{2\pi}{T}\right) + \varepsilon(t),$$

для оценки параметров *A и B* за интервал времени t_1 используется метод наименьших квадратов [3], за счет этого прогнозируется значение $V(t_2)$, что необходимо для дальнейшей адаптации параметров сети.

Основой событийной логики является матрица разрешения передачи PIG (Permission Information Matrix). Каждый элемент матрицы обозначается как pig_{ij} и содержит информацию о возможности передачи от *i*-того перехода к *j*-тому переходу, в рамках предложенной системы адаптивного управления сетью Wi-Fi это означает, что клиентское устройство *i* ассоции-

ровано с точкой доступа j. Управление структурой сети осуществляется посредством управляющего вектора US, при этом, во избежание одновременного подключения одного клиента к нескольким точкам доступа было введено ограничение, задающегося выражением

$$\forall j \in T_{\text{тд}},$$
$$\sum_{i \in T_{\text{ку}}} pig_{ij} \leq 1$$

Для точек доступа было задано ограничение в целях борьбы с интерференцией между соседними точками доступа. Влияние на результирующую матрицу PIG выражается как маркер состояния

$$state_j \leq 1$$

$$\text{при } | ch_j - ch_{j^`} | < \Delta f_{th},$$

где ch_j – это частотный канал точки доступа j, а Δf_{th} – это порог, при котором каналы будут считаться подверженными интерференции.

Также было создано графическое представление механизма адаптивного управления высокоплотными сетями Wi-Fi на основе сетей Петри (рисунок 1).

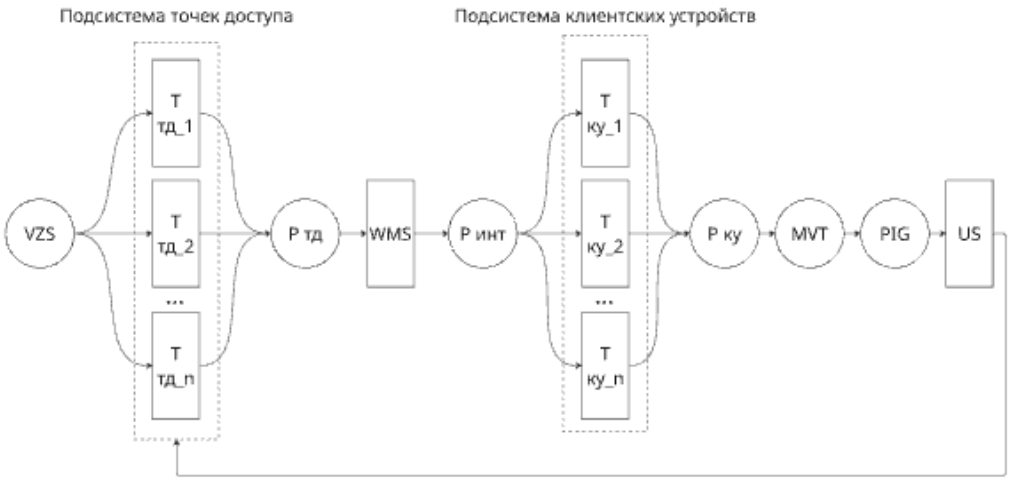


Рис. 1. Механизм адаптивного управления сетью *Wi-Fi* на основе сети Петри

Такой подход к архитектуре адаптивного управления высокоплотных сетей Wi-Fi открывает широкие возможности по интеграции этого метода в качестве основы для создания программного обеспечения по планированию сетей такого типа.

В целях тестирования работы механизма адаптивного управления сетью Wi-Fi было проведено моделирование, где в качестве исследуемого параметра была выбрана пропускная способность доступная пользователю, в зависимости от времени, в которое использовалась сеть. Моделирование было произведено на языке программирования Python [4], с использованием библиотеки для построения графиков matplotlib [5]. В качестве объекта исследования была смоделирована сеть Wi-Fi из 9 точек доступа, для 100 клиентских устройств. На рисунке 2 изображены результаты моделирования предложенного механизма адаптивного управления. Девять графиков представляют собой значения пропускной способности, доступной клиенту, который подключен к одной из девяти точек доступа в определенный момент времени работы сети.

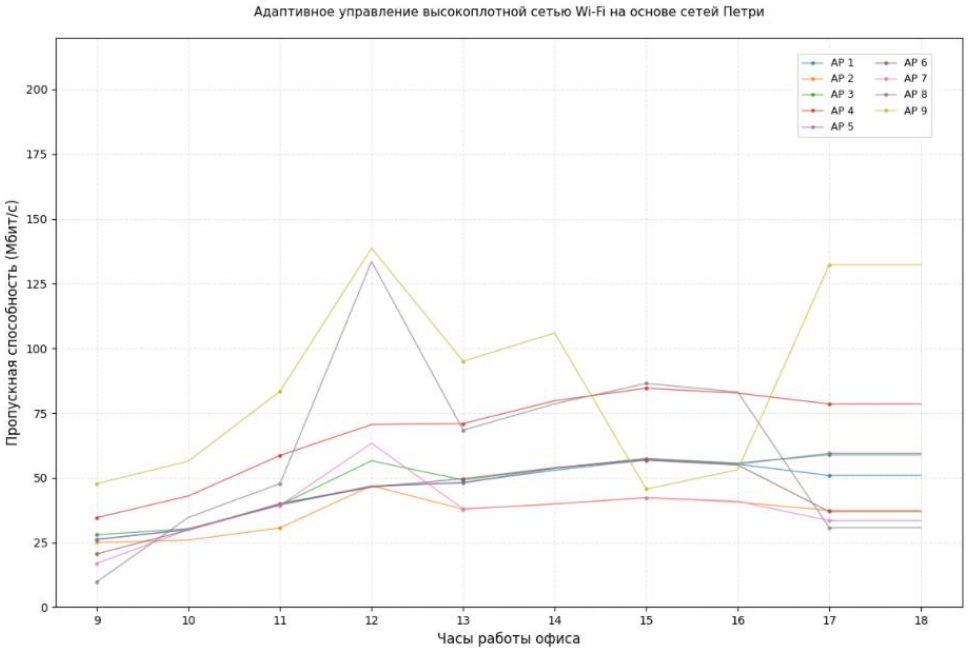


Рис. 2. Результаты моделирования значения пропускной способности сети, на основе адаптивного управления

На рисунке 2 видно, что в пиковые часы загрузки (с 11:00 до 13:00) пропускная способность каждой точки доступа увеличивается на 52 % для наиболее загруженных точек доступа (*AP* 8 и *AP* 9), для менее загруженных точек доступа (*AP* 1-7) прирост пропускной способности составил 35 %, счет прогнозирования состояния сети, таким образом обеспечивая улучшение показателя в моменты загруженности.

Предложенный в рамках данной статьи механизм адаптивного управления сетями Wi-Fi высокой плотности может быть использован при разработке программного обеспечения по планированию сетей Wi-Fi. Математический аппарат сетей Петри позволяет создать динамическую симуляцию

сети. Следует отметить, что предложенное решение сохраняет модульную структуру и может быть расширено с использованием большего количества подсистем.

Список используемых источников

1. Проститенко О. В. Моделирование дискретных систем на основе сетей Петри: учебное пособие / О. В. Проститенко, В. И. Халимон, А. Ю. Рогов. СПб.: СПбГТИ(ТУ), 2017. 69 с.

2. Качур С. А. Адаптивное управление структурой сложных стохастических систем на основе сетей Петри // Радиоэлектроника и информатика. 2005. № 4.

3. Сочнев А. Н. Представление возмущающих воздействий в имитационных моделях производства на основе сетей Петри // Вестник ВГТУ. 2011. № 8.

4. Python Software Foundation. Python Language Reference, version 3.x [Электронный ресурс]. URL: python.org (дата обращения: 25.03.2026).

5. User guide // matplotlib URL: https://matplotlib.org (дата обращения: 27.03.2026).

Статья представлена научным руководителем, кандидатом технических наук, доцентом О. А. Симониной.

УДК 654.937

РЕАЛИЗАЦИЯ СИСТЕМЫ БЕСПРОВОДНОЙ СВЯЗИ ПОДВИЖНОГО ОБЪЕКТА НА ОСНОВЕ СТАНДАРТА BLUETOOTH

Ю. В. Шарихина (к.ф.-м.н., доцент, доцент кафедры физики СПбГУТ)
Л. А. Шувалов (студент гр. ИКТ-2562 СПбГУТ), shuvalov.la@sut.ru

В современном мире, где технологический прогресс играет ключевую роль в нашей повседневной жизни, вопросы беспроводной связи становятся более актуальными и значимыми. В этом контексте, реализация системы беспроводной связи для подвижных объектов на основе стандарта Bluetooth представляет собой важное направление разработки. Эта тема не только отражает стремительные изменения в области информационных технологий, но и подчеркивает потенциал технологии Bluetooth в обеспечении надежной и эффективной связи для подвижных устройств. В данной работе спроектирована система беспроводной связи для подвижного объекта на базе Bluetooth и контроллера Arduino Uno.

Bluetooth, связь с подвижным объектом, Arduino, C++, 2-Turn NLoS

Модель распространения радиоволн для метода 2-Turn NLoS одинаковым образом учитывает оба оконечных радиоустройства на обоих концах. С точки зрения модели не имеет значения, какой терминал является передатчиком, а какой – приемником. В связи с этим используют термины «станция 1» и «станция 2», обозначающие терминалы в начале и конце трассы распространения радиосигнала соответственно [1, 2].

2-Turn NLoS – это преобладающий тип трассы в условиях городской зоны многоэтажной застройки для всех типов сот. Он часто встречается в микро- и пикосотах городской зоны плотной застройки в условиях городской зоны малоэтажной застройки. Определение всех параметров для случая 2-Turn NLoS требует двумерного анализа зоны вокруг подвижного терминала [3] (рис. 1).

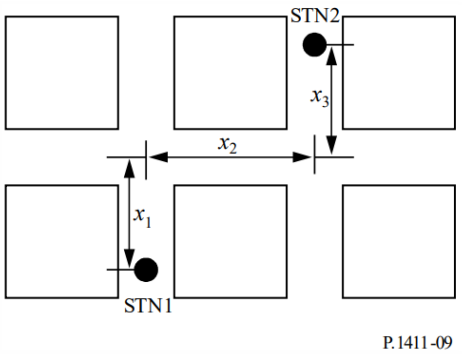


Рис. 1. Определение расстояния между станциями 1 и 2 для случая 2-Turn NLoS

Соответствующие параметры для этой ситуации представлены в таблице 1.

ТАБЛИЦА 1. Параметры для случая NLoS2

Обозначение	Параметр
x_1	расстояние от станции 1 до перекрестка (м)
x_2	расстояние от станции 2 до перекрестка (м)
x_3	расстояние от станции 3 до перекрестка (м)

Разработка системы беспроводного управления мобильным объектом.

Схема устройства

На рисунке 2 представлена функциональная схема устройства

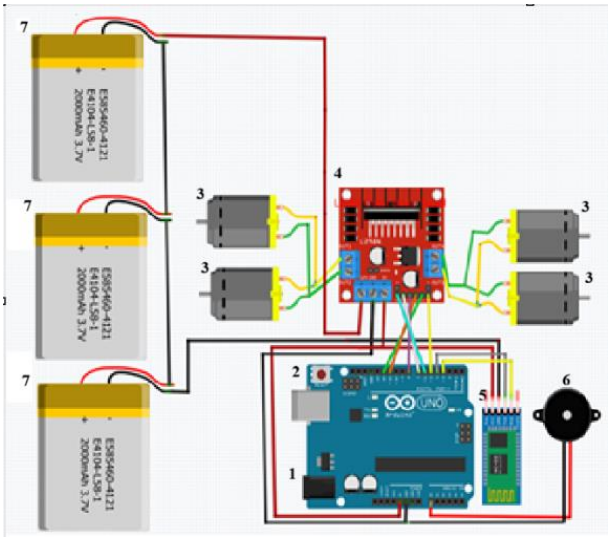


Рис. 2. Функциональная схема устройства

Компоненты устройства перечислены и пронумерованы в таблице 2.

ТАБЛИЦА 2. Перечень компонентов

№	Компонент	Количество, шт
1	Контроллер Arduino Uno	1
2	Плата Arduino Sensor Shield V5.0	1
3	DC моторы	4
4	Драйвер L298N	1
5	Bluetooth-модуль HC-06	1
6	Пьезо-пищалка	1
7	Аккумулятор Li-ion 18650 2000 мАч 3.7 В	3

Программная реализация подвижного объекта

Прием команд осуществляется с помощью Bluetooth терминала. В нашем случае это Bluetooth RC Controller. Это линейно-ориентированное приложение терминала/консоли для микроконтроллеров, Arduino и других устройств с последовательным интерфейсом/UART, подключенным с помощью преобразователя Bluetooth в serial к устройству Android [5].

Испытания подвижного объекта

Предварительные расчеты

Для линии 2-Turn NLoS можно задавать несколько маршрутов распространения. усиление по мощности принимаемого сигнала (от станции 1 до станции 2) рассчитывают с учетом всех маршрутов 2-Turn. [4]

Основные потери передачи между станцией 1 и станцией 2 рассчитывают по формуле:

$$L_{2-Turn} = L_{Los} + 10\log_{10}\frac{x_1 *, x_2, * x_3}{x_1 + x_2 + x_3} - 20\log_{10} S_1 - 20\log_{10} S_2$$

$$L_{Los} - \text{потери на всем расстоянии } 115 \text{ м}$$

S_1, S_2 – Параметр рассеяния/дифракции для поворота в первой и второй угловой точке (Дб)

$$L_{LoS} = L_S + 6 + 30\log_{10}\left(\frac{d}{R_s}\right) = 60 + 30\log_{10}\left(\frac{115}{20}\right) = 82 \text{ дБ}$$

Основные потери передачи:

$$L_S = |20\log_{10}\left(\frac{\lambda}{2\pi R_s}\right)| = 20\log_{10}\left(\frac{0{,}12}{2\pi * 20}\right) = 60 \text{ дБ}$$

$R_s -$ эталлонное расстояние (20 м), $\lambda -$ длина волны при $f =$ 2.4 ГГц (м).

Расстояние: $d = x_1 + x_2 + x_3 = 50 + 35 + 30 = 115$ м.

Параметр рассеяния/дифракции для поворота в первой угловой точке:

$$S_1 = (3{,}45 * 10^4) * f^{-0.46} = 1{,}06.$$

Параметр воздействия для поворота во второй угловой точке:

$$S_2 = 0{,}54 * f^{0.046} = 2.91.$$

Таким образом, основные потери передачи между станцией 1 и 2:

$$L_{2-Turn} = L_{LoS} + 10\log_{10}\frac{x_1*x_2*x_3}{x_1+x_2+x_3} - 20\log_{10} S_1 - 20\log_{10} S_1 = 98 \text{ дБ}.$$

Методика испытаний

Подвижный объект подвергается следующим испытаниям:

- испытания опытного образца машинки с целью проверки соответствия заявленным требованиям Bluetooth модуля hc-06;
- испытания заявленного функционала машинки.

Средства испытания:

- мобильной телефон на базе OS (IOS или Android) с наличием модуля Bluetooth;
- ПО «Bluetooth RC Controller»;
- ПО «Bluetooth Scanner».

Результаты испытаний

Результаты испытаний занесены в таблице 3 и 4.

ТАБЛИЦА 3. Полученные результаты

Цели испытаний	Метод испытаний	Заявленные характеристики и функционал	Полученные характеристики и функционал
Испытания опытного образца машинки с целью проверки соответствия заявленным требованиям Bluetooth модуля hc-06;	Расположить на открытом участке местности с прямой видимостью машинку на удаленности 10, 20, 30 метров от источника сигнала. С помощью ПО «Bluetooth Scanner» определить скорость передачи данных. Измерения проведены 10 раз для каждой точки удаленности от источника сигнала. Результат испытаний рассчитан по формуле: $v_{\text{ср}=\frac{v_1+v_n}{n}}$ где n – количество измерений	Дальность связи до 30 м; Скорость передачи данных от 1 кбит/ с до 1.1 Мбит/с.	Максимальная дальность связи 35 м; Скорость передачи данных до 1 Мбит/с.

Таблица 4. Измеренные характеристики

Расстояние от источника сигнала до объекта	Скорость передачи данных по Bluetooth	Среднее значение скорости передачи данных по Bluetooth
10 метров	0,97 мбит/с	0,96 мбит/с
	1,00 мбит/с	
	0,91 мбит/с	
	0,89 мбит/с	
	1,05 мбит/с	
	0,9 мбит/с	
	1,01 мбит/с	
	1,00 мбит/с	
	0,92 мбит/с	
	0,94 мбит/с	
20 метров	0,80 мбит/с	0,74 мбит/с
	0,85 мбит/с	
	0,76 мбит/с	
	0,70 мбит/с	
	0,72 мбит/с	
	0,63 мбит/с	
	0,64 мбит/с	
	0,68 мбит/с	
	0,80 мбит/с	
	0,78 мбит/с	
30 метров	0,5 мбит/с	0,47 мбит/с
	0,42 мбит/с	
	0,62 мбит/с	
	0,64 мбит/с	
	0,47 мбит/с	
	0,53 мбит/с	
	0,51 мбит/с	
	0,42 мбит/с	
	0,30 мбит/с	
	0,32 мбит/с	

Список используемых источников

1. Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. М.: Издательский дом «Вильямс», 2021.

2. BLUETOOTH SPECIFICATION Version 2.0 + EDR. http://www.bluetooth.com (дата обращения 10.03.2026).

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение, 2-е издание.: Пер. с англ. М.: Издательский дом «Вильямс», 2020.

4. Феер К. Беспроводная цифровая связь. М.: «Радио и связь», 2018. 11 с.

5. Корендясев А. И., Саламандра Б. Л., Тывес Л. И. Теоретические основы робототехники. В 2 кн. Институт машиноведения им. А. А. Благонравова РАН. М.: Наука, 2006. Кн. 1, 468 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

УДК 004.932.2

АРХИТЕКТУРА RESNET18 КАК ОСНОВА ДЛЯ ГИБРИДНЫХ ДЕТЕКТОРОВ ДИПФЕЙКОВ: ОБОБЩАЮЩАЯ СПОСОБНОСТЬ И МЕТОДЫ АДАПТАЦИИ

А. И. Абакарова (студент группы ИСТ-223 СПбГУТ) abakarova.ai@sut.ru

Рост доступности технологий синтеза изображений лиц требует разработки эффективных методов их детектирования. В работе рассматривается архитектура ResNet18 как основа для построения гибридных классификаторов, сочетающих пространственный и частотный анализ; обсуждаются методы адаптации предобученной модели, включая замену классификационного слоя и применение механизмов внимания. Анализ последних исследований подтверждает высокую эффективность предложенного подхода, достигающего точности до 99 % при сохранении устойчивости к новым типам подделок.

дипфейк, ResNet18, сверточные нейронные сети, трансферное обучение, гибридные детекторы, частотный анализ, обобщающая способность

Современные генеративные модели – в частности, генеративно-состязательные сети и диффузионные архитектуры – достигли уровня реалистичности синтезированных изображений, при котором визуальное различение подлинных и поддельных фотографий человеческих лиц становится затруднительным даже для подготовленного наблюдателя [1]. Данный факт создает серьезные угрозы в области информационной безопасности: дипфейки активно применяются для мошенничества, манипуляции общественным мнением, создания компрометирующих материалов и обхода биометрических систем защиты [2]. В связи с этим разработка надежных и быстрых автоматических детекторов синтезированных изображений является одной из актуальных задач компьютерного зрения.

Среди множества нейросетевых архитектур, используемых для обнаружения дипфейков, значительное место занимают сверточные нейронные сети семейства ResNet, что расшифровывается как Residual Network. Ключевая особенность ResNet – остаточные связи, называемые также skip connections, которые позволяют эффективно обучать глубокие модели, решая проблему исчезающего градиента. Архитектура ResNet18, как наиболее легкая среди практических версий данного семейства, содержит около 11,7 миллиона параметров. Этого объема, как показывают многочисленные эксперименты, достаточно для выделения сложных текстурных и структурных признаков, но при этом модель не требует чрезмерных вычислительных ресурсов – в отличие от более глубоких вариантов, например ResNet50, имеющей 25,6 миллиона параметров. В исследованиях неоднократно отмечалось, что именно ResNet18 обеспечивает наилучший компромисс между точностью классификации и скоростью работы, особенно в задачах, где важна возможность развертывания на ограниченном оборудовании [3].

Обычно практикуется использование модели ResNet18, предварительно обученной на крупномасштабном наборе данных ImageNet, который содержит более миллиона изображений, распределенных по 1000 классов. Такой подход получил название трансферного обучения, или transfer learning. Суть его в том, что сеть уже научилась выделять универсальные визуальные признаки – края, углы, текстуры, формы объектов – и эти знания могут быть перенесены на решаемую задачу бинарной классификации, где требуется отличить подлинное изображение от синтезированного [4]. Для адаптации модели достаточно заменить ее финальный полносвязный слой, ранее выдававший вероятности для 1000 классов, на новый линейный слой с двумя выходами. После этой замены модель дообучается на датасете дипфейков. При правильном выборе гиперпараметров, а именно скорости обучения, размера батча и типа оптимизатора, а также при достаточном объеме размеченных данных такая адаптированная сеть, как следует из публикаций, демонстрирует высокую точность на тестовых выборках – до 94–97 процентов [5].

Однако прямое применение стандартной процедуры трансферного обучения без дополнительных мер часто приводит к тому, что детектор хорошо работает только на тех типах дипфейков, которые присутствовали в обучающей выборке, и значительно теряет в точности при появлении подделок, созданных иными генеративными алгоритмами. Данное явление в литера-

туре получило название доменного сдвига, или domain shift. Причина кроется в том, что разные генераторы, например StyleGAN, ProGAN или диффузионные модели, оставляют различные артефакты: одни создают характерные частотные аномалии, другие – искажения в текстуре кожи или нереалистичные отражения в глазах. Модель, обученная на одном наборе артефактов, не обобщает свои знания на другие.

Для преодоления этого ограничения исследователями предлагаются гибридные архитектуры, в которых ResNet18 выступает не как изолированный классификатор, а как один из компонентов более сложной системы. Один из распространенных подходов – двухпоточная нейронная сеть. Первый поток, построенный на базе ResNet18, обрабатывает исходное изображение в пространственной области, выделяя такие признаки, как нарушения симметрии лица, аномалии освещения, несоответствия в текстуре волос и кожи. Второй поток – обычно более легкая сверточная сеть – работает с частотным представлением того же изображения, полученным, например, с помощью дискретного косинусного преобразования или быстрого преобразования Фурье. В частотной области артефакты, порожденные генеративными моделями, часто проявляются в виде повторяющихся пиков или нехарактерного распределения энергии по высоким частотам. Такие аномалии, подчеркнем, трудно заметить визуально, но нейронная сеть способна их надежно детектировать.

Эксперименты показывают, что двухпоточные гибридные системы, где один поток представлен ResNet18, достигают точности до 99 процентов на стандартных тестовых наборах. Что еще более важно, они демонстрируют лучшую устойчивость к доменному сдвигу по сравнению с однопоточными моделями. Механизмы внимания, например кросс-внимание между пространственным и частотным потоками, тоже повышают обобщающую способность. А еще методы интерпретации вроде Grad-CAM показывают, какие участки изображения повлияли на решение модели [4].

Для обучения устойчивых детекторов важна аугментация данных. К обучающим изображениям применяют случайные отражения по горизонтали на 0.5, небольшие повороты на 10–15 градусов, меняют яркость, контрастность и насыщенность. Так имитируется естественная вариативность входных данных и снижается риск переобучения. Если размеченных данных мало, используют заморозку базовых слоев (freeze_backbone). Веса всех сверточных слоев, кроме финального классификатора, остаются неизмен-

ными – обновляется только новый слой. Это помогает избежать катастрофического забывания и сохранить признаки, полученные при предобучении на ImageNet. Такое убедительно показано в работах [4; 5].

Проблема доменного сдвига до конца не решена. В недавних публикациях предлагают разные стратегии адаптации детекторов под новые типы дипфейков. Одна из них – мета-обучение: модель обучают на множестве задач, где каждая задача соответствует одному генератору, а потом она быстро подстраивается под новый генератор за несколько шагов градиентного спуска. Другой подход – ансамбли моделей: каждый классификатор обучается на своем подмножестве данных, итоговое решение принимается голосованием или усреднением вероятностей.

Еще одно перспективное направление – облегченные версии детекторов на базе ResNet18 для мобильных устройств и встраиваемых систем. Это достигается квантизацией (переход с 32-битных на 8-битные веса) и дистилляцией знаний – компактная студенческая сеть учится имитировать выходы более крупной и точной учительской сети. Правда, такие методы ведут к некоторой потере точности. Вопрос, какое сжатие минимально допустимо без серьезного ухудшения качества, пока остается открытым.

Итак, ResNet18 сама по себе не универсальный детектор любых дипфейков. Но ее предсказуемость, умеренная вычислительная сложность и хорошее извлечение пространственных признаков делают эту сеть удобным базовым блоком для гибридных и адаптивных детекторов. Наиболее эффективные современные системы сочетают ResNet18 с частотным анализом, механизмами внимания и мета-обучением. Дальнейшее развитие, скорее всего, пойдет по пути углубления такой интеграции и создания методов быстрой донастройки под новые генеративные модели без полного переобучения.

Список используемых источников

1. Загурский Я. Д., Когут С. Н. Deepfake и способы его распознавания // Молодой ученый. 2025. № 49 (600). С. 315–319. URL: https://moluch.ru/archive/600/ (дата обращения: 28.03.2026).

2. Дворецкая П. С. Эволюция подходов к созданию дипфейк-изображений и видео // Молодой ученый. 2025. № 50 (601). С. 1–4. URL: https://moluch.ru/archive/601/ (дата обращения: 29.03.2026).

3. Алпатов А. Н., Терлоев Э. З., Матчин В. Т. Архитектура трехмерной сверточной нейронной сети для детектирования факта фальсификации видеоряда // Информационные технологии и вычислительные системы. 2024. № 3. С. 45–57. URL: https://www.elibrary.ru/ item.asp?id=72626019 (дата обращения: 29.03.2026).

4. Румянцева М. С. Разработка и исследование алгоритма обнаружения дипфейков с использованием двухпоточной нейронной сети и частотного анализа // Научные труды

МИЭТ. 2025. № 2 (78). С. 112–121. URL: https://www.elibrary.ru /item.asp?id=82426924 (дата обращения: 30.03.2026).

5. Мирзоев А. З., Якубов А. З. Методы глубокого обучения в задаче распознавания фейковых изображений и видео // Вестник Дагестанского государственного университета. 2025. Т. 40. № 3. С. 66–71/ URL: https://www.elibrary.ru /item.asp?id=85562651 (дата обращения: 30.03.2026).

Статья представлена научным руководителем, доцентом кафедры СОД СПбГУТ, кандидатом технических наук В. А. Медведевым.

УДК 004.8

ПЕРСПЕКТИВЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОГРАММИРОВАНИИ

Б. А. Аль-Нами (доцент кафедры ИКД СПбГУТ)
И. М. Стародубцев (студент группы ИСТ-421 СПбГУТ),
starodubtsev.im@sut.ru

В статье анализируется влияние искусственного интеллекта на сферу программирования в контексте его стремительного развития и популяризации. На основе данных itWeek и опроса Stack Overflow за 2025 год (78 % разработчиков используют ИИ) автор рассматривает ключевые преимущества нейросетей: высокую скорость генерации кода, отсутствие усталости и масштабируемость. Особое внимание уделяется недостаткам, включая ненадежность генерируемого кода, необходимость ручной отладки, проблему «галлюцинаций» и парадоксальное негативное влияние на рынок труда (сокращение числа неопытных специалистов и риск кадрового голода).

искусственный интеллект, программная инженерия, генерация кода, интент-формализация, промпт-инжиниринг, ИИ-галлюцинация

Последние годы в сфере IT отметились взрывным ростом возможностей нейросетей, который, в свою очередь, привел к их популяризации и широкому применению в самых разнообразных сферах – в повседневно-бытовой, развлекательной, профессиональной.

В общем смысле ИИ – это набор инструментов, позволяющий решать задачи, в которых требуется уровень мышления, сопоставимый с человеческим (например, те, что подразумевают обучение, сбор информации, ее преобразование и компиляцию). Его развитие и использование в программировании изначально подстегнула нехватка специалистов – как квалифицированных, для выполнения сложных задач и разработки инновационных решений, так и низкого уровня, для выполнения повторяющихся, паттернизированных задач. Результатом стало возникновение множества различных нейросетевых инструментов, в массе представляющих собой большие языковые модели (БЯМ; англ. large language model, LLM), то есть модели, проходящие самообучение на массивах неразмеченного текста.

Прежде чем говорить о перспективах применения искусственного интеллекта в программировании в будущем, стоит оценить его успешность и целесообразность в настоящем, выделить аспекты, в которых ИИ уже успел показать себя на уровне, соответствующем требованиям, а также его недостатки, систематически возникающие проблемы и методы их решения.

По данным издания itWeek, сейчас в компании МТС нейросети пишут 8 % кода, а к 2027 году планируется, что это количество вырастет до 25 %, то есть четверти от общего массива [1], а опрос Stack Overflow за 2025 год показал, что 78 % разработчиков используют нейросети в той или иной форме, что на 16 % чем годом ранее [2] (рис. 1).

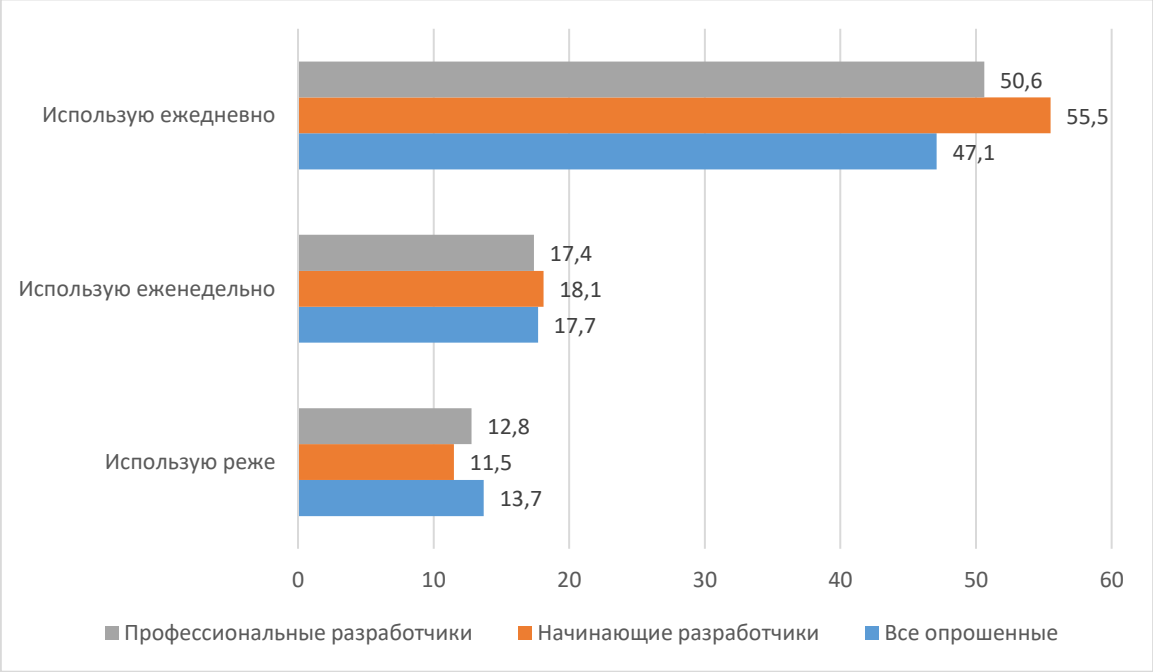


Рис. 1. Данные опроса об использовании ИИ среди разработчиков

Главным и самым очевидным преимуществом языковой модели над человеком является скорость, с которой она может писать код – у новейших моделей она достигает более 1000 токенов в секунду [3], что многократно превышает человеческие возможности.

Также в качестве положительного аспекта можно указать, что нейросеть для выполнения каждой отдельной категории задач нуждается лишь в однократном обучении. Единожды обученная языковая модель может выполнять задачи для большого количества компаний, в том числе одновременно.

Нейросети также не подвержены влиянию усталости и человеческого фактора, из чего следует их способность анализировать огромные массивы информации с целью нахождения в них несостыковок и ошибок с неизменной точностью.

Среди недостатков же можно выделить в первую очередь ненадежность генерируемого кода – нейросеть имеет возможности проверить его на правильность как логически, так и обращаясь к справочным ресурсам, в следствие чего оценка, отладка кода и поиск ошибок в нем продолжает

оставаться прерогативой человека, иногда требуя даже больше усилий, чем если бы код был написан собственноручно [4]. К тому же ИИ не всегда в состоянии понять контекст задачи, что тоже может приводить к ошибкам, в том числе совершенно неочевидным. Отдельно можно вынести феномен «галлюцинирования» [5] нейронной сети – то есть компиляции и выдачи ложных данных, не имеющих практически никакого отношения к действительности в ситуации, когда нейросеть не имеет доступа к данным, точно отвечающим на заданный запрос.

Стоит также отметить с первого взгляда парадоксальное негативное влияние ИИ на рынок труда в программировании, в частности, на рост безработицы – с одной стороны, уже имея возможности для достаточно качественного выполнения и автоматизации задач низкого уровня, нейросети снижают требуемое количество специалистов в целом, а с другой – делают гораздо менее востребованными неопытных программистов, затрудняя их обучение на практике и в конечном счете препятствуя росту количества профессионалов высокого уровня [6].

И если для первой проблемы решение является концептуально очевидным и являет собой закономерное продолжение развития и обучения самих нейросетей наряду с адаптацией технологической и кадровой среды для их использования, то вторая проблема остается актуальной, и предпосылок для ее решения в ближайшем будущем не наблюдается. Это может привести к серьезному кадровому голоду, уменьшению количества программистов всех уровней, и даже к ограничениям использования ИИ. Единственный представляющийся возможным вариант смягчения негативных последствий – это квоты на рабочую практику для неопытных специалистов, а также продление и/или увеличение интенсивности обучения для доведения навыков до минимально конкурентного уровня.

И все же дальнейшее неизбежное внедрение ИИ в разработку ПО не приведет к исчезновению профессии программиста даже в худшем из сценариев, хотя и может изменить ее роль до неузнаваемости. Акцент в работе сместится с ручного прописывания кода на поиск глобальных структурных решений и интеграцию нейросетевых продуктов в рабочие процессы. В конечном счете, для тех разработчиков, которые научатся воспринимать ИИ не как конкурента, а как полезный инструмент, ситуация окажется наиболее выигрышной. Чтобы оставаться востребованными, программистам придется осваивать новые навыки – прежде всего связанные с анализом и проверкой решений, предлагаемых ИИ, а также навыки

промпт-инжиниринга, то есть умение корректно и полно формулировать запросы. Важными станут контроль качества, глубокое понимание алгоритмов и критическое мышление, поскольку искусственный интеллект пока не способен полностью заменить человека в принятии решений. Также будут цениться специалисты, умеющие не только писать код, но и обучать модели, настраивать нейросети и выстраивать взаимодействие между человеком и машиной. Развитие ИИ в IT может пойти по разным сценариям: от роли вспомогательного инструмента до почти полной автономности. Однако наиболее вероятен компромиссный вариант – ИИ будет выполнять рутинные задачи, а разработчики сосредоточатся на планировании, тестировании и управлении проектами, сохраняя контроль и повышая эффективность работы [7-10].

Список используемых источников

1. ИИ в разработке 2025 // RB.RU. URL: https://rb.ru/news/ii-v-razrabotke-25/ (дата обращения: 25.03.2026).

2. Stack Overflow Developer Survey 2025 // Stack Overflow. URL: https://survey.stackoverflow.co/2025/ai (дата обращения: 25.03.2026).

3. Introducing GPT-5.3 Codex Spark // OpenAI. URL: https://openai.com/zh-Hans-CN/index/introducing-gpt-5-3-codex-spark/ (дата обращения: 25.03.2026).

4. Иванова Л. А. Искусственный интеллект при написании научных статей – положительный или вредоносный фактор? // Crede Experto: транспорт, общество, образование, язык. 2024. № 4 (43).

5. Шевченко А. А. «Галлюцинации» ИИ как новая форма эпистемической ошибки // Respublica Literaria. 2025. Т. 6. № 4. С. 93–98.

6. Файзуллин Р. В., Отоцкий П. Л., Горлачева Е. Н. [и др.]. Сценарии развития рынка труда России с учетом оценки влияния искусственного интеллекта: отраслевой разрез // [Название журнала]. 2025. № 1.

7. Казырский Н. А. Как ИИ меняет программирование: угрозы и возможности // Научный лидер. 2025. № 11 (212).

8. Михайлов Е. А., Куваева Е. Н. Перспективы внедрения нейронных сетей и искусственного интеллекта в сфере программирования // Вестник науки. 2025. Т. 3. № 7 (88).

9. Петров Л. Ю., Ахметшина Э. Г. Искусственный интеллект и машинное обучение в разработке ПО // Вестник науки. 2025. Т. 3. № 9 (90).

10. Мирабова Л., Худайназарова М. Искусственный интеллект и машинное обучение в программировании: тенденции и перспективы // Ceteris Paribus. 2023. № 10.

УДК 378.1

РАЗВИТИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ПЕРСОНАЛИЗИРОВАННОГО ОБУЧЕНИЯ

Б. А. Аль-Нами (доцент кафедры ИКД СПбГУТ)
И. М. Стародубцев (студент группы ИСТ-421 СПбГУТ)
starodubtsev.im@sut.ru

В последние годы искусственный интеллект стал важным инструментом в образовательной сфере, особенно в контексте персонализированного обучения. Его применение открывает возможности для более гибкого обучения студентов, а также позволяет снизить нагрузку на преподавателей. В этой статье будет рассмотрена проблематика технологий искусственного интеллекта, применяемых в персонализированном обучении, их преимущества и вызовы, меры, осуществляемые для этого государством, а также перспективы дальнейшего развития этой области.

образование, персонализация, искусственный интеллект, ИИ, e-learning, AI

До того, как технологии, связанные с искусственным интеллектом (ИИ), стали достаточно общедоступными и совершенными, существовало только два способа обучения – самостоятельно и при посредничестве преподавателя, по составляемой им программе. Оба метода обнаруживают серьезные недостатки; в первом случае это трудность и риск ошибок в составлении учебного плана, а также пониженную эффективность восприятия информации (ввиду невозможности получить точный ответ на некоторые вопросы); наличие преподавателя хоть и решает многие из этих проблем, но вместе с тем создает новые – как, например, невозможность дать ответ на вопрос ученика в любое время, возможное несовпадение графиков, человеческий фактор. К тому же, даже при наличии хорошего образования и широкого доступа к образовательным ресурсам, преподаватель не способен искать требуемую информацию мгновенно; особенно остро эта проблема стоит в контексте работы с узкоспециализированными темами и/или специфическими факторами. Искусственный интеллект, в свою очередь, дает нам возможности для решения многих вышеозначенных проблем, будучи использованным в сфере обучения.

Есть несколько различных способов применения ИИ в обучении [1-15]. Первый – алгоритмы машинного обучения, подстраивающие образовательную программу под нужды и способности каждого обучающегося. На осно-

вании получаемых данных они могут делать выводы об успеваемости студента и предлагать материал, наиболее подходящий для его способностей и текущего уровня подготовки. С их помощью ученики могут определить свои слабые места и сосредоточиться на них, оптимизировав тем самым процесс усвоения материала. Исследования показывают, что использование таких алгоритмов значительно повышает успеваемость и мотивацию студентов [9]. Также с их помощью возможно оптимизировать уже существующие методики, такие как дифференциация обучения, то есть разделение учащихся по уровню их подготовки, заинтересованности, стилю обучения и т.д.

Кроме того, возможно использование нейросетей в качестве «виртуальных учителей» для взаимодействия с учащимися, проверки их знаний в любое время и формирования структуры курса обучения. Такой подход исключает влияние человеческого фактора, чем снижает погрешность не только в качестве предоставляемой информации и формировании курса, но и в оценке успеваемости. К тому же, виртуальный учитель не требует от ученика подстройки графика под свой, что позволяет обучаться практически в любом месте и любых условиях.

Несмотря на наличие безусловных преимуществ использования ИИ вместо преподавателя-человека, существуют и определенные сложности, связанные с этим. Краткая сводка по преимуществам и недостаткам ИИ в обучении представлена в таблице ниже (см. табл. 1).

ТАБЛИЦА 1. Преимущества и недостатки ИИ в обучении

Преимущества		Недостатки (вызовы)	
Адаптивность	Может подстроиться под каждого обучающегося индивидуально	Неточность алгоритмов	Алгоритм сам не осознает формулируемую им информацию, что, с учетом обширности области его применения, приводит к грубым фактическим ошибкам
Беспристрастность	Фактор личного отношения к студенту отсутствует (справедливо и обратное)	Требовательность к точности формулировок	Некорректно сформулированный запрос может быть понят ИИ неверно/не понят совсем

Преимущества		Недостатки (вызовы)	
Скорость поиска и охват	ИИ в состоянии осуществить поиск по всем доступным ресурсам в краткие сроки	Недостаток «живого присутствия»	Не всякие аспекты обучения могут быть осуществлены исключительно с помощью текстовой коммуникации
Отсутствие человеческого фактора	Невозможность совершения ИИ ошибок по невнимательности, забывания материала, недостатка навыков работы с медиаматериалом	Технические требования	Для эффективной работы с искусственным интеллектом требуется специализированное ПО, а также стабильный доступ к Интернету

Отдельно хотелось бы рассмотреть проблему проведения границы между оптимизацией обучения и злоупотреблением нейросетями, т.к. не всегда очевидно, было ли использование ИИ оправдано и помогло ли оно на самом деле усвоению материала. Так 27 % опрошенных студентов и 45 % преподавателей дали отрицательный или скорее отрицательные ответ на вопрос о допустимости использования ИИ при написании учебных работ, 52 % студентов и 40 % преподавателей ответили в той или иной мере положительно, причем среди последних однозначно положительный ответ дали менее процента [14] (рис. 1).

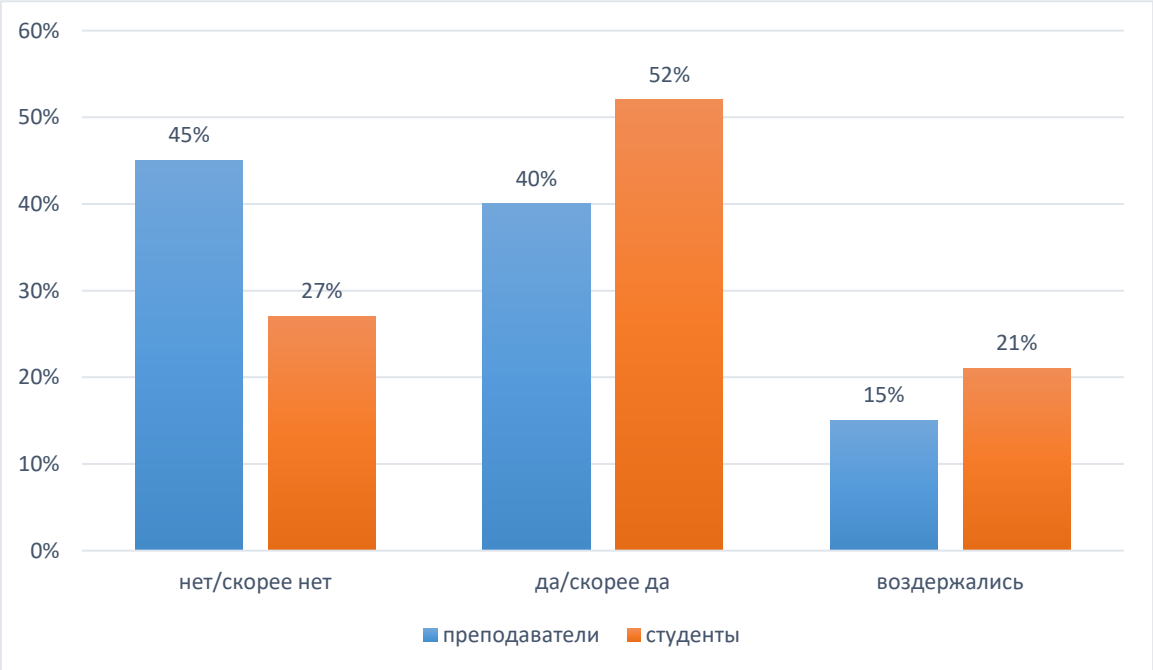


Рис. 1. Результаты опроса о допустимости использования ИИ в учебном процессе среди преподавателей и студентов

Динамика же фактического использования генеративного ИИ демонстрирует значительный рост; проведенное исследование показало, что с марта по сентябрь 2023 года количество преподавателей, использующих ИИ, выросло с 9 до 22 %, а студентов – с 27 % до 49 % (рис. 2).

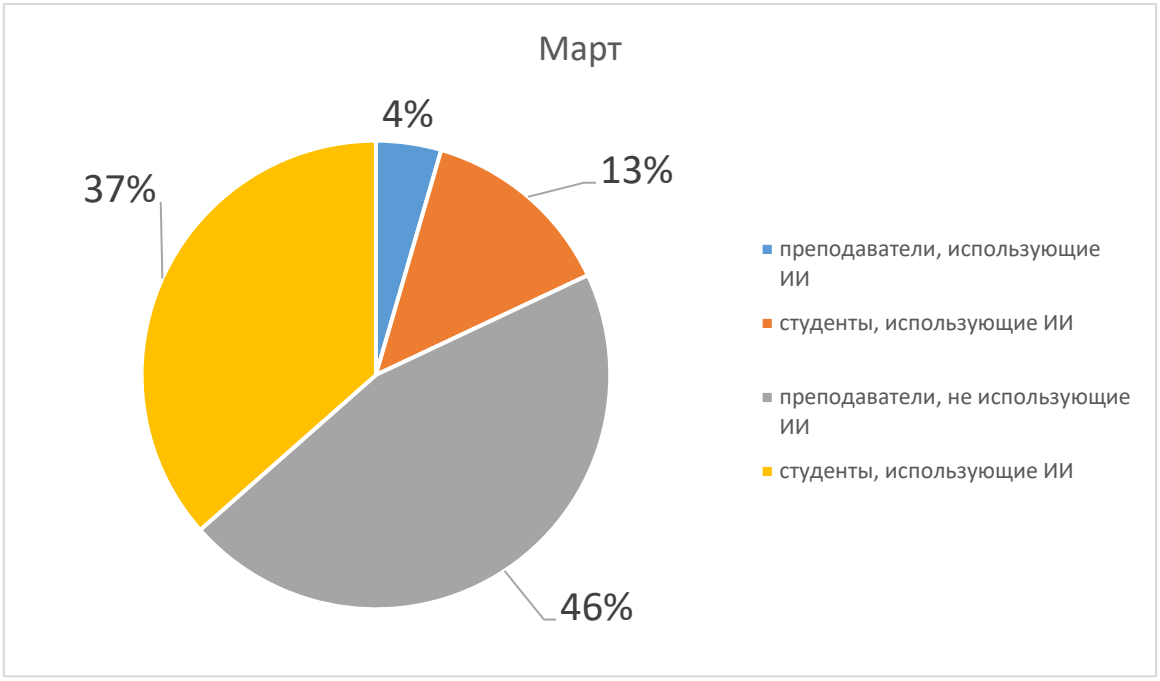


Рис. 2. Результаты опроса об использовании ИИ среди преподавателей и студентов за сентябрь 2023 года

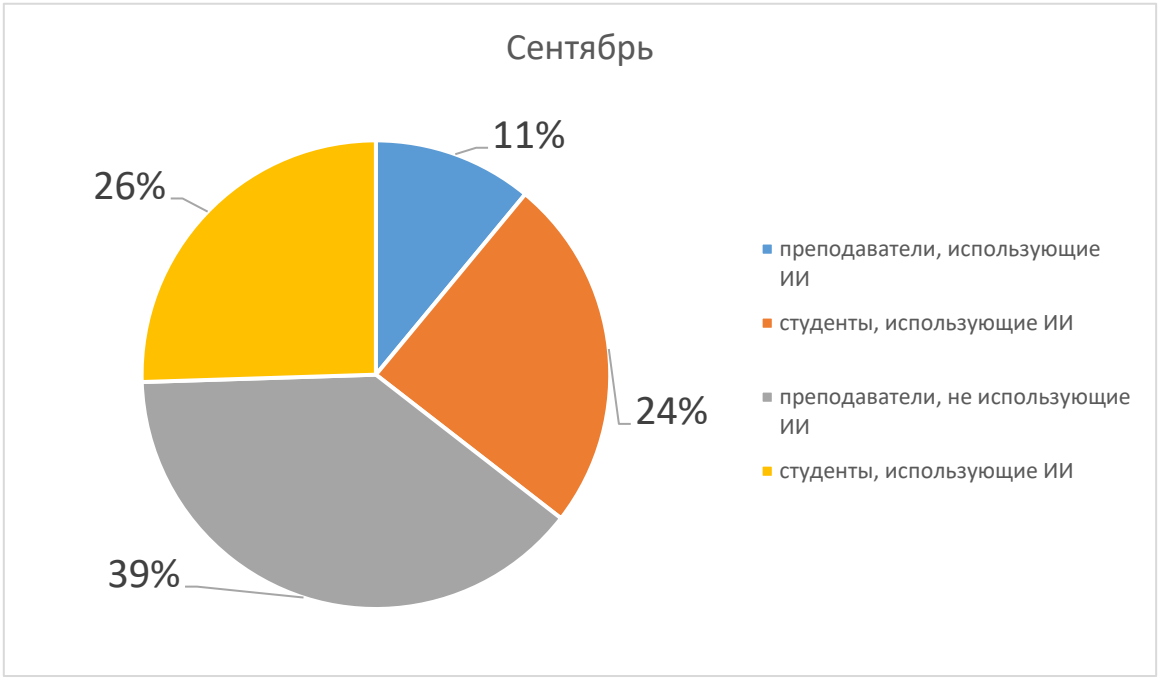


Рис. 3. Результаты опроса об использовании ИИ среди преподавателей и студентов за сентябрь 2023 года

Наиболее очевидным методом преодоления существующих вызовов и ограничений является совершенствование программного обеспечения, что позволит алгоритмам ИИ лучше понимать живую речь и избегать неточностей в выдаче. Значительный прогресс в этом направлении мы можем наблюдать уже сейчас – на фоне нескольких предыдущих лет возможности нейросетей значительно улучшились и продолжают совершенствоваться.

Решением трудности с корректной формулировкой запросов может стать постепенное введение практики взаимодействия с нейросетями в учебные программы.

Для преодоления недостатка «живого присутствия» можно использовать смешанный стиль обучения, когда значительную часть работы с учениками выполняет ИИ, но при этом преподаватель осуществляет контроль как за успеваемостью, так и за корректностью работы алгоритма.

Кроме прочего, существуют государственные инициативы, направленные на решение вышеуказанных проблем. Необходимость в подобных мерах обусловлена статусом ИИ-направления как очень значительного и перспективного, а также отставанием действующего законодательства от реального уровня технологий. Примерами таких инициатив может послужить Распоряжение Правительства Российской Федерации от 18 октября 2023 г. N2 2894-р «Стратегическое направление в области цифровой трансформации образования, относящейся к сфере деятельности Министерства просвещения Российской Федерации» [7], наряду с Указами Президента Российской Федерации, в том числе от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [12], от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [11], от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [10].

С учетом всех приведенных преимуществ и недостатков ИИ можно сделать вывод о его роли в обучении в будущем как об очень перспективной -использование нейросетевых технологий более чем в значительной мере облегчает анализ всей доступной информации и нахождение среди нее необходимой, а также облегчает обучение в целом. О многом говорит масштабное внедрение ИИ во многие образовательные сервисы уже на данный момент.

Примеры образовательных платформ, в которых задействован искусственный интеллект: DreamBox, Khan Academy, Gradescope, Coursera, SAS EVAAS.

В ходе этого исследования была рассмотрена проблематика использования искусственного интеллекта и, в частности, нейросетей в сфере персонального обучения. Были определены преимущества ИИ перед преподавателем-человеком, а также его недостатки и трудности, связанные с внедрением в существующие структуры. На основании собранных данных был сделан вывод о рассматриваемом направлении как об очень перспективном и быстроразвивающемся. Развитие искусственного интеллекта в сфере персонализированного обучения открывает новые возможности для образовательного процесса, адаптивные технологии помогают создавать более эффективные и увлекательные учебные среды, учитывающие индивидуальные потребности студентов, а количество людей, одобряющих использование ИИ в учебе, неуклонно растет, как и количество людей, непосредственно применяющих их регулярно. Поэтому, несмотря на существование определенных вызовов, преодоление которых потребует усилий и средств, развитие ИИ в целом и в сфере персонализированного образования является не только многообещающим, но и просто необходимым, во избежание технологического и морального устаревания системы образования. В данный момент государство принимает обширные меры, позволяющие в том числе частным компаниям активно совершенствовать нейросети и находить способы их внедрения в нашу повседневность.

Список используемых источников

1. Аль-Нами Б. А. Анализ современных методов обнаружения и защиты от кибератак на базе машинного обучения / Б. А. Аль-Нами, А. М. Сидельников // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сборник научных статей XII Международной научно-технической и научно-методической конференции: в 4 т. / под редакцией С. И. Макаренко; составители: В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2023. С. 228–231.

2. Аль-Нами Б. А. Анализ оптимизаторов глубокого обучения / Б. А. Аль-Нами, С. К. Борисов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сборник научных статей XII Международной научно-технической и научно-методической конференции: в 4 т. / под редакцией С. И. Макаренко; составители: В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2023. С. 72–76.

3. Аль-Нами Б. А. Области применения искусственного интеллекта / Б. А. Аль-Нами, С. М. Сидорова, А. Ю. Чупрова // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сборник научных статей XII Международной научно-технической и научно-методической конференции: в 4 т. / под редакцией С. И. Макаренко; составители: В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2023. С. 236–239.

4. Аль-Нами Б. А. Роль информационных технологий и безопасности информационных систем в современном обществе / Б. А. Аль-Нами, Д. Н. Бугеря, С. А. Рогозин // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сборник научных статей XII Международной научно-технической и научно-методической конференции: в 4 т. / под редакцией С. И. Макаренко; составители: В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2023. С. 76–79.

5. Аль-Нами Б. А. Использование искусственного интеллекта в социальных сетях / Б. А. Аль-Нами, А. А. Мазур // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сборник научных статей XII Международной научно-технической и научно-методической конференции: в 4 т. / под редакцией С. И. Макаренко; составители: В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2023. С. 173–176.

6. Ван Цзинъяо. Применение и оценка эффективности искусственного интеллекта в персонализированном обучении // КиберЛенинка: научная электронная библиотека. URL: https://cyberleninka.ru/article/n/primenenie-i-otsenka-effektivnosti-iskusstvennogo-intellekta-v-personalizirovannom-obuchenii/viewer (дата обращения: 15.10.2025).

7. Видова Т. А. Возможности применения технологий искусственного интеллекта в образовательном процессе // КиберЛенинка: научная электронная библиотека. URL: https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-tehnologiy-iskusstvennogo-intellekta-v-obrazovatelnom-protsesse/viewer (дата обращения: 15.10.2025).

8. Гогитидзе К. Искусственный интеллект – угроза или помощник для человечества? / К. Гогитидзе // BBC News Русская служба: официальный сайт. 2017. 16 февраля. URL: https://www.bbc.com/russian/features-38931070 (дата обращения: 15.10.2025).

9. Мантуленко В. В. Влияние искусственного интеллекта на успеваемость, познавательную активность и качество обучения студентов // КиберЛенинка: научная электронная библиотека. URL: https://cyberleninka.ru/article/n/vliyanie-iskusstvennogo-intellekta-na-uspevaemost-poznavatelnuyu-aktivnost-i-kachestvo-obucheniya-studentov/viewer (дата обращения: 15.10.2025).

10. О развитии искусственного интеллекта в Российской Федерации: указ Президента Российской Федерации от 10 октября 2019 г. № 490 // Президент России: официальный сайт. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 15.10.2025).

11. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента Российской Федерации от 07 мая 2018 г. № 204 // Официальный интернет-портал правовой информации. URL: https://ds405-donetsk-r897.gosweb.gosuslugi.ru/netcat_files/19/8/ukaz_prezidenta_rf_ot_7_maya_2018_g.pdf (дата обращения: 15.10.2025).

12. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 09 мая 2017 г. № 203 // Официальный интернет-портал правовой информации. URL: https://sh-shostenskaya-r62.gosweb.gosuslugi.ru/netcat_files/32/315/6.ukaz_prezidenta_rf_ot_09.05.2017_n_203_o_strategii.pdf (дата обращения: 15.10.2025).

13. Паскова А. А. Технологии искусственного интеллекта в персонализации электронного обучения / А. А. Паскова // Вестник Майкопского государственного технологического университета. 2019. № 3 (42). С. 113–122. URL: https://cyberleninka.ru/article/n/tehnologii-iskusstvennogo-intellekta-v-personalizatsii-elektronnogo-obucheniya/viewer (дата обращения: 10.04.2026).

14. Сережкина А. Е. Применение искусственного интеллекта в образовании / А. Е. Сережкина // Цифровая гуманитаристика и технологии в образовании (DHTE 2024): сборник статей V международной научно-практической конференции, 14–15 ноября

2024 г. / под редакцией В. В. Рубцова, М. Г. Сороковой, Н. П. Радчиковой. Москва: Издательство ФГБОУ ВО МГППУ, 2024. С. 743–755. URL: psyjournals.ru (дата обращения: 15.10.2025).

15. Терехова Е. С. Анализ востребованности использования нейросетей для решения учебных задач / Е. С. Терехова, Н. Н. Пучкова, Л. В. Новикова // КиберЛенинка: научная электронная библиотека. URL: https://cyberleninka.ru/article/n/analiz-vostrebovannosti-ispolzovaniya-neyrosetey-dlya-resheniya-uchebnyh-zadach/viewer (дата обращения: 15.10.2025).

УДК 004: 004.738.2

БРОКЕРЫ СООБЩЕНИЙ И ИХ РОЛЬ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Е. А. Барабошкин (студент группы ИСТ-223 СПбГУТ),
baraboshkin.ea@sut.ru
Е. В. Коровкина (ассистент кафедры СОД СПбГУТ)

При разработке распределенных и микросервисных систем одной из ключевых задач является организация надежного и масштабируемого взаимодействия между компонентами. Прямое синхронное взаимодействие сервисов зачастую приводит к высокой связности, снижению отказоустойчивости и проблемам при масштабировании. В данной статье рассматривается понятие брокеров сообщений и анализируются основные проблемы распределенных систем, которые они позволяют эффективно решать.

брокеры сообщений, распределенные системы, микросервисная архитектура, асинхронное взаимодействие, очереди сообщений

Брокер сообщений представляет собой программный компонент, предназначенный для передачи данных между различными частями распределенной системы в виде сообщений [1]. В отличие от прямых синхронных вызовов, брокер сообщений позволяет отправителю и получателю работать независимо друг от друга, обеспечивая асинхронное взаимодействие. Сообщения могут представлять собой запросы, ответы или события, а брокер берет на себя задачи маршрутизации, хранения и доставки данных [2].

Одной из ключевых проблем распределенных систем является жесткая связность компонентов. При использовании синхронных протоколов, таких как HTTP, отказ или задержка в работе одного сервиса, может привести к блокировке других компонентов системы. Например, в интернет-магазине недоступность сервиса уведомлений может привести к сбою при оформлении заказа. Использование брокера сообщений позволяет избежать подобной ситуации: сервис оформления заказа передает сообщение брокеру и продолжает работу, а сервис уведомлений обрабатывает сообщение тогда, когда становится доступным (рис. 1). Такой подход значительно повышает устойчивость системы и упрощает ее развитие.

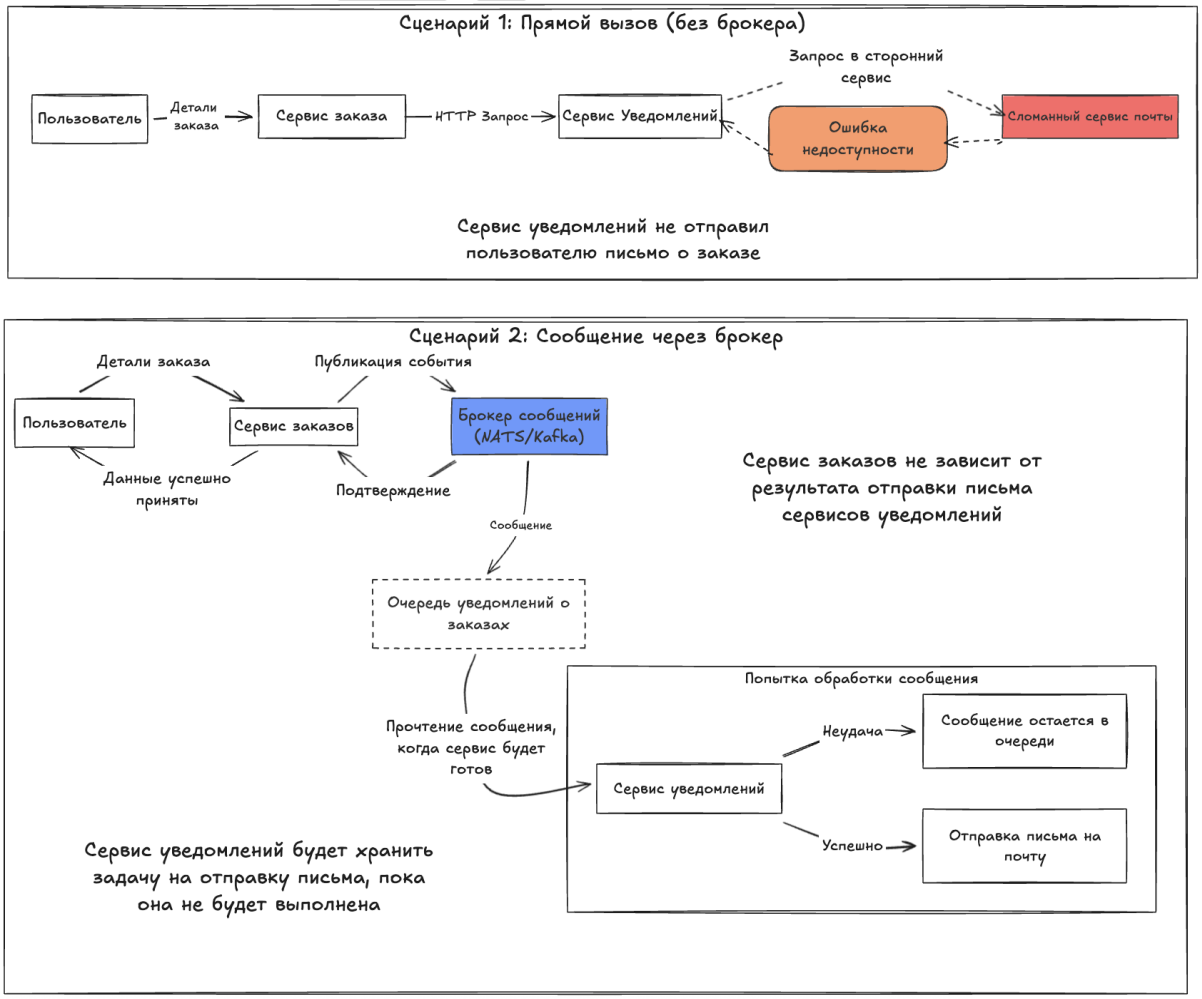


Рис. 1. Уменьшение связности компонентов при помощи брокера сообщений

Еще одной важной задачей является обеспечение отказоустойчивости и надежной доставки данных. В распределенной среде сбои являются неизбежными, поэтому система должна корректно функционировать даже при временной недоступности отдельных компонентов. Брокеры сообщений обеспечивают гарантированную доставку сообщений за счет их сохранения во внутреннем хранилище. Так, если платежный сервис временно недоступен, сообщения о транзакциях сохраняются в очереди и будут обработаны после восстановления сервиса (рис. 2). Это позволяет избежать потери критически важных данных и повышает доверие к системе со стороны пользователей.

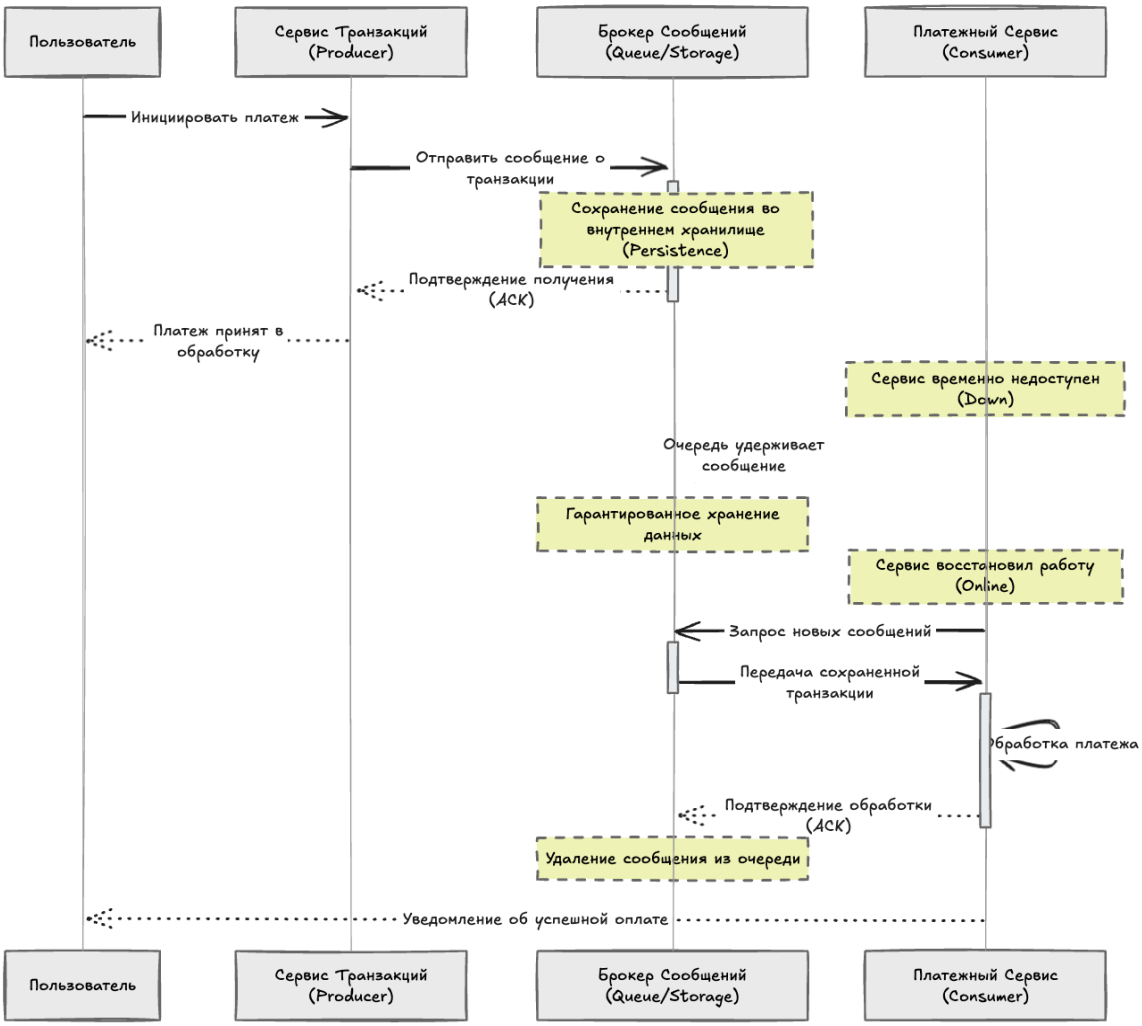


Рис. 2. Обеспечение надежности с помощью брокера сообщений

Проблема масштабируемости и обработки пиковых нагрузок особенно актуальна для систем с большим количеством пользователей или высоким объемом событий [3]. В периоды повышенной активности сервисы могут не успевать обрабатывать все входящие запросы. Брокеры сообщений позволяют буферизовать поток данных и распределять нагрузку между несколькими экземплярами потребителей. Так, в системе обработки логов или аналитики событий сообщения могут поступать с высокой скоростью, а потребители обрабатывают их параллельно, что обеспечивает стабильную работу системы даже при значительном росте нагрузки (рис. 3).

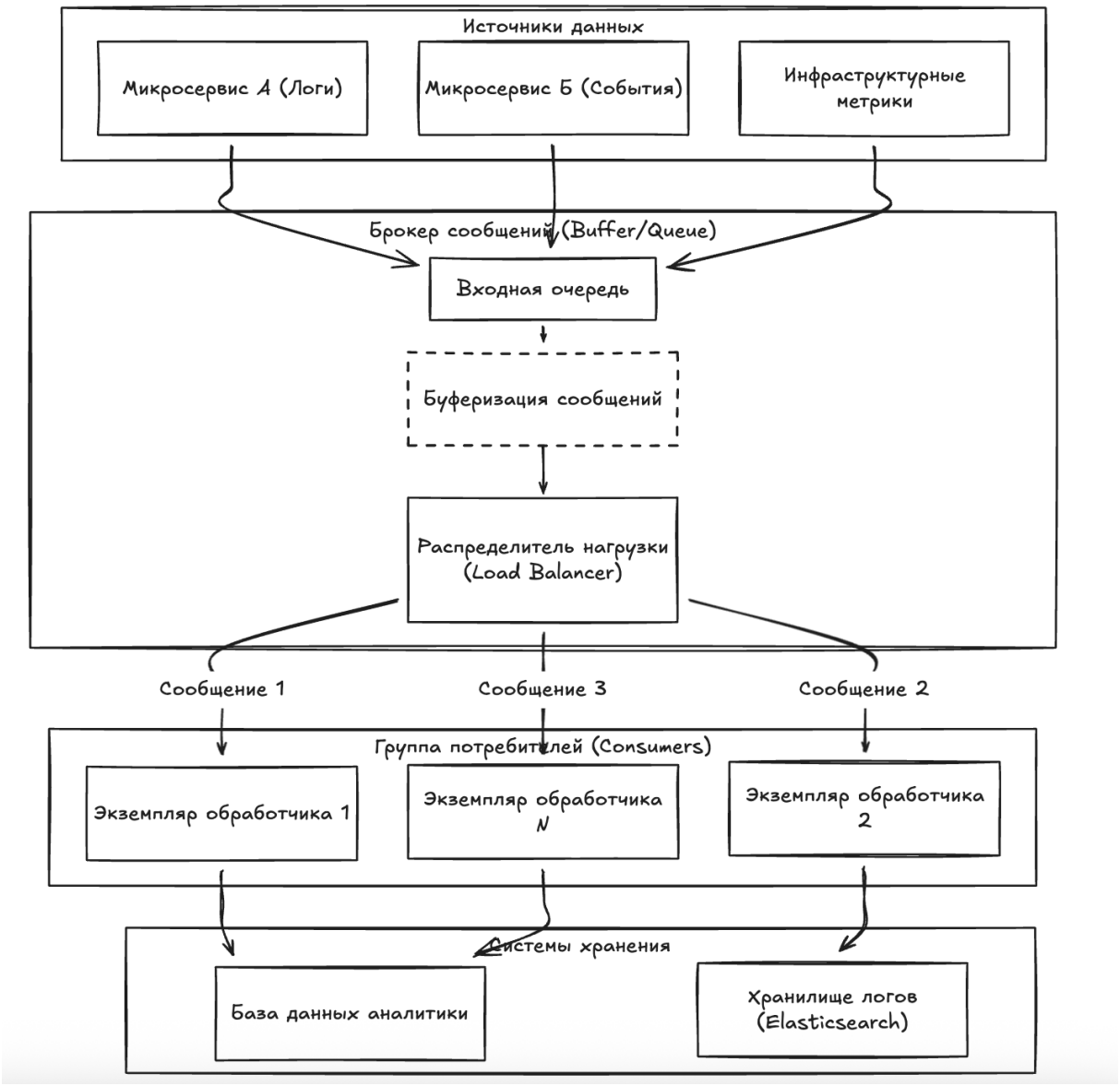


Рис. 3. Решение проблемы масштабируемости системы

Широкое применение брокеров, также стало возможно из-за простоты реализации событийно-ориентированной архитектуры с их помощью. Использование модели публикации-подписки позволяет нескольким независимым сервисам реагировать на одно и то же событие. Например, событие об успешной оплате заказа может быть обработано сервисом склада, службой уведомлений и аналитическим модулем одновременно (рис. 4). При этом отправитель не знает, какие именно сервисы получат сообщение, что обеспечивает слабую связность компонентов и упрощает добавление новых функциональных модулей в систему [4].

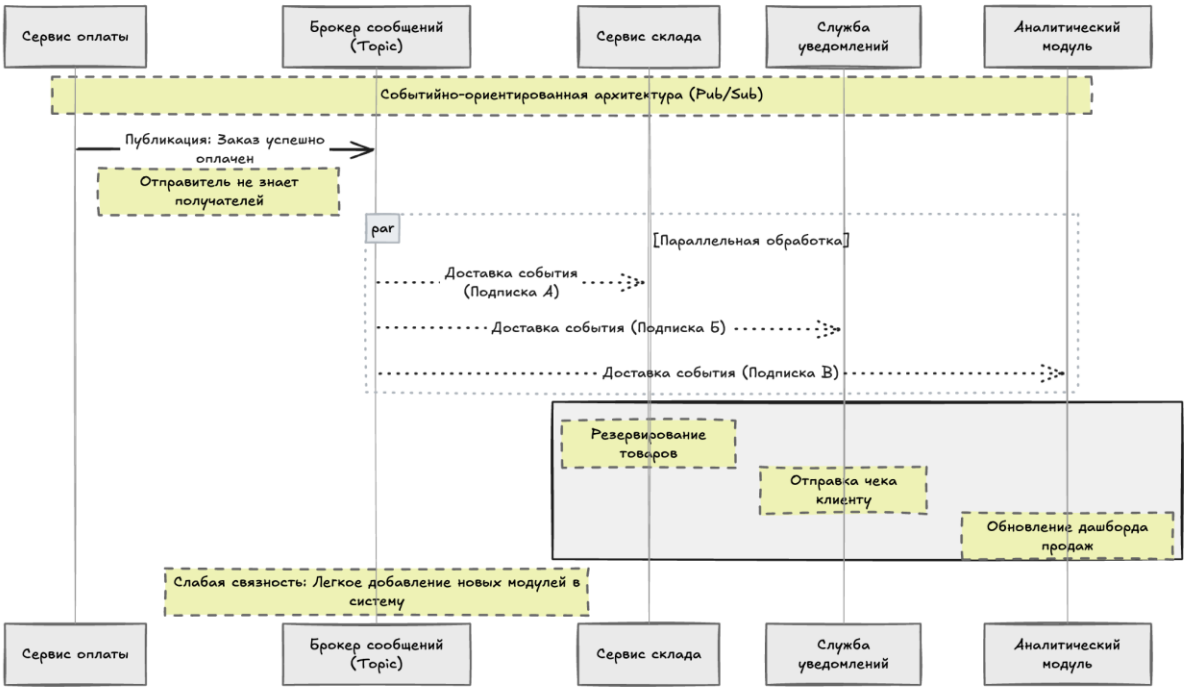


Рис. 4. Использование брокера сообщений в событийно-ориентированной архитектуре

Брокеры сообщений являются важным архитектурным элементом распределенных систем. Они решают ключевые проблемы, связанные с асинхронным взаимодействием, отказоустойчивостью, масштабируемостью и событийной обработкой данных. Применение брокеров сообщений позволяет создавать гибкие и надежные системы, способные эффективно функционировать в условиях высокой нагрузки и постоянных изменений требований.

Список используемых источников

1. Ньюмен С. Создание микросервисов. 2-е изд. СПб.: Питер, 2023. 624 с.

2. Селезнев А. И., Селезнев И. Л. Брокеры сообщений в системах обработки данных // Молодой ученый. 2025. № 46 (597). С. 15–18.

3. Брокеры сообщений – что это, из чего состоят, плюсы и минусы: сравниваем Apache Kafka, Redis и RabbitMQ // Mediasoft: [сайт]. URL: https://academy.mediasoft.team/article/brokery-soobshenii-chto-eto-iz-chego-sostoyat-plyusy-i-minusy-sravnivaem-apache-kafka-redis-i-rabbitmq/ (дата обращения: 13.01.2026)

4. Беллемар А. Создание событийно-управляемых микросервисов: пер. с англ. СПб.: БХВ-Петербург, 2022. 320 с.

Статья представлена и. о. заведующего кафедрой СОД СПбГУТ, кандидатом технических наук, доцентом Ю. М. Бородянским.

УДК 004.7

МИНИМАЛЬНЫЙ СОСТАВ ИНФРАСТРУКТУРЫ ДЛЯ СЕРВИСА ТЕЛЕПРИСУТСТВИЯ НА РАННЕМ ЭТАПЕ РАЗРАБОТКИ: ПОДХОДЫ И РИСКИ

Д. К. Баразенко (студент группы МСТ-2561 СПбГУТ),
barazenko.dk@sut.ru
О. И. Пантюхин (к.т.н., доцент кафедры ССиПД СПбГУТ)

В работе рассматриваются подходы к выбору минимального состава инфраструктуры для сервиса телеприсутствия на раннем этапе разработки. Под таким составом понимается наименьший набор компонентов, обеспечивающий воспроизводимое развертывание, базовую наблюдаемость и контроль качества сервиса. На основе анализа нормативных и методических источников выделены обязательные и откладываемые компоненты, а также риски отсрочки их внедрения. Основным результатом является таблица, связывающая компонент инфраструктуры с его назначением, минимальной реализацией, риском отсрочки и триггером включения. Показано, что на раннем этапе достаточно минимального, но измеримого инфраструктурного контура.

телеприсутствие, инфраструктура, ранний этап разработки, развертывание, наблюдаемость, качество сервиса

Сервис телеприсутствия относится к интерактивным аудиовизуальным системам, в которых ухудшение качества связи быстро становится заметным пользователю. В рекомендациях ITU-T телеприсутствие определяется как система функций, устройств и сетевых элементов, обеспечивающая захват, доставку, управление и отображение высококачественных интерактивных аудио- и видеосигналов [1]. Поэтому на раннем этапе разработки для такого класса сервисов недостаточно просто получить «запуск приложения»: требуется инфраструктурный контур, который позволяет воспроизводимо выпускать изменения и одновременно контролировать базовые показатели качества.

На раннем этапе возникает типичное противоречие. Команда еще не готова строить полнофункциональную эксплуатационную среду, но чрезмерное упрощение инфраструктуры быстро приводит к потере управляемости: становится трудно понять, какое изменение ухудшило поведение сервиса, как быстро восстановиться после сбоя и когда инфраструктурный контур уже пора усиливать. С этой точки зрения минимальный состав инфраструктуры должен определяться через измеримость поведения сервиса и процесса поставки [2, 3].

Под минимальным составом инфраструктуры далее понимается наименьший набор компонентов и практик, который одновременно обеспечивает воспроизводимость развертывания, базовую наблюдаемость и возможность оценивать последствия изменений по ограниченному набору метрик качества и восстановления [2, 3, 4].

Исследовательские вопросы. В статье рассматриваются три вопроса: 1) какие инфраструктурные компоненты являются минимально необходимыми на раннем этапе разработки сервиса телеприсутствия; 2) какие компоненты допустимо отложить без критической потери управляемости; 3) по каким признакам следует принимать решение о включении отложенных компонентов в следующий этап развития среды.

Методика. Использован краткий структурированный анализ пяти источников. Нормативная рамка телеприсутствия взята из рекомендации ITU-T [1]. Критерии измеримого управления качеством сервиса опираются на подход SLI/SLO [2]. Оценка последствий изменений использует метрики DORA [3]. Требования к воспроизводимому развертыванию и отделению конфигурации опираются на подход Twelve-Factor App [4]. Минимальный контур наблюдаемости рассмотрен через модель сигналов и сбора телеметрии OpenTelemetry [5].

Минимальный состав инфраструктуры для раннего этапа разработки представлен в табл. 1. Таблица фиксирует не только обязательные компоненты, но и те элементы, которые на начальной стадии допустимо отложить при условии понимания возникающих рисков.

ТАБЛИЦА 1. Минимальный состав инфраструктуры для раннего этапа разработки

Что входит	Зачем	Статус	Минимум	Риск	Когда нужен	Что входит
Репозиторий	История изменений	Обязателен	Один репозиторий с управляемой историей	Ручные расхождения и потеря контекста	Сразу [4]	Репозиторий
Конвейер	Повторяемый выпуск версий	Обязателен	Один конвейер для тестовой среды	Неясный состав релиза и ручные ошибки	Частые изменения или сбои [3, 4]	Конвейер

Что входит	Зачем	Статус	Минимум	Риск	Когда нужен	Что входит
Конфигурация	Переносимость среды	Обязателен	Внешние параметры и единые переменные	Скрытые различия между средами	Несколько сред или участников [4]	Конфигурация
Логи и метрики	Диагностика и контроль качества	Обязателен	Сбор журналов и базовых метрик	Деградации не локализуются	Испытания и инциденты [2, 5]	Логи и метрики
SLI/SLO	Приемлемый уровень сервиса	Обязателен	2–3 индикатора	Решения становятся субъективными	Выпуск и сравнение версий [2]	SLI/SLO
Метрики DORA	Стабильность изменений	Обязателен	Частота развертываний, сбои, восстановление	Улучшения среды нечем проверить	Откаты и рост времени восстановления [3]	Метрики DORA
Трассировка	Поиск межсервисных задержек	Можно отложить	Единый формат телеметрии без полного внедрения	Причина сложных деградаций ищется дольше	Рост числа сервисов [5]	Трассировка
Кластер/ резерв	Масштабирование и устойчивость	Можно отложить	Простая среда и регламент восстановления	Преждевременный рост сложности	Переход к эксплуатации	Кластер/ резерв

Из табл. 1 видно, что ядро минимального состава образуют шесть компонентов: единый репозиторий, автоматизированная сборка и развертывание, отделение конфигурации от кода, базовая наблюдаемость, минимальные показатели качества сервиса и метрики качества изменений. Эти элементы не делают среду «полнофункциональной», но позволяют команде видеть последствия изменений и управлять развитием инфраструктуры на основе измеримых признаков [2, 3, 4].

Одновременно таблица показывает, что часть компонентов действительно может быть отложена. Прежде всего это относится к распределенной трассировке, кластерной оркестрации и географическому резервированию.

Их преждевременное внедрение на раннем этапе часто увеличивает сложность сопровождения быстрее, чем дает выигрыш в управляемости. Однако такая отсрочка допустима только тогда, когда уже существуют базовые показатели качества сервиса и минимальные метрики процесса поставки [2, 3, 5].

Ограничения. Работа не претендует на описание полной промышленной инфраструктуры сервиса телеприсутствия. В ней сознательно не рассматриваются детальная архитектура медиатракта, выбор конкретных протоколов и вопросы многоузловой эксплуатации. Предлагаемый состав относится именно к пилотной реализации, внутренним испытаниям и первым пользовательским проверкам [1].

Недочеты. Предложенный состав задает инженерную опору для раннего этапа, но не заменяет последующую детализацию требований к качеству. Кроме того, статья не проводит количественного сравнения стоимости разных вариантов среды и не устанавливает универсальный порог, при котором тот или иной компонент становится обязательным; в этом смысле таблица является инструментом обоснованного выбора, а не жестким стандартом.

Рекомендации. На раннем этапе целесообразно начинать с четырех вещей: воспроизводимого развертывания, внешней конфигурации, базовой наблюдаемости и 2–3 показателей качества сервиса. Если растут число релизов, длительность восстановления или количество межсервисных отказов, это должно рассматриваться как явный сигнал к включению отложенных компонентов, прежде всего трассировки и более устойчивой среды выполнения [2, 3, 5].

Вывод. В работе предложен компактный подход к выбору минимального состава инфраструктуры для сервиса телеприсутствия на раннем этапе разработки. Практическая ценность результата состоит в том, что каждому компоненту сопоставлены его назначение, обязательность, риск отсрочки и триггер включения. Такой подход позволяет избежать двух крайностей: опасного упрощения среды и преждевременного усложнения инфраструктуры без доказанной необходимости.

Список используемых источников

1. Recommendation ITU-T F.734 (10/2014). Definitions, requirements and use cases for telepresence systems [Электронный ресурс]. URL: https://www.itu.int/rec/T-REC-F.734 (дата обращения: 25.02.2026).

2. Jones C., Wilkes J., Murphy N., Smith C. Service Level Objectives // Site Reliability Engineering: How Google Runs Production Systems [Электронный ресурс]. URL: https://sre.google/sre-book/service-level-objectives/ (дата обращения: 20.03.2026).

3. Forsgren N., Humble J., Kim G. Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations. Portland: IT Revolution Press, 2018. 288 p. ISBN 978-1-942788-33-1.

4. Wiggins A. The Twelve-Factor App [Электронный ресурс]. URL: https://www.12factor.net/ (дата обращения: 14.03.2026).

5. OpenTelemetry. Overview [Электронный ресурс]. URL: https://opentelemetry.io/docs/reference/specification/overview/ (дата обращения: 05.03.2026).

УДК 621.39:004.89

АНАЛИЗ КРИТЕРИЕВ ОЦЕНКИ СИСТЕМ АГЕНТНОГО ИИ В СЕТЯХ СВЯЗИ

М. А. Белов (студент группы МСТ-2561 СПбГУТ), belov.ma@sut.ru
А. С. А. Мутханна (профессор кафедры ССиПД, д.т.н. СПбГУТ)
М. А. Сурков (студент группы РМ-21 СПбГУТ), surkov.ma@sut.ru

В статье предложена матрица проверяемых критериев разграничения систем класса «ИИ-агент» (AI agent) и «Агентный ИИ» (Agentic AI) на основе сопоставления признаков, выделяемых в современной литературе, с семью структурными компонентами определения ИИ-системы Рекомендации Совета ОЭСР. Показано, что отнесение системы к агентному классу не определяется отдельным признаком, а фиксируется одновременным усилением характеристик по всем компонентам определения. Построена матрица проверяемых критериев, согласующаяся с архитектурным каркасом ITU-T Y.3172.

ИИ-агент, агентный ИИ, IMT-2020, IMT-2030, автономность, агентность, матрица проверяемых критериев, MLFO, ML-песочница

Резкий рост интереса к классу систем агентного ИИ – кратное увеличение числа поисковых запросов в 2025 году и более чем девятикратный прирост числа репозиториев на GitHub, использующих агентные программные платформы [1], – опередил процесс концептуальной стабилизации термина. В литературе понятия «AI agent» и «Agentic AI» используются как взаимозаменяемые, хотя за ними стоят различные архитектурные решения. Настоящая работа развивает данный тезис в направлении построения матрицы проверяемых критериев классификации.

Для целей телекоммуникационного применения – в частности, для развертывания агентного ИИ в сетях IMT-2020 и IMT-2030 – необходимы не описательные, а проверяемые критерии отнесения системы к агентному классу. Без таких критериев невозможно однозначно сформулировать требования к узлу политики, ML-песочнице и функциям оркестратора (MLFO), предписываемым стандартом ITU-T Y.3172 [2]. Цель настоящей работы – построить такую матрицу, привязанную к семи компонентам определения ИИ-системы Рекомендации Совета ОЭСР, и проверить ее применимость для формального отнесения конкретной системы к агентному классу.

Определение ИИ-системы ОЭСР выделяет семь структурных компонентов: цели, входные данные, вывод модели (от англ. inference – инференс), выходы, влияние на физическую или виртуальную среду, автономия

и адаптивность. Каждый из компонентов трансформируется при переходе от одиночного ИИ-агента к мультиагентной системе агентного ИИ.

Одиночный ИИ-агент работает с узкими, краткосрочными целями, явно заданными пользователем, и статичными входными данными. Агентная система делает иначе: планирующий агент автоматически разбивает пользовательскую задачу на подзадачи и распределяет их между специализированными агентами. Горизонт планирования при этом расширяется, а источники входных данных становятся динамичными: данные поступают из интерактивной среды и от других агентов, а архитектура должна поддерживать их горячее подключение без перезапуска ML-конвейера.

Вывод модели одиночного агента реализуется как одношаговое обращение к одному экземпляру модели. Агентный ИИ характеризуется распределенным выводом модели: внутренними цепочками рассуждений, многоагентной критикой и саморефлексией. Архитектурно это реализуется через цепочку логических узлов ML-конвейера (источник данных, сборщик, препроцессор, модель, политика, распределитель, приемник), которые могут размещаться на различных уровнях сети. Пространство действий одиночного агента ограничено заранее заданным набором функций. Агентные системы оперируют расширенным пространством действий, включая прямое взаимодействие с инструментами, программными интерфейсами и графическими интерфейсами пользователя. Принципиально важно, что именно узел политик выступает главным архитектурным барьером, который жестко ограничивает это расширенное пространство действий: прежде чем система агентного ИИ применит свои решения к живой сети, они в обязательном порядке фильтруются узлом P в соответствии с операторскими политиками, что предотвращает деструктивное воздействие на сетевую инфраструктуру.

Одиночный агент работает в замкнутых цифровых экосистемах с предсказуемыми последствиями; агентные системы проектируются для открытых сред, где последствия действий заранее неизвестны. Именно эта неопределенность требует предварительной верификации в ML-песочнице до выпуска в живую сеть.

По шкале автономии ОЭСР (no-action … high-action) агентные системы находятся на верхнем полюсе и включают автономное обнаружение инструментов. Важное уточнение: высокая автономия не означает агентности – изолированный ML-модуль может работать полностью автономно, но не формировать целей и не взаимодействовать с другими агентами [3].

Адаптивность, в свою очередь, выражается в способности перестроить последовательность подзадач при изменении среды или частичных отказах; ITU-T Y.3172 реализует это через мониторинг KPI и перевыбор ML-моделей оркестратором MLFO.

Описанные атрибуты необходимы, но недостаточны: пока для каждого из них не задан конкретный проверяемый критерий, архитектор не может однозначно ответить, является ли система агентной. Таблица 1 дает ответ по каждому из семи компонентов.

ТАБЛИЦА 1. Матрица проверяемых критериев отнесения системы к классу «Agentic AI»

Компонент	Агентный признак	Проверяемый критерий	Метод верификации
Цели	Декомпозиция и делегирование	Наличие планирующего агента, автоматически разбивающего пользовательскую цель не менее чем на две подзадачи, делегируемые другим агентам	Трассировка вызовов в журнале оркестратора
Входные данные	Динамические интерактивные источники	Поддержка горячего подключения новых источников данных без перезапуска ML-конвейера	Сценарный тест на подключение нового SRC-узла в работающем конвейере
Вывод модели	Распределенное рассуждение	Наличие не менее двух взаимодействующих узлов вывода модели с протоколом обмена результатами	Анализ топологии ML-конвейера
Выходы	Расширенное пространство действий	Способность системы вызывать внешние инструменты и API без ручной маршрутизации	Перечень разрешенных действий в декларативной спецификации (ML Intent)
Влияние на среду	Работа в открытой среде	Документально подтвержденное функционирование в среде с заранее неизвестным набором состояний	Прогон в ML-песочнице с симулированной нижележащей сетью

Компонент	Агентный признак	Проверяемый критерий	Метод верификации
Автономия	Уровень human-out-of-the-loop	Подтвержденная способность выполнять полный цикл задачи без вмешательства человека в течение порогового интервала Tmin. При этом значение Tmin динамически калибруется, исходя из SLA (соглашения об уровне обслуживания) конкретной телеком-услуги: например, для задач балансировки нагрузки в радиосети оно измеряется миллисекундами, тогда как для задач планирования сети – часами	Сценарный тест с фиксацией продолжительности автономной работы
Адаптивность	Реконфигурация в реальном времени	Перевыбор стратегии или ML-модели при выходе KPI за допустимый порог	Запись событий перевыбора модели в журнале MLFO

Система относится к классу «Agentic AI» при одновременном выполнении критериев по всем семи строкам матрицы. Частичное соответствие – например, выполнение критериев лишь по компонентам «цели» и «выходы» при невыполнении критерия автономии – свидетельствует о принадлежности к классу одиночных ИИ-агентов и не дает оснований для классификации системы как агентной. Указанная матрица согласуется с архитектурными требованиями ITU-T Y.3172 в части необходимости узла политики и ML-песочницы перед выпуском системы в живую сеть.

Для иллюстрации практической применимости предложенной матрицы рассмотрим сценарий анализа первопричин сбоев в сети. Если система лишь классифицирует журналы событий и выдает вероятную причину инцидента, по нашим критериям она соответствует классу базового «ИИ-агента»: задача не декомпозируется, вывод модели одношаговый, автономия ограничена. Иная картина возникает, когда система декомпозирует задачу RCA между специализированными агентами – один собирает метрики сети, второй анализирует журналы, третий сверяет выявленные закономерности со стандартами ITU-T, – координируя их работу через оркестратор (MLFO). Гипотезы о первопричине при этом тестируются в изолированной

ML-песочнице на симулированной подсети согласно ITU-T Y.3172, а итоговое решение перед применением к живой сети проходит фильтрацию через узел политик, минимизируя риск деструктивного воздействия. Именно вторая архитектура проходит все семь проверок матрицы; первая – нет.

Термин «agentic AI» до сих пор используется описательно: система «агентная», если выглядит достаточно сложной. Предложенная матрица меняет эту ситуацию: вопрос «является ли система агентной?» получает однозначный ответ: соответствует ли она всем семи критериям одновременно. Матрица применима напрямую в процедурах архитектурного аудита, при формировании ML Intent и настройке MLFO согласно ITU-T Y.3172.

Список используемых источников

1. OECD AI Papers N 56 (2026). The agentic AI landscape and its conceptual foundations. Paris: OECD Publishing.

2. ITU-T Y.3172 (2019). Architectural framework for machine learning in future networks including IMT-2020. Recommendation. Geneva: ITU.

3. ITU-T YSTR.NAIA (2026). Terms and definitions related to the AI Agent topic in future networks. Draft new Technical Report, Q20/13, Study Group 13. Geneva: ITU.

УДК 004.75

АНАЛИЗ СТРАТЕГИЙ ДОСТАВКИ СООБЩЕНИЙ В МИКРОСЕРВИСНЫХ АРХИТЕКТУРАХ В УСЛОВИЯХ ДЕГРАДАЦИИ ОТДЕЛЬНЫХ УЗЛОВ СИСТЕМЫ

Белый М. С. (студент группы ИКПИ-24 СПбГУТ), bely.ms@sut.ru
Краева Е. В. (старший преподаватель кафедры ПИиВТ СПбГУТ)

В статье исследуется проблема управления качеством обслуживания с целью обеспечения стабильности сетевой нагрузки в распределенных микросервисных архитектурах, где масштабирование и интенсивное асинхронное взаимодействие создают риски каскадной перегрузки. Предложен адаптивный метод на базе паттерна защитного отключения. Результаты подтверждают прямую зависимость выбора стратегии от требований соглашения об уровне обслуживания: для систем, критичных к целостности данных, обосновано внедрение механизмов адаптивной буферизации, тогда как для сервисов, чувствительных к задержкам, целесообразно использование конфигураций с жестким ограничением времени ожидания.

микросервисная архитектура, брокер сообщений, надежность доставки, очередизация сообщений, деградация системы, персистентность

Введение

Микросервисная архитектура порождает риски каскадной перегрузки вследствие деградации отдельных узлов под избыточной нагрузкой, что ведет к росту задержек и потере пакетов. Плотная связанность компонентов требует компромисса между согласованностью данных и производительностью системы.

Анализ стандартных стратегий доставки сообщений

Промежуточное ПО, ориентированное на сообщения, традиционно опирается на две семантики доставки: «по крайней мере один раз» и «ровно один раз». Первая обеспечивает надежность через повторные попытки доставки до получения подтверждения, однако при деградации узлов ожидание отклика провоцирует скопление сообщений в очереди брокера и сетевую избыточность. Вторая минимизирует нагрузку на каналы, не требуя подтверждений, но допускает потерю данных при переполнении буферов [1]. Рассмотрим особенности каждой стратегии в условиях нестабильности:

1. «По крайней мере один раз» обеспечивает надежность через повторные попытки доставки до получения подтверждения. Но когда узлы деградируют, ожидание отклика приводит к скоплению сообщений брокера и сетевой избыточности.

2. «Ровно один раз» снижает нагрузку на каналы, поскольку не требует подтверждений. Нельзя исключить потерю части сообщений при переполнении буферов.

Исследования RabbitMQ и Kafka подтверждают, что пропускная способность варьируется в условиях высокой задержки, приводя к непропорциональному росту времени отклика [2, 3]. Стандартные таймауты не различают отказавшие компоненты от медленно функционирующих, порождая паразитную избыточность повторных отправок.

Адаптивный метод. Для решения указанных проблем предлагается метод на базе паттерна Circuit Breaker. Система динамически изолирует деградировавший узел после трех последовательных неудач, перенаправляя трафик в резервную очередь (Dead Letter Queue, DLQ), что исключает накопление «заторов» в основном контуре и предотвращает каскадную перегрузку (рис. 1).

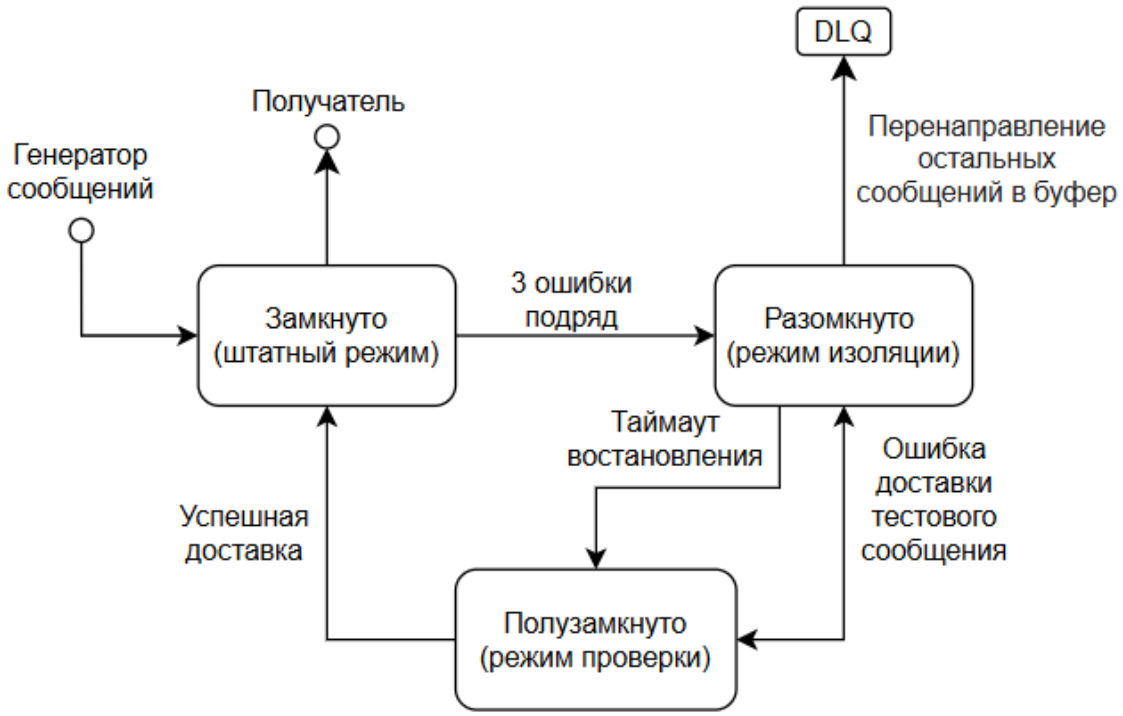


Рис. 1. Диаграмма состояний адаптивной стратегии доставки

● замкнуто – штатный режим доставки напрямую с отслеживанием ошибок;

● разомкнуто – режим изоляции после трех ошибок: сообщения перенаправляются в DLQ без обратных связей к потребителям, функционирующую как автономный накопитель для исключения «шторма повторных попыток»;

● полузамкнуто – проверочный режим с тестовой доставкой по истечении таймаута восстановления.

Проведение эксперимента

Параметры и условия моделирования

Имитационная модель реализована методом дискретно-событийного моделирования в контейнеризированной среде Docker, что обеспечивает воспроизводимость условий. Генератор на базе Python Asyncio формирует пакеты по 2 КБ с интенсивностью до 1000 сообщений/сек, моделируя насыщение сети (пропускная способность канала 2 МБ/с). Кластер брокеров эмулируется тремя логическими узлами с циклической балансировкой нагрузки.

Инжекция сбоев реализована программным прокси-слоем, вносящим задержку 100–500 мс и имитирующим потерю 15 % пакетов. Управление логикой обработки базируется на механизме защитного отключения (Circuit Breaker) [4], обеспечивающем автоматическое переключение узла в режим изоляции с перенаправлением сообщений в DLQ (рис. 2).

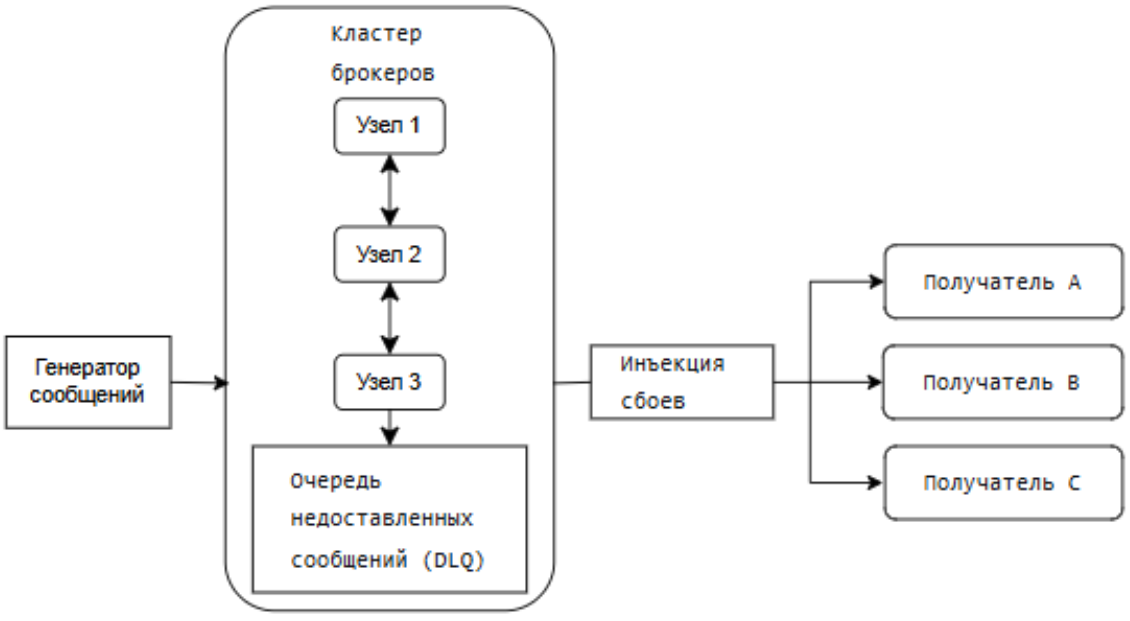


Рис. 2. Архитектура стенда для моделирования сбоев

Данный подход Chaos Engineering позволяет имитировать деградацию компонентов без нарушения целостности остальной инфраструктуры. Управление логикой обработки сбоев базируется на механизме защитного отключения (Circuit Breaker) [4]. Данный подход позволяет отслеживать состояние каждого компонента и автоматически переключать узел в режим изоляции после нескольких последовательных неудач. В этом состоянии новые сообщения перенаправляются в очередь DLQ, что предотвращает блокировку всей системы из-за одного деградировавшего узла-получателя.

Сравнительный анализ стратегий доставки

В ходе моделирования анализировались три подхода: “Fast-Fail” (минимальные таймауты, без повторов), “Reliable-Wait” (длительное ожидание подтверждения) и “Adaptive-Buffer” на базе Circuit Breaker. Ключевые метрики сведены в таблицу 1.

ТАБЛИЦА 1: Сравнение стратегий доставки по метрикам надежности и производительности

Стратегия	Доставлено, шт.	% потерь	Задержка, мс	Время восстановления, сек	Повторные попытки
Fast-Fail	613	38,7	45	0,8	0
Reliable-Wait	1000	0,0	320	4,2	179
Adaptive-Buffer	1000	0,0	180	2,1	181

Стратегия «Fast-Fail» демонстрирует минимальную задержку, однако при деградации узла теряется значительное количество сообщений, из-за отсутствия механизмов повторной отправки.

Конфигурация «Reliable-Wait» обеспечивает полную доставку, но задержка возрастает, а время восстановления составляет около 4 сек из-за необходимости обработки скопившейся очереди с дисковой персистентностью.

Адаптивный метод «Adaptive-Buffer» показывает оптимальный баланс: нулевые потери при умеренной задержке и сокращении времени восстановления вдвое по сравнению со статической гарантированной доставкой. Оперативный вывод проблемного узла из критического контура после трех неудач устраняет эффект “затора” в основной очереди путем перенаправления трафика в DLQ (табл. 2).

ТАБЛИЦА 2. Сравнительный анализ стратегий доставки: преимущества и недостатки

Стратегия	Преимущества	Недостатки	Рекомендуемые сценарии применения
Fast-Fail	-Минимальная задержка обработки -Отсутствие накопления сообщений в очередях -Низкая нагрузка и задержка	-Высокие потери данных -Непригодна для критических транзакций -Не обеспечивает гарантий доставки	Мониторинг, логи, метрики, где задержка критична
Reliable-Wait	-Нулевая потеря данных -Простота реализации и понимания -Гарантированная целостность	-Рост задержки -Длительное восстановление -Риск каскадной перегрузки при деградации узлов	Критические финансовые операции, где потеря недопустима, а скорость вторична
Adaptive-Buffer	-Нулевая потеря данных -Умеренная задержка -Ускоренное восстановление -Изоляция проблемных узлов	-Более сложная реализация -Дополнительные накладные расходы на хранение отложенных сообщений -Необходимость восстановления DLQ	Рекомендована для большинства микросервисных систем

Выявленные закономерности подтверждают: для высоконагруженных архитектур с жесткими требованиями к SLA асинхронная модель с динамической изоляцией сбоев эффективнее статических подходов.

Заключение

Экспериментальное сравнение подтвердило, что статические конфигурации не обеспечивают предсказуемого баланса между целостностью данных и стабильностью сетевой нагрузки. Адаптивный подход на базе Circuit Breaker демонстрирует способность динамически перераспределять нагрузку, сохраняя нулевой уровень потерь при сокращении времени восстановления. Для систем, критичных к задержкам, целесообразны стратегии с жестким ограничением ожидания; для обеспечения целостности данных при сохранении доступности сети – асинхронные паттерны с изоляцией проблемных контуров.

Список используемых источников

1. Newman, S. Building Microservices: Designing Fine-Grained Systems. 2nd ed. O'Reilly Media, 2021. Глава 5: «Communication Between Services», стр. 113–145. Идентификатор: O'Reilly ID: 9781492034018. URL: https://internet-lab.ru/building_microservices (дата обращения: 10.04.2026).

2. Richardson, C. Microservices Patterns: With examples in Java. Manning Publications, 2019. Глава 10: «Developing production-ready services», стр. 321–358. Идентификатор: ISBN: 978-1-617-29454-9. URL: https://www.oreilly.com/library/view/microservices-patterns/9781617294549/ https://livebook.manning.com/book/microservices-patterns/table-of-contents (дата обращения: 10.04.2026).

3. Maharjan, R., et al. Benchmarking Message Queues // Engineering Proceedings. 2023. URL: https://www.mdpi.com/2673-4001/4/2/18 (дата обращения: 10.04.2026). DOI: 10.3390/telecom4020018.

4. Fowler, M. Circuit Breaker Pattern. 2014. URL: https://martinfowler.com/ bliki/CircuitBreaker.html (дата обращения: 10.04.2026).

УДК 004.852:658.58

АРХИТЕКТУРА МЕТОДА ПРОГНОЗИРОВАНИЯ КОРНЕВЫХ ПРИЧИН ОТКАЗОВ ПРОИЗВОДСТВЕННОГО ОБОРУДОВАНИЯ НА ОСНОВЕ ДИНАМИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ

Р. М. Вивчарь (к.т.н., доцент кафедры ПИиВТ СПбГУТ)
М. А. Рябинкин (студент группы ИКПИ-22 СПбГУТ), ryabinkin.ma@sut.ru
Д. М. Ткач (студент группы ИКПИ-22 СПбГУТ), tkach.dm@sut.ru

Описывается архитектура метода прогнозирования корневых причин отказов производственного оборудования, основанного на динамических байесовских сетях. Модель строится как двухсрезовая байесовская сеть и включает три уровня переменных: скрытые корневые причины организационного и технического характера, скрытые технические состояния и наблюдаемые показания датчиков. Приводится состав переменных применительно к сценарию интеллектуального производственного цеха. Описан алгоритм байесовского фильтра для обновления апостериорных вероятностей при поступлении новых измерений, а также процедура идентификации корневой причины через ранжирование скрытых узлов первого уровня.

динамические байесовские сети, прогнозирование отказов, анализ корневых причин, предиктивное обслуживание, байесовский фильтр

Незапланированные остановки производственного оборудования влекут за собой прямые финансовые потери и сбои технологических цепочек. По оценкам работы [1], доля таких потерь составляет от 5 до 20 % суммарной производительности предприятия. Причина отказа и его внешнее проявление в большинстве случаев разделены во времени: когда показания датчиков выходят за допустимые границы, деградация нередко уже набрала критическую скорость.

Методы FMEA и FTA систематизируют известные сценарии неисправностей, но не учитывают, как вероятность отказа меняется по мере износа компонентов [2]. Нейросетевые подходы точнее работают с нелинейными зависимостями между параметрами, однако не дают ответа на вопрос, какое именно событие стало первопричиной нарушения [3]. Динамические байесовские сети сочетают вероятностный причинно-следственный вывод с явным учетом временной динамики, что делает их пригодным инструментом для раннего обнаружения деградации оборудования [4]. В настоящей работе описывается трехуровневая архитектура такой модели применительно к сценарию интеллектуального производственного цеха.

Структура динамической байесовской сети

Динамическая байесовская сеть задается двумя компонентами. Начальная сеть B_0 задает распределение переменных при $t = 0$. Переходная сеть $B \rightarrow$ описывает, как переменные эволюционируют от среза t к срезу $t + 1$. Такое представление называется двухсрезовой байесовской сетью [5].

В предлагаемой модели все переменные разбиты на три уровня. Уровень L1 содержит скрытые корневые причины. Часть из них носит технический характер: недостаток смазки и возраст компонента. Другая часть отражает организационные факторы: пропуск планового технического обслуживания, уровень квалификации оператора, перегрузку оборудования и нарушение регламентов. Включение организационных переменных принципиально важно, поскольку именно они порождают значительную долю реальных отказов в производственных условиях.

Уровень L2 содержит скрытые технические состояния, которые не измеряются напрямую, но восстанавливаются через байесовский вывод: степень износа подшипника, риск перегрева и уровень механического напряжения. Уровень L3 образуют наблюдаемые переменные – показания датчиков вибрации, температуры шпинделя, потребляемого тока, уровня шума и доля производственного брака. Именно эти значения поступают на вход системы в режиме реального времени. Причинно-следственные связи между переменными всех трех уровней представлены на рис. 1, полный состав переменных приведен в таблице 1.

ТАБЛИЦА 1. Состав переменных ДБС-модели умного производственного цеха

Уровень	Переменная	Тип	Состояния
L1	Пропуск ТО	Организационный	нет / однократный / систематический
L1	Квалификация	Организационный	высокая / средняя / низкая
L1	Перегрузка	Организационный	штатная / повышенная / критическая
L1	Нарушение регламента	Организационный	нет / легкое / грубое
L1	Смазка	Технический	норма / дефицит / критично
L1	Возраст компонента	Технический	новый / средний / изношенный

Уровень	Переменная	Тип	Состояния
L2	Износ подшипника	Скрытое техн.	норма / деградация / критично / отказ
L2	Риск перегрева	Скрытое техн.	низкий / средний / высокий / критический
L2	Механическое напряжение	Скрытое техн.	норма / повышенное / критичное
L3	Вибрация	Наблюдаемый	норма / повышенный / высокий / критический
L3	Температура	Наблюдаемый	норма / повышенная / высокая / критическая
L3	Ток	Наблюдаемый	норма / повышенный / высокий
L3	Шум	Наблюдаемый	норма / повышенный / высокий
L3	Брак	Наблюдаемый	норма / повышенная / высокая

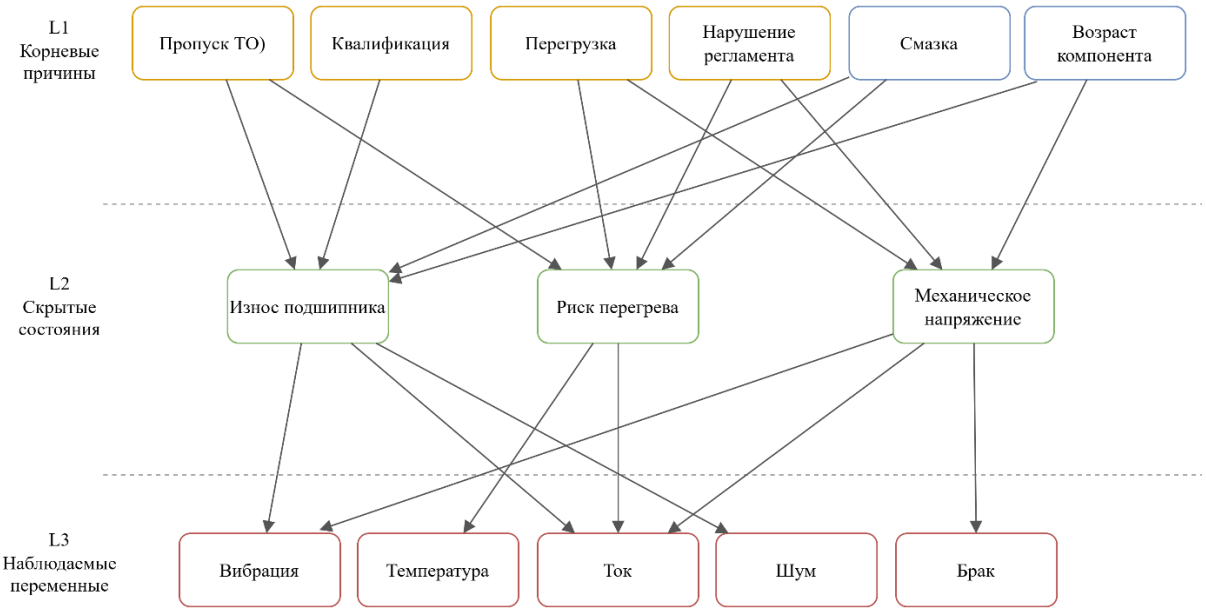


Рис. 1. Граф динамической байесовской сети умного производственного цеха

Алгоритм байесовского фильтра

На каждом такте в систему поступают новые значения переменных уровня L3. Алгоритм выполняет шаг фильтрации: апостериорные вероятности всех узлов обновляются с учетом наблюдений. Совместное распределение переменных по временным срезам с 1 по T записывается в виде [4]:

$$P(X^{1:T}) = P_0(X^1) \times \prod_{t=2}^{T} P(X^t | X^{t-1})$$

где X^t – вектор переменных в срезе t, $P(X^t \mid X^{t-1})$ – матрица условных вероятностей перехода, задаваемая переходной сетью B.

Реализация фильтра строится на методе прямого прохода. Маргинальные распределения узлов из среза t переносятся в срез $t + 1$ как мягкие доказательства. Если для переменной пришло конкретное показание датчика, системе назначается жесткое доказательство с вероятностью 1,0 для наблюдаемого состояния. Если показание в данный момент отсутствует, используются маргиналы предыдущего шага. Это позволяет модели корректно работать при частичном выходе из строя датчиков или временных пропусках в данных [5].

Таблицы условных вероятностей задаются экспертно на основе технических характеристик оборудования и данных об истории отказов. При накоплении достаточного объема архивных записей параметры уточняются с применением алгоритма EM.

Идентификация корневых причин

После шага фильтрации система ранжирует переменные уровня L1 по риску. Для каждой из них вычисляется взвешенная оценка вероятности нежелательных состояний, нормированная по числу состояний. Переменная с наибольшей оценкой признается наиболее вероятной первопричиной зарегистрированного отклонения.

Для формирования объяснения диагноза используется концепция марковского одеяла: для каждого L1-узла извлекается множество его родителей, дочерних узлов и совместных родителей дочерних узлов. На основе кратчайшего пути в графе между L1-узлом и сработавшими датчиками L3 строится цепочка «причина – следствие», которую система предъявляет оператору в виде текстового отчета.

Помимо текущей диагностики, система выполняет прогнозирование: вероятности состояний передаются через переходную матрицу итеративно на k шагов вперед без новых наблюдений. Это позволяет оценить момент наступления критического состояния до того, как датчики зафиксируют явные отклонения [6].

В работе описана трехуровневая архитектура динамической байесовской сети для прогнозирования корневых причин отказов производственного оборудования. Граф на 14 переменных охватывает технические и организационные факторы деградации, что важно для корректного отражения реальных условий эксплуатации. Алгоритм прямого прохода обеспечивает корректную работу при частично отсутствующих данных датчиков, а процедура ранжирования L1-узлов позволяет указать наиболее вероятную причину нарушения до момента отказа.

Список используемых источников

1. Mobley R. K. An Introduction to Predictive Maintenance. 2nd ed. Oxford: Butterworth-Heinemann, 2002. 456 p.

2. Lokrantz A., Gustavsson E., Jirstrand M. Root cause analysis of failures and quality deviations in manufacturing using machine learning // Procedia CIRP. 2018. Vol. 72. PP. 1057–1062. DOI: 10.1016/j.procir.2018.03.229.

3. Lipton Z. C. The mythos of model interpretability // ACM Queue. 2018. Vol. 16. Iss. 3. PP. 31–57. DOI: 10.1145/3236386.3241340.

4. Murphy K. P. Dynamic Bayesian Networks: Representation, Inference and Learning: PhD thesis / K. P. Murphy. Berkeley: University of California, 2002. 225 p.

5. Половко А. М., Гуров С. В. Основы теории надежности. 2-е изд. СПб.: БХВ-Петербург, 2006. 560 с.

6. Shiguihara P., Lopes A. A., Mauricio D. Dynamic Bayesian network modeling, learning, and inference: a survey // IEEE Access. 2021. Vol. 9. PP. 117639–117648. DOI: 10.1109/ACCESS.2021.3105520.

УДК 004.052.32:004.89

Р. М. Вивчарь (к.т.н., доцент кафедры ПИиВТ СПбГУТ)
М. А. Рябинкин (студент группы ИКПИ-22 СПбГУТ), ryabinkin.ma@sut.ru
Д. М. Ткач (студент группы ИКПИ-22 СПбГУТ), tkach.dm@sut.ru

ПОИСК ПЕРВОПРИЧИН СБОЕВ В МИКРОСЕРВИСНЫХ СИСТЕМАХ НА ОСНОВЕ КОНТРФАКТИЧЕСКОГО НЕЙРОСЕТЕВОГО МОДЕЛИРОВАНИЯ

Рассматривается задача автоматического поиска первопричин сбоев в микросервисных системах. Существующие нейросетевые подходы обладают двумя фундаментальными ограничениями: непрозрачность вывода и смешение корреляции с причинностью. Предлагается архитектура, объединяющая гиперграфовое нейросетевое моделирование с контрфактическим причинно-следственным выводом. Ключевая идея состоит в том, что контрфактическое вмешательство выполняется как дифференцируемая операция внутри нейросети: модель предсказывает, как изменилось бы состояние системы при нормализации каждого компонента. Нормальное состояние каждого компонента описывается адаптивной моделью, которая учитывает текущую нагрузку, время суток и версию развертывания. Описаны модуль обнаружения скрытых общих факторов, каскадная воронка для масштабируемости и формальная верификация причинного графа по пяти аксиомам.

микросервисные системы, поиск первопричин, причинно-следственный вывод, контрфактическое рассуждение, гиперграфовые нейронные сети, интерпретируемость, скрытые общие факторы

Микросервисная архитектура, благодаря своей гибкости и масштабируемости, стала ключевым элементом современных методик разработки программного обеспечения [1, 2]. Однако рост числа сервисов приводит к тому, что последствия неисправности одного компонента распространяются по цепочке зависимостей, затрагивая десятки других компонентов одновременно. Задача поиска первопричины состоит в определении того компонента, устранение неисправности которого восстановит нормальную работу всей системы.

Существующие подходы на основе графовых нейронных сетей обладают двумя ограничениями. Во-первых, непрозрачность вывода: модель выдает результат, не предоставляя обоснования [3]. Во-вторых, смешение корреляции с причинностью: совместное отклонение показателей может объясняться ненаблюдаемым общим фактором, а не причинной связью [4, 5].

Целью данной работы является разработка архитектуры, преодолевающей оба ограничения через интеграцию контрфактического причинно-следственного вывода в дифференцируемый вычислительный граф гиперграфовой нейронной сети.

Архитектура. Предлагаемая архитектура состоит из трех фаз: восприятие, рассуждение и объяснение.

В фазе восприятия разнородные данные телеметрии (метрики, журналы, трассировки) преобразуются в векторные представления. Метрики кодируются двуветвевым кодировщиком: ветвь устойчивых закономерностей на основе модели пространства состояний [6] извлекает долгосрочные паттерны, ветвь обнаружения разрывов вычисляет степень отклонения текущего состояния от недавнего прошлого [7]. Далее строится гиперграф с тремя типами статических ребер (вызовы, совместное размещение, балансировка нагрузки) и обучаемыми адаптивными ребрами [3, 8].

Условная модель нормального состояния. Нормальное состояние микросервиса зависит от условий эксплуатации: загрузка процессора при 100 и 10 000 запросах в секунду различается в разы, и оба значения являются нормой. Вместо единственного статического эталона используется условная смесь из D гауссовых компонент, параметры которой (центры, ковариации, веса) являются функциями контекстного вектора, описывающего текущую нагрузку, время суток и версию развертывания. При контрфактическом вмешательстве вектор компонента заменяется на условный прототип – центр наиболее вероятной компоненты при текущем контексте [5, 9].

Контрфактический интервенционный модуль. Ядро архитектуры реализует переход от корреляции к причинности через три шага. На первом шаге (абдукция) для каждого компонента вычисляется экзогенная переменная, описывающая собственный причинный вклад, отделенный от влияния соседей. Дополнительно вводятся латентные переменные скрытых общих факторов – ненаблюдаемых причин, одновременно влияющих на несколько компонентов [4, 10]. На втором шаге (вмешательство) вектор компонента-кандидата заменяется на условный прототип, что соответствует оператору *do()* в исчислении причинности Перла [4]. На третьем шаге (предсказание) измененные векторы пропускаются через гиперграфовую свертку, и вычисляется причинный эффект – разность аномальности системы до и после вмешательства.

Принципиальное отличие от существующих подходов состоит в дифференцируемости вмешательства: контрфактическая операция является частью вычислительного графа нейросети, а функция потерь штрафует ситуации, когда причинный эффект настоящей первопричины ниже, чем у другого компонента. В работе [5] контрфактический анализ выполняется после обучения как отдельная процедура.

На рисунке 1 показано сравнение двух подходов на примере системы из четырех компонентов. Корреляционный подход (рис. 1, а) ранжирует компоненты по степени отклонения от нормы и указывает на компонент *frontend* как на наиболее аномальный, однако высокая задержка *frontend* является следствием перегрузки *checkout*, а не самостоятельной неисправностью. Контрфактический подход (рис. 1, б) выполняет виртуальную нормализацию каждого кандидата и оценивает, насколько улучшится состояние всей системы. Нормализация *checkout* восстанавливает все остальные компоненты, поэтому его причинный эффект (ПЭ) максимален и равен 0,78, что однозначно указывает на него как на первопричину.

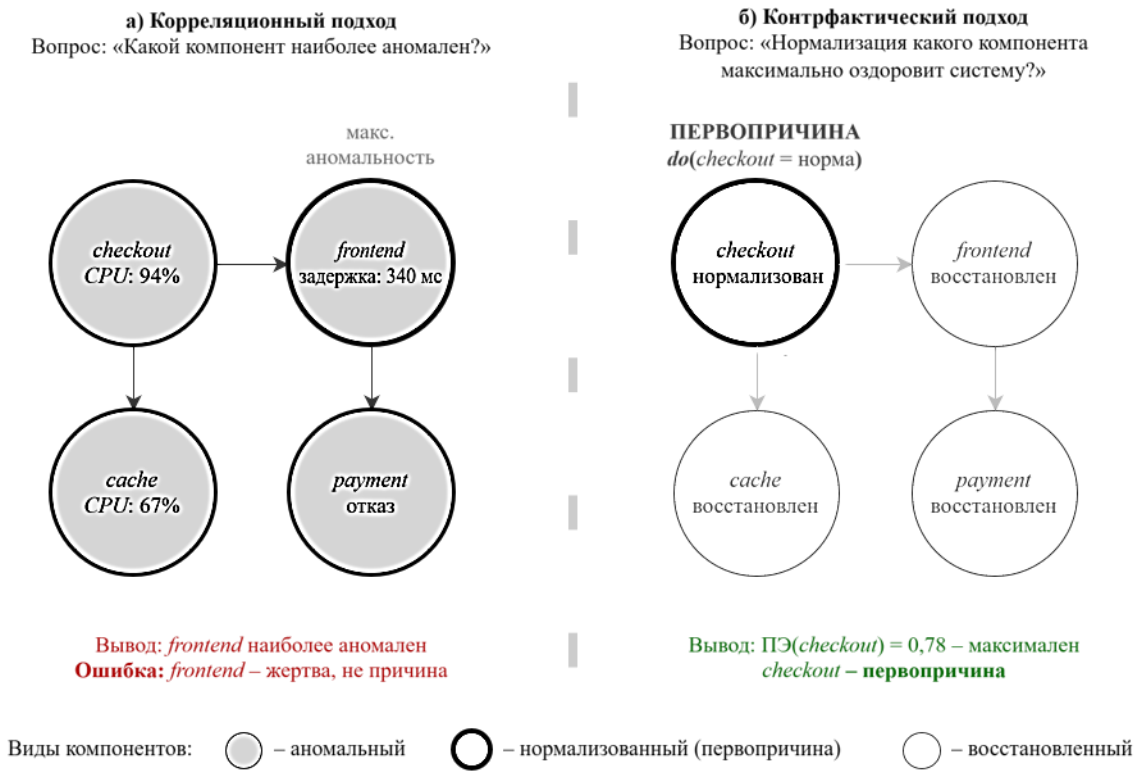


Рис. 1. Сравнение корреляционного (а) и контрфактического (б) подходов к поиску первопричины сбоя

Для обеспечения масштабируемости предложена трехступенчатая каскадная воронка (таблица 1): быстрый фильтр сужает пространство кандидатов, приближенный причинный анализ на локальных подграфах отбирает финалистов, и только они проходят полный контрфактический анализ.

ТАБЛИЦА 1. Характеристики ступеней каскадной воронки для системы из 500 компонентов

Ступень	Кандидаты	Время	Метод
Быстрая фильтр.	500 → 30	≈ 2 мс	*NLL* + профиль соседей
Приближ. анализ	30 → 5	≈ 50 мс	Подграф. интервенция
Полный анализ	5 → 1	≈ 200 мс	Контрфактика + верифик.

Верификация причинного графа. Причинный граф, построенный нейронной сетью, проверяется верификатором на соответствие пяти аксиомам: ацикличность (направленный граф не содержит циклов), темпоральная согласованность (причина не начинается позже следствия), транзитивность причинного эффекта, согласованность с топологией системы и монотонность вмешательства (эффект первопричины не ниже эффекта промежуточных компонентов). По результатам проверки каждому выводу присваивается оценка достоверности.

Обработка множественных первопричин. Реализованы три режима декомпозиции. Аддитивный режим применяется, если причины не взаимодействуют: эффект первой первопричины вычитается, на остатке запускается повторный поиск. Совместный режим перебирает подмножества кандидатов при нелинейном взаимодействии причин. Вероятностный режим на основе работы [11] назначает каждому компоненту апостериорную вероятность быть первопричиной.

В фазе объяснения формируется проверяемая цепочка доказательств – направленный подграф от первопричины к симптомам с аннотациями типов связей и их силы [12]. Текстовое объяснение генерируется каскадом из шаблонного генератора и локальной языковой модели, после чего проверяется набором логических правил [13]. При нарушении правил объяснение отклоняется и заменяется шаблонным.

Обоснование новизны. Предлагаемая архитектура отличается от существующих подходов по четырем ключевым аспектам. Во-первых, контрфактическое вмешательство является дифференцируемой операцией внутри

нейросети: модель обучается различать причины и следствия. Во-вторых, условная модель нормального состояния адаптируется к условиям эксплуатации, обеспечивая устойчивость к дрейфу распределения. В-третьих, латентные переменные скрытых общих факторов позволяют обнаруживать ненаблюдаемые причины ложных корреляций. В-четвертых, формальная верификация причинного графа по пяти аксиомам дополняет нейросетевой вывод формальными гарантиями.

Заключение. Предложена архитектура, преодолевающая проблемы непрозрачности и корреляционного подхода через интеграцию контрфактического причинно-следственного вывода, обнаружения скрытых общих факторов и формальной верификации причинного графа. Дальнейшая работа направлена на реализацию прототипа и экспериментальную валидацию на общедоступных наборах данных GAIA, TrainTicket и RCAEval.

Список используемых источников

1. Fu N., Cheng G., Teng Y., Dai G., Yu S., Chen Z. Intelligent Root Cause Localization in MicroService Systems: A Survey and New Perspectives // ACM Computing Surveys. 2025. Vol. 57. Iss. 12. 37 p. URL: https://dl.acm.org/doi/10.1145/3736755 (дата обращения: 14.03.2026).

2. Notaro P., Cardoso J., Gerndt M. A Survey of AIOps Methods for Failure Management // ACM Transactions on Intelligent Systems and Technology. 2021. Vol. 12. Iss. 6. PP. 1–45. URL: https://dl.acm.org/doi/10.1145/3483424 (дата обращения: 11.04.2026).

3. Zhao Z., Wang Z., Zhang T. и др. CHASE: A Causal Hypergraph based Framework for Root Cause Analysis in Multimodal Microservice Systems // arXiv preprint. 2024. URL: https://arxiv.org/abs/2406.19711 (дата обращения: 22.04.2026).

4. Pearl J., Mackenzie D. The Book of Why: The New Science of Cause and Effect. New York: Penguin Books, 2019. 418 p.

5. Tian X. и др. CRFD: Causal and Interpretable Fault Diagnosis Using Counterfactual Reasoning for Microservices on Multi-source Observability Data // ACM Transactions on Software Engineering and Methodology. 2026. URL: https://dl.acm.org/doi/10.1145/3796706 (дата обращения: 26.04.2026).

6. Zhou W. и др. SSMGNN: Spectral Temporal Graph Neural Network with State Space Models for Multivariate Time-series Forecasting // Preprint submitted to Neurocomputing. 2025.

7. Zhang S. и др. DynaCausal: Dynamic Causality-Aware Root Cause Analysis for Distributed Microservices // arXiv preprint. 2025. URL: https://arxiv.org/abs/2510.22613 (дата обращения: 23.04.2026).

8. Xie S. и др. Root Cause Analysis for Microservice Systems via Cascaded Conditional Learning with Hypergraphs // arXiv preprint. 2025. URL: https://arxiv.org/abs/2511.17566 (дата обращения: 09.04.2026).

9. Георги М. Ю. Методы извлечения причинности из данных наблюдений в практике искусственного интеллекта // Известия ЮФУ. Технические науки. 2023.

10. Han X., Absar S., Zhang L., Yuan S. Root Cause Analysis of Anomalies in Multivariate Time Series through Granger Causal Discovery // ICLR. 2025.

11. Jha S. и др. Causal AI-based Root Cause Identification: Research to Practice at Scale // arXiv preprint. 2025. URL: https://arxiv.org/abs/2502.18240 (дата обращения: 20.04.2026).

12. Hou J. Research on Fault Diagnosis and Root Cause Analysis Based on Full Stack Observability // arXiv preprint. 2025. URL: https://arxiv.org/abs/2509.12231 (дата обращения: 19.04.2026).

13. Galitsky B., Rybalov A. Neuro-Symbolic Verification for Preventing LLM Hallucinations in Process Control // Processes. 2026. Vol. 14. Iss. 2. 322. URL: https://www.mdpi.com/2227-9717/14/2/322 (дата обращения: 29.03.2026).

УДК 780.6

Е. П. Вильготский (студент группы ИСТ-221 СПбГУТ),
vilgotsky.ep@sut.ru
Е. В. Коровкина (ассистент кафедры СОД СПБГУТ)

ВЕБ-ПРИЛОЖЕНИЕ ГИТАРНЫЙ ТЮНЕР С ГЕЙМИФИЦИРОВАННОЙ СРЕДОЙ ДЛЯ ОБУЧЕНИЯ

В статье рассматривается проблема высокой степени отсева начинающих гитаристов, связанная со сложностью настройки инструмента и низкой вовлеченностью в процесс обучения. Предлагается решение в виде веб-приложения, интегрирующего высокоточный алгоритмический тюнер на основе анализа звукового сигнала с микрофона и геймифицированную среду обучения. Анализируются современные подходы к геймификации образования и их применимость для повышения мотивации при освоении базовых музыкальных навыков. Описываются архитектура приложения, алгоритмы обработки аудиосигнала и игровые механики, направленные на формирование устойчивого интереса к регулярным занятиям.

геймификация образования, веб-приложение, гитарный тюнер, обработка аудиосигнала, мотивация, музыкальное образование, цифровая педагогика

В настоящее время наблюдается устойчивый рост интереса к обучению игре на музыкальных инструментах, в частности на гитаре. Как отмечают аналитики, гитары стабильно составляют около 30 % от общего объема продаж акустических музыкальных инструментов в мире [1]. Однако путь начинающего музыканта сопряжен с трудностями. Исследования показывают, что новички испытывают значительные сложности с первоначальной настройкой инструмента, а около 40 % бросают занятия в первые полгода из-за недостатка мотивации [2]. Традиционные методы настройки требуют опыта и развитого слуха, а специализированные устройства (тюнеры) создают дополнительные финансовые и физические барьеры.

Современные информационные технологии позволяют комплексно подойти к решению этих проблем. С одной стороны, алгоритмы цифровой обработки сигналов дают возможность создать точный и бесплатный инструмент для настройки, доступный на любом устройстве с микрофоном и браузером. С другой стороны, методология геймификации предлагает инструменты для превращения рутинных упражнений в увлекательный процесс. Геймификация образования определяется как стратегия повышения вовлеченности путем включения игровых элементов в образовательную

среду [3]. Ее цель – создать уровни вовлеченности, сопоставимые с тем, что обычно могут дать игры.

Однако, как подчеркивает В. Д. Емельяненко, применение игровых технологий не является универсальным трендом и имеет свои пределы. Эффективность геймификации напрямую зависит от ценностно-мировоззренческой сферы обучающихся и социальных условий образовательной среды [4]. Важно, чтобы игровые механики не подменяли собой образовательные цели, а служили средством их достижения. Исследователи также предупреждают, что при недостаточной внутренней мотивации учащегося геймификация может привести к формированию мотивации не к обучению, а к самой игре [3-5]. Поэтому при разработке геймифицированных систем необходимо тщательно проектировать сценарии, в которых игровые элементы направлены на достижение конкретных педагогических результатов.

Разрабатываемое веб-приложение «Гитарный тюнер с геймифицированной средой для обучения» призвано реализовать комплексный подход. Ключевое отличие предлагаемого решения от существующих аналогов заключается в интеграции двух функциональных модулей в едином веб-интерфейсе:

1. Модуль точной настройки, который на основе алгоритмов цифровой обработки сигналов анализирует частоту звука с микрофона в реальном времени. Входной аудиосигнал x(t), представленный дискретными отсчетами x[n], подвергается дискретному преобразованию Фурье (ДПФ), позволяющему перейти от временного представления к частотному:

$$X[k] = \sum_{n=0}^{N-1} x\,[n] \cdot \mathrm{e}^{-j\frac{2\pi}{N}kn}$$

где $X[k]$ – комплексная амплитуда k-й частотной составляющей. Пиковые значения амплитудного спектра $|X[k]|$ соответствуют основным частотам звучащих струн, которые затем сравниваются с эталонными частотами $f_{эталон}$ для выбранного строя (E2, A2, D3, G3, B3, E4 для стандартного строя). Полученная разница $\Delta f = f_{измеренная} - f_{эталонная}$ визуализируется пользователю, указывая направление подстройки колка.

2. Геймифицированный учебный модуль, в котором отработка базовых аккордов и упражнений представлена в виде интерактивных заданий. Система включает следующие игровые механики:

- начисление очков за точность и скорость выполнения упражнений;
- систему уровней и достижений (бейджей);

- визуализацию прогресса;

Для наглядности представим сравнение традиционного подхода к начальному обучению и предлагаемого геймифицированного решения (табл. 1).

ТАБЛИЦА 1. Сравнение подходов к обучению

Параметр сравнения	Традиционный подход	Геймифицированный подход
Настройка инструмента	Тюнер-устройство или на слух (требует опыта)	Встроенный алгоритмический тюнер в веб-браузере
Мотивация	Внешняя (необходимость, дисциплина)	Внутренняя и внешняя (интерес, соревнование, награды)
Обратная связь	Отсроченная (педагог)	Мгновенная (визуализация, звук)
Доступность	Ограничена местом и временем	24/7 с любого устройства с микрофоном
Отслеживание прогресса	Самостоятельно или с педагогом	Автоматизированное (статистика, достижения)

Научная новизна работы заключается в комплексном применении методов геймификации к специфической предметной области – начальному музыкальному образованию – с одновременной интеграцией инструментальных средств в единую веб-среду.

Практическая значимость исследования состоит в создании доступного инструмента, который может быть использован как для самостоятельного обучения, так и в качестве вспомогательного средства в музыкальных школах и студиях. Система не требует установки дополнительного программного обеспечения, работает на любых устройствах и не предъявляет высоких требований к аппаратному обеспечению.

Таким образом, создание подобного программного комплекса направлено на повышение эффективности начального музыкального образования. Интеграция точного инструментария и игровых методов обучения позволяет снизить порог вхождения для новичков, нивелировать «человеческий фактор» при настройке и создать устойчивую мотивацию для регулярных занятий, что в итоге может способствовать снижению уровня отсева среди начинающих музыкантов.

Список используемых источников

1. NAMM. NAMM Global Report 2023: Industry insights. 2023. URL: https://www.namm.org/sites/default/files/2023-12/2023_NAMM_IndustryInsights_Final.pdf (дата обращения: 18.02.2026).

2. Sailer U. J. J., et al. Survival of musical activities. When do young people stop making music? // PLoS ONE. 2021. Vol. 16. № 11. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8612519/ (дата обращения: 18.02.2026).

3. Мурзагалина Г. М., Тихомирова Г. В., Филиппова О. В., Корнеева Н. Ю., Галиакберова В. Н. Геймификация в образовании как фактор повышения интереса к усвоению учебного материала // Московский экономический журнал. 2022. № 4. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-4-2022-29/ (дата обращения: 18.02.2026). DOI: 10.55186/2413046X_2022_7_4_227.

4. Емельяненко В. Д. Геймификация в образовании: пределы применения (ценностно-мировоззренческий подход) // Философия образования. 2018. № 75, вып. 2. С. 130–146. DOI: 10.15372/PHE20180211.

5. Sailer M., Homner L. The Gamification of Learning: a Meta-analysis // Educational Psychology Review. 2020. Vol. 32. № 1. P. 77–112. URL: https://link.springer.com/ article/10.1007/s10648-019-09498-w (дата обращения: 18.02.2026).

Статья представлена и. о. заведующего кафедрой СОД СПбГУТ, кандидатом технических наук, доцентом Ю. М. Бородянским.

УДК 004.056.55

СОВРЕМЕННЫЕ ПРОБЛЕМЫ КРИПТОГРАФИИ ПРИ ПОЯВЛЕНИИ КВАНТОВЫХ КОМПЬЮТЕРОВ

А. В. Герасимов (студент группы ИСТ-223 СПбГУТ),
gerassimov.av@sut.ru
Ю. Я. Перевозник (к.п.н., доцент кафедры СОД СПбГУТ)

Статья посвящена анализу современных проблем криптографии в условиях появления квантовых компьютеров и формирования квантовой угрозы для классических криптосистем. Рассматриваются ограничения алгоритмов RSA и криптографии на эллиптических кривых при наличии квантовых вычислительных средств и описывается сценарий «собрать сейчас – расшифровать позже». Обобщены основные подходы постквантовой криптографии, включая решеточные, хеш-основанные и код-основанные схемы, а также результаты международной стандартизации. Особое внимание уделено практическим задачам миграции на постквантовые алгоритмы и использованию гибридных криптографических решений в защищенных информационных системах.

квантовые вычисления, классические криптосистемы, постквантовая криптография, квантовые угрозы, алгоритм Шора, решетчатые задачи, гибридные криптографические схемы

Современное информационное общество опирается на массовое использование криптографии: она защищает электронные платежи, государственные сервисы, корпоративные сети и персональные данные пользователей. На протяжении десятилетий основой такой защиты были классические алгоритмы на открытых ключах, в первую очередь RSA и криптография на эллиптических кривых, которые обеспечивали приемлемый уровень стойкости против известных атак. Их безопасность связывали со сложностью математических задач факторизации больших чисел и вычисления дискретного логарифма, для которых у классических компьютеров нет эффективных алгоритмов.

Появление и развитие квантовых вычислений приводит к качественно новой ситуации [1, 2]. Алгоритм Шора показал, что квантовый компьютер принципиально способен эффективно решать задачи, на которых основаны RSA и многие схемы на эллиптических кривых. Это означает, что при достижении достаточного уровня развития квантовых устройств значительная часть существующей криптографической инфраструктуры утратит стойкость [1, 3]. Важно, что речь идет не только о будущих данных: сценарий «собрать сейчас – расшифровать позже» предполагает, что перехваченные

сегодня зашифрованные сообщения могут быть раскрыты спустя годы, когда квантовые средства станут практически доступны [3, 4].

Такая перспектива особенно чувствительна для сфер, где информация должна оставаться закрытой длительное время. К ним относятся государственное управление, оборонная и финансовая сферы, здравоохранение и другие виды деятельности, где утечка данных может иметь долгосрочные последствия [2, 4]. В результате квантовая угроза воспринимается не как абстрактный научный риск, а как фактор, который уже сейчас необходимо учитывать при проектировании и эксплуатации информационных систем [2, 4].

Ответом на эти вызовы становится развитие постквантовой криптографии [2, 5, 6, 7]. Под этим термином понимают набор криптографических схем, которые считаются устойчивыми к известным квантовым атакам и при этом могут реализовываться на обычных, неквантовых вычислительных платформах [5, 6, 7]. В отличие от RSA и ECC такие алгоритмы опираются на другие классы математических задач: решеточные и кодовые задачи, хеш-функции, системы многочленов от нескольких переменных [5, 8, 9, 6, 7, 10]. Для них на сегодняшний день не найдено квантовых алгоритмов, сопоставимых по эффекту с алгоритмом Шора, а значит, они рассматриваются как перспективная основа для обновленной криптографической инфраструктуры [2, 6, 7].

В последние годы наиболее активно развиваются решеточные схемы [5, 6, 7, 8]. Они связаны с задачами поиска кратчайшего и ближайшего вектора в высокоразмерных решетках и с задачей Learning with Errors, в которой необходимо восстановить секретную информацию по набору линейных соотношений с небольшими случайными искажениями [6, 7]. Преимуществом такого подхода является сочетание теоретических гарантий и приемлемой производительности на практических платформах [5, 6, 7, 8]. В результате именно решеточные алгоритмы стали основой первых государственных стандартов постквантовой криптографии [5, 8].

Значимым этапом в формировании нового криптографического ландшафта стал процесс стандартизации, инициированный Национальным институтом стандартов и технологий США [2, 4, 5, 8, 9]. В его рамках были собраны, проанализированы и сопоставлены десятки предложенных схем, после чего к 2024 году опубликованы первые стандарты для постквантового распределения ключей и цифровой подписи [4, 5, 8, 9]. Эти документы ори-

ентированы на широкое практическое применение: от протоколов защищенного соединения в интернете до инфраструктуры открытых ключей и государственных информационных систем [2, 4, 5, 8, 9].

Однако появление стандартов – лишь часть задачи. Не менее сложной проблемой оказывается реальная миграция существующих систем на новые алгоритмы [2, 4]. В отличие от теоретических моделей, где можно просто «заменить одну функцию на другую», в практической инфраструктуре криптография встроена в протоколы, программное обеспечение, аппаратные модули и организационные процессы [2, 4]. Постквантовые алгоритмы часто требуют более крупных ключей и подписей, что влияет на объем передаваемых данных, требования к памяти и пропускной способности сетей, особенно в условиях ограниченных устройств интернета вещей [4, 9].

Существенные вызовы возникают и на уровне инфраструктуры открытых ключей. Необходимо пересматривать форматы сертификатов, механизмы проверки статуса ключей, процедуры выпуска и отзыва, а также учитывать, что в период перехода в обращении будут одновременно находиться классические и постквантовые сертификаты [2, 4]. Аналогичные проблемы возникают для аппаратных модулей безопасности, которые проектировались под ограниченный набор классических алгоритмов и требуют модернизации или замены для поддержки новых схем [2, 4].

На переходный период все большее значение приобретают гибридные решения [2, 4]. Под ними понимают совместное использование классических и постквантовых алгоритмов в рамках одного протокола или системы, когда стойкость считается приемлемой при условии сохранения безопасности хотя бы одного из компонентов [2, 4]. Такой подход позволяет одновременно учитывать квантовую угрозу и не полностью отказываться от проверенных классических механизмов, снижающих риск возможных ошибок в новых схемах [2, 4]. Гибридные протоколы уже обсуждаются и внедряются в современных стандартах защищенных соединений и инфраструктуры открытых ключей [2, 4].

Планируемая миграция на постквантовую криптографию требует системного подхода. Организациям предлагается начинать с инвентаризации используемых криптографических механизмов, оценки сроков, в течение которых должна сохраняться конфиденциальность данных, и выделения наиболее критичных систем. На следующем этапе целесообразно развертывать пилотные проекты с использованием постквантовых и гибридных схем, отрабатывать интеграцию в конкретных протоколах и программных

продуктах, а затем постепенно расширять область применения. Важным принципом становится криптографическая «ловкость»: архитектура систем должна позволять относительно легко заменять алгоритмы и параметры по мере появления новых требований и результатов исследований [2, 4].

Таким образом, современные проблемы криптографии при появлении квантовых компьютеров носят комплексный характер. С одной стороны, речь идет о фундаментальной смене математической базы, на которой строится стойкость используемых алгоритмов. С другой стороны, требуется глубокая модернизация действующей инфраструктуры и организационных процессов. Постквантовая криптография уже перешла из области академических исследований в сферу практической стандартизации, и в ближайшие годы именно от качества ее внедрения будет зависеть устойчивость цифровой инфраструктуры к будущим квантовым угрозам [2, 4, 5, 8, 9].

Список используемых источников

1. Shor P.W. Algorithms for quantum computation: Discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. 1994. p. 124–134.

2. Chen L., Moody D., Shen Y. NIST Post-Quantum Cryptography Standardization // NIST Interagency Report 8105, 2016.

3. Gidney C., Ekera M. How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits // arXiv preprint.

4. NIST IR / SP по переходу к постквантовой криптографии (Transition to Post-Quantum Cryptography Standards). NIST, 2024.

5. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). U.S. Dept. of Commerce, 2024.

6. Regev O. On lattices, learning with errors, random linear codes, and cryptography // Proceedings of the 37th Annual ACM Symposium on Theory of Computing. 2005. p. 84–93.

7. Peikert C. Public-key cryptosystems from the worst-case shortest vector problem // Proceedings of the 41st Annual ACM Symposium on Theory of Computing. 2009. p. 333–342.

8. National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA). U.S. Dept. of Commerce, 2024.

9. National Institute of Standards and Technology. FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SHA-DSA). U.S. Dept. of Commerce, 2024.

10. Bernstein D.J. et al. SPHINCS: Practical stateless hash-based signatures // EUROCRYPT. 2015.

УДК 004.5

DATA-INFORMED DESIGN В ПРОЕКТИРОВАНИИ ЦИФРОВЫХ ИНТЕРФЕЙСОВ

Д. А. Гребенщиков (студент группы ИКВТ-21 СПбГУТ),
grebenshikov.da@sut.ru

В статье рассматривается подход Data-Informed Design в проектировании цифровых интерфейсов. Раскрывается его сущность, описываются виды данных, используемых в процессе разработки, а также механизмы применения на практике. Проводится сравнение с Data-Driven подходом, выделяются ограничения и риски. Отдельное внимание уделяется перспективам развития, связанным с аналитикой, искусственным интеллектом и персонализацией интерфейсов. Показано, что использование данного подхода позволяет принимать более обоснованные проектные решения и повышать качество пользовательского опыта.

UX/UI, пользовательский опыт, анализ данных, цифровые интерфейсы, Data-Informed Design

Современные цифровые интерфейсы должны быть не только визуально привлекательными, но и удобными, понятными и эффективными для пользователя. В условиях высокой конкуренции и постоянного роста требований к качеству взаимодействия традиционного подхода, основанного только на интуиции дизайнера, уже недостаточно. По этой причине все большую значимость приобретает Data-Informed Design, при котором решения принимаются с опорой на данные о поведении пользователей, но сами данные не подменяют собой процесс проектирования. Они помогают точнее увидеть проблему, понять контекст использования продукта и проверить гипотезу, а итоговое решение формируется с учетом целей продукта, потребностей аудитории и профессионального суждения дизайнера [1].

Такой подход отличается от Data-Driven Design ролью данных в принятии решения [2]. Если Data-Driven подход чаще предполагает прямую реакцию на метрики и результаты экспериментов, то Data-Informed Design рассматривает данные как важный, но не единственный источник выводов. В процессе проектирования обычно используются два типа данных. Количественные данные отражают измеримые показатели поведения пользователей, к ним относятся активность аудитории, удержание, конверсия, кликабельность элементов, показатель отказов, время взаимодействия с интерфейсом и успешность выполнения задач. Эти данные помогают понять, что именно делает пользователь в системе. Качественные данные,

напротив, позволяют ответить на вопрос, почему это происходит. Сюда относятся пользовательские интервью, юзабилити-тестирование, отзывы и наблюдение за взаимодействием с интерфейсом. Именно сочетание количественных и качественных данных дает более целостное представление о пользовательском опыте [3].

В практической работе Data-Informed Design реализуется как последовательный итерационный процесс. Сначала анализируются данные и выявляется проблемная зона, например отказ пользователей от регистрации, незавершенное оформление заказа или игнорирование ключевой функции. Затем формулируется гипотеза, объясняющая причину наблюдаемого поведения. После этого в интерфейс вносятся изменения, упрощается сценарий взаимодействия, уточняется визуальная иерархия, перерабатываются тексты, логика экранов и пользовательские пути. На заключительном этапе обновленное решение проверяется с помощью аналитики, пользовательских исследований или A/B-тестирования. Если гипотеза подтверждается, изменения закрепляются, если нет, цикл повторяется. В таком процессе данные дают ответ на вопрос, что происходит, а эмпатия, исследования и дизайнерская интерпретация помогают понять, почему это происходит и как именно следует изменить интерфейс.

Логику этого цикла можно представить следующим образом (рис. 1) [1].

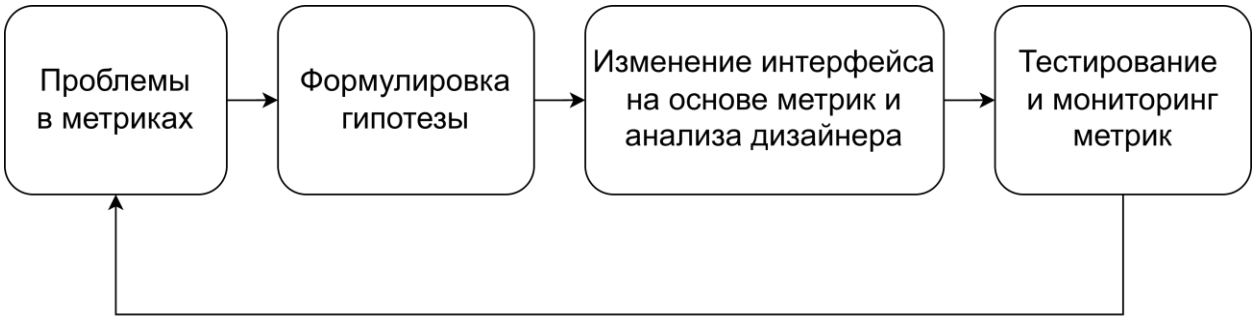


Рис. 1. Итерационный процесс Data-Informed Design

Благодаря такому подходу интерфейс перестает быть статичным и развивается на основе реального пользовательского поведения. Это особенно важно в тех сферах, где ошибка в проектном решении напрямую влияет на конверсию, удобство и восприятие продукта. Data-Informed Design применяется в UX/UI и продуктовой разработке, в электронной коммерции и маркетинге, в веб-проектах, ориентированных на рост, а также в играх, медиа и цифровых сервисах [2]. В каждой из этих сфер данные помогают

выявлять слабые места интерфейса и принимать более обоснованные решения.

ТАБЛИЦА 1. Области применения Data-Informed Design и примеры использования

Область применения	Примеры использования
UX/UI и продуктовая разработка	Оптимизация интерфейсов, A/B-тесты, разработка новых функций на основе пользовательских данных
E-commerce и маркетинг	Персонализация предложений, анализ Customer Journey, улучшение креативов и конверсии
Веб и Growth-Driven Design	Запуск MVP, развитие продукта по данным, проверка гипотез после запуска
Игры, медиа, цифровые сервисы	Балансировка геймплея, персонализация контента, анализ поведения аудитории

Приведенные в таблице 1 примеры показывают, что Data-Informed Design позволяет выявлять слабые места интерфейсов, такие как сложная навигация, перегруженные экраны и лишние действия пользователя, и на основе этого улучшать цифровые продукты [2].

На практике ценность Data-Informed Design проявляется еще и в том, что он позволяет избежать механического подчинения метрикам. Даже высокий объем аналитики не всегда объясняет мотивы и ожидания пользователей. Большие массивы данных хорошо показывают действия людей, но не раскрывают их эмоции, намерения и причины выбора. Поэтому для качественного проектирования цифровых интерфейсов важно сочетать поведенческую аналитику с более глубокими исследовательскими методами. Такой баланс помогает не только фиксировать проблему, но и понимать ее смысл в контексте реального пользовательского опыта [1].

Несмотря на преимущества, данный подход имеет и ограничения. Не все характеристики пользовательского опыта можно выразить в числах, поскольку доверие, удобство и эмоциональное восприятие интерфейса плохо сводятся к одной метрике. Кроме того, качество выводов напрямую зависит от качества собранных данных. Ошибки в аналитике, некорректная интерпретация результатов, ложные причинно-следственные связи, смещение подтверждения и переоптимизация под отдельные показатели способны привести к неверным решениям. Еще одно ограничение связано с тем, что

данные описывают уже совершившееся поведение пользователей и не всегда позволяют точно предсказать будущие сценарии использования продукта [2].

Перспективы развития Data-Informed Design связаны с дальнейшим усложнением аналитики и ростом роли интеллектуальных инструментов обработки данных. Уже сегодня становится очевидно, что проектирование все чаще опирается не на один источник информации, а на сочетание поведенческих сигналов, исследовательских наблюдений и цифровых следов пользователей [4]. Это создает основу для более адаптивных, персонализированных и контекстно чувствительных интерфейсов, в которых решения принимаются точнее и быстрее. Однако даже при усилении роли искусственного интеллекта и автоматизированной аналитики ключевой задачей дизайнера остается интерпретация данных через призму человеческого опыта и целей продукта [1].

Таким образом, Data-Informed Design можно рассматривать как современный и сбалансированный подход к проектированию цифровых интерфейсов. Он объединяет анализ данных и человеко-ориентированное мышление, позволяет выявлять проблемные зоны интерфейса, формулировать и проверять гипотезы, а также принимать более точные и аргументированные проектные решения. Использование данного подхода помогает создавать не только более эффективные, но и более удобные, понятные и устойчивые цифровые продукты.

Список использованных источников

1. Wong C. K. Understanding Data-Informed Design, the job niche that's kept me in demand. URL: https://dataanddesign.substack.com/p/understanding-data-informed-design (дата обращения: 15.03.2026).

1. Simpson A. Data Driven Design vs. Data Informed Design in Enterprise Products. URL: https://marvelapp.com/blog/data-driven-vs-data-informed-design-enterprise-products/ (дата обращения: 15.03.2026).

3. What is data-driven vs. data-informed design? URL: https://www.educative.io/answers/what-is-data-driven-vs-data-informed-design (дата обращения: 14.03.2026).

4. Pavliscak P. Data-Informed Product Design. URL: https://ru.scribd.com/document/335516010/Data-Informed-Product-Design (дата обращения: 12.03.2026).

Статья представлена доктором технических наук, заведующий кафедрой ИКС СПбГУТ, доцентом М. А. Маколкиной.

УДК 656.13.021.2:519.876.5

ИССЛЕДОВАНИЕ МЕТОДОВ НЕЧЕТКОГО ПРОГНОЗИРОВАНИЯ ПЛОТНОСТИ ТРАНСПОРТНОГО ПОТОКА ДЛЯ ПРЕДОТВРАЩЕНИЯ ОБРАЗОВАНИЯ ЗАТОРОВ

А. Н. Губин (к.т.н., доцент, доцент кафедры ИУС СПбГУТ)
Н. Т. Райымбеков (студент группы МКТ-2511 СПбГУТ),
raiymbekov.nt@sut.ru

Рассматриваются современные методы нечеткого прогнозирования плотности транспортного потока как инструмент повышения эффективности управления дорожным движением. Проведен анализ существующих подходов к моделированию транспортных потоков, включая классические детерминированные и вероятностные модели. Особое внимание уделено применению аппарата нечеткой логики для обработки неопределенных и неполных данных, характерных для транспортных систем. Разработана модель прогнозирования плотности потока на основе нечетких правил, учитывающих скорость движения, интенсивность потока и дорожные условия. Представлены результаты моделирования, демонстрирующие повышение точности прогнозирования и снижение вероятности образования заторов.

нечеткая логика, транспортный поток, плотность движения, прогнозирование, интеллектуальные транспортные системы, заторы

Введение

Современные транспортные системы характеризуются высокой степенью загруженности, что приводит к частому образованию заторов. Проблема управления транспортными потоками является одной из ключевых задач городского планирования и интеллектуальных транспортных систем. Традиционные методы моделирования, основанные на строгих математических зависимостях, зачастую не учитывают неопределенность и вариативность дорожных условий.

В связи с этим актуальным становится применение методов нечеткой логики, позволяющих учитывать неточности и субъективные оценки параметров транспортного потока. Целью данной работы является исследование методов нечеткого прогнозирования плотности транспортного потока для предотвращения образования заторов.

Основная часть

1. Анализ существующих методов прогнозирования плотности транспортного потока

Плотность транспортного потока q (авт./км) является одним из ключевых макроскопических параметров, наряду с интенсивностью I (авт./час)

и средней скоростью v (км/ч). Фундаментальное соотношение гидродинамической аналогии связывает эти три величины выражением $q = I/v$ [1]. Данное уравнение справедливо для стационарных и однородных потоков, однако в реальных городских условиях динамика движения носит резко нестационарный характер, что существенно усложняет прямое измерение плотности. На практике прямое определение плотности требует применения видеодетекции или лазерного сканирования, что сопряжено с высокими вычислительными затратами и чувствительностью к погодным условиям. Поэтому чаще используются косвенные оценки плотности на основе данных индуктивных петлевых детекторов, радаров или GPS-треков отдельных транспортных средств [2].

Существующие методы прогнозирования плотности транспортного потока могут быть классифицированы на три основные группы:

- детерминированные модели (модель Лайтхилла – Уизема – Ричмонда) – хорошо описывают макроскопическую динамику, но требуют точных начальных и граничных условий;
- статистические методы (ARIMA, экспоненциальное сглаживание) – адекватны при стационарных режимах, но не справляются с резкими всплесками плотности;
- нейросетевые подходы – обладают высокой точностью, но требуют больших размеченных выборок и трудно интерпретируемы.

Недостатком классических моделей является их низкая устойчивость к неопределенности входных данных. В реальных условиях такие параметры, как скорость, плотность и интенсивность, не могут быть точно измерены.

Нечеткие модели занимают промежуточное положение: они устойчивы к шумам, используют экспертные правила и легко адаптируются под конкретный участок дорожной сети.

2. Нечеткая модель прогнозирования плотности

В работе предлагается нечеткая модель типа Сугено первого порядка с двумя входами: текущая интенсивность $I(t)$ и средняя скорость $v(t)$. Выход – прогнозируемая плотность $q(t + T)$ (см. рис. 1) [3].

2.1 Фаззификация входных переменных

Для каждого входа определены лингвистические термы:

- интенсивность I: «низкая» (Low), «средняя» (Medium), «высокая» (High);

● скорость v: «очень низкая» (VL), «низкая» (L), «нормальная» (N), «высокая» (H).

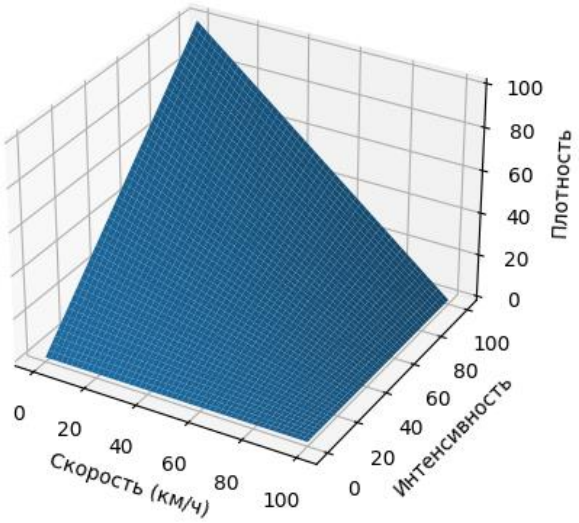


Рис. 1 Зависимость плотности от скорости и интенсивности

На рис. 1 показано, что при снижении скорости и увеличении интенсивности наблюдается резкий рост плотности транспортного потока.

2.2 База нечетких правил

База нечетких правил представляет собой конечное множество лингвистических высказываний вида «ЕСЛИ – ТО», формализующих эвристические зависимости между входными переменными [4]. Общее число правил в базе знаний составляет 12, что соответствует комбинации термов, имеющих содержательную интерпретацию с точки зрения теории транспортных потоков.

Каждое правило имеет следующую структуру:

$$R^{(k)}\text{:ЕСЛИ } I \in A_i^{(k)} \text{ И } v \in B_j^{(k)} \text{ ТО } \hat{q} = f^{(k)}(I, v) \quad (1)$$

где $A_i^{(k)}$, $B_j^{(k)}$ – нечеткие множества, определенные на универсумах интенсивности и скорости соответственно; $f^{(k)}(I, v)$ – функция заключения правила [5].

В настоящем исследовании использована модель Сугено первого порядка, в которой функция заключения линейна относительно входных переменных:

$$f^{(k)}(I, v) = a_k \cdot \frac{I}{v} + b_k \quad (2)$$

где a_k, b_k – вещественные параметры, настраиваемые по эмпирическим данным; I/v – отношение интенсивности к скорости, являющееся оценкой мгновенной плотности.

Формирование базы правил осуществлялось на основе фундаментальной диаграммы транспортного потока, а также экспертной информации, полученной от специалистов центров организации дорожного движения. Фрагмент базы правил с указанием типовых режимов приведен в табл. 1.

Таблица 1. База нечетких правил указанием типовых режимов

№ правила	условие	заключение
1	I – «низкая» и v – «высокая»	$\hat{q}$ = 0,85·(I/v) (свободный режим)
2	I – «средняя» и v – «нормальная»	$\hat{q}$ = 1,00·(I/v) (устойчивый режим)
3	I – «высокая» и v – «очень низкая»	$\hat{q}$ = 1,15·(I/v) (режим насыщения, предиктор затора)
4	I – «высокая» и v – «низкая»	$\hat{q}$ = 1,25·(I/v)+2 (формирующийся затор)
5	I – «низкая» и v – «очень низкая»	$\hat{q}$ = 0,90·(I/v) (аномальное торможение, локальное событие)
6	I – «средняя» и v – «высокая»	$\hat{q}$ = 0,95·(I/v) (разрежение потока)

2.3 Дефаззификация

Для правила R_i с весом срабатывания w_i (произведение степеней принадлежности по входу) выходное значение определяется как взвешенное среднее:

$$\hat{q} = \frac{\sum_{i=1}^{12} w_i \cdot (a_i \cdot (I/v) + b_i)}{\sum_{i=1}^{12} w_i} \quad (3)$$

где a_i, b_i – параметры линейной функции Сугено.

Вывод

В результате проведенного исследования установлено, что методы нечеткого прогнозирования являются эффективным инструментом анализа плотности транспортного потока в условиях неопределенности исходных данных. В отличие от классических детерминированных и вероятностных подходов, нечеткая логика позволяет учитывать неточность измерений скорости и интенсивности движения, а также формализовать экспертные знания в виде системы правил.

Разработанная модель, основанная на алгоритме Сугено, обеспечивает поэтапное преобразование входных параметров через фаззификацию, применение базы нечетких правил, агрегирование и дефаззификацию, что позволяет получать интерпретируемый численный прогноз плотности транспортного потока.

Анализ результатов моделирования показал, что при снижении скорости движения и увеличении интенсивности наблюдается устойчивый рост плотности, что соответствует условиям формирования заторов. Использование нечеткого подхода позволяет повысить точность прогнозирования и своевременно выявлять критические состояния транспортной системы.

Список используемых источников

1. ОДМ 218.2.020-2012. Методические рекомендации по оценке пропускной способности автомобильных дорог. М.: Информавтодор, 2012. 148с.

2. Капитанов В. Т., Хилажев Е. Б. Управление транспортными потоками в городах. М.: Транспорт, 1985.

3. Lighthill M. J. On kinematic waves. II. A theory of traffic flow on long crowded roads / M. J. Lighthill, G. B. Whitham // Proceedings of the Royal Society, Series A. Volume 229, London, 1955, PP. 281-345.

4. Судаков В. А. Прогнозирование авиационных перевозок методами статистического анализа и машинного обучения / В. А. Судаков, М. А. Тимофеев. Москва: ИПМ им. М. В. Келдыша РАН, 2022. 14 с/

5. Shankar H. Multi Model Criteria for the Estimation of Road Traffic Congestion from Traffic Flow Information Based on Fuzzy Logic / H. Shankar, P. L. N. Raju, K. R. M. Rao // Journal of Transportation Technologies. 2012. 50-62.

УДК 004.942

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К ОЦЕНКЕ ЧАСТОТЫ СЕРДЕЧНЫХ СОКРАЩЕНИЙ ПО ФОТОПЛЕТИЗМОГРАММЕ: ВРЕМЕННАЯ И ЧАСТОТНАЯ ОБЛАСТИ

Р. В. Давыдов (к. ф.-м. н., доцент кафедры ИКД СПбГУТ)
В. А. Никандров (студент группы МТД-2521 СПбГУТ)
Ж. В. Устинина (студент группы МТД-2521 СПбГУТ), ustinina.zv@sut.ru

Проведен сравнительный анализ временного и частотного подходов к оценке ЧСС по фотоплетизмограмме. Временной метод обеспечивает низкую задержку и анализ HRV, но чувствителен к артефактам; частотный устойчив к шумам, но требует длительного сигнала и не позволяет оценивать HRV. Методы сопоставлены по точности, устойчивости, вычислительной сложности и применимости в носимых устройствах.

фотоплетизмография, ЧСС, временной анализ, частотный анализ, спектральный анализ, детекция пиков, двигательные артефакты, вариабельность сердечного ритма, HRV

По данным аналитических агентств, рынок носимых устройств вырос с 15 млрд долларов в 2020 году до 62 млрд долларов в 2025 году, причем около 80 % устройств используют ФПГ-датчики. [1, 2, 3].

Основная проблема применения ФПГ в реальных условиях – высокая чувствительность к двигательным артефактам. При ходьбе, беге или даже наборе текста на клавиатуре сигнал искажается настолько, что погрешность оценки ЧСС может достигать 20–30 % [4, 5]. Для извлечения ЧСС из ФПГ-сигнала существуют два классических подхода: временной (основанный на поиске пиков пульсовой волны) и частотный (спектральный анализ) [6, 7, 8]. Каждый из них имеет свои сильные и слабые стороны, и выбор метода существенно влияет на точность, задержку и вычислительную сложность конечной системы.

Статья посвящена сравнительному анализу временного и частотного подходов к оценке ЧСС по ФПГ-сигналу. Сравнение проводится по следующим критериям: точность (средняя абсолютная ошибка MAE), устойчивость к шумам и артефактам, вычислительная сложность, способность отслеживать быстрые изменения ЧСС, а также возможность получения дополнительных параметров (например, вариабельности сердечного ритма, HRV).

Временной подход имитирует ручной подсчет пульса: на ФПГ-сигнале производится поиск локальных максимумов (пики), соответствующие сокращениям сердца, а ЧСС вычисляется по интервалам между ними [9-11]. Ниже приведено детальное описание алгоритма.

Исходные данные: ФПГ-сигнал $x[n]$, оцифрованный с частотой дискретизации F_s (Гц), где $n = 0,1, \dots, N-1$. Длительность обрабатываемого фрагмента обычно составляет 2–10 секунд.

1. Полосовая фильтрация

Сигнал пропускается через полосовой фильтр с границами, соответствующими физиологическому диапазону ЧСС (например, 0.8–3 Гц). На выходе получаем $x_f[n]$. Это подавляет медленные тренды и высокочастотные шумы.

2. Детекция пиков

Пики определяются как локальные максимумы, удовлетворяющие критериям по амплитуде и минимальному временному расстоянию.

Локальный максимум в точке n (при $1 \le n \le N-2$):

$$x_f[n] > x_f[n-1] \text{ и } x_f[n] \ge x_f[n+1].$$

Амплитудный порог $A_{thr}(n)$ вычисляется адаптивно, например, как половина среднего значения локальных максимумов за последние 2–3 секунды.

Рефрактерный период (минимальное расстояние между пиками) задается исходя из максимальной ожидаемой ЧСС HR_{max}:

$$\Delta t_{min} = \frac{60}{HR_{max}} \text{ (в секундах).}$$

В отсчетах: $N_{min} = \Delta t_{min} \cdot F_s$. Пик регистрируется, если его амплитуда превышает $A_{thr}(n)$ и он отстает от предыдущего пика не менее чем на N_{min} отсчетов.

3. Вычисление межпиковых интервалов (IBI)

Пусть найдены моменты пиков $t_1, t_2, \dots, t_M$ (в секундах). Тогда

$$IBI_i = t_{i+1} - t_i, i = 1,2, \dots, M-1.$$

4. Отбраковка выбросов

Интервалы, выходящие за физиологические пределы, исключаются:

$$IBI_{valid} = \{IBI_i \mid 0.25 \text{ с} \le IBI_i \le 2.0 \text{ с}\}.$$

Дополнительно можно отбросить интервалы, отличающиеся от медианы более чем на 30 %.

5. Расчет ЧСС

Итоговая ЧСС вычисляется по медиане оставшихся интервалов (устойчива к выбросам):

$$\mathrm{HR} = \frac{60}{\mathrm{median}(\mathrm{IBI}_{\mathrm{valid}})}\,(\text{уд/мин}).$$

6. Оценка качества детекции

Для количественной оценки используются чувствительность Se и точность PPV:

$$\mathrm{Se} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}, \mathrm{PPV} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}},$$

где TP – истинные пики (найдены и верны), FN – пропущенные истинные пики, FP – ложные пики.

Временной подход имеет вычислительную сложность $O(N)$ и задержку в доли секунды после поступления каждого нового пика. Благодаря последовательности IBI_i (формула (3)) он позволяет напрямую оценивать вариабельность сердечного ритма (HRV). Основной недостаток – сильная чувствительность к двигательным артефактам и аритмиям [12].

Частотный подход основан на том, что пульсовая волна является периодическим сигналом, поэтому в ее спектре мощности присутствует ярко выраженный пик на частоте, соответствующей ЧСС [13]. Детальный алгоритм включает следующие этапы, описанные ниже.

Исходные данные: фрагмент ФПГ-сигнала $x[n]$ фиксированной длины N (обычно $N = 256, 512, 1024$), длительностью $T = N/F_s$ (рекомендуется 6–10 секунд для достаточного частотного разрешения).

1. Предобработка

Удаление постоянной составляющей:

$$\tilde{x}[n] = x[n] - \frac{1}{N}\sum_{j=0}^{N-1} x[j].$$

● удаление тренда (вычитание полиномиальной аппроксимации 1-го или 2-го порядка);

● применение оконной функции $w[n]$ (например, Ханна) для уменьшения спектрального вытекания:

$$x_w[n] = \tilde{x}[n] \cdot w[n], n = 0, \dots, N-1.$$

2. Вычисление спектра мощности

Используется периодограмма (или метод Уэлча для снижения дисперсии):

$$P[k] = \frac{1}{N} | \sum_{n=0}^{N-1} x_w [n] \, e^{-j2\pi kn/N} |^2, k = 0,1, \dots, N-1.$$

Частота, соответствующая индексу k:

$$f_k = \frac{k \cdot F_s}{N} (\text{Гц}).$$

3. Поиск доминирующей частоты

Ограничиваемся физиологическим диапазоном $f \in [0.8, 3.0]$ Гц. Находим индекс k_{max}, при котором $P[k]$ максимальна в этом диапазоне. Грубая оценка:

$$f_{HR}^{(0)} = \frac{k_{max} \cdot F_s}{N}.$$

Частотное разрешение составляет $\Delta f = F_s/N$. При типичных параметрах ($F_s = 100$ Гц, $N = 256$) $\Delta f \approx 0.39$ Гц, что соответствует ~23 уд/мин. Для повышения точности применяется параболическая интерполяция по трем точкам спектра.

Пусть $y_{-1} = P[k_{max} - 1]$, $y_0 = P[k_{max}]$, $y_{+1} = P[k_{max} + 1]$. Уточненное положение пика:

$$\delta = \frac{y_{-1} - y_{+1}}{2(y_{-1} - 2y_0 + y_{+1})}.$$

Тогда уточненная частота:

$$f_{HR} = f_{HR}^{(0)} + \delta \cdot \Delta f.$$

4. Расчет ЧСС

$$HR = 60 \cdot f_{HR} (\text{уд/мин}).$$

5. Оценка надежности

Отношение сигнал/шум в спектре:

$$\mathrm{SNR_{spec}} = \frac{\mathrm{P[k_{max}]}}{\frac{1}{\mathrm{W}} \sum_{|\mathrm{k}-\mathrm{k_{max}}|>\mathrm{D}} \mathrm{P[k]}},$$

где W – число бинов в окрестности, исключенной из расчета шума (например, $\mathrm{D} = 2$ бина). Если $\mathrm{SNR_{spec}} < 3$, результат считается ненадежным.

Частотный подход имеет вычислительную сложность $\mathrm{O(N \log N)}$ и задержку, равную длительности анализируемого окна T. Он устойчив к шумам и артефактам движения благодаря усреднению спектра (формула (9)), но не позволяет оценивать HRV и плохо отслеживает быстрые изменения ЧСС [6, 8].

В условиях, чувствительных к шуму, для временного метода вероятность ложного пика экспоненциально растет при снижении SNR, и уже при умеренных артефактах метод становится ненадежным. Для частотного метода эффективное SNR в спектре возрастает пропорционально длине окна (см. формулу (15)), что позволяет выделять пик даже тогда, когда во временной области сигнал визуально полностью зашумлен.

Скорость работы методов также различается. Временной метод дает низкую задержку (доли секунды), но его точность сильно зависит от качества сигнала. Частотный метод требует длительного накопления (несколько секунд в соответствии с длиной окна T), поэтому он непригоден для отслеживания быстрых изменений ЧСС, но в стационарных условиях (покой, сон) обеспечивает более высокую точность [6, 8].

Отмечая различия данных методов, только временной метод позволяет анализировать HRV на основе последовательности $\mathrm{IBI_i}$ (3), что является важным диагностическим параметром для оценки вегетативной нервной системы. Частотный метод, в свою очередь, может быть расширен для оценки частоты дыхания по низкочастотной модуляции ФПГ-сигнала.

Количественное и качественное сравнение подходов по основным критериям представлено в таблице 1.

ТАБЛИЦА 1. Сравнение временного и частотного подходов к оценке ЧСС по ФПГ-сигналу

Критерий	Временной подход	Частотный подход
Точность (MAE), уд/мин	2–10 (зависит от качества сигнала)	1–5 (в стационарных условиях)
Устойчивость к двигательным артефактам	Низкая (сбои при SNR < 10 дБ)	Высокая (работает при отрицательном SNR)
Задержка (латентность)	< 1 с (после последнего пика)	5–30 с (зависит от длины окна)
Анализ вариабельности сердечного ритма (HRV)	Да (на основе IBI)	Нет
Вычислительная сложность	O(N) – низкая	O(Nlogf_0N) – высокая (БПФ)
Чувствительность к настройкам	Высокая (пороги, рефрактерный период)	Низкая (только диапазон частот)
Отслеживание быстрых изменений ЧСС	Хорошее (пошаговое обновление)	Плохое (требуется накопление окна)

Как следует из таблицы 1, ни один из методов не является универсальным. Временной подход выигрывает в режиме реального времени и возможности анализа HRV, он идеален для фитнес-трекеров с хорошим сигналом (покой, умеренная активность). Частотный подход – лидер по устойчивости к шумам, подходит для экстремальных условий (бег, спорт). Ни один из методов не является универсальным: временной сбоит при артефактах, частотный – имеет высокую задержку. Перспективным направлением является разработка гибридных алгоритмов, переключающих режим работы в зависимости от уровня артефактов, а также использование акселерометра для адаптивной коррекции.

Список используемых источников

1. Wearables Market Size & Share 2025 – 2034 [Электронный ресурс] // Global Market Insights: Industry Analysis. URL: https://www.gminsights.com/ru/industry-analysis/wearables-market (дата обращения: 14.04.2026).

2. Рынок безманжетных тонометров. Анализ и прогноз рынка до 2035 года [Электронный ресурс] // Global Insight Services. URL: https://www.globalinsightservices.com/ru/сообщениях/рынок-тонометров-без-манжеты/ (дата обращения: 14.04.2026).

3. Носимая электроника (мировой рынок) [Электронный ресурс] // Tadviser. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/Статья:Носимая_электроника_(мировой_рынок) (дата обращения: 14.04.2026).

4. Федотов А. А., Акулова А. С., Акулов С. А. Обобщенный метод цифровой обработки сигнала пульсовой волны // Journal of Biomedical Photonics & Engineering. Самара: СГАУ, 2016.

5. Какова нормальная частота пульса? [Электронный ресурс] // Aktif International Hospital. URL: https://www.aktifinternational.com/ru/какова-нормальная-частота-пульса/ (дата обращения: 14.04.2026).

6. Chae J. E., Kim D. Y., Lee K. K., Park C. H. Assessment of Heart Rate Derivation Methods and Applicability in Remote Photoplethysmography // Journal of the Institute of Electronics and Information Engineers. 2023. Vol. 60. N 10. PP. 35–42. DOI: 10.5573/ieie.2023.60.10.35.

7. Wójcikowski M., Pankiewicz B. Photoplethysmographic Time-Domain Heart Rate Measurement Algorithm for Resource-Constrained Wearable Devices and its Implementation // Sensors. 2020. Vol. 20, N 6. P. 1783. DOI: 10.3390/s20061783.

8. Elgendi M., Fletcher R.R., Norton I., Brearly M., Abbott D., Lovell N.H., Schuurmans D. Frequency analysis of photoplethysmogram and its derivatives // Computer Methods and Programs in Biomedicine. 2015. Vol. 122. Pp. 503–512. DOI: 10.1016/j.cmpb.2015.09.021.

9. Time Domain Analysis vs Frequency Domain Analysis [Электронный ресурс] // Study Electrical. 2023. URL: https://studyelectrical.com/2023/05/time-domain-analysis-vs-frequency-domain-analysis.html (дата обращения: 14.04.2026).

10. Манышев Д. М. Структурный анализ кардиосигналов для оценки показателей вариабельности сердечного ритма // Молодой ученый. 2020. № 23 (313). С. 42–47.

11. Dunn C. E., Monroe D. C., Crouzet C., Hicks J. W., Choi B. Speckleplethysmographic (SPG) Estimation of Heart Rate Variability During an Orthostatic Challenge // Scientific Reports. 2019. Vol. 9. Article number: 14079. DOI: 10.1038/s41598-019-50526-0.

12. Киселев А. Р., Караваев А. С., Гриднев В. И., Прохоров М. Д., Пономаренко В. И., Боровкова Е. И., Шварц В. А., Посненкова О. М., Безручко Б. П. Метод оценки степени синхронизации низкочастотных колебаний в вариабельности ритма сердца и фотоплетизмограмме // Кардио-ИТ. 2016. Т. 3. № 1. e0101. DOI: 10.15275/cardioit.2016.0101.

13. Pozniak M. A., et al. Spectral and color Doppler artifacts // Radiographics. 1992. Vol. 12. N 1. PP. 35-44. DOI: 10.1148/radiographics.12.1.1734480.

УДК 004.451.9

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К ТРАССИРОВКЕ ЯДРА LINUX ДЛЯ МОНИТОРИНГА СИСТЕМ ХРАНЕНИЯ ДАННЫХ

А. С. Диденко (студент группы ИКПИ-24 СПбГУТ), didenko.as@sut.ru
С. А. Коробов (к.п.н., доцент, доцент кафедры ПИиВТ СПбГУТ)

При разработке и отладке драйверов систем хранения данных возникает необходимость анализа поведения системы на уровне ядра. Драйверы функционируют в контексте ядра, и события, связанные с обработкой команд, недоступны стандартным средствам пользовательского пространства. Для их перехвата ядро Linux предоставляет несколько механизмов трассировки. В данной работе реализована утилита для перехвата событий ядра и сбора статистики в реальном времени с использованием подсистемы tracefs и технологии eBPF. Проведено экспериментальное сравнение трех вариантов реализации на реальном оборудовании и определен наиболее подходящий вариант для задач мониторинга при высокой интенсивности операций.

трассировка ядра, системы хранения данных, eBPF, tracefs, libbpf, производительность

Существующие публикации рассматривают механизмы трассировки ядра Linux в общем контексте [1, 2], однако их сравнительный анализ применительно к задачам мониторинга СХД при высокой интенсивности операций практически отсутствует. Это создает необходимость в экспериментальном исследовании, включающем разработку утилиты с использованием различных подходов и их сравнение на реальном оборудовании.

Ядро Linux предоставляет несколько механизмов трассировки для перехвата событий [3]. В данной работе исследуются два из них: подсистема tracefs и технология eBPF [4].

Подсистема tracefs предоставляет доступ к кольцевому буферу инфраструктуры ftrace через виртуальную файловую систему [3]. При срабатывании точки трассировки ядро записывает событие в буфер, выделенный для каждого процессора. Чтение и разбор событий выполняются в пользовательском пространстве с помощью библиотек libtracefs и libtraceevent.

Технология eBPF позволяет загружать программы непосредственно в ядро [4]. Программа подключается к точке трассировки и получает прямой доступ к полям события через типизированный контекст. Перед загрузкой программа проходит верификатор и JIT-компилятор, транслирующий байткод в нативные инструкции. Библиотека libbpf выполняет загрузку BPF-объекта, создание карт и подключение к точкам трассировки. Механизм CO-RE обеспечивает переносимость программ между версиями ядра без перекомпиляции [2].

Разработанная утилита перехватывает события драйвера СХД на пяти уровнях обработки команд. Каждому уровню соответствует пара событий: начало и завершение обработки. При получении события начала обработки утилита создает запись о команде с уникальным идентификатором. Подкоманды наследуют идентификатор родительской команды, что позволяет объединить все события одной операции в логическую цепочку. Для быстрого поиска команд используются хеш-таблицы, отдельные для каждого типа.

Реализовано три варианта утилиты. В варианте на основе tracefs отдельный поток периодически фиксирует состояние кольцевого буфера и передает пакет событий на обработку. В BPF-варианте с кольцевым буфером каждая программа копирует поля события в типизированную структуру и передает ее в общий кольцевой буфер [5], откуда приложение читает и обрабатывает события. В BPF-варианте с агрегацией в ядре вся логика обработки и сбора статистики вынесена в BPF-программы, а пользовательское пространство только читает итоговые данные из карт.

Для измерения влияния на производительность использовался генератор нагрузки fio в режимах последовательного чтения и записи на томе размером 5T RAID 6. Замеры производились на реальном оборудовании. Вариант на основе tracefs оказался непригодным: при высокой интенсивности операций ядро генерирует события быстрее, чем пользовательское пространство успевает их обработать, что приводит к неустранимой потере событий. Результаты сравнения BPF-вариантов представлены в таблице 1.

ТАБЛИЦА 1. Накладные расходы BPF-вариантов

Вариант	Чтение, МБ/с	Запись, МБ/с	Накладные расходы, %
Без трассировки	675	585	-
Включение точек трассировки	608	527	10
BPF с кольцевым буфером	594	512	12-13
BPF с агрегацией в ядре	547	484	17-19

Как видно из таблицы 1, простое включение точек трассировки без какой-либо обработки снижает пропускную способность примерно на 10 %. BPF-вариант с кольцевым буфером добавляет к этому лишь 2–3 %, при этом на чтении пропускная способность составила ~594 МБ/с, на записи – ~512

МБ/с. Вариант с агрегацией в ядре показал более существенное снижение (~547 МБ/с на чтении, ~484 МБ/с на записи) из-за операций с картами (поиск, обновление, удаление) на каждое событие.

Помимо производительности, варианты различаются возможностями анализа. Вариант с кольцевым буфером передает полные структуры событий, тогда как вариант с агрегацией – только итоговую статистику.

По результатам экспериментов BPF-вариант с кольцевым буфером оказался наиболее подходящим для задач мониторинга СХД при высокой нагрузке. Подход на основе tracefs применим при низкой интенсивности событий, однако в условиях описанного эксперимента потеря событий оказалась неустранимой.

Список используемых источников

1. Gregg B. BPF Performance Tools: Linux System and Application Observability // Addison-Wesley Professional. 2019. 880 p.

2. Rice L. Learning eBPF // O'Reilly Media. 2023. 236 p.

3. ftrace – Function Tracer [Электронный ресурс]. URL: https://www.kernel.org/doc/html/latest/trace/ftrace.html (дата обращения: 05.02.2026).

4. BPF Documentation [Электронный ресурс]. URL: https://www.kernel.org/doc/html/latest/bpf/index.html (дата обращения: 24.02.2026).

5. Nakryiko A. BPF ring buffer [Электронный ресурс]. URL: https://nakryiko.com/posts/bpf-ringbuf/ (дата обращения: 06.03.2026).

УДК 376.1

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЛОГОПЕДИЧЕСКОЙ ДИАГНОСТИКИ И АНАЛИЗА ДИНАМИКИ РЕЧЕВОГО РАЗВИТИЯ МЛАДШИХ ШКОЛЬНИКОВ

Т. В. Ермакова (старший преподаватель кафедры ПИиВТ СПбГУТ)
С. В. Новикова (студент группы ИКПИ-21 СПбГУТ), novikova.sv@sut.ru

В работе рассматривается проблема логопедической диагностики и анализа динамики речевого развития младших школьников. Проведен анализ существующих программных решений, выявлены их основные недостатки, связанные с ограниченной функциональностью, отсутствием автоматизированного анализа и сложностью использования. Предложено программное обеспечение, обеспечивающее автоматизацию процесса диагностики, хранение и обработку данных, а также анализ динамики речевого развития. Система направлена на повышение эффективности работы логопеда и улучшение качества диагностики.

логопедическая диагностика, речевое развитие, младшие школьники, программное обеспечение, анализ динамики, автоматизация, языковая карточка

Речевое развитие детей младшего школьного возраста играет ключевую роль в формировании их учебных навыков, коммуникативных способностей и социальной адаптации [1]. Нарушения речи могут негативно влиять на освоение чтения, письма и понимание учебного материала, что делает своевременную диагностику особенно важной [2,3].

В практике логопедов диагностика речевого развития часто осуществляется с использованием бумажных носителей или разрозненных цифровых инструментов. Это приводит к ряду проблем: высокая трудоемкость обработки информации, сложность хранения и структурирования данных, отсутствие автоматизированного анализа динамики, вероятность ошибок при ручном вводе данных [4].

Особую сложность представляет анализ динамики речевого развития, так как специалисту необходимо отслеживать изменения показателей во времени и делать обоснованные выводы.

В связи с этим актуальной задачей является разработка программного обеспечения, позволяющего автоматизировать диагностику, хранение и анализ речевых данных.

Анализ современных программных продуктов показывает, что существующие решения можно разделить на несколько категорий: обучающие

приложения, игровые платформы и специализированные диагностические системы:

1. Обучающие мобильные приложения (например, приложение «Привет, логопед!», некий логопедический тренажер для детей);

2. Интерактивные образовательные платформы (например, платформа «Мерсибо»);

3. Узкоспециализированные приложения (например, приложение «ГоВоРун»);

4. Игровые онлайн-ресурсы (например, платформа «Логотека»)

5. Профессиональные программные комплексы (например, комплекс «Логопедическое обследование детей 4–8 лет» по методике В. М. Акименко) [5].

Ниже представлена сравнительная характеристика с преимуществами и недостатками по существующим решениям (см. табл. 1):

ТАБЛИЦА 1. Сравнительная характеристика существующих решений.

Существующее решение	Преимущества	Недостатки
«Привет, логопед!»	+ Направленность на запуск речи у детей; + Использование игровых элементов; + Доступность для широкой аудитории.	- Ориентированность на самостоятельную работу родителей, а не на профессиональную диагностику; - Необходимость подключения к интернету; - Ограниченность платформы (мобильные устройства); - Отсутствие автоматизированного анализа (диагностика ведется вручную).
«Мерсибо»	+ Широкий набор интерактивных упражнений; + Методическая поддержка специалистов; + Проведение обучающих мероприятий.	- Отсутствие полноценной системы диагностики; - Зависимость от интернет-соединения; - Наличие платной подписки; - Ориентированность на развитие, а не на анализ.
«ГоВоРун»	+ Простота использования; + Направленность на запуск речи.	- Ограниченный функционал (работа только со слогами); - Отсутствие комплексной диагностики; - Платная модель распространения; - Доступность только на мобильных устройствах.

Существующее решение	Преимущества	Недостатки
«Логотека»	+ Разнообразие игр; + Привлекательный интерфейс.	- Отсутствие диагностического функционала; - Необходимость самостоятельного анализа результатов; - Зависимость от интернета и платной подписки.
«Логопедическое обследование детей 4–8 лет»	+ Ведение индивидуальных речевых карт; + Проведение поэтапной диагностики; + Анализ и хранение данных; + Построение динамики развития; + Формирование отчетов и графиков.	- Высокая стоимость (около 75 000 рублей); - Ограниченная доступность; - Сложность внедрения.

Проведенный анализ показал, что большинство решений ориентированы на обучение, а не на диагностику.

Также отсутствует баланс между функциональностью и доступностью, а профессиональные системы либо дорогие, либо сложные по внедрению. У многих решений отсутствуют удобные инструменты для анализа динамики.

В рамках разработки, программное обеспечение направлено на автоматизацию логопедической диагностики и анализа динамики речевого развития.

При разработке будут учтены следующие требования:

- простота использования;
- доступность для специалистов/логопедов;
- автоматизация обработки данных;
- поддержка анализа динамики;
- возможность офлайн-работы.

Из ключевых функциональных возможностей можно выделить следующее: работу с данными учащихся (создание и редактирование записей, хранение истории обследований, централизованное хранение данных); языковые карточки, которые имеют формат карты обследования речевого развития школьников с использованием нейропсихологических методов (по Фотековой Т. А., Ахутиной Т. В., Иншаковой О. Б. [6]); анализ динамики (в

отличие от большинства аналогов, будет реализовано сравнение результатов обследований, отображение динамики развития); формирование отчетов (автоматическая генерация отчетов по динамике развития речи ребенка, печать и сохранение языковых карточек в PDF-формате); удобный интерфейс (адаптация под работу логопеда, интуитивная навигация).

В ходе исследования проанализирована проблема логопедической диагностики и рассмотрены существующие программные решения. Выявлено, что большинство из них либо ориентированы на обучение, либо имеют ограничения по функциональности, стоимости или удобству использования.

Наш подход по разработке программное обеспечение позволяет:

- автоматизировать процесс диагностики;
- упростить работу логопеда;
- обеспечить хранение и структурирование данных;
- реализовать анализ динамики речевого развития.

Практическая значимость работы заключается в возможности применения системы в образовательных учреждениях и логопедической практике.

Список используемых источников

1. Кударинова А. С., Жусупбекова З. Д., Ашимханова Г. С., Садвакасова Н. А., Арбабаева А. Т. Значение логопедической диагностики в развитии речи детей // Международный журнал прикладных и фундаментальных исследований. 2015. № 2 (часть 1). С. 42-45.

2. Мертвищева К. З. Задержка речевого развития детей младшего дошкольного возраста: основные аспекты, диагностика и основные способы коррекции / К. З. Мертвищева. Текст: непосредственный // Молодой ученый. 2021. № 18 (360). С. 342-344.

3. Дяйкина В. В., Масленникова В. А. Современные методы и средства логопедической диагностики речевого развития детей раннего возраста // Специальное образование. 2021. № 1. С. 114-126.

4. Лелик В. П., Дьячкова М. Д., Дорофеева С. В. Инструменты оценки речевого и языкового развития детей дошкольного и младшего школьного возраста: обзор литературы. Вопросы современной педиатрии. 2024. № 23(3). С. 131-144.

5. Дюканова О. В. Применение информационных компьютерных технологий в логопедической работе / О. В. Дюканова. Текст: непосредственный // Вопросы дошкольной педагогики. 2023. № 4 (63). С. 19-21.

6. Фотекова Т. А. Нейропсихологические методы в изучении возрастных особенностей пространственных представлений // Вестник по педагогике и психологии Южной Сибири. 2013. № 3. С. 63-72.

УДК 004.724

РАЗРАБОТКА УЧЕБНО-МЕТОДИЧЕСКОГО КОМПЛЕКСА ПО ФОРМИРОВАНИЮ НАВЫКОВ НАСТРОЙКИ СЕРВИСОВ L2/L3VPN В ГЕТЕРОГЕННЫХ СЕТЯХ НА БАЗЕ ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ

Д. И. Карташов (студент группы ИКТК-21 СПбГУТ), kartashov.di@sut.ru
И. А. Ушаков (и. о. заведующего кафедрой ИБКС, к.т.н., доцент, доцент кафедры ИКС СПбГУТ)

Статья посвящена разработке методического комплекса для обучения настройке сервисов L2/L3 VPN в гетерогенных сетях. На базе эмулятора PNETLab реализована мультивендорная среда, объединяющая решения Eltex vESR, Cisco и MikroTik. В рамках работы подготовлен цикл практических задач от настройки базовой связности до реализации типовых отраслевых решений по объединению филиалов компаний с обеспечением изоляции трафика.

L2VPN, L3VPN, MPLS, гетерогенные сети, эмуляция сетей

1. Введение

На сегодняшний день сформировалась тенденция на уход крупных зарубежных телекоммуникационных вендоров. Это повлекло за собой активное развитие отечественных решений. Такой подход сформировал потребность в подготовке специалистов, которые должны иметь практические навыки настройки и эксплуатации сервисов в мультивендорных средах.

В рамках статьи обозревается разработанный учебно-методический комплекс, ориентированный на форматирование навыков по работе с L2/L3VPN [1, 2] в гетерогенных средах с использованием виртуального отечественного оборудования в эмуляционной среде.

2. Архитектура учебно-методического комплекса

Методическое пособие реализуется на базе виртуальной лабораторной среды. В качестве основной платформы используется сетевой эмулятор PNETLab, обеспечивающий запуск оригинальных образов операционных систем различных производителей и полноценную эмуляцию сетевых протоколов.

Применение PNETLab позволяет моделировать мультивендорные среды без ограничений, характерных для симуляторов, и обеспечивает воз-

можность работы с реальным стеком протоколов, включая MPLS [3] и связанные с ним сервисы. Это создает условия, максимально приближенные к эксплуатации сетей операторского уровня и корпоративной инфраструктуры.

В качестве основного отечественного решения в комплексе используются виртуальные маршрутизаторы Eltex vESR, интегрируемые в общую топологию совместно с оборудованием других вендоров. Такой подход позволяет реализовать сценарии межвендорного взаимодействия и отработку задач интеграции отечественного оборудования в существующие сети.

Архитектура комплекса предусматривает построение лабораторных топологий различной сложности, включающих магистральный MPLS-сегмент и граничные устройства различных производителей. Дополнительно в учебный процесс интегрированы средства анализа сетевого трафика, что позволяет выполнять детальное исследование передаваемых пакетов и углубленно изучать принципы работы сетевых протоколов.

3. Практическая реализация комплекса

Практическая реализация учебно-методического комплекса представлена в виде цикла лабораторных работ, направленных на поэтапное освоение технологий построения виртуальных частных сетей. Курс начинается с базовой настройки LDP, далее идут работы, связанные с развертыванием L2VPN в двух вариациях, и заканчивается на технологии L3VPN.

В работах также используются крупные зарубежные решения (Cisco и Mikrotik) для эмуляции работы реальной сети, где не только один вендор. В современных сетях используется именно такой подход, чтобы не зависеть только от одной компании. Это позволяет учащимся изучить межвендорное взаимодействие, которое зачастую имеет нестандартные решения.

В каждой работе студенты будут использовать инструмент Wireshark, который позволяет анализировать структуру пакетов. Обучающиеся будут исследовать MPLS-пакеты, метки на пакетах и базовые сетевые сценарии. Это формирует навыки диагностики и устранения неисправностей, востребованные в профессиональной деятельности.

Итогом обучения являются комплексные лабораторные работы, моделирующие функционирование реальных корпоративных сетей.

На рис. 1 представлена топология одной из завершающих лабораторных работ, в которой моделируется взаимодействие двух корпоративных за-

казчиков – условных компаний «Газпром» и «Сбербанк», имеющих филиалы в Санкт-Петербурге и Москве. Перед студентами ставится задача организации изолированных каналов связи между офисами каждой компании с использованием сервиса L3VPN.

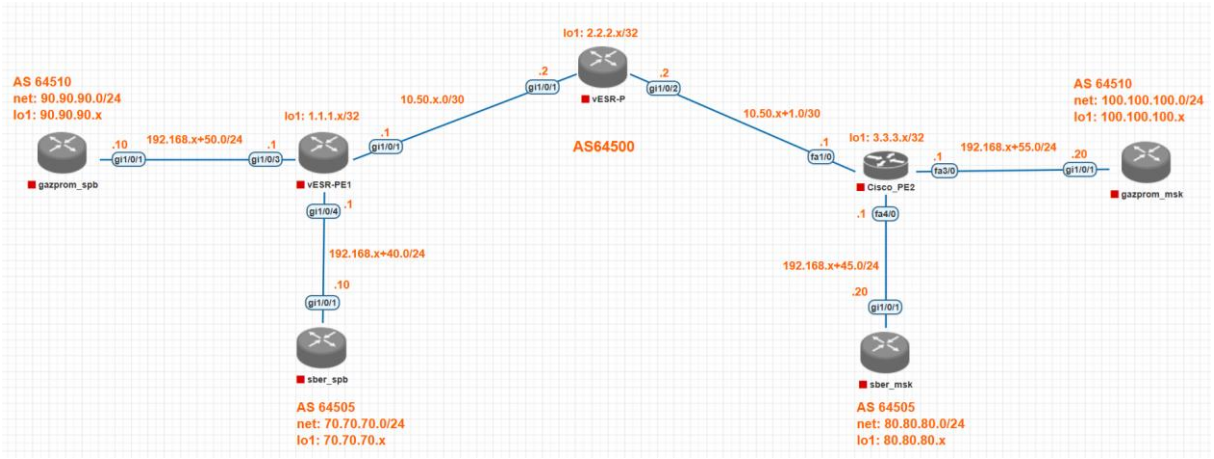


Рис. 1. Топология лабораторной работы «Обеспечение межвендорного взаимодействия L3VPN в сегментированной сети»

В качестве транспортной среды выступает сеть провайдера «Ростелеком», реализующая MPLS-инфраструктуру. Граничные маршрутизаторы заказчиков представлены оборудованием различных вендоров: в одном сегменте используется маршрутизатор Eltex vESR, в другом – Cisco C7200. Такой подход позволяет отработать сценарии межвендорного взаимодействия в условиях, приближенных к реальной эксплуатации.

В рамках выполнения лабораторной работы осуществляется настройка маршрутизации, распределения MPLS-меток и механизмов изоляции трафика, обеспечивающих независимость сетей различных клиентов. Рассматриваемый сценарий позволяет наглядно продемонстрировать принципы построения операторских сетей и закрепить навыки конфигурирования сервисов L3VPN в гетерогенной среде.

4. Заключение

Разработанный учебно-методический комплекс обладает высокой прикладной ценностью, поскольку ориентирован на формирование у студентов практических навыков, востребованных в реальной профессиональной деятельности. Использование мультивендорной среды и работа с технологиями MPLS и VPN позволяют приблизить процесс обучения к условиям эксплуатации современных корпоративных и операторских сетей.

Применение сетевого эмулятора PNETLab в сочетании с виртуальными маршрутизаторами Eltex обеспечивает высокую степень реалистичности учебной среды. Студенты получают возможность работать с полноценным стеком сетевых протоколов, анализировать реальный трафик и решать задачи, аналогичные тем, с которыми сталкиваются специалисты в области сетевых технологий.

Перспективы развития комплекса связаны с расширением перечня изучаемых технологий, включая механизмы Traffic Engineering, обеспечение качества обслуживания (QoS) и передачу мультикаст-трафика. Дополнительно рассматривается возможность интеграции виртуальной лабораторной среды с физической инфраструктурой, что позволит реализовать более сложные сценарии тестирования и внедрения отечественных решений.

Список используемых источников

1. Rosen E., Rekhter Y. BGP/MPLS IP Virtual Private Networks (VPNs) [Электронный ресурс] // RFC 4364. 2006. URL: https://datatracker.ietf.org/doc/html/rfc4364 (дата обращения: 21.04.2026).

2. Martini L., Rosen E., El-Aawar N. Pseudowire Setup and Maintenance Using LDP [Электронный ресурс] // RFC 4447. 2006. URL: https://datatracker.ietf.org/doc/html/rfc4447 (дата обращения: 21.04.2026).

3. Гольдштейн А. Б., Гольдштейн Б. С. Технология и протоколы MPLS. СПб.: БХВ-Петербург, 2005. 304 с.

УДК 004.85

ГИБРИДНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

З. В. Ким (студент группы ИКПИ-24 СПбГУТ), kim.zv@sut.ru

Традиционные сигнатурные системы обнаружения вторжений (IDS/IPS) неэффективны для киберфизических систем (КФС) в условиях роста зашифрованного трафика и атак «нулевого дня». В работе обоснован переход к поведенческому анализу на основе машинного обучения и предложена гибридная архитектура обнаружения аномалий, объединяющая XGBoost (известные угрозы) и Isolation Forest (неизвестные аномалии) с синтезом решений по правилу максимума, что минимизирует пропуск атак. Делается вывод, что при сильном дисбалансе классов (доля аномалий более 1 %) наиболее надежными метриками являются F1-мера и PR-AUC, при этом гибридный подход обеспечивает синергетический эффект, значительно повышая безопасность КФС.

поведенческий анализ, обнаружение вторжений, потоковые признаки, ансамблевые методы, обучение без учителя, метрики оценки

Введение

Киберфизические системы (КФС) объединяют вычислительные ресурсы с физическими процессами, поэтому их безопасность приобретает критическое значение. В отличие от традиционных информационных систем, кибератаки на КФС способны привести не только к утечке данных, но и к прямому физическому ущербу, нарушению технологических процессов или угрозе для жизни людей. С ростом масштаба таких системы объемы сетевого трафика резко увеличиваются, что существенно усложняет задачу мониторинга безопасности. Современный спектр киберугроз отличается высокой динамикой и изощренностью. Наиболее опасными видами атак являются DDoS-воздействия нового поколения, полиморфное вредоносное программное обеспечение, а также скрытые каналы управления, маскирующиеся под легитимный трафик [1]. В этих условиях традиционные сигнатурные системы обнаружения и предотвращения вторжений (IDS/IPS) демонстрируют прогрессирующую неэффективность. Сама логика работы у них реактивная: пока атака не зафиксирована и не разобрана, сигнатуры для нее попросту нет, а значит, против угроз «нулевого дня» защита не срабатывает. К этому добавляется еще одна сложность. На TLS и HTTPS сегодня приходится больше 90 % сетевого трафика, и пакеты в большинстве

своем идут зашифрованными. Чтобы разобрать их содержимое, нужны ресурсы, которых либо нет, либо не хватает, чтобы успевать в реальном времени.

Отсюда следует, что сигнатурный анализ как основной инструмент защиты себя исчерпал, и его место должен занять поведенческий мониторинг с опорой на машинное обучение. Ниже разбирается гибридная схема, где работают сразу два типа моделей – с учителем и без учителя; цель – показать, насколько такой подход уместен для поиска сетевых аномалий в киберфизических системах.

Методы машинного обучения для обнаружения сетевых аномалий

Обучение с учителем: градиентный бустинг (XGBoost)

XGBoost работает по схеме градиентного бустинга на деревьях решений. Деревья добавляются в ансамбль одно за другим, и каждое новое подгоняется под остатки ошибок предыдущих – функция потерь при этом постепенно уменьшается [2]. В задачах сетевой безопасности ключевыми преимуществами XGBoost являются эффективная работа с разреженными данными, встроенная L1 и L2 регуляризация, обеспечивающая устойчивость к переобучению, а также высокая скорость и точность при обработке табличных данных. Среди алгоритмов градиентного бустинга XGBoost часто показывает лучшие результаты в системах обнаружения вторжений [3]. Однако основное ограничение метода связано с необходимостью использования больших объемов размеченных данных и слабой способностью выявлять ранее неизвестные атаки.

Обучение без учителя: изолирующий лес (Isolation Forest)

Isolation Forest – это алгоритм обучения без учителя, основанный на принципе быстрой изоляции аномалий. Он реализует рекурсивное случайное разбиение пространства признаков, при котором аномальные объекты изолируются за меньшее число разбиений по сравнению с нормальными данными [4]. Оценка аномальности экземпляра x рассчитывается по формуле:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (1)$$

где $E(h(x))$ – средняя высота изоляции, $c(n)$ – средняя высота неудачного поиска в бинарном дереве поиска с n элементами. Чем ближе значение

$s(x, n)$ к 1, тем выше вероятность аномалии. Для киберфизических систем преимущества Isolation Forest особенно значимы. Алгоритм обладает линейной вычислительной сложностью $O(n \log n)$, не требует наличия размеченных данных и демонстрирует высокую эффективность при обнаружении атак «нулевого дня», особенно в высокомерных пространствах.

Гибридная архитектура обнаружения аномалий

Признаковое пространство и векторизация трафика

Эффективность любой модели машинного обучения в задачах сетевой безопасности напрямую определяется качеством признакового пространства. Современный подход предполагает переход от анализа отдельных пакетов к потоковому представлению на основе набора из пяти признаков, включающего исходный и целевой IP-адреса, порты источника и назначения, а также используемый протокол [5]. Такое решение позволяет существенно снизить вычислительную нагрузку.

Рекомендуемый набор включает 45 поведенческих признаков, сгруппированных по следующим категориям:

- объемно-временные признаки, включающие длительность потока, объем переданных байтов и пакетов, а также интенсивность передачи в расчете на пакет и на байт;
- признаки временной структуры, представляющие собой статистические характеристики межпакетных интервалов;
- протокольно-поведенческие признаки, отражающие распределение TCP-флагов;
- статистические и энтропийные признаки, включающие расчет энтропии Шеннона для портов, IP-адресов и флагов.

Перед подачей в модели признаки проходят процедуру нормализации, что обеспечивает корректную работу алгоритмов и повышает стабильность процесса обучения.

Синтез решений

Предлагаемая гибридная архитектура объединяет сильные стороны обоих рассмотренных подходов. Для каждого сетевого потока параллельно вычисляются две независимые оценки. Модель XGBoost, обученная на известных паттернах атак, выдает вероятность принадлежности потока к вре-

доносному классу P_{xgb} [2]. Алгоритм Isolation Forest, в свою очередь, формирует нормированную оценку аномальности S_{IF} [4]. Итоговая гибридная оценка формируется по правилу максимума [5]:

$$Score_{hybrid} = \max(P_{XGB}, S_{IF}) \quad (2)$$

Выбор именно этого оператора синтеза решений обоснован приоритетом минимизации пропуска реальных атак, которые в терминах машинного обучения обозначаются как False Negatives. Данное требование является критическим для систем безопасности КФС. В отличие от усреднения или взвешенного суммирования, правило максимума обеспечивает наибольшую чувствительность к потенциальным угрозам. Предложенная архитектура реализует принцип «лучшее из двух миров» (рис. 1).

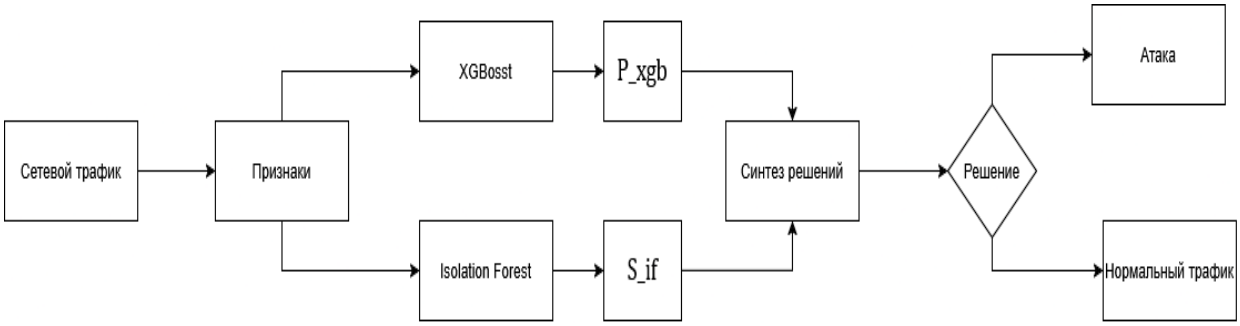


Рис. 1. Архитектура гибридной системы обнаружения аномалий в КФС с объединением оценок по правилу максимума

Метрики оценки эффективности в условиях дисбаланса классов

В реальных сетях КФС доля аномального трафика обычно составляет менее 1 %, что создает крайне несбалансированную задачу классификации [6]. В таких условиях традиционные метрики, ориентированные на общую точность, становятся неинформативными. Более адекватными являются метрики, ориентированные на редкий положительный класс. В таблице 1 представлены основные из них с указанием формул и особенностей применения при сильном дисбалансе.

ТАБЛИЦА 1. Метрики оценки качества классификации в условиях дисбаланса классов

Метрика	Формула	Применимость в условиях дисбаланса
Точность	$\frac{TP}{TP + FP}$	Снижения ложных срабатываний

Метрика	Формула	Применимость в условиях дисбаланса
Полнота	$\frac{TP}{TP+FN}$	Минимизация пропусков атак
F1-мера	$2 \times \frac{P*R}{P*R}$	Баланс точность и полноты
ROC-AUC	Площадь под ROC-кривой	Завышает оценку при сильном дисбалансе
PR-AUC	Площадь под «точность-полнота» кривой	Фокус на редком классе

F1-мера, представляющая собой гармоническое среднее между точностью и полнотой, а также площадь под «точность-полнота» кривой наиболее объективно отражают реальную эффективность модели при сильном дисбалансе. Обе метрики чувствительны к качеству распознавания именно редких аномалий, а это и есть тот результат, ради которого выстраивается защита КФС.

Заключение

Проведенный анализ позволяет сформулировать следующие основные выводы:

1) Сигнатурные IDS/IPS в нынешних условиях перестали справляться со своей задачей. Шифрование основной массы трафика и регулярное появление атак «нулевого дня» делают глубокий разбор пакетов ресурсозатратным, а сам сигнатурный подход – реактивным по своей сути и потому непригодным для упреждающей защиты.

2) Связка XGBoost и Isolation Forest дает результат, который заметно превосходит возможности каждой модели по отдельности. На XGBoost ложится точное распознавание уже известных типов атак, а Isolation Forest подхватывает аномалии, которых нет в обучающей выборке, и обходится без разметки.

3) Применение правила максимума при объединении оценок сокращает долю пропущенных атак – а для киберфизических систем именно пропуск, а не ложная тревога, обходится дороже всего.

4) При сильном дисбалансе классов опираться на точность (accuracy) и ROC-AUC рискованно: обе метрики склонны завышать картину. Более показательны F1-мера и площадь под кривой «точность–полнота».

Сочетание XGBoost и Isolation Forest, рассмотренное в работе, имеет смысл развивать как один из путей укрепления безопасности киберфизических систем перед лицом текущих угроз. Дальнейшие шаги видятся в нескольких направлениях: подключение инкрементального обучения для подстройки моделей под дрейф концептов, расширение перечня поддерживаемых промышленных протоколов и встраивание методов объяснимого ИИ.

Список используемых источников

1. Sindhuja P. et al. Real Time Intrusion Detection using XGBoost and Decision Tree Classifier // 2025 8th International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2025. С. 1550-1556.
2. Fan Z., You Z. Research on network intrusion detection based on XGBoost algorithm and multiple machine learning algorithms //Theoretical and Natural Science. 2024. Т. 31. №. 1. С. 161-166.
3. Dhaliwal S. S., Nahid A. A., Abbas R. Effective intrusion detection system using XGBoost //Information. 2018. Т. 9. №. 7. С. 149.
4. Liu F. T., Ting K. M., Zhou Z. H. Isolation forest // 2008 eighth IEEE International conference on data mining. IEEE, 2008. С. 413-422.
5. Parambil E., Krishna A. A Hybrid Ensemble Model using XGBoost and AdaBoost to detect and distinguish zero-day attacks: дис. Dublin, National College of Ireland, 2025.
6. Hosain Y., Çakmak M. XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems //Scientific Reports. 2025. Т. 15. №. 1. С. 22278.

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ПИиВТ СПбГУТ М. А. Бирюковым.

УДК 004.414

АНАЛИЗ АРХИТЕКТУРНЫХ ПОДХОДОВ К РАЗРАБОТКЕ ПРИЛОЖЕНИЙ ДЛЯ СИСТЕМАТИЗАЦИИ ЧИТАТЕЛЬСКОГО ОПЫТА

В. М. Коретко (студент гр. ИКПИ-24 СПбГУТ), koretko.vm@sut.ru

Статья посвящена сравнительному анализу архитектурных подходов к разработке приложений для систематизации читательского опыта. На основе анализа портретов целевой аудитории и вытекающих из них требований к надежности и доступности данных проведено сравнение архитектурных паттернов с позиции способа развертывания и типа клиентской части. Для каждого подхода выделены ключевые характеристики, определяющие их применимость в контексте решаемой задачи. В результате определено оптимальное архитектурное решение для приложений данного класса, обоснованное требованиями надежности, доступности и удобства использования

архитектура программных приложений, веб-приложение, читательский дневник, монолитная архитектура, тонкий клиент, трехуровневая архитектура

Современный человек в своей профессиональной и учебной деятельности сталкивается с необходимостью обработки больших объемов текстовой информации. Книги, научные статьи, учебные пособия формируют обширный читательский опыт, требующий систематизации. Традиционные бумажные дневники и заметки в телефоне становятся непрактичными: они не обеспечивают надежного хранения, не позволяют структурировать информацию и часто не адаптированы для оперативного поиска ранее сделанных записей.

Как отмечается в исследовании ВЦИОМ, интерес к чтению среди населения растет, при этом молодое поколение активно использует цифровые устройства для потребления контента [1]. Однако ключевая проблема заключается не в фиксации прочитанного, а в оперативном доступе к систематизированным результатам чтения. Пользователи – студенты, преподаватели, специалисты – часто читают в условиях дефицита времени: в транспорте, между парами, в командировках. Им необходимо иметь возможность быстро извлечь ранее сделанные заметки, цитаты или выводы для использования в профессиональной деятельности или образовательном процессе. Это требует программного решения, обеспечивающего надежное хранение данных и их доступность независимо от местоположения пользователя.

Для корректного выбора архитектурного решения необходимо определить целевую аудиторию и вытекающие из ее потребностей требования к системе. Целевая аудитория включает следующие категории пользователей:

- любители книг, желающие систематизировать свои читательские впечатления, сохранять понравившиеся цитаты и отслеживать прогресс чтения;
- школьники, читающие литературу по школьной программе и готовящиеся к написанию сочинений и экзаменов;
- студенты, которым необходимо оперативно фиксировать и извлекать информацию из учебной и научной литературы для подготовки к занятиям и экзаменам;
- преподаватели, использующие литературу для подготовки методических материалов и нуждающиеся в структурированном доступе к источникам;
- специалисты, вынужденные следить за новинками профессиональной литературы и быстро возвращаться к ранее прочитанным материалам.

Общей характеристикой всех перечисленных категорий является потребность в надежной систематизации читательского опыта и необходимость доступа к сохраненным результатам с разных устройств в различных условиях. Для школьников и студентов дополнительным фактором является дефицит времени в период подготовки к экзаменам. Для преподавателей и специалистов ключевым требованием выступает оперативный доступ к профессиональной информации. Любители книг, в свою очередь, ценят удобство ведения записей и наглядность статистики.

Таким образом, анализ целевой аудитории позволяет сформулировать ключевые требования к разрабатываемому приложению:

- надежное хранение данных, исключающее их потерю при поломке или смене устройства;
- доступ к данным с любых устройств, независимо от операционной системы;
- возможность быстрого добавления записей без сложных процедур;
- низкий порог входа для новых пользователей: отсутствие необходимости установки, интуитивно понятный интерфейс;
- возможность взаимодействия между пользователями (просмотр и добавление отзывов о книгах).

В современной программной инженерии выделяют различные архитектурные паттерны, каждый из которых имеет свои характеристики, преимущества и ограничения [2]. Для решения задачи систематизации читательского опыта целесообразно провести сравнение по двум ключевым измерениям: по способу развертывания – монолитная или микросервисная архитектура, и по типу клиентской части – «толстый» или «тонкий» клиент [3].

Монолитная архитектура представляет собой единый программный блок, где все функциональные компоненты тесно связаны и разделяют общую базу кода. Такой подход обеспечивает простоту разработки на начальных этапах, отсутствие сложностей с распределенными вызовами и более прямолинейное тестирование. Монолит может быть развернут как единое целое на одном хосте, что упрощает управление инфраструктурой [3].

Микросервисная архитектура, напротив, разбивает приложение на множество небольших, независимых сервисов, каждый из которых выполняет конкретную бизнес-функцию и может быть разработан, развернут и масштабирован автономно [4]. Такой подход обеспечивает высокую масштабируемость и гибкость разработки, но требует значительных затрат на развертывание, мониторинг и поддержку инфраструктуры.

Для приложения с ограниченным функционалом и небольшой целевой аудиторией, каким является читательский дневник, применение микросервисной архитектуры является избыточным и экономически неоправданным. Монолитная архитектура в данном случае предпочтительнее, так как позволяет быстрее вывести продукт на рынок и снижает операционные расходы [3].

В рамках клиент-серверного взаимодействия ключевым вопросом является распределение бизнес-логики между клиентом и сервером. Здесь выделяют два основных подхода [3].

«Толстый» клиент (нативное приложение) берет на себя значительную часть обработки данных. Большая часть бизнес-логики выполняется на стороне клиента, а сервер в основном служит хранилищем данных. Примерами являются классические десктопные программы или мобильные приложения для iOS/Android. Преимуществами такого подхода являются высокая производительность и возможность полноценной работы без интернета. Однако он требует установки, разработки отдельных версий для разных платформ и ручного обновления.

«Тонкий» клиент (веб-приложение) выполняет минимум логики на стороне пользователя, передавая основную обработку серверу. Основная работа по реализации бизнес-логики и доступу к данным выполняется на сервере, а клиент в основном отвечает за отображение интерфейса и отправку запросов. Тонкий клиент не требует установки, обеспечивает кроссплатформенность, автоматически получает обновления, но зависит от наличия интернет-соединения.

Как показано в таблице 1, монолитная архитектура с «тонким» веб-клиентом наилучшим образом соответствует требованиям, предъявляемым к приложению для систематизации читательского опыта. Она обеспечивает централизованное хранение данных, доступность с любых устройств, низкий порог входа и автоматическое обновление. Микросервисная архитектура избыточно сложна, а «толстый» клиент требует установки и ручного обновления, что создает дополнительные барьеры для пользователей.

ТАБЛИЦА 1. Сравнение архитектурных подходов

Критерий	Монолит («толстый» клиент)	Монолит («тонкий» клиент)	Микросервисы
Доступ с разных устройств	Нет (привязка к ОС)	Да (любой браузер)	Да
Сохранность данных при поломке устройства	Нет (данные локально)	Да (данные на сервере)	Да
Необходимость установки	Да	Нет	Нет
Обновления	Ручные	Автоматические	Автоматические
Работа без интернета	Да	Нет	Нет
Взаимодействие пользователей	Нет / ограничено	Да	Да
Сложность реализации	Средняя	Средняя	Высокая

Рассматриваемая клиент-серверная архитектура с «тонким» веб-клиентом фактически представляет собой трехуровневую архитектуру, в которой выделяются три логических уровня: клиентский, сервер приложений и уровень хранения данных [5]. Такое разделение позволяет централизованно управлять данными, обеспечить их сохранность и доступность с разных клиентских устройств.

Важным аспектом проектирования является выбор модели данных. Характер использования данных предполагает частое добавление новых записей, периодическое редактирование существующих и интенсивные операции чтения (поиск, фильтрация). Данные логически связаны между собой: пользователь может иметь множество книг, книга может иметь множество отзывов. Указанные характеристики делают реляционную модель данных наиболее подходящей, так как она обеспечивает целостность связей, поддержку транзакций и эффективное выполнение сложных запросов [6].

Вопрос организации физического хранения данных также является важным архитектурным решением. Возможны варианты использования публичного облака, частного облака или собственного серверного оборудования (NAS) [7]. Для разрабатываемого приложения, ориентированного на ограниченную аудиторию, оптимальным является аренда облачного сервера (VPS), что обеспечивает баланс между надежностью, стоимостью и сложностью поддержки.

Клиент-серверная архитектура с «тонким» веб-клиентом и монолитным развертыванием позволяет реализовать все выявленные требования. Централизованное хранение данных на сервере гарантирует сохранность записей и доступность с разных устройств [8]. Единое хранилище отзывов обеспечивает возможность взаимодействия пользователей [5]. Выбор веб-формата для клиентской части обусловлен необходимостью сделать приложение максимально доступным: оно не требует установки, работает на любом устройстве с браузером и автоматически обновляется.

Таким образом, сочетание трехуровневой архитектуры с монолитным развертыванием, веб-клиентом («тонким» клиентом) и реляционным хранилищем данных представляет собой оптимальное решение для разработки читательского дневника, отвечающее современным требованиям доступности, надежности и удобства. Предложенное архитектурное решение учитывает четыре ключевых измерения архитектуры программных систем: архитектурные характеристики, архитектурные решения, логические компоненты и архитектурный стиль [9], что обеспечивает системный подход к проектированию.

Список используемых источников

1. Книга в эпоху цифры: аналитический обзор // Всероссийский центр изучения общественного мнения (ВЦИОМ): официальный сайт. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/kniga-v-ehpokhu-cifry (дата обращения: 20.03.2026).

2. Гагарина Л. Г. Проектирование и архитектура программных систем: учебное пособие / Л. Г. Гагарина, А. Р. Федоров, П. А. Федоров. 2-е изд., испр. и доп. Москва: ИНФРА-М, 2025. 334 с.

3. Популярные виды архитектуры приложений к 2025 году // Skyeng: официальный сайт. URL: https://skyeng.ru/it-industry/it/populyarnyye-vidy-arkhitektury-prilozheniy-2025/ (дата обращения: 02.04.2026).

4. Ричардсон К. Микросервисы. Паттерны разработки и рефакторинга / К. Ричардсон; пер. с англ. С. Черникова. Санкт-Петербург: Питер, 2025. 544 с.

5. Трехуровневая клиент-серверная архитектура // Skypro Wiki: официальный сайт. URL: https://sky.pro/wiki/sql/trehurovnevaya-klient-servernaya-arhitektura/ (дата обращения: 29.03.2026).

6. Архитектура данных: выбор модели хранения // Хабр: официальный сайт. URL: https://habr.com/ru/companies/otus/articles/911874/ (дата обращения: 29.03.2026).

7. Выбор типа хранилища данных: публичное облако, частное облако, NAS // Хабр: официальный сайт. – URL: https://habr.com/ru/companies/finops_ru/articles/976842/ (дата обращения: 28.03.2026).

8. Клиент-серверная архитектура: что это и зачем нужно // Skypro Wiki: официальный сайт. URL: https://sky.pro/wiki/sql/klient-servernaya-arhitektura-chto-eto-i-zachem-nuzhno/ (дата обращения: 18.03.2026).

9. Форд Н. Архитектура программного обеспечения. Трудные аспекты / Н. Форд, М. Ричардс, П. Садаладж, З. Дегхани. Санкт-Петербург: Питер, 2022. 400 с.

Статья представлена научным руководителем, старшим преподавателем кафедры ПИиВТ СПбГУТ О. Б. Петровой.

УДК 004.4’2:004.8

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПЕРСОНАЛИЗАЦИИ СИСТЕМ УПРАВЛЕНИЯ ЗАДАЧАМИ

Е. В. Коровкина (ассистент кафедры СОД СПбГУТ)
А. П. Куркин (студент группы ИСТ-221 СПбГУТ), kurkin.ap@sut.ru

В статье исследуется проблема недостаточной персонализации современных систем управления задачами и обосновывается необходимость применения технологий искусственного интеллекта для ее решения. Проводится анализ рынка программного обеспечения для управления задачами, демонстрирующий устойчивый рост спроса на интеллектуальные инструменты планирования. Рассматриваются ключевые причины низкой эффективности существующих методов тайм-менеджмента, включая когнитивную перегрузку и отсутствие адаптивности. На основе сравнительного анализа популярных систем управления задачами выявлены их системные недостатки. Обосновывается применение больших языковых моделей как инструмента автоматической генерации персонализированных планов, декомпозиции долгосрочных целей и диалогового управления расписанием.

искусственный интеллект, управление задачами, тайм-менеджмент, персонализация, языковые модели, когнитивная нагрузка, планирование

Эффективное управление личным временем является одной из ключевых компетенций современного человека. Рост информационной нагрузки, необходимость совмещать учебу, работу и саморазвитие приводят к тому, что задача планирования становится самостоятельной проблемой, требующей значительных когнитивных ресурсов.

Актуальность данного направления подтверждается динамикой мирового рынка программного обеспечения для управления задачами. По данным аналитической компании The Business Research Company, объем рынка составил 5,1 млрд долларов США в 2025 году и, согласно прогнозу, достигнет 9,52 млрд долларов к 2030 году при среднегодовом темпе роста 12,8 % [1]. Среди ключевых факторов роста выделяются увеличение спроса на интеллектуальные инструменты повышения продуктивности, внедрение технологий искусственного интеллекта для приоритизации задач и расширение рынка мобильных приложений [1]. Вместе с тем существующие решения не в полной мере удовлетворяют потребности пользователей в части персонализации и адаптивности планирования.

Исследования в области когнитивной психологии показывают, что планирование само по себе является ресурсоемким процессом. Явление, известное как «усталость от принятия решений», приводит к снижению качества планов по мере роста их сложности [2]. Дополнительным фактором является игнорирование биологического ритма продуктивности: уровень концентрации и работоспособности человека существенно варьируется в течение дня, однако традиционные системы управления задачами не учитывают этот параметр при составлении расписания.

В практике личной продуктивности широко применяется ряд структурированных методов: SMART-целеполагание, матрица Эйзенхауэра, техника «Помодоро». Вместе с тем все перечисленные методы обладают общим системным недостатком: они требуют от пользователя высокого уровня самодисциплины и регулярного самоконтроля, при этом не адаптируются автоматически к изменяющейся загруженности или эмоциональному состоянию пользователя. Исследования показывают, что большинство людей прекращают применение структурированных методов планирования в течение нескольких недель [2].

Для выявления системных недостатков существующих решений проведен сравнительный анализ пяти распространенных инструментов управления задачами, результаты которого представлены в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ систем управления задачами

Критерий	Trello	Habitica	MS Project	Motion	ClickUp Brain
Персонализация под пользователя	Нет	Частично	Нет	Частично	Нет
AI-генерация задач	Нет	Нет	Нет	Нет	Да
Автоматическое планирование дня	Нет	Нет	Нет	Да	Нет
Учет уровня энергии	Нет	Нет	Нет	Нет	Нет
Диалоговое управление	Нет	Нет	Нет	Нет	Частично
Декомпозиция целей	Нет	Нет	Да	Нет	Да
Доступность в РФ	Нет	Да	Да	Нет	Нет

Как видно из таблицы 1, даже среди систем с интеграцией искусственного интеллекта ни одно из рассмотренных решений не обеспечивает учета уровня энергии пользователя при составлении плана, не поддерживает персонализацию под личные интересы и недоступно для пользователей на территории Российской Федерации без дополнительных технических средств [3, 4, 5].

Развитие больших языковых моделей открывает принципиально новые возможности для построения адаптивных систем планирования. В отличие от детерминированных алгоритмов, языковые модели способны учитывать контекст пользователя в его полноте: интересы, текущее состояние, историю выполнения задач и долгосрочные цели. Интеграция языковой модели в систему управления задачами позволяет реализовать три ключевых сценария: автоматическую генерацию персонального плана дня с учетом уровня энергии пользователя, декомпозицию долгосрочных целей на последовательные шаги с промежуточными дедлайнами, а также диалоговое управление планом через запросы на естественном языке.

Применение данного подхода позволяет снизить когнитивную нагрузку, связанную с процессом планирования, и обеспечить адаптивность расписания к изменяющемуся контексту пользователя – задаче, которую традиционные системы управления задачами принципиально не способны решить.

Таким образом, проведенное исследование показало, что существующие системы управления задачами не обеспечивают персонализированного планирования с учетом индивидуального ритма и текущего состояния пользователя. Применение больших языковых моделей позволяет преодолеть выявленные ограничения: автоматизировать процесс планирования, обеспечить адаптацию плана к текущему состоянию пользователя и реализовать интуитивное диалоговое взаимодействие. Дальнейшие исследования в данном направлении представляются перспективными с точки зрения повышения эффективности личного тайм-менеджмента.

Список используемых источников

1. The Business Research Company. Task Management Software Market Report 2026 [Электронный ресурс]. URL: https://www.thebusinessresearchcompany.com (дата обращения: 20.03.2025).

2. Baumeister R. F., Tierney J. Willpower: Rediscovering the Greatest Human Strength. New York: Penguin Press, 2011. 291 p.

3. Trello Help Center. Getting started with Trello [Электронный ресурс]. URL: https://support.atlassian.com/trello (дата обращения: 20.03.2025).

4. Motion. AI-Powered Calendar and Task Manager [Электронный ресурс]. URL: https://www.usemotion.com (дата обращения: 20.03.2025).

5. ClickUp. ClickUp Brain: AI-Powered Task Management [Электронный ресурс]. URL: https://clickup.com/features/ai (дата обращения: 20.03.2025).

Статья представлена и. о. заведующего кафедрой СОД СПбГУТ, кандидатом технических наук, доцентом Ю. М. Бородянским.

УДК 004.056.53:004.032.26

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ПОИСКА И ИСПРАВЛЕНИЯ УЯЗВИМОСТЕЙ В КОДЕ: ОТ ОПИСАНИЯ НА ЕСТЕСТВЕННОМ ЯЗЫКЕ К ЗАЩИТЕ

Р. Я. Лабковская (к.т.н, доцент кафедры ИУС СПбГУТ)
А. М. Негина (студент группы ИСТ-361 СПбГУТ), kurdina.am@sut.ru
А. А. Стороженко (студент группы ИСТ-312 СПбГУТ), storozhenko.aa@sut.ru

Интеллектуальные системы поиска и исправления уязвимостей становятся важными из-за роста сложности программного обеспечения. Методы машинного обучения и генеративные модели автоматизируют обнаружение и исправление дефектов, снижая зависимость от ручной экспертизы. Однако остаются проблемы качества данных, интерпретируемости и рисков автоматического исправления, что требует дальнейших исследований и интеграции с формальной верификацией.

интеллектуальный анализ кода, уязвимости программного обеспечения, машинное обучение, генерация исправлений

Интеллектуальные системы поиска и исправления уязвимостей в программном коде находятся на пересечении безопасной разработки, статического анализа, машинного обучения и генеративных моделей. Их назначение состоит в поддержке полного цикла работы с дефектами: обнаружения, интерпретации, исправления и последующей верификации. Актуальность данного направления обусловлена ростом объема программного кода и усложнением архитектурных зависимостей, что повышает требования к качеству анализа [1-3].

В нормативных документах уязвимость определяется как состояние или поведение системы, нарушающее явную или неявную политику безопасности. В российском стандарте уязвимости кода выделены в отдельный класс [1]. Это важно для прикладной безопасности: объектом анализа становится не только работающее приложение, но и исходный код, его конфигурация, архитектура и процессы сопровождения. Современные подходы формируют цепочку «обнаружение – интерпретация – исправление – проверка», в которой интеллектуальные методы используются как средство повышения полноты и скорости обработки дефектов.

Классические методы сигнатурного и традиционного статического анализа сталкиваются с фундаментальными ограничениями. Они надежно

работают главным образом для известных шаблонов уязвимостей и хуже обобщаются на новые или модифицированные сценарии атак. По этой причине наблюдается постепенный переход к машинному и глубокому обучению. Такие модели извлекают закономерности из больших корпусов кода и учитывают синтаксические и семантические признаки, используя последовательности токенов, абстрактные синтаксические деревья, а также графы потока управления и данных.

Настоящая работа носит концептуально-обзорный характер. Научная проблема заключается в отсутствии систематизированного сопоставления современных интеллектуальных методов обнаружения и исправления уязвимостей по ключевым критериям: архитектуре модели, объяснимости, устойчивости к адверсариальным воздействиям на саму модель и способности сохранять семантику программы при автоматической генерации патчей.

Исходная гипотеза состоит в том, что гибридные схемы, объединяющие графовые нейросети, трансформеры и формальные верификаторы, позволяют обеспечить более полное покрытие жизненного цикла дефекта, чем изолированное применение любого из этих классов методов.

Вклад работы заключается в следующем:

1) критическом сопоставлении подходов на базе GNN, Transformer и генеративных патч-моделей с учетом их архитектурных особенностей и ограничений;

2) структурной классификации рисков автоматического исправления, включая overpatching, semantic divergence, угрозы внедрения бэкдоров и снижение детерминированности;

3) формулировании перспективных направлений развития (верифицируемый ИИ, федеративное обучение, стандарты сертификации AI-патчей) с опорой на действующие нормативные рамки (NIST SSDF, ISO/IEC 29147/30111, ГОСТ Р 56546-2015).

Поскольку работа является тематическим обзором, а не систематическим исследованием, схема отбора источников по PRISMA не применялась; вместо нее использована экспертная тематическая группировка публикаций, датасетов и промышленных инструментов за 2018–2024 гг.

Одним из ранних примеров является модель Devign – графовая нейронная сеть для классификации функций на языке C как уязвимых или безопасных [4-6]. Модель обучалась на размеченном коде реальных open-source проектов и продемонстрировала улучшение метрики accuracy примерно на 10,5 % относительно базового уровня (baseline). Полученные результаты

подтверждают, что модели с явным учетом структурных зависимостей эффективны в задачах, где существенны контекст, поток данных и взаимосвязи между элементами программы.

Для обучения и оценки подобных моделей используют открытые датасеты. Среди наиболее известных – NIST Software Assurance Reference Dataset (SARD) и Juliet 1.1 C/C++ and Java Test Suite [7, 8]. Набор Juliet 1.1 содержит более 81 тысячи синтетических тестовых программ на C/C++ и Java с заранее известными дефектами, охватывающими 181 категорию CWE. Эти корпуса обеспечивают воспроизводимое сравнение инструментов, хотя и не полностью отражают распределение дефектов в промышленном коде.

Анализ таблицы 1 показывает, что показатели качества обнаружения и исправления уязвимостей зависят от типа модели и решаемой задачи, а автоматическая генерация патчей требует дополнительной верификации.

ТАБЛИЦА 1. Сравнительная характеристика подходов к обнаружению и автоматическому исправлению уязвимостей

Подход	Precision	Recall	F1	False Positive Rate	Интерпретация
GNN-based detection (Devign-class)	высокая	высокая	высокий	низкий	лучше при графовых зависимостях
Transformer-based detection (CodeBERT/ CodeT5-class)	средневысокая	средневысокая	сопоставимый	средний	удобен при больших корпусах
NL-to-Patch / LLM repair (PatchLM-class)	непрямо сравнима	непрямо сравнима	не основной	не применим	требует тестов и верификации

Для генерации исправлений метрики Precision, Recall, F1 и False Positive Rate следует дополнять семантической проверкой, прохождением тестов и оценкой overpatching.

От задачи обнаружения уязвимостей системы переходят к их автоматическому исправлению. Подзадача NL-to-Patch, то есть генерация патча

по описанию проблемы, получила развитие в работах типа PatchLM. Модель, дообученная на парах исправлений из коммитов, связанных с реальными CVE, продемонстрировала превосходство над базовыми CodeT5 и CodeLlama по метрикам CodeBLEU и ROUGE. Практические инструменты уже внедряют подобные возможности: GitHub Copilot Autofix, Snyk Agent Fix и AI-возможности GitLab позволяют автоматически предлагать исправления и даже формировать merge request. При этом все зрелые реализации предполагают обязательную проверку человеком, статический анализ и тестирование в CI.

Развитие таких систем тесно связано с обработкой естественного языка. Код рассматривается как особый вид структурированного текста, что позволяет применять методы NLP для преобразования кода в удобные для нейросетей представления, а также для анализа описаний уязвимостей и требований безопасности. Появляются подходы, использующие рекуррентные сети, LSTM, векторные встраивания и обучение с подкреплением, где поиск уязвимостей моделируется как последовательность решений в марковской среде.

Однако ограничения остаются существенными. Для этапа обнаружения основными проблемами являются дефицит качественных реальных датасетов, дисбаланс классов, ограниченная переносимость моделей между языками и проектами, компромисс между точностью и скоростью работы, а также низкая интерпретируемость. При генерации исправлений дополнительно возникают риски overpatching, semantic divergence, синтаксически корректного, но семантически неверного кода, нарушения бизнес-логики, внедрения бэкдоров, утечки интеллектуальной собственности и снижения детерминированности исправлений. Поэтому интеллектуальные системы следует рассматривать как инструмент поддержки эксперта, а не как полностью автономное решение.

С нормативной точки зрения развитие таких систем должно быть согласовано с NIST SSDF версии 1.1 [3], ISO/IEC 29147:2018 [9], ISO/IEC 30111:2019 [10] и ГОСТ Р 56546-2015 [1]. Для AI-патчей особенно важны трассируемость изменений, возможность воспроизведения результата, интеграция с code review и формализованные процедуры аудита и приемки.

Перспективными направлениями являются верифицируемый ИИ, гибридные схемы, сочетающие формальные методы и LLM, федеративное обучение на промышленном коде без вывода исходников за периметр орга-

низации, а также стандартизация процедур сертификации AI-патчей. Особое значение имеют контроль источников обучающих данных, оценка устойчивости к backdoor-атакам, проверка сохранения семантики программы и обеспечение воспроизводимости предложенных исправлений.

В целом интеллектуальные системы поиска и исправления уязвимостей представляют собой многоуровневую инфраструктуру, в которой стандарты определяют требования и границы, датасеты обеспечивают сопоставимость экспериментов, модели обнаруживают дефекты, а генеративные компоненты формируют кандидаты исправлений.

Список используемых источников

1. ГОСТ Р 56546-2015. Информационная технология. Методы и средства обеспечения безопасности. Уязвимости программного обеспечения. Общие положения. М.: Стандартинформ, 2015.

2. National Institute of Standards and Technology (NIST). National Vulnerability Database (NVD). URL: https://nvd.nist.gov/vuln (дата обращения: 10.03.2026).

3. National Institute of Standards and Technology (NIST). Secure Software Development Framework (SSDF) Version 1.1 (SP 800-218). 2022. URL: https://csrc.nist.gov/publications/detail/sp/800-218/final (дата обращения: 10.03.2026).

4. Zhou Y., et al. Devign: Effective Vulnerability Identification via Graph Neural Networks. 2019. URL: https://arxiv.org/abs/1909.03496 (дата обращения: 04.03.2026).

5. Feng Z., et al. CodeBERT: A Pre-Trained Model for Programming and Natural Languages. 2020. URL: https://arxiv.org/abs/2002.08155 (дата обращения: 10.03.2026).

6. Wang Y., et al. CodeT5: Identifier-aware Unified Pre-trained Encoder-Decoder Models for Code Understanding and Generation. 2021. URL: https://arxiv.org/abs/2109.00859 (дата обращения: 07.03.2026).

7. National Institute of Standards and Technology (NIST). Software Assurance Reference Dataset (SARD). URL: https://samate.nist.gov/SARD/ (дата обращения: 10.03.2026).

8. Boland J., Black P. Juliet 1.1 C/C++ and Java Test Suite. National Institute of Standards and Technology, 2012. URL: https://samate.nist.gov/SARD/test-suites/112 (дата обращения: 10.03.2026).

9. ISO/IEC. ISO/IEC 29147:2018 Information technology Security techniques Vulnerability disclosure. Geneva: ISO, 2018.

10. ISO/IEC. ISO/IEC 30111:2019 Information technology Security techniques Vulnerability handling processes. Geneva: ISO, 2019.

УДК 004.89

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ТИПОВЫХ СТРУКТУР ИНТЕЛЛЕКТА В ЗАДАЧАХ УПРАВЛЕНИЯ СЛОЖНЫМИ СИСТЕМАМИ

И. Р. Лебедев (студент группы МАП-2512 СПбГУТ), lebedev.ir@sut,ru

При построении интеллектуальных систем управления и мониторинга для промышленных объектов, энергосетей или транспортных комплексов одним из ключевых проектных решений становится выбор архитектуры обработки информации. В теории интеллектуальных систем сложилось несколько типовых структур, различающихся порядком взаимодействия сенсорных, аналитических и исполнительных модулей. Наиболее часто рассматриваются иерархическая (вертикальная), сетевая (горизонтальная, децентрализованная) и гибридная структуры. Каждая из них имеет известные качественные преимущества: иерархия дает высокую скорость в статике, сеть обеспечивает живучесть при отказах, а гибрид претендует на баланс свойств. Однако количественные сравнения этих структур при изменении нагрузки, появлении помех и отказов узлов в литературе представлены фрагментарно, что затрудняет обоснованный выбор при проектировании.

интеллектуальные системы, типовые структуры интеллекта, иерархическая структура, сетевая структура, гибридная структура, управление сложными системами, мониторинг, сравнительный анализ

Современные объекты управления – от производственных линий до распределенных энергосетей – предъявляют жесткие требования к скорости обработки сигналов и устойчивости к сбоям [1]. Как показывает практика, классическая иерархия с единым центром принятия решений нередко становится узким местом при резких скачках нагрузки или при выходе из строя верхних уровней [2]. Альтернативные архитектуры – сетевая и гибридная – потенциально способны повысить живучесть, однако их сравнительная эффективность в идентичных условиях почти не исследована количественно [3, 4]. Большинство существующих работ ограничиваются либо качественным описанием, либо тестированием только двух структур на одном типе сценариев [5, 6]. В результате проектировщики вынуждены полагаться на интуицию, а не на объективные данные.

В связи с этим целью настоящей работы стало численное сравнение трех типовых структур – иерархической, сетевой и гибридной – на едином наборе сценариев, включающих стационарный режим, перегрузку, зашумление каналов и отказ узла. В отличие от известных публикаций [7, 8], здесь предложена унифицированная методика, обеспечивающая одинаковые

условия для всех архитектур. Для каждой структуры фиксировались правила маршрутизации сигналов и принятия решений: в иерархии сигнал движется снизу вверх и сверху вниз с возможной модификацией на каждом уровне; в сети узлы обмениваются сообщениями и достигают консенсуса простым большинством; в гибриде система разбивается на кластеры с внутренней иерархией, а кластеры взаимодействуют по сетевым принципам [9].

Оценка проводилась на имитационной модели, где последовательность тактов длилась 1000 шагов. Для каждого из четырех сценариев эксперимент повторялся 30 раз. Использовались следующие критерии: средняя задержка от поступления сигнала до выдачи управляющего воздействия; доля правильных решений в условиях 20 % ложных сигналов; коэффициент роста времени реакции при удвоении количества узлов; а также вычислительные затраты в расчете на один узел [10]. Такой набор показателей позволяет всесторонне охарактеризовать каждую структуру и выявить области ее наилучшего применения. Параметры моделирования сведены в таблицу 1.

ТАБЛИЦА 1. Параметры эксперимента

Параметр	Значение	Описание
Количество узлов в структуре	5, 10, 20	Масштаб системы
Длительность моделирования	1000 тактов	Время устойчивой работы
Количество сценариев	4	Норма, нагрузка, помехи, отказ
Интенсивность сигналов	10–50 сигналов/такт	Переменная нагрузка
Доля помех (сценарий с помехами)	20 %	Ложные/противоречивые сигналы

Результаты моделирования показали, что в стационарном режиме иерархическая структура лидирует по скорости: среднее время реакции составило 2,1 такта против 3,8 у сетевой и 2,9 у гибридной. Однако при резком возрастании потока данных иерархия начинает заметно проигрывать – время реакции растет до 8,4 такта из-за перегрузки верхних уровней. Сетевая структура в этих условиях демонстрирует 9,1 такта, а гибридная – лишь 5,2 такта. При внесении 20 % помех лучшую устойчивость показывает сеть: 92 % верных решений при задержке 4,5 такта. Иерархия в условиях шумов ошибается в 22 % случаев. Отказ одного узла наиболее драматично сказы-

вается на иерархии: время реакции возрастает до 15,2 такта. Сетевая структура перестраивается за 7,6 такта, гибридная – за 6,1 такта. Полные сравнительные данные по времени реакции приведены в таблице 2.

ТАБЛИЦА 2. Сравнение типовых структур интеллекта (время реакции, такты)

Структура	Сценарий A (норма)	Сценарий B (нагрузка)	Сценарий C (помехи)	Сценарий D (отказ)
Иерархическая	2.1	8.4	6.3	15.2
Сетевая	3.8	9.1	4.5	7.6
Гибридная	2.9	5.2	3.8	6.1
Структура	Сценарий A (норма)	Сценарий B (нагрузка)	Сценарий C (помехи)	Сценарий D (отказ)

Анализ устойчивости и масштабируемости (таблица 3) подтверждает, что сетевая структура обеспечивает наилучшую помехоустойчивость (92 % верных решений), но требует вдвое больших вычислительных затрат на один узел по сравнению с иерархической. Гибридная структура занимает промежуточное положение: устойчивость 88 %, вычислительная сложность 1,8 против 2,4 у сети. При удвоении числа узлов время реакции в иерархии вырастает более чем вдвое (коэффициент 2,1), тогда как в сети – всего в 1,3 раза, а в гибридной – в 1,5 раза.

ТАБЛИЦА 3. Устойчивость и масштабируемость

Структура	Устойчивость к помехам (вероятность верного решения), %	Рост времени реакции при удвоении узлов (коэффициент)	Вычислительная сложность на узел (усл. ед.)	Структура	Устойчивость к помехам (вероятность верного решения), %
Иерархическая	78	2.1 ×	1.0	Иерархическая	78
Сетевая	92	1.3 ×	2.4	Сетевая	92
Гибридная	88	1.5 ×	1.8	Гибридная	88
Иерархическая	78	2.1 ×	1.0	Иерархическая	78

На основе полученных данных сформулированы практические рекомендации (таблица 4). Если система работает в стабильных условиях с низкой вероятностью отказов, а главным приоритетом является минимальное время реакции, предпочтительна иерархическая структура. В распределенных средах с высоким уровнем шумов и частыми отказами узлов лучше всего подходит сетевая архитектура. Когда интенсивность нагрузки непредсказуема и требуется одновременно приемлемая скорость и надежность, наиболее эффективна гибридная структура: ее интегральный рейтинг (4,5) значительно лучше, чем у иерархической (7,2) и сетевой (6,3). Для систем с ограниченными вычислительными ресурсами на узел стоит выбирать иерархию или гибрид. При необходимости быстрого наращивания числа узлов (масштабирования) предпочтительны сетевая либо гибридная архитектура, так как они слабо увеличивают задержки при расширении.

ТАБЛИЦА 4. Рекомендации по выбору типовой структуры интеллекта

Условия применения	Рекомендуемая структура	Обоснование	Условия применения	Рекомендуемая структура	Обоснование
Жесткие требования к скорости в статике, централизация	Иерархическая	Минимальная задержка при отсутствии отказов	Жесткие требования к скорости в статике, централизация	Иерархическая	Минимальная задержка при отсутствии отказов
Высокая вероятность отказов и помех, распределенная среда	Сетевая	Лучшая устойчивость и живучесть	Высокая вероятность отказов и помех, распределенная среда	Сетевая	Лучшая устойчивость и живучесть
Переменная нагрузка, потребность и в скорости, и в надежности	Гибридная	Оптимальный баланс по интегральному рейтингу	Переменная нагрузка, потребность и в скорости, и в надежности	Гибридная	Оптимальный баланс по интегральному рейтингу
Ограниченные вычислительные ресурсы на узел	Иерархическая или гибридная	Более низкие затраты на узел	Ограниченные вычислительные ресурсы на узел	Иерархическая или гибридная	Более низкие затраты на узел
Необходимость быстрой масштабируемости	Сетевая или гибридная	Слабый рост времени реакции при расширении	Необходимость быстрой масштабируемости	Сетевая или гибридная	Слабый рост времени реакции при расширении

Таким образом, проведенное исследование показало, что выбор типовой структуры интеллекта не может быть универсальным – он должен определяться ожидаемыми условиями эксплуатации. Иерархическая структура проигрывает при нестационарной нагрузке и помехах, но остается незаменимой в сверхбыстрых детерминированных контурах. Сетевая структура выигрывает в робастности, но платит за это вычислительными накладными расходами. Гибридная структура, не будучи лучшей в каждом отдельном сценарии, оказывается наиболее универсальной, что делает ее разумным выбором при отсутствии жестких априорных знаний о среде. Практическая значимость работы заключается в формировании табличных рекомендаций (таблица 4), которые позволяют разработчикам интеллектуальных систем мониторинга и управления обоснованно выбирать архитектуру, повышая тем самым эффективность и отказоустойчивость проектируемых систем.

Список используемых источников

1. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Вильямс, 2021. 1408 с.

2. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям. М.: Эдиториал УРСС, 2020. 352 с.

3. Поспелов Д. А. Ситуационное управление: теория и практика. М.: Наука, 2022. 288 с.

4. Wooldridge M. An Introduction to MultiAgent Systems. Wiley, 2019. 528 p.

5. Ларичев О. И. Теория и методы принятия решений. М.: Логос, 2018. 296 с.

6. Гаврилова Т. А., Хорошевский В. Ф. Базы знаний интеллектуальных систем. СПб.: Питер, 2020. 384 с.

7. Милов В. Р. Структуры интеллекта в автоматизированных системах управления // Автоматика и телемеханика. 2021. № 3. С. 45–59.

8. Лорьер Ж.-Л. Системы искусственного интеллекта. М.: Мир, 1991. 568 с.

9. Поляков А. А. Моделирование сложных систем с гибридной архитектурой интеллекта // Известия РАН. Теория и системы управления. 2022. № 2. С. 78–91.

10. Фомин В. Н. Интеллектуальные системы управления динамическими объектами. М.: Физматлит, 2019. 272 с.

Статья представлена кандидатом технических наук, заведующим кафедры ИУС СПбГУТ, доцентом В. Л. Литвиновым.

УДК 004.738

ИССЛЕДОВАНИЕ АКТУАЛЬНОСТИ РАЗРАБОТКИ ПРОТОТИПА МУЗЫКАЛЬНОГО СЕРВИСА С ФУНКЦИЕЙ СОВМЕСТНОГО ПРОСЛУШИВАНИЯ

В. А. Ломакин (студент группы ИСТ-222 СПбГУТ), lomakin.va@sut.ru
Ю. Я. Перевозник (к.п.н., доцент кафедры СОД СПбГУТ)

Статья посвящена комплексному исследованию актуальности создания современных музыкальных стриминговых сервисов, в архитектуру которых на базовом уровне интегрирована функция совместного прослушивания аудиоконтента в режиме реального времени. В работе детально рассматриваются социально-психологические аспекты потребления музыки в цифровую эпоху, выявляются критические недостатки существующих на рынке решений для группового прослушивания, а также анализируется технологическая готовность современных веб-стандартов для реализации систем потоковой синхронизации данных. Обоснована техническая и пользовательская значимость разработки независимого веб-ориентированного прототипа, способного решить проблемы кроссплатформенности и обеспечить высокое качество аудиопотока.

стриминговые сервисы, совместное прослушивание, веб-приложения, синхронизация данных, потоковое аудио, WebSocket, распределенные системы

В последнее десятилетие индустрия потребления музыкального контента претерпела кардинальные изменения, окончательно закрепив стриминговую модель в качестве доминирующего стандарта. Мировая статистика показывает: долю доходов музыкальной индустрии сегодня генерирует именно стриминг, а аудитория таких сервисов перевалила за сотни миллионов [1]. Искать и слушать треки стало просто благодаря умным рекомендациям и плейлистам, чутко подстраивающимся под вкусы человека. Но у этого комфорта есть обратная сторона – потребление музыки ушло в глубокую изоляцию. Раньше музыкальные переживания объединяли людей вокруг радиоприемника, на концерте или у проигрывателя. Сейчас ситуация в корне изменилась. Платформы отчаянно борются за внимание каждого отдельного слушателя, погружая его в персональный «пузырь фильтров». Тем самым из музыкального опыта практически полностью вычеркивается живое социальное взаимодействие. Осознание этой проблемы в академическом и технологическом сообществах делает задачу возвращения социальной компоненты в музыкальные сервисы крайне актуальной [2].

Социально-психологическая актуальность разработки сервиса с функцией совместного прослушивания (ко-листенинга) резко возросла на фоне

глобальных изменений в обществе. Глобализация, увеличение числа распределенных IT-команд, развитие форматов удаленной работы и учебы, а также возросшая мобильность населения приводят к тому, что друзья, семьи и единомышленники зачастую оказываются разделены тысячами километров. В этих условиях цифровые инструменты становятся единственным способом поддержания межличностных связей. Если для обмена текстовой или визуальной информацией существует множество решений, то для совместного синхронного переживания аудиального опыта удобных универсальных инструментов крайне мало. Совместное прослушивание музыки позволяет создавать эффект виртуального присутствия, что критически важно для поддержания эмоциональной близости на расстоянии.

Анализ рынка и существующих программных решений выявляет явный дефицит качественных продуктов в этой нише, что подтверждает высокую потребительскую актуальность разработки нового прототипа. На сегодняшний день пользователи, желающие послушать музыку вместе с друзьями в реальном времени, сталкиваются с рядом серьезных барьеров. Сегодняшний рынок предлагает лишь два крайних сценария для группового прослушивания: встроенные инструменты экосистем (Apple SharePlay, Spotify Group Session) и неофициальные обходные пути вроде трансляций экрана или ботов в мессенджерах. Главная слабость фирменных функций – их закрытость. Они требуют жесткой привязки к платформе, а часто и наличия премиум-подписки у каждого участника сессии. Собрать в одном легальном пространстве пользователя Android с локальным сервисом и владельца iOS с другой подпиской попросту невозможно. Сторонние методы, такие как трансляция звука через голосовые каналы Discord, стирают платформенные границы, но безжалостно портят звук. Голосовые движки заточены исключительно под человеческую речь, поэтому их алгоритмы компрессии безвозвратно срезают частоты, критически важные для восприятия оригинального музыкального микса. Для современного пользователя, особенно ценящего Hi-Fi звучание и качественную акустику, такие компромиссы неприемлемы.

Следовательно, на рынке существует явная потребность в разработке независимого, кроссплатформенного веб-приложения, которое могло бы объединять пользователей независимо от их операционной системы или установленных нативных клиентов, предоставляя при этом высокое качество транслируемого звука без потерь, характерных для VoIP-систем.

С технической точки зрения актуальность создания такого прототипа именно в настоящее время обоснована достижением определенного уровня зрелости веб-технологий. Реализация синхронного воспроизведения медиаконтента у множества независимых клиентов – это сложнейшая инженерная задача. Архитектура классического веб-приложения, построенная на парадигме запрос-ответ (HTTP), принципиально не подходит для поддержания стабильной синхронизации плееров с точностью до миллисекунд.

Ключевой технологией, делающей создание подобного прототипа возможным в рамках браузера, является протокол WebSocket. Он обеспечивает полнодуплексную связь между клиентом и сервером поверх одного TCP-соединения, позволяя обмениваться управляющими сообщениями (пауза, воспроизведение, перемотка, синхронизация таймкодов) с минимальными задержками [3]. В отличие от HTTP-запросов, WebSocket устраняет необходимость постоянной передачи громоздких заголовков, что критически важно для систем реального времени, где счет идет на миллисекунды.

Более того, разработка сервиса совместного прослушивания требует решения проблемы рассинхронизации, вызванной непредсказуемостью сетевых задержек (ping). Если сервер отправляет команду «Play» одновременно двум пользователям, один из которых находится в Европе, а другой в Азии, пакеты данных дойдут до них в разное время. В результате трек начнет воспроизводиться рассинхронизировано, что разрушит эффект совместного присутствия. Для решения этой проблемы в разрабатываемом прототипе необходимо исследовать и внедрять сложные алгоритмы вычисления смещения времени (time offset) между клиентом и сервером, аналогичные алгоритмам протокола NTP, но адаптированные для выполнения в среде веб-браузера.

Кроме реализации сетевого взаимодействия на клиентской стороне, огромный научный и практический интерес представляет серверная архитектура такого сервиса. Управление тысячами одновременных сессий («комнат»), маршрутизация сообщений между конкретными участниками одной комнаты и обеспечение отказоустойчивости требуют применения современных паттернов распределенных систем [4]. Монолитная архитектура в данном случае быстро покажет свою неэффективность при масштабировании.

С архитектурной точки зрения наиболее оправданным решением видится микросервисная модель. Асинхронный обмен данными между модулями логично выстроить через брокеры сообщений уровня RabbitMQ или

Apache Kafka. Изоляция авторизации, каталога треков и WebSocket-сервера для комнат прослушивания в независимые блоки сделает приложение стабильнее и заложит базу для будущего масштабирования [5]. Разработка такого прототипа дает шанс на практике изучить поведение распределенных систем под нагрузкой потокового медиа.

Проект закрывает сразу несколько острых потребностей цифрового мира. Людям явно не хватает инструментов для сокращения дистанции и преодоления изоляции, что формирует стабильную аудиторию. Параллельно проприетарные ограничения и технические компромиссы существующих стримингов оставляют открытой нишу для независимых платформ с честным звуком. Для инженеров реализация подобной архитектуры становится серьезным испытанием. Создание надежного продукта требует глубокой экспертизы в протоколах реального времени, алгоритмах синхронизации и микросервисах. В совокупности это превращает разработку прототипа в технически сложную и практически значимую задачу.

Список используемых источников

1. IFPI Global Music Report 2025. State of the Industry. International Federation of the Phonographic Industry, 2025 [Электронный ресурс]. URL: https://www.ifpi.org/ (дата обращения: 22.02.2026).

2. Андреева, Г. М. Социальная психология: учебник для высших учебных заведений / Г. М. Андреева. М.: Аспект Пресс, 2021. 363 с.

3. Fette I., Melnikov A. The WebSocket Protocol: RFC 6455 IETF, December 2011. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc6455 (дата обращения: 13.03.2026).

4. Стин ван М., Таненбаум Э. С. Распределенные системы / пер. с англ. В. А. Яроцкого. – М.: ДМК Пресс, 2021. 584 с.

5. Клеппман М. Высоконагруженные приложения. Программирование, масштабирование, поддержка / пер. с англ. А. А. Слинкина. СПб.: Питер, 2018. 640 с.

УДК 004.057.4

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ И АЛГОРИТМОВ СЖАТИЯ ДЛЯ ПОТОКОВОЙ ПЕРЕДАЧИ АУДИО ВЫСОКОГО КАЧЕСТВА (HI-FI) В ВЕБ-СРЕДЕ

В. А. Ломакин (студент группы ИСТ-222 СПбГУТ), lomakin.va@sut.ru
Ю. Я. Перевозник (к.п.н., доцент кафедры СОД СПбГУТ)

Статья посвящена исследованию сетевых протоколов и аудиокодеков, применяемых для трансляции высококачественного звука (Hi-Fi) в системах совместного прослушивания музыки. Проведен сравнительный анализ протоколов доставки медиаданных и механизмов сжатия, в частности, кодеков Opus и FLAC. Оценено влияние психоакустических алгоритмов с потерями на сохранение частотного и динамического диапазона в сложных музыкальных композициях. Рассмотрены архитектурные подходы к реализации побитово-точного (lossless) воспроизведения и компенсации сетевых задержек в браузере с применением технологии Web Audio API.

аудиокодеки, совместное прослушивание, потоковое аудио, Hi-Fi, FLAC, WebRTC, Opus, Web Audio API, синхронизация потоков

В последние годы развитие веб-технологий и увеличение пропускной способности сетей связи привели к существенному росту требований пользователей к качеству потребляемого медиаконтента. Если на ранних этапах развития интернета стандартом де-факто являлись форматы с высокими коэффициентами сжатия с потерями (например, MP3 с низким битрейтом), то сегодня мы наблюдаем отчетливый переход к форматам аудио высокого разрешения (Hi-Fi). Это особенно актуально для разрабатываемых информационных систем и прототипов музыкальных веб-сервисов, в которых качество звука выступает ключевым конкурентным преимуществом. Сегодня музыкальным сервисам уже недостаточно просто открывать пользователю доступ к аудиотеке. На первый план выходит социальное взаимодействие, в частности – возможность слушать треки совместно и синхронно. Создавая такую систему, инженеры сталкиваются с базовой проблемой: как сбалансировать сетевую задержку (latency) и ширину канала (bandwidth). Традиционно в клиент-серверных приложениях медиапоток идет по HTTP, который, в свою очередь, опирается на протокол TCP. И хотя TCP отлично справляется с загрузкой файлов благодаря стопроцентной гарантии доставки, для синхронного воспроизведения музыки он подходит плохо. Его главная слабость кроется в самой механике пересылки потерянных данных

(retransmission) [1]. Малейший сбой или скачок нагрузки в сети приводит к потере пакета, из-за чего TCP блокирует доставку всей последующей очереди (возникает эффект head-of-line blocking). Передача замирает до тех пор, пока потерянный фрагмент не будет успешно принят заново.

Это вызывает непредсказуемые паузы (буферизацию) в воспроизведении, полностью разрушающие эффект синхронности у пользователей. В качестве альтернативы в сетях традиционно используется протокол UDP (User Datagram Protocol), который отправляет данные непрерывным потоком без проверок доставки. Проблема заключается в том, что стандартный веб-браузер по соображениям безопасности не имеет низкоуровневого доступа к UDP-сокетам, что требует адаптации других веб-технологий под нужды трансляции аудио.

Проблему высокоскоростной передачи медиаданных в браузере отчасти решает технология WebRTC, изначально спроектированная для видеоконференций и голосовых звонков. WebRTC использует протоколы SRTP/UDP под капотом, обеспечивая передачу данных с минимально возможной задержкой. Обязательным компонентом для обработки аудио в WebRTC, согласно спецификации IETF RFC 7874, является поддержка браузерами кодека Opus [2].

Кодек Opus, стандартизированный в документе RFC 6716, представляет собой гибридное алгоритмическое решение, объединяющее технологии линейного предсказания (SILK), отлично подходящие для речи, и модифицированного дискретного косинусного преобразования (CELT), применяемого для музыки [3]. Главное преимущество Opus заключается в его исключительной адаптивности: кодек способен динамически менять битрейт от 6 до 510 кбит/с и размер кадра «на лету», реагируя на ухудшение качества интернет-соединения пользователя.

Тем не менее, у этого подхода есть существенная обратная сторона. Opus – это кодек с потерями (lossy codec). Его алгоритмы базируются на психоакустической модели человеческого слуха: они математически вычисляют и навсегда удаляют те компоненты аудиосигнала, отсутствие которых среднестатистический слушатель теоретически не должен заметить. К сожалению, подобные алгоритмы часто вносят нежелательные артефакты в сложный или специфический музыкальный материал. Например, при воспроизведении партий акустической или электрогитары тонкие высокочастотные обертоны и естественная реверберация инструмента часто урезаются алгоритмом компрессии, из-за чего звук становится плоским.

Аналогичным образом, плотные инструментальные миксы, характерные для альтернативного рока или эмо-музыки, часто страдают от «сплющивания» динамического диапазона. Эмоциональный накал и резкие перепады громкости, заложенные в такие жанры на этапе студийного сведения, требуют хирургической точности при декодировании. Для пользователей, применяющих качественную Hi-Fi аппаратуру, такое урезание спектра делает совместное прослушивание через стандартные каналы WebRTC неприемлемым.

Следовательно, для обеспечения бескомпромиссного студийного качества в разрабатываемых сервисах необходимо внедрять поддержку форматов без потерь (lossless). Золотым стандартом для этих целей является кодек FLAC (Free Lossless Audio Codec), недавно получивший официальный статус предложенного стандарта IETF в документе RFC 9639 [4].

В отличие от психоакустических кодеков, FLAC применяет строгие математические алгоритмы сжатия данных. Архитектура формата разбивает аудиопоток на независимые блоки (фреймы). Внутри каждого блока кодек использует предикторы для поиска математической закономерности в изменении звуковой волны. FLAC сохраняет не саму звуковую волну в явном виде, а лишь компактное описание формулы предсказания и небольшой "остаток" (residual) – разницу между предсказанным и реальным сигналом, которая кодируется методом Голомба-Райса.

В результате применения этих методов исходный аудиопоток уменьшается в размере на 50–70 %, но при декодировании на стороне слушателя восстанавливается с абсолютной точностью до последнего бита. Интеграция формата FLAC позволяет транслировать музыку без малейших фазовых искажений. Разработчикам информационных прикладных систем и технологий, проектирующим платформы для совместного прослушивания, необходимо учитывать, что потоковая передача FLAC обычно требует битрейта от 800 до 1400 кбит/с для стерео в CD-качестве. Так как WebRTC в браузерной реализации плохо масштабируется для передачи медиапотоков с таким высоким и неравномерным битрейтом на большое количество слушателей, более целесообразным архитектурным решением является передача бинарных чанков аудиоданных через протокол WebSocket или использование Media Source Extensions (MSE) поверх HTTP-инфраструктуры.

За декодирование и синхронное воспроизведение полученных чанков без потерь на стороне клиента отвечает стандарт W3C – Web Audio API [5]. Эта технология предоставляет разработчику доступ к низкоуровневому

графу маршрутизации аудиоузлов. В архитектуре сервиса данные FLAC, поступающие по сети, передаются в метод decodeAudioData() интерфейса AudioContext. Важнейшим фактом является то, что Web Audio API выполняет внутреннюю обработку звука с разрядностью 32-bit, что полностью исключает возможность клиппинга (перегрузки) внутри цифрового микшера браузера и сохраняет исходный динамический диапазон.

Для того чтобы обеспечить одновременное воспроизведение аудио у множества пользователей, недостаточно просто доставить данные без потерь. Необходим строгий механизм синхронизации времени. Если один участник комнаты находится в Европе, а другой в Азии, время доставки управляющего сигнала (RTT – Round Trip Time) от центрального сервера будет существенно различаться. Для компенсации этой разницы клиентское приложение должно высчитывать дельту между локальными часами устройства и системными часами сервера (по аналогии с алгоритмами протокола NTP).

Получив аудиофрагмент по сети, приложение использует высокоточные аппаратные таймеры AudioContext.currentTime и метод start(when). Сервер передает команду: «начать воспроизведение трека в абсолютное серверное время T». Клиент, зная свое смещение относительно сервера, пересчитывает время T в локальное время контекста и приказывает браузеру начать декодирование строго в заданную миллисекунду. Это переносит ответственность за синхронизацию с нестабильного сетевого уровня на уровень точных аппаратных часов процессора, гарантируя, что высококачественный Hi-Fi звук заиграет у всех участников одновременно, не создавая неприятного эффекта эха.

Подводя итог, можно сказать, что проектирование стриминговых сервисов для совместного прослушивания всегда сводится к поиску компромисса: либо минимальный пинг, либо высокое разрешение аудио. Привычные решения на базе WebRTC и Opus отлично справляются с задержками и спасают при медленном соединении, но их психоакустическая компрессия совершенно не годится для Hi-Fi сегмента. Если цель – передать слушателю звук без искажений, ограничения lossy-кодеков можно обойти, связав формат FLAC, протокол WebSocket и Web Audio API. Такое строгое математическое сжатие позволяет вещать музыку напрямую в браузер, сохраняя оригинальную динамику.

Список используемых источников

1. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach, Global Edition. – Pearson Education, 2021. 856 p.

2. Valin J. M., Bran C. WebRTC Audio Codec and Processing Requirements: RFC 7874 – IETF, 2016. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc7874 (дата обращения: 25.03.2026).

3. Valin J. M., Vos K., Terriberry T. Definition of the Opus Audio Codec: RFC 6716 – IETF, 2012. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc6716 (дата обращения: 20.03.2026).

4. Van Beurden M. Q. C., Weaver A. Free Lossless Audio Codec (FLAC): RFC 9639 – IETF, 2024. Proposed Standard [Электронный ресурс]. URL: https://www.rfc-editor.org/rfc/rfc9639 (дата обращения: 20.03.2026).

5. Adenot P., Toy R. Web Audio API – W3C, 2021. W3C Recommendation [Электронный ресурс]. URL: https://www.w3.org/TR/webaudio/ (дата обращения: 25.03.2026).

УДК 004.738.5

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ ПРИ ОБНОВЛЕНИИ КОРПОРАТИВНЫХ ХРАНИЛИЩ: МЕТОД СНАПШОТОВ В МИКРОСЕРВИСНОЙ АРХИТЕКТУРЕ

В. В. Луконин (студент группы ИКПИ-24 СПбГУТ), lukonin.vv@sut.ru
П. В. Плотников (к.ф.-м.н., доцент, заведующий кафедрой ВМ СПбГУТ)

В данной работе рассматривается проблема актуализации данных в корпоративных ИИ-ассистентах без потери доступности сервиса. Предложен метод синхронизации «Снапшот и подмена» (Snapshot & Swap), разработанный для микросервисных архитектур, взаимодействующих с разнородными источниками данных. Благодаря изоляции ETL-процесса в отдельном контейнере и использованию атомарной замены файлов, метод позволяет осуществлять обновления без простоя (Zero-Downtime). Экспериментальные результаты подтверждают, что синхронизация не увеличивает задержку ответа бота: время отклика остается стабильным даже в процессе полного обновления данных.

целостность данных; синхронизация данных; микросервисная архитектура; метод снапшотов; атомарная замена; корпоративные хранилища данных; ИИ-чат-бот; нулевое время простоя

Введение

Корпоративные ИИ-ассистенты давно перестали быть просто интерфейсом к языковым моделям. Сегодня от них ожидают работы с живыми внутренними данными: актуальными графиками, реестрами сертификатов, свежими регламентами и документацией. На практике эти сведения редко консолидированы в одном хранилище. Они распределены между SaaS-платформами, таблицами, облачными дисками и внешними REST-интерфейсами. Запрашивать каждый источник в реальном времени означает терять скорость и быстро упираться в квоты API. Локальное кэширование или репликация становятся необходимостью, но тогда возникает техническая дилемма: как обновлять рабочую копию, не прерывая обслуживание и не подсовывая клиентам «половинчатые» или рассогласованные данные?

Традиционные схемы синхронизации в таких условиях дают нежелательный компромисс. Прямая запись в активную базу создает конкуренцию за блокировки и провоцирует фантомные чтения, а плановые окна обслуживания нарушают принцип непрерывной работы, критичный для современных корпоративных сервисов. В микросервисной среде эти ограничения усиливаются: любые блокирующие операции в одном контуре быстро превращаются в каскадные задержки по всей цепочке вызовов.

1. Анализ существующих подходов к синхронизации

Поддерживать локальные реплики в распределенной среде – это, по сути, не про простую замену файлов. На практике проектировщику постоянно нужно держать в голове два требования, которые тянут в разные стороны: чтобы сервис отвечал быстро, и чтобы пользователю уходили свежие данные. Тут есть и теоретический предел – CAP-теорема [1]. Она показывает, что при сетевых задержках строго держать согласованность и при этом сохранять непрерывную доступность сразу не получится. Из-за этого схему обновления нельзя сделать одной на все случаи: стратегию синхронизации всегда выбирают с оглядкой на конкретные SLA системы, и где-то приходится сильнее жертвовать скоростью, а где-то – целостностью данных.

Самый прямой вариант – прямая запись в активное хранилище (Direct Write). Данные обновляются сразу, как только приходят, без промежуточных шагов. На бумаге это выглядит удобно и заметно режет задержки, но в живой системе быстро вылезают гонки состояний (Race Condition) и фантомные чтения. Чтобы не допустить чтения записи, которая еще изменяется, систему приходится прикрывать блокировками, а под нагрузкой именно они и начинают тормозить сильнее всего [2].

Кардинально решить проблему целостности позволяет плановое окно обслуживания (Maintenance Window). Сервис временно переводится в режим ограниченного доступа или полностью останавливается, после чего производится безопасная замена данных. Однако такой сценарий полностью противоречит требованиям к современным корпоративным ассистентам, от которых ожидается круглосуточная работа. Для бизнес-процессов, зависящих от ИИ-агентов, даже кратковременный простой недопустим.

В enterprise-сегменте часто применяют паттерны Transactional Outbox и Log-Based CDC. Они действительно гарантируют атомарность и высокую надежность, но требуют тесной интеграции с журналом транзакций основной БД. В нашем контексте это создает избыточную нагрузку и усложняет поддержку: источники информации разнородны (внешние REST API, SaaS-платформы, облачные диски), и подписаться на их внутренние журналы изменений архитектурно несовместимо с текущим стеком [3].

ТАБЛИЦА 1. Сравнительный анализ методов синхронизации данных

Метод	Целостность	Доступность	Нагрузка на основную БД	Сложность реализации
Прямая запись (Direct Write)	Низкая (риск частичных данных)	Средняя (возможны блокировки)	Низкая	Низкая
Окно обслуживания	Высокая	Отсутствует (простой сервиса)	Низкая	Низкая
Outbox / CDC	Высокая (Атомарность)	Высокая (Без простоя)	Высокая	Высокая
Снапшот и подмена	Высокая (Полный слепок)	Высокая (Zero-Downtime)	Низкая (Изолирована)	Средняя

Как показано в таблице 1, метод «Снапшот и подмена» обеспечивает оптимальный баланс для задач МСБ, гарантируя полную целостность за счет изолированной обработки без накладных расходов, характерных для корпоративных CDC-инструментов.

2. Предлагаемое решение: ETL-архитектура со снапшотами

В основе предложенного решения лежит концепция «Снапшот и подмена». Вместо обновления активной базы данных «на лету», система генерирует полную реплику данных в изолированной среде

2.1 Компоненты архитектуры

Процесс следует модифицированному конвейеру ETL (Extract, Transform, Load):

1. Извлечение (Extract): Асинхронный сервис выгружает данные из Yclients, Google Таблиц и Drive, используя адаптивную пагинацию для соблюдения лимитов запросов.

2. Трансформация (Transform): Данные нормализуются и валидируются внутри изолированного ETL-контейнера Docker, что гарантирует, что ошибки преобразования не повлияют на работу основного сервиса.

3. Загрузка и подмена (Load & Swap): Обработанные данные записываются в промежуточный файл SQLite (staging-зона). После завершения сборки система выполняет атомарную замену (swap) рабочего файла базы данных.

2.2 Технический стек

Реализация выполнена на языке Python с использованием фреймворка FastAPI. В качестве движка хранения выбрана SQLite, что обусловлено ее файловой природой, облегчающей атомарную «подмену» через системный вызов rename(). Этот механизм гарантирует, что в момент переключения рабочий процесс получает доступ к новому, полностью сформированному слепку данных без промежуточных состояний [4]. Контейнеризация с помощью Docker позволяет изолировать вычислительные затраты ETL-процесса от основной бизнес-логики ИИ-ассистента [1, 5].

3. Экспериментальные результаты и тестирование

Было проведено тестирование чтобы понять, как синхронизация влияет на производительность ИИ-ассистента. В первую очередь смотрели на то, сколько бот отвечает в обычном режиме и во время полного цикла синхронизации, который занимает 3–4 минуты. Результаты собраны в таблице 2.

ТАБЛИЦА 2. Влияние синхронизации на производительность

Показатель	Значение	Примечание
Время полной синхронизации	3–4 минуты	ETL в изолированном контейнере
Время ответа бота (обычный режим)	2.5–4.0 сек	~4× быстрее LLM
Время ответа бота (во время синхронизации)	3.2–4.5 сек	~4× быстрее LLM
Простой сервиса	0 секунд	Zero-Downtime подтвержден

Картина получилась довольно ровной: во время обновлений бот отвечает почти так же стабильно, как и обычно. Небольшие скачки связаны с задержкой внешнего LLM-сервиса – обычно это 10–100 сек, а к доступу к базе данных это отношения не имеет. Система показала отсутствие простоя, то есть Zero-Downtime: атомарная подмена занимает миллисекунды, и пользователь этого вообще не замечает.

5. Заключение

Разработанный метод «Снапшот и подмена» справляется с задачей агрегации разнородных корпоративных данных. Если сравнивать его с традиционными Enterprise-подходами к управлению данными, которые обычно

завязаны на транзакционные БД [3, 4], этот вариант сокращает простой системы и сохраняет целостность данных за счет физической изоляции среды подготовки и среды эксплуатации. Экспериментальные данные показывают, что метод подходит для систем, где к доступности предъявляются жесткие требования, включая Zero-Downtime [5].

Список используемых источников

1. Ньюмен С. Создание микросервисов (2-е изд.). СПб.: Питер. 2023. 624 с.
2. Клеппман М. Высоконагруженные приложения. Программирование, масштабирование, поддержка. СПб.: Питер. 2024. 688 с.
3. Richardson C. Microservices Patterns: With examples in Java. Manning. 2018.
4. Fowler M. Patterns of Enterprise Application Architecture. Addison-Wesley Professional. 2012. (Reprint 2022).
5. Байерс К. Проектирование данных в облаке: методы и технологии. М.: ДМК Пресс. 2022.

УДК 004.056.52

РАЗРАБОТКА ГИБРИДНЫХ МЕХАНИЗМОВ МОНИТОРИНГА И УПРАВЛЕНИЯ СЕТЕВЫМ ТРАФИКОМ В ОС ANDROID НА БАЗЕ ТЕХНОЛОГИЙ VPNSERVICE И EBPF

А. В. Марочкина (к.т.н., доцент кафедры ССиПД СПБГУТ), strelchuk.av@sut.ru
К. А. Новиков (студент группы ИКТУ-23 СПбГУТ), novikov.ka@sut.ru

Настоящая работа посвящена разработке и исследованию эффективных способов контроля сетевой активности на мобильных устройствах под управлением ОС Android. В статье предложен гибридный подход к мониторингу, который позволяет решать задачи анализа трафика в зависимости от уровня доступа к системе. В первой части работы реализован механизм на базе официального интерфейса VpnService, обеспечивающий безопасный сбор метаданных (IP-адреса, порты, объемы данных) на стандартных устройствах без прав суперпользователя. Во второй части описано внедрение технологии eBPF на уровне ядра системы, что позволило достичь расшифровку HTTPS-трафика в открытом виде и точную привязку пакетов к конкретным процессам (PID/UID). Практическая значимость исследования подтверждена успешным тестированием механизмов активной блокировки нежелательных соединений.

Extended Berkeley Packet Filter (eBPF), root-доступ, no-root решения

Сегодня мобильный трафик растет огромными темпами, и вопрос его контроля в ОС Android становится все более важным. Мониторинг сети нужен для самых разных задач: от проверки работы обычных приложений до поиска вирусов и предотвращения утечек данных [1-6].

Однако стандартные инструменты Android ограничены политикой безопасности системы. Каждое приложение работает в своей «песочнице», что не дает возможности просто так следить за активностью других программ. Кроме того, почти весь современный трафик зашифрован (HTTPS), из-за чего обычные методы анализа видят лишь набор случайных символов, а не реальные данные.

Чтобы решить эти проблемы, в данной работе предлагается использовать сразу два подхода. Первый – это официальный сервис VpnService, который позволяет безопасно перехватывать трафик на любом телефоне. Второй – это современная технология eBPF, работающая на уровне ядра системы. Она дает возможность просмотреть данные в тот момент, когда они еще не зашифрованы.

Основная задача этого исследования – разработать и протестировать на практике оба метода. Авторы пройдут путь от простого сбора метаданных (IP-адреса и порты) до расшифровки HTTPS-запросов и полной блокировки нежелательных соединений. Это позволит понять, как можно добиться максимального контроля над сетевой активностью в Android.

Целью работы является анализ и сравнение двух разных способов контроля сетевого трафика в Android. Важно понять, как можно эффективно следить за сетью на обычных устройствах и как получить полный доступ к данным на смартфонах с root-правами.

Первым этапом данной работы стало создание инструмента, который может работать на любом стандартном Android-смартфоне без необходимости получения root-прав. Для этого авторы использовали официальный программный интерфейс – VpnService. [5]

Принцип работы этого метода довольно прост: данное приложение создает в системе виртуальный сетевой интерфейс. Как только пользователь нажимает кнопку «Activate Traffic Control» и дает свое согласие в системном окне, операционная система начинает перенаправлять абсолютно все исходящие и входящие пакеты не напрямую в сеть, а внутрь нашего приложения. Это своего рода «ловушка» для трафика, которая позволяет нам изучить данные до того, как они покинут устройство или попадут в другие программы.

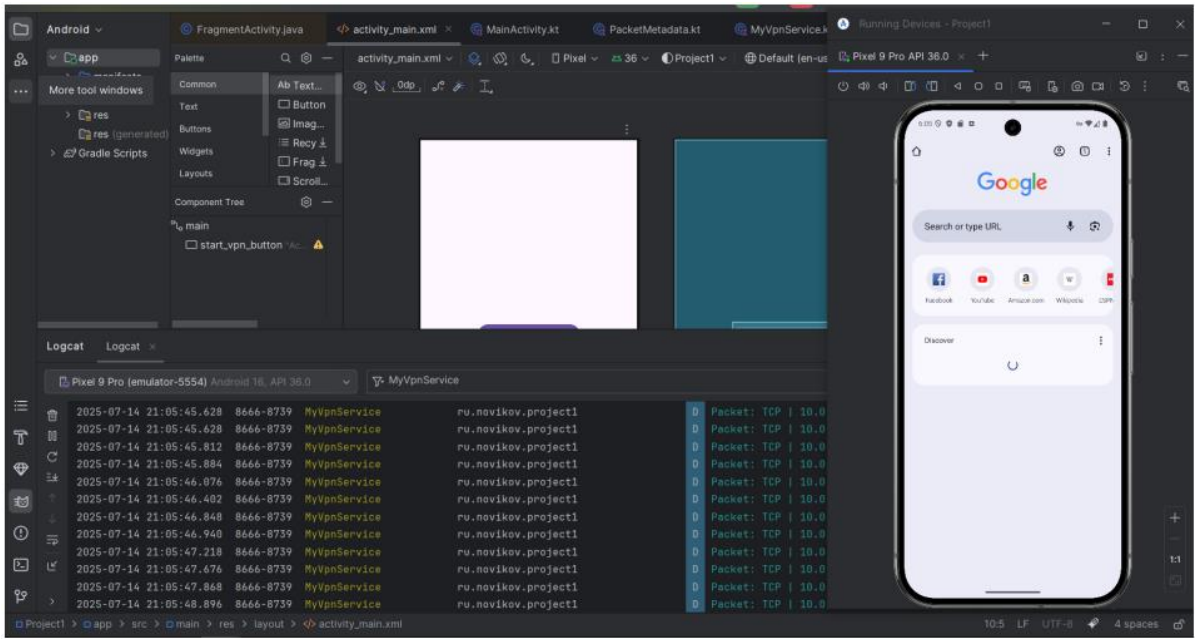


Рис. 1. Мониторинг сетевой активности в Android Studio

На рисунке 1 наглядно показан процесс работы такой системы. Виден результаты перехвата в реальном времени. Приложение успешно фиксирует

каждый TCP-пакет, определяя его размер и направление. Главный плюс этого подхода в том, что он полностью безопасен для системы и позволяет пользователю самому контролировать процесс мониторинга [6]. Однако у него есть и минус: мы видим только заголовки данных, в то время как само содержимое зашифрованных сообщений остается для нас скрытым.

Если предыдущий метод с использованием VpnService был ограничен только «внешними» данными, то для получения полной картины происходящего внутри смартфона авторы применили решение – технологию eBPF (extended Berkeley Packet Filter). Этот подход требует наличия прав суперпользователя (root), так как он позволяет запускать наш программный код непосредственно внутри ядра операционной системы [2].

Главное преимущество eBPF заключается в том, что здесь могут перехватывать данные прямо в момент их обработки сетевым стеком Android. В отличие от обычных приложений, eBPF-программы работают на уровне ядра, что делает их практически невидимыми для систем защиты и крайне быстрыми. Это позволяет не просто смотреть на пакеты со стороны, а «вклиниваться» в сам процесс передачи информации.

Использование eBPF дает возможность использовать механизмы uprobes – специальные точки перехвата, которые можно расставить в системных библиотеках смартфона. Таким образом, авторы получаеют доступ к данным в тот критический момент, когда они уже сформированы приложением, но еще не зашифрованы для отправки в интернет. Это открывает путь к решению самой сложной задачи нашего исследования – анализу содержимого HTTPS-трафика [4].

Одной из сложных задач в современном анализе трафика является обход TLS-шифрования. Использование eBPF позволяет нам решить эту проблему, перехватывая информацию в тот момент, когда она уже готова, но еще не скрыта алгоритмами шифрования.

Для этого был привязан eBPF-код к функциям системной библиотеки libssl.so, которая отвечает за безопасность в Android. В момент, когда браузер или любое другое приложение вызывает функцию отправки данных, наш код срабатывает как невидимый наблюдатель и копирует содержимое запроса в специальный буфер.

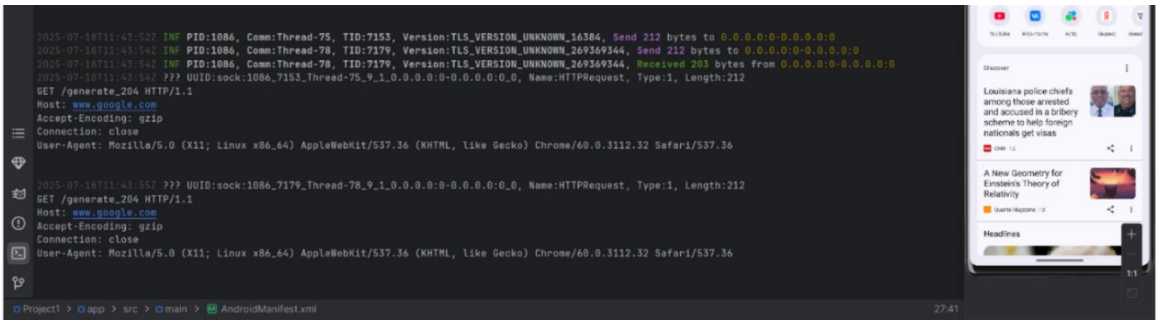


Рис. 2. Дешифрованный HTTP-трафик (Payload) в консоли загрузчика eBPF

На рисунке 2 представлен результат такой работы. В консоли нашего загрузчика виден полный текст HTTP-запроса к серверам Google в открытом виде. Здесь отображаются не только технические заголовки (Host, User-Agent), но и сама суть обращения приложения [2].

Для обычного сетевого анализатора этот поток данных выглядел бы как случайный набор символов, но благодаря eBPF мы получили прозрачность трафика. Такой метод является мощным инструментом для проверки безопасности приложений и поиска скрытых угроз, которые могут прятаться внутри зашифрованных соединений [3].

Для детального изучения собранных данных мы использовали программу Wireshark. Этот инструмент позволяет наглядно увидеть структуру сетевого обмена. На рисунке 3 выделяются DNS-запросы, с помощью которых устройства ищут адреса сайтов, и последующая передача данных [6].

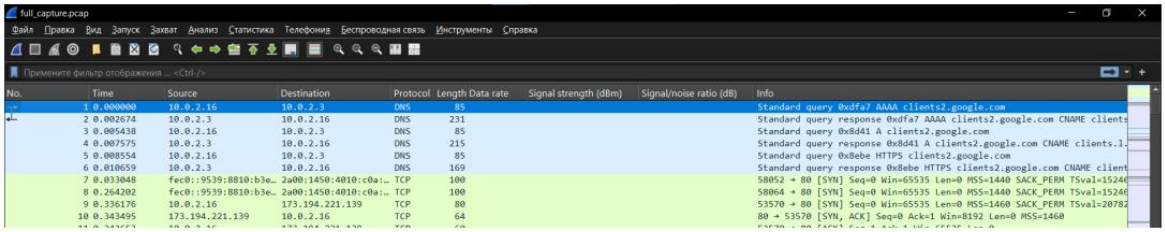


Рис. 3. Визуализация структуры DNS-запросов и ответов в анализаторе Wireshark

Важной частью исследования стала возможность точной идентификации отправителя. Используя системные идентификаторы PID (номер процесса) и UID (номер пользователя), мы научились связывать конкретные пакеты с определенными приложениями, например, браузером Google Chrome. Это позволяет полностью изолировать активность одной программы от общего сетевого трафика [1].

```
emu64xa:/ # ps -ef | grep chrome
u0_a148       6054   460 0 11:34:33 ?     00:00:00 com.android.chrome_zygote
u0_a148       6674   460 1 11:39:26 ?     00:00:16 com.android.chrome
u0_a148       6732   460 0 11:39:27 ?     00:00:03 com.android.chrome:privileged_p
rocess0
u0_i23        7075  6054 0 11:40:48 ?     00:00:00 com.android.chrome:sandboxed_pr
ocess0:org.chromium.content.app.SandboxedProcessService0:12
root          7462  7455 0 12:12:28 pts/2 00:00:00 grep chrome
emu64xa:/ #
```

Рис. 4. Идентификация процессов и поиск UID/PID целевого приложения (Google Chrome)

Таким образом, были успешно решены все поставленные задачи и получены важные практические результаты. Главным итогом работы стала разработка комплексного инструментария, который позволяет эффективно контролировать сетевую активность в ОС Android на разных уровнях доступа.

Во-первых, было создано мобильное приложение на базе VpnService, которое способно осуществлять мониторинг трафика на любых стандартных устройствах без необходимости внесения изменений в систему. Этот метод доказал свою эффективность для сбора метаданных в безопасном для пользователя режиме.

Во-вторых, была успешно освоена и применена технология eBPF. Благодаря ей удалось реализовать механизм изоляции сетевой активности конкретных процессов (например, браузера Chrome). Был успешно перехвачен зашифрованный HTTPS-трафик в открытом виде.

В-третьих, разработанный инструментарий показал свою универсальность. Он одинаково стабильно работает как на обычных смартфонах, так и на инженерных образцах с полным root-доступом, обеспечивая глубокую видимость всех сетевых процессов. Практические тесты по блокировке нежелательных соединений подтвердили, что созданная система позволяет не только наблюдать за сетью, но и активно управлять безопасностью устройства.

Список используемых источников

1. Кузьминых Е. С., Маслова М. А. Анализ основных мобильных угроз и способы защиты от вирусов // Научный результат. Информационные технологии. Т. 7. № 2, 2022. С. 28-34. DOI: 10.18413/2518-1092-2022-7-2-0-3

2. What is eBPF? An Introduction and Deep Dive into the eBPF Technology // eBPF.io: The Official eBPF Website. URL: https://ebpf.io/what-is-ebpf/ (дата обращения: 15.11.2025).

3. Evans D., Petracca G. BPF on Android: Challenges and Opportunities // Proceedings of the 2021 Workshop on Mobile Security Technologies (MoST '21). Association for Computing Machinery, New York, NY, USA, 2021. PP. 33–38.

4. Gregg B. BPF Performance Tools: Linux System and Application Observability. Addison-Wesley Professional, 2019. 880 p.

5. What is the term "no root access " mean in Android phone? // Quora. 2024. URL: https://www.quora.com/What-is-the-term-no-root-access-mean-in-Android-phone?topAns=27919360 (дата обращения: 15.11.2025).

6. Gorenburg. Root или не Root, вот в чем вопрос// Хабр. 2011. URL: https://habr.com/ru/articles/114645/ (дата обращения: 15.11.2025).

УДК 004.62:612.16

СРАВНИТЕЛЬНАЯ ОЦЕНКА МЕТОДОВ СБОРА ФОТОПЛЕТИЗМОГРАФИЧЕСКИХ ДАННЫХ С УМНЫХ ЧАСОВ

М. Е. Марушина (студент группы ИСТ-431м СПбГУТ),
marushina.me@sut.ru

В последние годы, все более востребованным способом для непрерывного отслеживания показателей жизнедеятельности становится ношение умных часов со способностью получения фотоплетизмографического сигнала. Широкое распространение данной технологии обусловлено ее доступностью, неинвазивностью и удобством эксплуатации в повседневной жизни. Однако регистрация качественного ФПГ-сигнала осложнена высокой чувствительностью сенсоров к наличию артефактов движения, что приводит к искажению результатов и определением их как некорректных со стороны программного обеспечения. В данной работе представлено экспериментальное исследование двух стратегий агрегации фотоплетизмографических данных с умных часов. Проведенный анализ позволил оценить относительную эффективность предложенных подходов и выявить наиболее надежные методы мониторинга сердечного ритма в носимом устройстве.

умные часы, фотоплетизмография, фотоплетизмографический сигнал, приложение, сбор данных, частота сердечных сокращений, носимые устройства, мониторинг здоровья

В настоящее время все большую популярность приобретают носимые устройства: умные часы, наушники, кольца, фитнес-браслеты. Если на старте своего существования, умные часы имели весьма ограниченный функционал, то сейчас они включают в себя множество датчиков, способных отлеживать физиологические показатели организма человека [1]. Так, основной интерес на данный момент представляет PPG-сенсор, его основная задача – это сбор фотоплетизмографического сигнала.

Метод фотоплетизмографии основывается на неинвазивном отслеживании изменения наполнения кровью микроциркуляторного русла, за счет использования оптического датчика. Оптический датчик состоит из светодиода и фотодетектора, светодиод просвечивает участок кожи, после чего, фотодетектор регистрирует интенсивность отраженного от эритроцитов света [2]. ФПГ-сигнал позволяет получить такие важные показатели как: вариабельность сердечного ритма, частота сердечных сокращений, сатурация крови и т.д [3]. Схема работы фотоплетизмографического метода представлена на рисунке 1.

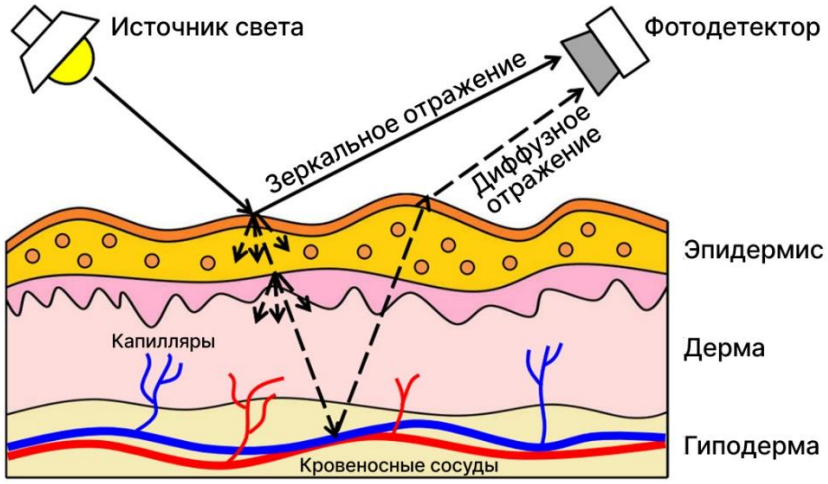


Рис. 1. Схема устройства фотоплетизмографического метода

На данный момент сбор ФПГ-сигнала с умных часов осложнен частым наличием артефактов движения и нестабильным контактом сенсора с кожей носителя, что приводит к ухудшению собираемых данных.

Данная работа посвящена исследованию возможности уменьшения потери качества данных при сборе фотоплетизмографического сигнала с умных часов. Чтобы изучить возможности получения более точных данных, было разработано авторское программное обеспечение, которое собирает ФПГ-сигнал, с применением двух различных методов агрегации данных. Разработка собственного приложения позволяет получить полный контроль над процессом сбора и «выгрузкой» сигнала, чего не удается добиться при использовании встроенных в часы приложений, за счет закрытости алгоритмов производителя.

Для платформы Wear OS было разработано приложение, реализующие следующие режимы агрегации ФПГ-сигнала:

- PPG_CONTINUOUS – включает сбор фотоплетизмограммы в зеленом, инфракрасном и красном диапазонах, с частотой дискретизации 25 Гц. Оптимизирован для энергосбережения, за счет стандартного непрерывного потока данных.
- PPG_ON_DEMAND – включает сбор фотоплетизмограммы в зеленом, инфракрасном и красном диапазонах, с частотой дискретизации 100 Гц. Максимально использует возможности сенсора, что значительно повышает плотность выборки.

В качестве эталонного сигнала используются данные, полученные с медицинского монитора пациента COMENSTAR 8000B, который использовался синхронно с умными часами Galaxy Watch 7, во время проведения эксперимента.

Для проведения анализа сигналов с использованием разных методов сбора данных, был проведен эксперимент с участием шести добровольцев. В процессе эксперимента, испытуемые следовали следующему сценарию действий: 2 минуты в покое, 2 минуты ходьбы, 2 минуты в покое. Во время проведения эксперимента на левом запястье испытуемого находились умные часы Galaxy Watch 7, а к пальцу левой руки был прикреплен датчик монитора пациента COMENSTAR 8000B.

После проведения эксперимента, полученные ФПГ-данные были выгружены на стороннее оборудование и подверглись обработке и анализу. Анализ проводился в несколько этапов: проверка полноты полученных данных, сегментация данных на окна по 8 секунд и фильтрация Винера.

Особое внимание в момент анализа сигнала стоит обратить на метод фильтрации данных. Фильтр Винера представляет собой метод оптимальной линейной фильтрации, целью которого является восстановление полезного сигнала из смеси сигнала и шума. Стандартные полосовые фильтры зачастую просто отсекают определенные частоты, в то время как фильтр Винера работает на основе статистического анализа и минимизирует среднеквадратическую ошибку (Mean Squared Error, MSE) между истинным и оцененным сигналом.

В частотной области передаточная функция классического фильтра Винера выражается формулой:

$$H(f) = \frac{P_s(f)}{P_s(f) + P_n(f)}$$

где $P_s(f)$ – спектральная плотность мощности полезного сигнала, $P_n(f)$ – спектральная плотность мощности шума.

В задачах обработки ФПГ-сигналов, основным критерием валидации алгоритма служит средняя абсолютная ошибка (Mean Absolute Error, MAE). Данная статистическая метрика часто используется для оценки точности математических моделей и алгоритмов за счет своей устойчивости к выбросам. Расчет средней абсолютной ошибки производится по формуле:

$$MAE = \frac{1}{n}\sum_{i=1}^{n} |y_i - \hat{y}_i|$$

где n – количество проанализированных временных сегментов, y_i – истинное значение ЧСС, $\hat{y}_i$ – расчетное значение ЧСС, $|y_i - \hat{y}_i|$– абсолютное отклонение для каждого конкретного сегмента.

В контексте анализа фпг-данных хорошим результатом MAE в покое считается показатель 2-5 уд/мин, для активности – 5-10 уд/мин.

На рисунках 2-3 представлен пример визуализации результатов обработки сигнала с часов в сравнении с эталонными значениями с монитора пациента.

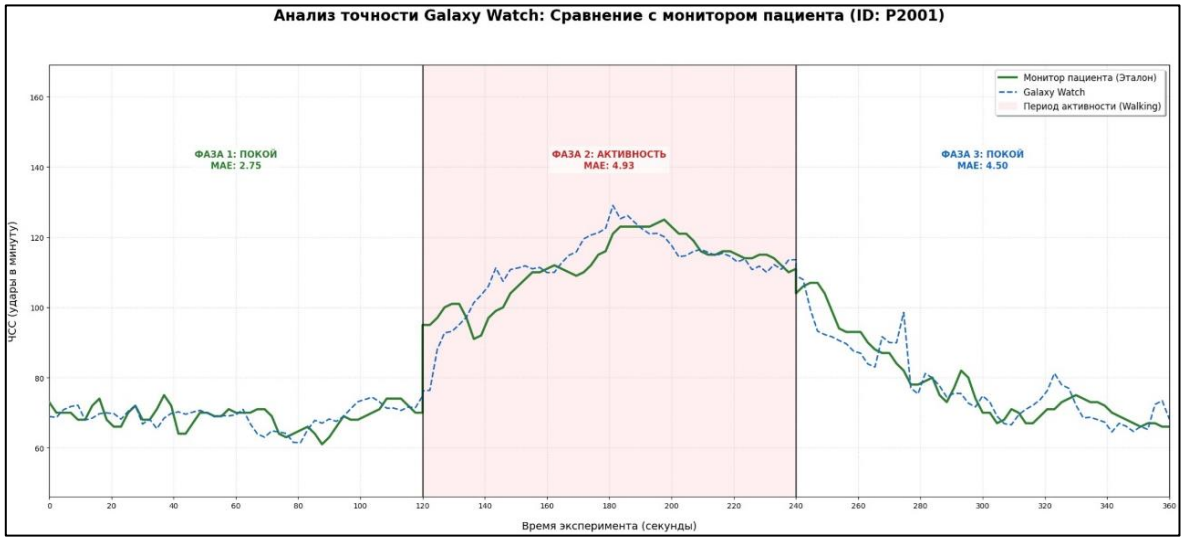


Рис. 2. График анализа точности, режим PPG_CONTINUOUS

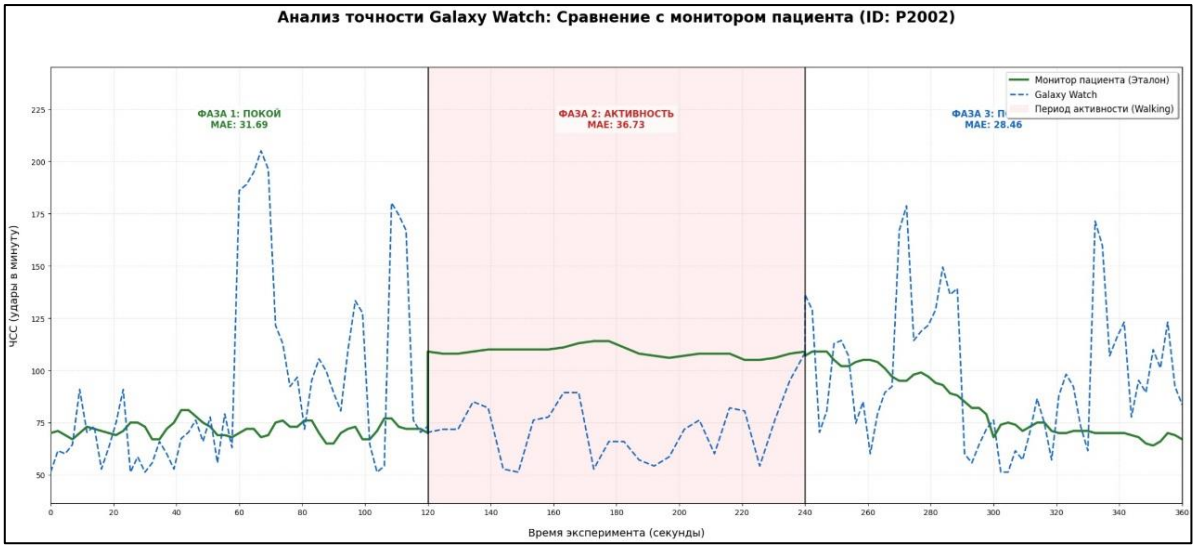


Рис. 3. График анализа точности, режим PPG_ON_DEMAND

Как видно из представленных графиков, режим сбора данных PPG_ON_DEMAND имеет более низкую точность по сравнению с режимом PPG_CONTINUOUS. Для каждого испытуемого, для обоих режимов сбора данных был рассчитан показатель средней абсолютной ошибки. Все результаты расчета MAE представлены в таблице 1.

ТАБЛИЦА 1. Антропометрические данные испытуемых

Испытуемый	Режим сбора данных	Покой, MAE, уд/мин	Нагрузка, MAE, уд/мин	Отдых, MAE, уд/мин
1	PPG_CONTINUOUS	8,67	6,93	16,15
	PPG_ON_DEMAND	15,62	15,90	17,25
2	PPG_CONTINUOUS	2,75	4,93	4,50
	PPG_ON_DEMAND	31,69	36,73	28,46
3	PPG_CONTINUOUS	2,34	13,17	6,64
	PPG_ON_DEMAND	16,84	32,39	24,65
4	PPG_CONTINUOUS	7,43	5,60	6,88
	PPG_ON_DEMAND	32,12	38,11	20,84
5	PPG_CONTINUOUS	2,74	7,16	5,54
	PPG_ON_DEMAND	14,67	18,57	12,70
6	PPG_CONTINUOUS	3,51	4,78	4,27
	PPG_ON_DEMAND	14,23	33,99	24,13

На основе результатов эксперимента можно сделать вывод о том, что режим сбора данных PPG_ON_DEMAND, несмотря на высокую частоту дискретизации и повышенную чувствительность датчика в данном режиме, значительно уступает в точности записи фотоплетизмографических данных режиму PPG_CONTINUOUS и не может быть использован для получения достоверного сигнала.

Список используемых источников

1. Лущик М. В., Макеева А. В., Остроухова О. Н., Болотских В. И., Наговицин А. К. Применение фотоплетизмографии для оценки состояния микроциркуляторного русла в качестве метода диагностики заболеваний сердечно-сосудистой системы [Электронный ресурс] // ВНМТ. 2022. №3. С. 91-95. URL: https://cyberleninka.ru/article/n/primenenie-fotopletizmografii-dlya-otsenki-sostoyaniya-mikrotsirkulyatornogo-rusla-v-kachestve-metoda-diagnostiki-zabolevaniy (дата обращения: 08.04.2026).

2. Алексеев В. А., Юран С. И., Усольцев В. П. Система скрининга сосудистой системы человека с применением относительного описания фотоплетизмограмм [Электронный ресурс] // Приборы и методы измерений. 2025. №4. С. 395–405. URL:

https://cyberleninka.ru/article/n/sistema-skrininga-sosudistoy-sistemy-cheloveka-s-primeneniem-otnositelnogo-opisaniya-fotopletizmogramm (дата обращения: 08.04.2026).

3. Волков Иван Юрьевич, Сагайдачный Андрей Александрович, Фомин Андрей Владимирович Фотоплетизмографическая визуализация гемодинамики и двухмерная оксиметрия [Электронный ресурс] // Изв. Сарат. ун-та Нов. сер. Сер. Физика. 2022. №1. С. 15-45. URL: https://cyberleninka.ru/article/n/fotopletizmograficheskaya-vizualizatsiya-gemodinamiki-i-dvuhmernaya-oksimetriya (дата обращения: 06.04.2026).

Статья представлена научным руководителем, кандидатом физико-математических наук, доцентом кафедры ИКД СПбГУТ Р. В. Давыдовым.

УДК 004.738

СИСТЕМА ОБМЕНА ТЕКСТОВЫМИ СООБЩЕНИЯМИ НА ОСНОВЕ ПРОТОКОЛА ESP-NOW ДЛЯ АВТОНОМНЫХ УСТРОЙСТВ

К. Б. Миронов (студент группы ИКПИ-492м СПбГУТ), mironov.kb@sut.ru

Актуальность создания автономных средств текстовой коммуникации обусловлена зависимостью традиционных мессенджеров от сетевой инфраструктуры и внешних серверов. Для локального обмена сообщениями между пользовательскими устройствами перспективным решением является применение протокола ESP-NOW, обеспечивающего прямую передачу данных без точки доступа и подключения к сети Интернет. Использование микроконтроллеров ESP32 позволяет реализовать компактные устройства-пейджеры с клавиатурным вводом и экранным отображением сообщений. Протокол ESP-NOW сочетает малую задержку, невысокое энергопотребление и достаточную дальность связи, что делает его пригодным для построения автономных систем обмена текстовыми сообщениями.

ESP-NOW, ESP32, обмен сообщениями, пейджер, автономные устройства, беспроводная связь, Интернет вещей, peer-to-peer

Современные средства обмена сообщениями в большинстве случаев основаны на использовании развитой сетевой инфраструктуры, включающей точки доступа Wi-Fi, мобильные сети и облачные серверы. Такой подход обеспечивает высокий уровень масштабируемости и интеграции, однако делает коммуникацию зависимой от внешней среды. При отсутствии доступа к инфраструктуре, при ее отказе либо в условиях локального автономного взаимодействия использование традиционных мессенджеров оказывается затруднительным или невозможным.

В связи с этим представляет интерес построение простых децентрализованных систем обмена текстовыми сообщениями, способных функционировать напрямую между двумя устройствами без маршрутизатора, сервера и подключения к сети Интернет. Подобные решения могут быть востребованы в полевых условиях, в автономных локальных системах связи, а также как основа для специализированных пользовательских устройств.

В качестве технологической основы в работе рассматриваются микроконтроллеры семейства ESP32 и поддерживаемый ими протокол ESP-NOW. ESP32 – это микроконтроллер с интегрированными средствами беспроводной связи, разработанный компанией Espressif Systems и предназначенный

для создания устройств Интернета вещей и встраиваемых систем. ESP32 построен на базе двухъядерного процессора с архитектурой Xtensa и работает на частоте до 240 МГц. Он содержит встроенную оперативную память и флеш-память. Одной из ключевых особенностей является наличие радиомодуля, обеспечивающего работу по Wi-Fi (802.11 b/g/n), что позволяет реализовывать беспроводные системы без дополнительных модулей [1, 2].

Протокол ESP-NOW обеспечивает прямую передачу пакетов между устройствами по MAC-адресам, что позволяет реализовать схему обмена данными типа peer-to-peer [3]. В данной работе исследуется возможность использования ESP-NOW для пересылки текстовых сообщений между двумя пользовательскими устройствами-пейджерами.

Каждое устройство представляет собой компактный пейджер, состоящий из микроконтроллера ESP32, клавиатуры для ввода символов, дисплея для отображения пользовательского интерфейса и сообщений, а также автономного источника питания. Оба устройства являются равноправными узлами связи: каждое из них способно как принимать, так и передавать сообщения. Такая архитектура позволяет отказаться от выделенного центрального устройства и реализовать симметричную схему взаимодействия.

Структурная схема системы представлена на рисунке 1.

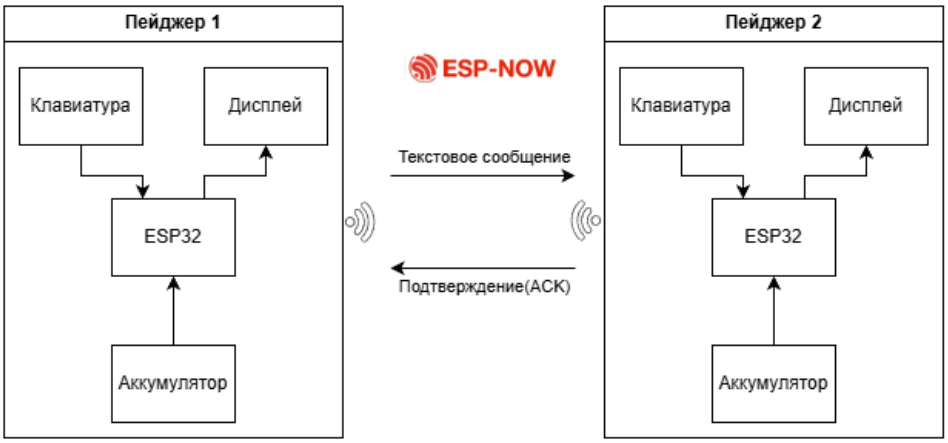


Рис. 1. Структурная схема системы обмена текстовыми сообщениями

Как видно из рисунка 1, ввод текста осуществляется пользователем с клавиатуры, после чего данные обрабатываются микроконтроллером, преобразуются в формат передачи и отправляются по каналу ESP-NOW на второе устройство. Полученный текст собирается, сохраняется в истории сообщений и выводится на экран.

Протокол ESP-NOW работает поверх физического уровня IEEE 802.11, однако не использует полноценный стек TCP/IP в своей архитектуре [3].

Благодаря этому обеспечивается уменьшение накладных расходов, снижение времени доставки пакетов и уменьшение энергопотребления по сравнению с классическим Wi-Fi взаимодействием.

Вместе с тем ESP-NOW имеет ряд ограничений. В частности, размер полезной нагрузки одного пакета ограничен 250 байтами, вследствие чего длинные сообщения необходимо разбивать на несколько фрагментов [3].

Для передачи текстовых сообщений в предлагаемой системе используется прикладной формат пакета, показанный в таблице 1. Пакет включает идентификатор сообщения, номер текущего фрагмента, общее число фрагментов, полезную нагрузку и признак подтверждения доставки. Это позволяет не только передавать короткие сообщения в одном пакете, но и поддерживать отправку более длинного текста за счет сегментации.

ТАБЛИЦА 1. Формат пакета сообщения

Поле	Описание
msg_id	Идентификатор сообщения
seq	Номер фрагмента
total	Общее количество фрагментов
payload	Часть текстового сообщения
ack	Флаг подтверждения

Работа системы организована следующим образом. Пользователь набирает текст на клавиатуре, после чего сообщение передается программному модулю обработки. Если длина текста не превышает допустимый объем одного пакета, он отправляется непосредственно. Если сообщение длиннее, оно разбивается на несколько фрагментов, каждый из которых снабжается служебной информацией и передается отдельно. На принимающей стороне осуществляется накопление фрагментов, их проверка и сборка исходного текста. После этого сообщение отображается на экране устройства и может быть помещено в локальную историю переписки.

Для повышения надежности в системе реализуется подтверждение доставки. После успешного получения пакета принимающая сторона формирует короткий ответ с установленным флагом ack. Если в течение заданного интервала подтверждение не получено, передающее устройство может повторно отправить пакет. Подобный механизм повышает устойчивость обмена сообщениями в условиях кратковременных помех и потери отдельных кадров.

Пользовательский интерфейс устройства ориентирован на реализацию минимально необходимой функциональности чата. На экране отображаются введенный текст, история переданных и полученных сообщений, а также индикация статуса доставки.

В рамках экспериментальной оценки системы было установлено, что среднее время доставки текстовых сообщений составляет до 10 миллисекунд. В условиях прямой видимости до 100 метров связь остается устойчивой. Энергопотребление устройств остается сравнительно низким, до 10 мкА в спящем режиме и до 100 мА в момент передачи, такие показатели являются важным фактором для автономной работы от аккумулятора [4].

Перспективным направлением развития работы может являться расширение системы на несколько устройств с реализацией ретрансляции сообщений, а также совершенствование пользовательского интерфейса, например за счет организации списка диалогов и списка контактов.

В итоге можно сделать вывод, что протокол ESP-NOW может эффективно использоваться при построении автономных пользовательских устройств для текстовой коммуникации. Представленная система на базе двух пейджеров с клавиатурой и экраном демонстрирует возможность построения простого беспроводного чата без точки доступа, сервера и подключения к сети Интернет. Предложенный подход сочетает низкую задержку, достаточную дальность и невысокое энергопотребление, что делает его перспективным для применения в автономных системах обмена сообщениями.

Список используемых источников

1. Espressif Systems. ESP32 Technical Reference Manual. [Электронный ресурс]. URL: https://documentation.espressif.com/esp32_technical_reference_manual_en.pdf (дата обращения: 20.04.2026)

2. Espressif Systems. ESP32 Datasheet. [Электронный ресурс]. URL: https://documentation.espressif.com/esp32_datasheet_en.pdf (дата обращения: 20.04.2026)

3. Espressif Systems. ESP-NOW User Guide. [Электронный ресурс]. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/network/esp_now.html (дата обращения: 20.04.2026)

4. H. Demir, I. Selcuk and A. E. Cosgun, "Power Consumption Analysis of ESP32 and Arduino Nano for Low-Power Applications" // 2025 9th International Symposium on Innovative Approaches in Smart Technologies (ISAS), Gaziantep, Turkiye, 2025, pp. 1-4, doi: 10.1109/ISAS66241.2025.11101965.

Статья представлена научным руководителем, профессором кафедры ПИиВТ СПбГУТ, доктором технических наук, профессором В. И. Бобровским.

УДК 621.396

ОБЗОР И СРАВНЕНИЕ КЛАССОВ ПРОТОКОЛОВ ДЛЯ УСТОЙЧИВОЙ СВЯЗИ В VANET

М. В. Никитин (студент группы ИКТР-22 СПбГУТ), nikitin1.mv@sut.ru

В статье рассматриваются особенности организации маршрутизации в автомобильных самоорганизующихся сетях VANET, играющих ключевую роль в обеспечении безопасности и комфорта участников дорожного движения. Анализируются основные типы протоколов маршрутизации такие как: топологические, позиционные, многоадресные и широковещательные. Так же рассмотрены сценарии применения, и взаимосвязи с характеристиками радиоканала и радиопокрытием. Описаны преимущества и недостатки каждой группы протоколов, выделены условия, в которых их использование наиболее эффективно.

VANET, автомобильные самоорганизующиеся сети, маршрутизация, протоколы маршрутизации

В современном мире автомобильные самоорганизующиеся сети VANET имеют большую популярность в сфере безопасности и комфорта для водителей в автомобильной среде. Система “транспортное средство – устройство” (Vehicle-to-everythng, V2X) является универсальной, и позволяет организовывать взаимодействие между автомобилем и иными техническими компонентами дорожной инфраструктуры [1]. Операторы мобильных сетей выбирают концепцию самоорганизующейся сети (SON) как экономически эффективный метод развертывания сетей LTE/4G и удовлетворения ожиданий пользователей в отношении высокого качества обслуживания пропускной способности [2]. Одной из важнейших задач в рамках концепции V2X является надежная передача информации между транспортными узлами. Но из-за того, что автомобили большую часть времени находятся в движении возникают проблемы со связью, с быстрым изменением топологии, все это влияет на маршрутизацию в сети. Решением этой проблемы является введением различных протоколов маршрутизации в автомобильные самоорганизующиеся сети VANET. Протоколы маршрутизации представляю собой набор правил и алгоритмов, они должны решать задачу доставки информации в условиях, где узлы сети постоянно меняют свое положение [3]. В свою очередь протоколы делятся на четыре группы: топологическую, позиционную, многоадресную и широковещательную. Какие типы включают в себя эти группы можно увидеть в таблице 1.

ТАБЛИЦА 1. Типы протоколов

Топологические	Позиционные	Многоадресные	Широковещательные
Проактивные	Для сетей с частыми разрывами	Геокастные	Передача всем узлам
Реактивные	Для устойчивых сетей	Мобикастные	
Гибридные	Гибридные	Кластерные	

Топологические протоколы маршрутизации строят маршруты на основе информации о связях между узлами сети. Для этого используются специальные таблицы маршрутизации, которые содержат сведения о доступных путях к различным получателям [4]. Наиболее эффективное применение этого класса в случаях, когда структура сети относительно стабильна, а узлы не перемещаются с высокой скоростью. Например, на промышленных зонах, парковках, сети с часто повторяющимися маршрутами (рейсы общественного транспорта). Так же не малую роль играют характеристики радиоканала такие как: стабильность соединения, пропускная способность, радиус действия и задержки. Без прямой связи с радиодоступом сети VANET будут малоэффективны. Преимуществом данной группы протоколов является то, что проактивные протоколы обеспечивают мгновенную доступность маршрутов, гибридные решения сочетают скорость и экономию ресурсов, хорошо работают в стабильных или малоподвижных сетях. Недостатком является то, что они неэффективны при высокой динамике топологии и частых разрывах связи, большие задержки при реактивном поиске маршрута.

Позиционные протоколы маршрутизации в сетях VANET используют информацию о географическом положении узлов (автомобилей), полученную, как правило, с помощью GPS. В отличие от топологических протоколов, они не строят и не поддерживают сложные таблицы маршрутизации, а принимают решения о пересылке пакетов на основе текущих координат узлов. Чаще всего они используются в условиях высоких динамических сетях и мобильных узлах, что характерно для VANET. Например, городские и загородные трассы с высокой плотностью и скоростью движения, сети с частыми разрывами связи, системы экстренного оповещения и безопасности. Связь с радиоканалом заключается в том, что позиционные протоколы не требуют периодического обмена служебными сообщениями для поддержания таблиц

маршрутизации, что снижает нагрузку и уменьшает вероятность ошибок. Решения о пересылке принимаются на основе актуальных координат, что позволяет эффективно использовать радиоканал даже при частых изменениях топологии. Работа позиционных протоколов напрямую зависит от радио покрытия, например, в зонах с переменной плотностью там, где условия высокой плотности протоколы быстро находят оптимальный путь, а в разреженных сетях минимизируют количество пересылок. Преимуществом данной группы протоколов является то, что они не требуют сложных таблиц маршрутизации, быстро адаптируются к изменениям топологии, эффективны в условиях высокой мобильности. Недостатком является то, что они зависимы от точности GPS и наличия цифровых карт, а также в городских условиях возникают задержки и потери пакетов.

Многоадресные протоколы предназначены для эффективной доставки данных от одного источника сразу нескольким получателям (группе) в самоорганизующихся сетях транспортных средств. В VANET такие протоколы особенно востребованы для рассылки предупреждений о дорожных происшествиях, информирования о погодных условиях и т.д. Свое применение наши в областях экстренного оповещения и безопасности дорожного движения, например, рассылка предупреждений об авариях, заторах, опасных погодных условиях или дорожных работах всем транспортным средствам в определенной зоне или группе, обмен данными между автомобилями, движущимися в одном направлении или в одной зоне, для согласованных действий [5]. Многоадресные протоколы позволяют избежать многократной рассылки одних и тех же данных всем узлам сети, что уменьшает нагрузку на радиоканал и снижает вероятность коллизий, а также данные передаются только тем узлам, которые входят в целевую группу, что особенно важно в условиях ограниченной пропускной способности радиоканала. В ситуациях переменной плотности сети многоадресные протоколы хорошо адаптируются в плотном трафике они ограничивают число получателей, чтобы не перегружать канал, а более свободном используют механизмы хранения и пересылки, чтобы доставить данные даже при отсутствии прямой связи. Преимуществом данной группы протоколов является, эффективное распространение информации среди группы получателей, возможность учета специфики дорожной ситуации. Недостатком является, сложность поддержания актуальности групп получателей в условиях высокой мобильности, зависимость от точности позиционирования, а также возможны задержки при формировании групп.

Широковещательные протоколы предназначены для передачи информации от одного источника сразу всем узлам в сети. В контексте VANET такие протоколы используются для рассылки сообщений о дорожных условиях, авариях, погодных изменениях, экстренных ситуациях и других данных, которые должны быть получены всеми участниками движения в определенной области. В VANET их используют для задач, где важна максимальная оперативность и охват, например, экстренное оповещение, рассылка сообщений о ДТП, заторах, опасных погодных условиях, при перестроении колонны автомобилей или в системах коллективного вождения. В радиоканале при использовании широковещательных протоколов возникает высокая нагрузка, так как широковещательная рассылка приводит к резкому увеличению служебного трафика. В плотном трафике множество узлов одновременно пытаются передать сообщение, что увеличивает число ошибок и задержек. Широковещательные протоколы напрямую зависят от радиуса действия узлов и условий распространения сигнала [6]. В неблагоприятных условиях зона покрытия сужается, что требует более частых пересылок. В зонах с прерывистым радио покрытием протоколы могут терять эффективность, для преодоления этой проблемы применяются гибридные решения. Преимуществом данной группы протоколов является, оперативное информирование всех участников движения, а также простота реализации и масштабируемость. Недостатком является, риск «широковещательного шторма» при высокой плотности, высокая служебная нагрузка на сеть и увеличение задержек при передаче данных.

Проведенный анализ показывает, что выбор протокола маршрутизации для VANET должен основываться на специфике решаемых задач, характеристиках радиоканала и особенностях радио покрытия. Топологические протоколы эффективны в стабильных сетях с низкой мобильностью, но не справляются с высокой динамикой топологии.

Позиционные протоколы обеспечивают быструю адаптацию к изменениям, однако их работа зависит от точности GPS и качества цифровых карт. Многоадресные протоколы позволяют адресно доставлять информацию группам участников движения, снижая избыточность нагрузки на канал, но требуют механизмов поддержания актуальности групп. Широковещательные протоколы гарантируют оперативное информирование всех узлов, однако при высокой плотности трафика могут приводить к «широковещательному шторму» и перегрузке сети.

ТАБЛИЦА 2. Сравнение классов протоколов маршрутизации

Критерий	Топологические протоколы	Позиционные протоколы	Многоадресные протоколы	Широковещательные протоколы
Типичные представители	DSDV, AODV, ZRP	GPSR, GPCR, VADD, GeoDTN+Nav	IVG, Mobicast, CBR	DV-CAST
Сценарии применения	Стабильные сети, парковки, промышленные зоны, маршруты с низкой мобильностью	Городские и загородные трассы, сети с частыми разрывами, экстренные оповещения	Экстренное оповещение, информирование групп, согласованные маневры	Экстренное оповещение, обмен информацией о дорожной обстановке, поиск сервисов
Преимущества	Мгновенная доступность маршрутов (проактивные), баланс скорости и ресурсов (гибридные)	Не требуют сложных таблиц, быстрая адаптация к изменениям, эффективны при высокой мобильности	Эффективное распространение информации среди группы, снижение избыточности трафика	Оперативное информирование всех участников, простота реализации и масштабируемость
Недостатки	Высокие накладные расходы, неэффективны при высокой динамике, задержки при поиске маршрута	Зависимость от точности GPS и цифровых карт, возможны задержки и потери в городских условиях	Сложность поддержания актуальности групп, зависимость от позиционирования, задержки при формировании групп	Риск «широковещательного шторма», высокая служебная нагрузка, увеличение задержек
Связь с радиоканалом	Требуют частого обмена служебными сообщениями, чувствительны к стабильности канала	Минимизируют служебный трафик, быстро адаптируются к изменениям топологии	Снижают нагрузку на канал за счет передачи только группе получателей	Высокая нагрузка на канал, особенно без механизмов подавления избыточности
Связь с радиопокрытием	Эффективны при стабильном покрытии, теряют актуальность при частых разрывах	Хорошо работают в условиях переменной плотности, но зависят от качества GPS-сигнала	Адаптируются к плотности сети, используют механизмы хранения и пересылки в разреженных зонах	Эффективность зависит от радиуса действия и условий распространения сигнала, возможны потери в зонах с плохим покрытием

Таким образом, для современных VANET не существует универсального протокола маршрутизации. Эффективное решение задач безопасности и комфорта в автомобильной среде возможно только при комплексном под-

ходе, учитывающем динамику сети, характеристики радиоканала и специфику радио покрытия, а также при возможном комбинировании различных типов протоколов в зависимости от сценария применения.

Список используемых источников

1. Amina BENGAG, Mohamed EL BOUKHARI. Classification and Comparison of Routing Protocolsin VANETs// ISCV 2018.

2. Киричек Р. В., Филин Е. Д.. Модели взаимодействия беспилотного автотранспорта с инфраструктуры VANET для организации сетевой поддержки// Сборник статей АПИНО 2019.

3. Kashif Naseer Qureshi, Abdul Hanan Abdullah. Topology based routing protocols for VANET and their comparison with MANET// Journal of Theoretical and Applied Information Technology 2013.

4. Gaurav SharmaIsha, Isha Dhyani. A study of position based VANET routing protocols// International Conference on Computing, Communication and Automation (ICCCA) 2016.

5. Амани Ахмад Саббаг, Щербаков Максим Владимирович. Анализ производительности протоколов реактивной маршрутизации в VANET на базе NS3// Прикаспийский журнал: управление и высокие технологии 2021.

6. Ярцев С. В., Кучерявый Е. А., Владыко А. Г. Исследование структуры потоков широковещательного трафика в сетях VANET// Информатика, телекоммуникации и управление 2018.

Статья представлена научным руководителем, к.т.н., доцентом кафедры БТС СПБГУТ В. Е. Коротиным.

УДК 004.932.2

РАЗРАБОТКА ПОДХОДА К ВИЗУАЛИЗАЦИИ МУЗЫКАЛЬНОГО СИГНАЛА НА ОСНОВЕ СООТВЕТСТВИЯ ЧАСТОТ И ЦВЕТА

Н. А. Олейников (студент группы МТД-2521 СПбГУТ),
oleinikov.nr@sut.ru

В статье рассматривается подход к визуализации музыкального сигнала, основанный на сопоставлении частотных характеристик звука с цветовой моделью. Предлагается метод преобразования аудиосигнала в динамическое цветовое представление с использованием спектрального анализа и быстрого преобразования Фурье (FFT). Описывается принцип, при котором частота, амплитуда и временные изменения сигнала отображаются через оттенок, яркость и движение цвета. Такой способ визуализации позволяет сделать восприятие звука более наглядным и упрощает анализ его структуры, включая тембр и динамику. Рассматриваемый подход может применяться в обучении музыке, а также в задачах анализа и визуального представления аудиоданных.

визуализация звука, цветомузыка, аудио сигнал, спектральный анализ, FFT, частота, амплитуда, тембр, цифровая обработка сигналов

Эффективное изучение музыкального материала требует не только слухового восприятия, но и дополнительных способов анализа звука. На практике начинающим музыкантам бывает сложно понять структуру аудиосигнала, различать особенности тембра и выявлять ошибки исполнения только на слух. Чтобы лучше разобраться в особенностях музыкального звучания, можно использовать его графическое представление. Например, визуализация помогает увидеть частотный состав звука и изменения его интенсивности, которые не всегда легко определить на слух [1]. Для начинающих музыкантов такой способ может стать дополнительным инструментом при изучении музыкального материала.

Для анализа аудиосигналов применяются различные способы обработки звука. Среди наиболее распространенных – построение волновой формы, спектра и спектрограммы. Каждый из них позволяет изучить определенные характеристики сигнала. Однако человеку, который раньше не сталкивался с подобными графиками, бывает непросто разобраться в их значении. Поэтому для обучения музыке полезно рассмотреть и другие способы отображения звуковой информации.

В этой работе предлагается использовать цвет для отображения характеристик музыкального сигнала. Идея состоит в том, чтобы связать частотные составляющие звука с определенными оттенками, а изменение их амплитуды – с яркостью изображения. При этом изменения звучания во времени будут отражаться на самом изображении. Такой способ позволит наблюдать за звуком и его характеристиками без необходимости постоянно обращаться к числовым значениям.

Для определения частотного состава звука сначала необходимо обработать исходный аудиосигнал. В цифровой обработке для этой задачи часто применяют быстрое преобразование Фурье (FFT). С его помощью можно получить данные о частотах, из которых состоит записанный звук, и определить величину каждой частотной составляющей [2].

Применение FFT дает возможность определить, какие частоты присутствуют в сигнале и с какой интенсивностью. Это, в свою очередь, позволяет анализировать гармонический состав звука, оценивать чистоту ноты и выявлять особенности тембра. Подобный подход широко используется как в профессиональных музыкальных редакторах, так и в обучающих системах.

Процесс обработки аудиосигнала, как правило, включает несколько этапов [3]. Сначала выполняется захват звука с микрофона или из файла, затем производится его оцифровка и предварительная обработка [4], включающая фильтрацию и нормализацию. После этого применяется спектральный анализ, позволяющий получить распределение частот, а на заключительном этапе данные используются для построения визуального представления.

На рисунке 1 показана схема обработки аудио сигнала.

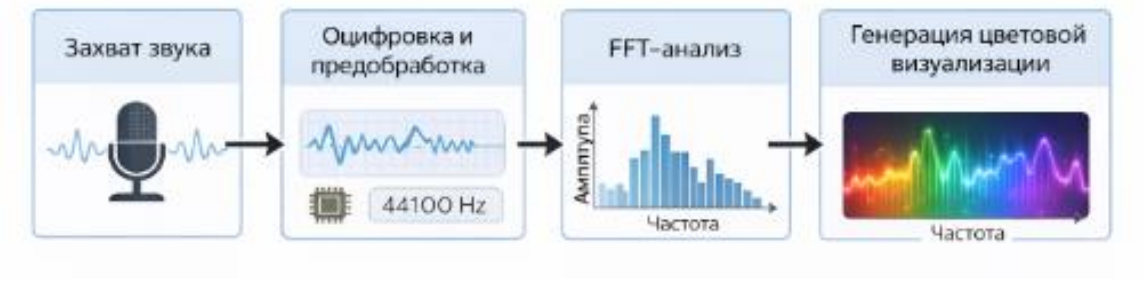


Рис. 1. Схема обработки аудиосигнала

Полученные в результате обработки параметры – частоты, амплитуды и временные характеристики – могут быть использованы не только для построения традиционных графиков, но и для более сложных форм визуали-

зации. Это открывает возможность перехода от классических методов отображения звука к альтернативным подходам, в частности, к цветомузыкальной визуализации.

На основе полученных спектральных данных можно перейти к построению цветовой визуализации звука. В предлагаемом подходе используется принцип сопоставления параметров аудиосигнала с характеристиками цветового представления.

Основная идея заключается в том, что различные диапазоны частот могут быть связаны с определенными участками цветового спектра. Это позволяет визуально разделять низкие, средние и высокие компоненты звука и воспринимать их не только как числовые значения, но и как наглядный образ.

В работе используется следующая схема соответствия:

- низкие частоты соотносятся с теплыми цветами (красный, оранжевый);
- средние частоты – с зелеными оттенками;
- высокие частоты – с холодными цветами (синий, фиолетовый).

Такое распределение выбрано не случайно, а с учетом интуитивного восприятия: низкие частоты воспринимаются как более “тяжелые” и глубокие, а высокие – как более «легкие» и резкие. Соответственно, цветовая шкала помогает быстрее ориентироваться в структуре сигнала.

На рисунке 2 показано соответствие диапазонов частот и цветового спектра.



Рис. 2. Соответствие диапазонов частот и цветового спектра

Если использовать только частоту, изображение будет показывать лишь часть информации о звуке. Поэтому в цветовой модели стоит учитывать и другие его характеристики. Это поможет показать не только частотный состав сигнала, но и то, как меняется звучание музыкального инструмента.

Одна из таких характеристик – амплитуда. В предлагаемом способе визуализации от нее зависит яркость отдельных цветовых участков. Например, если определенная частотная составляющая выражена сильнее, соответствующий ей участок изображения будет ярче. Когда ее амплитуда уменьшается, яркость также снижается. Благодаря этому можно увидеть, какие составляющие звука преобладают в определенный момент.

Звучание музыкального инструмента постоянно меняется. После извлечения ноты звук может постепенно затихать, а при исполнении следующей ноты меняется и его частотный состав. Эти изменения можно передать через движение графических элементов, их форму или расположение на экране. В результате изображение будет меняться одновременно со звуком.

Помимо частоты и амплитуды, при построении визуализации можно учитывать форму звуковой волны и обертоны. Например, два инструмента могут исполнять одну и ту же ноту, но звучать по-разному из-за различий в составе обертонов. В дальнейшем эту особенность можно использовать для изменения формы или текстуры изображения, чтобы визуально различать характер звучания инструментов.

На рисунке 3 показано, как отдельные параметры аудиосигнала связаны с элементами цветовой визуализации.



Рис. 3. Влияние параметров сигнала на цветовую визуализацию

Если объединить несколько характеристик звука в одном изображении, можно получить более подробное представление о его составе и изменениях. Цвет будет показывать частотные составляющие, яркость – их амплитуду, а движение элементов – изменения сигнала во времени.

Такой способ отображения звука можно использовать при обучении игре на музыкальных инструментах. Например, во время исполнения ноты ученик сможет одновременно слышать ее звучание и наблюдать за изменением изображения. Это позволит обратить внимание на частотный состав и интенсивность звука, а также проследить, как они меняются при игре.

Для начинающих музыкантов подобное представление может быть удобным дополнением к занятиям. Вместо изучения сложных графиков пользователь сможет наблюдать за цветовым изображением, которое меняется в зависимости от характеристик исполняемого звука.

Кроме того, данный подход может применяться при анализе качества звучания. Цветовая модель позволяет визуально выявлять искажения, нестабильность сигнала и особенности тембра, которые не всегда очевидны при обычном восприятии. Таким образом, визуализация может выступать в роли дополнительного инструмента контроля исполнения.

Также перспективным направлением является использование цветомузыкальной визуализации в мультимедийных и интерактивных системах. В таких приложениях она может применяться для создания динамических визуальных эффектов, синхронизированных с аудиосигналом.

В рамках данной работы рассматриваемый подход может быть реализован в виде отдельного модуля визуализации, объединяющего методы цифровой обработки сигналов и интуитивно понятное графическое представление. Такой модуль может использоваться как в образовательных, так и в исследовательских задачах.

Заключение

Таким образом, предложенный подход к визуализации музыкального сигнала на основе соответствия частот и цветовой модели позволяет по-новому представить структуру звука. Использование цветового отображения делает анализ аудиосигнала более наглядным и упрощает восприятие его основных характеристик.

В отличие от традиционных методов визуализации, ориентированных преимущественно на специалистов, рассматриваемый подход позволяет сделать процесс анализа доступным для более широкого круга пользователей, включая начинающих музыкантов.

Учет таких параметров, как частота, амплитуда и временные изменения сигнала, обеспечивает формирование более полной и информативной визуальной модели. Это позволяет не только анализировать звук, но и выявлять его особенности, включая тембр и динамику.

В дальнейшем представляется целесообразным развитие данного подхода, включая его реализацию в виде программного модуля и проведение экспериментальных исследований с использованием различных типов аудиосигналов.

Список используемых источников

1. Rossing T. D. The Science of Sound. 3rd ed. Boston: Addison-Wesley, 2002. 783 p.
2. Lyons R. Understanding Digital Signal Processing. 3rd ed. Upper Saddle River: Pearson, 2019. 992 p.
3. Zölzer U. Digital Audio Processing. 2nd ed. Hoboken: Wiley, 2022. 512 p.
4. Smith J. O. Spectral Audio Signal Processing. Stanford: Stanford University, 2011. 462 p.

Статья представлена научным руководителем, кандидатом педагогических наук, доцентом кафедры информатики и компьютерного дизайна СПбГУТ, доцентом А. А. Шияном.

УДК 004.415

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПОДДЕРЖКИ МАЛОМОБИЛЬНЫХ ГРУПП НАСЕЛЕНИЯ ПРИ ПЕРЕДВИЖЕНИИ ПО ГОРОДУ

Д. А. Пелих (ассистент кафедры ИУС СПбГУТ)
Е. П. Толоконникова (студент группы ИСТ-213 СПбГУТ),
tolokonnikova.ep@sut.ru

В работе предлагается концепция мобильного приложения, предназначенного для поддержки маломобильных граждан в городской среде. Система основана на принципе пользовательского контента: участники отмечают доступные и проблемные места и объекты городской среды, формируя живую карту города. Решение направлено на снижение барьеров передвижения и развитие культуры инклюзивности через цифровую взаимопомощь.

маломобильные люди, доступная среда, мобильное приложение, инклюзивность

Городская среда во многих случаях остается недостаточно приспособленной для людей, испытывающих сложности в передвижении. В ряде зданий и общественных пространств отсутствуют пандусы, подъемные платформы, широкие проходы и лифты, пригодные для использования инвалидных колясок. Даже при наличии формально доступной инфраструктуры пользователи могут сталкиваться с временными препятствиями – например, перекрытием проходов во время ремонтных работ. Из-за этого заранее оценить удобство маршрута бывает затруднительно. Наиболее заметно данная проблема проявляется в незнакомых районах, где информация о возможных барьерах отсутствует или оказывается неактуальной.

Современные картографические сервисы лишь частично учитывают вопросы доступности городской среды. В России отдельные элементы такой функциональности присутствуют в сервисе «Яндекс.Карты», однако сведения о доступности объектов представлены не системно и обновляются нерегулярно. Кроме того, отсутствуют специализированные решения, ориентированные именно на потребности маломобильных пользователей и предполагающие активное участие самих пользователей в наполнении базы данных.

В этих условиях возникает идея создания информационной системы, которая позволила бы людям с ограниченными возможностями делиться актуальной информацией о городской среде, отмечать проблемные участки,

удобные маршруты и комфортные места. Аналогичные исследования также подтверждают, что ключевыми проблемами являются не только физическая недоступность объектов, но и отсутствие актуальной информации о них [1]. В связи с этим особую значимость приобретают системы, основанные на пользовательском контенте, позволяющие формировать живую, постоянно обновляемую карту доступности. Такое приложение могло бы стать не только навигационным инструментом, но и площадкой для формирования сообщества взаимопомощи, где каждый пользователь вносит свой вклад в развитие более инклюзивной городской среды.

С целью выявления актуальных потребностей и проблем была проведена анкета среди маломобильных людей. Опрос охватил 10 респондентов, имеющих ограничения по передвижению и регулярно использующих городскую инфраструктуру.

Первый вопрос касался ситуаций, связанных с посещением незнакомых районов: «Бывают ли у вас случаи, когда вы оказываетесь в новом месте и не знаете заранее, есть ли там препятствия для передвижения?» Из десяти участников шесть ответили утвердительно, подтвердив, что сталкиваются с неопределенностью при планировании маршрутов. Особенно показательным стал ответ одного из респондентов: «Нет, я стараюсь не покидать свой район именно из-за этой трудности». Эта фраза наглядно демонстрирует, что отсутствие информации не просто создает неудобства – оно ограничивает свободу передвижения и ведет к самоизоляции.

Следующий вопрос предполагал выбор типичных барьеров в городской среде. Все респонденты, отметили наличие трудностей. Наиболее часто указывались отсутствие лифта, тяжелые или неудобные двери, отсутствие доступных туалетов, тесные проходы в кафе и общественных местах, а также отсутствие кнопок вызова персонала.

На основе проведенного опроса можно сделать вывод, что проблема носит системный характер и затрагивает различные сферы городской жизни.

Также в исследованиях, основанных на анализе пользовательских отзывов, отмечается, что именно общественные пространства, такие как кафе, парки, гостиницы, больницы становятся частыми темами обсуждения в контексте доступности для маломобильных групп населения [2].

Ключевой вопрос анкетирования касался готовности использовать специализированное приложение: «Вы бы пользовались платформой, где пользователи отмечают проблемные зоны, делятся информацией о комфортных

маршрутах и удобных местах?» Семь из десяти участников ответили положительно. При этом ни один из опрошенных не использует на данный момент аналогичные сервисы. Это свидетельствует о наличии реальной потребности в таком инструменте при полном отсутствии действующих решений на рынке.

Полученные результаты стали основанием для разработки концепции информационной системы, ориентированной на сбор, обмен и визуализацию данных о доступности городской инфраструктуры на основе реального пользовательского опыта.

Разрабатываемая информационная система представляет собой мобильное приложение, ориентированное на поддержку маломобильных групп населения при передвижении по городу. Основная идея проекта – создание платформы, где пользователи могут не только получать, но и сами формировать информацию о доступности городской инфраструктуры.

Разрабатываемая система основана на модели пользовательского взаимодействия, при которой участники одновременно используют информацию и дополняют ее новыми данными. За счет этого карта доступности может регулярно обновляться на основе практического опыта людей, ежедневно сталкивающихся с ограничениями городской среды.

Работа с приложением осуществляется через интерактивную карту. Для добавления нового объекта пользователь выбирает нужную точку, после чего указывает категорию объекта, его название, а также при необходимости прикрепляет комментарий, фотографию и оценку доступности.

Перед публикацией сведения проходят автоматическую проверку. Текстовые материалы анализируются на наличие недопустимых выражений, а изображения проверяются на соответствие правилам размещения контента. После завершения модерации информация становится доступной остальным пользователям приложения.

Для визуального отображения объектов используется цветовая маркировка. Зеленым цветом обозначаются места с удовлетворительным уровнем доступности, красным – участки, где пользователи сталкиваются с затруднениями.

Дополнительно реализована возможность фильтрации по категориям (например, «пандусы», «доступные туалеты», «ремонтные работы»), что позволяет целенаправленно искать нужную информацию.

Такой подход превращает приложение из простого навигатора в инструмент социальной взаимопомощи. Пользователи делятся личным опытом, предупреждают других о трудностях, рекомендуют удобные маршруты – формируя сообщество, направленное на повышение качества городской среды.

Информационная система реализуется как кроссплатформенное мобильное приложение с использованием современных технологий фронтенда и бэкенда. Архитектура построена по принципу клиент-серверного взаимодействия с разделением логики и данных.

Бэкенд системы разрабатывается на платформе ASP.NET Core с использованием языка C#. Основой серверной части является RESTful API, обеспечивающее стандартизированный обмен данными между клиентом и сервером. Такой подход позволяет гибко масштабировать систему и интегрировать сторонние сервисы.

Для хранения информации используется SQLite на этапе разработки, что обеспечивает простоту тестирования и локального развертывания. В перспективе планируется переход на PostgreSQL – СУБД с поддержкой распределенного хранения, репликации и высокой отказоустойчивости.

Фронтенд приложения реализуется с помощью React Native, что позволяет создавать нативные интерфейсы для платформ iOS и Android. Использование единой кодовой базы позволяет сократить затраты времени на разработку и обеспечить одинаковые принципы работы приложения на разных мобильных платформах.

Картографический модуль реализован на основе API «Яндекс.Карт», обеспечивающего отображение объектов на интерактивной карте и взаимодействие с пользовательскими метками [3].

Разрабатываемая система предназначена не только для упрощения навигации, но и для повышения информированности пользователей о состоянии городской инфраструктуры. Пользователи получают возможность обмениваться сведениями о доступности общественных мест, наличии препятствий и особенностях маршрутов.

Практическая значимость приложения связана прежде всего с возможностью предварительной оценки условий передвижения. Информация о наличии пандусов, лифтов, доступных входных групп позволяет более уверенно планировать посещение различных объектов городской среды.

Дополнительно собранные данные могут представлять интерес для муниципальных организаций. Информация о наиболее проблемных участках

способна использоваться при анализе состояния городской инфраструктуры, планировании ремонтных работ и оценке эффективности мероприятий по формированию безбарьерной среды.

Таким образом, разрабатываемая информационная система представляет собой инструмент сбора и распространения данных о доступности городской среды и может способствовать повышению уровня информированности маломобильных граждан.

Список используемых источников

1. Семенов С. П. Интерактивная геоинформационная система для маломобильных граждан / С. П. Семенов, А. О. Ташкин // Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования: Сборник научных статей международной конференции, Барнаул, 20–24 октября 2015 года / Алтайский государственный университет. – Барнаул: Алтайский государственный университет, 2015. С. 1007-1010. EDN UVOWON.

2. Низомутдинов, Б. А. Оценка доступности объектов благоустройства для маломобильных групп населения на основе отзывов в социальных сетях / Б. А. Низомутдинов, В. А. Казак // Научный сервис в сети Интернет. 2021. № 23. С. 244-250. DOI 10.20948/abrau-2021-19. EDN PXOMRV.

3. Яндекс.Карты. API документация [Электронный ресурс] // URL: https://yandex.ru/maps-api/docs (дата обращения: 29.04.2026).

Статья представлена кандидатом технических наук, заведующим кафедрой ИУС СПбГУТ, доцентом В. Л. Литвиновым.

УДК 004.89

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МУЛЬТИАГЕНТНОЙ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО СОСТАВЛЕНИЯ РАСПИСАНИЯ

Д. А. Пелих (ассистент кафедры ИУС СПбГУТ)
Я. П. Ястребов (студент группы ИСТ-213 СПбГУТ), yastrebov.yp@sut.ru

В статье рассматривается задача автоматизации составления расписаний. Представлены недостатки существующих методов и алгоритмов. Предложен подход, основанный на мультиагентной системе, который обеспечивает повышение гибкости, адаптивности и устойчивости процесса планирования. Описана архитектура разработанной системы и механизм кооперативного взаимодействия агентов.

мультиагентная система, автоматическое составление расписаний, распределенное решение задач, интеллектуальные агенты

Составление расписаний представляет собой одну из важнейших задач организации образовательного процесса. В рамках теории расписаний применяется множество методов, рассмотренных в работах [1, 2], однако на практике такие подходы нередко демонстрируют низкую эффективность при неполноте исходных данных, частом изменении ограничений и необходимости быстрого перепланирования.

Среди существующих подходов к автоматизации составления расписаний можно выделить алгоритмы оценки свободы расположения, генетические алгоритмы, методы логического программирования в ограничениях и алгоритмы раскраски графов. Однако каждый из них имеет ряд ограничений.

Алгоритмы оценки свободы расположения не учитывают типы занятий, особенности дисциплин и предпочтения преподавателей, а также плохо адаптируются к изменениям исходных данных. Генетические алгоритмы требуют высокой вычислительной мощности, сложной настройки параметров и недостаточно эффективно поддерживают локальные изменения расписания.

Методы логического программирования в ограничениях обеспечивают высокую точность решения, однако при увеличении числа ограничений значительно возрастает вычислительная нагрузка, а внесение изменений может

нарушить согласованность расписания. Алгоритмы раскраски графов ориентированы преимущественно на учет жестких ограничений и не позволяют полноценно учитывать специфику занятий, вместимость аудиторий и предпочтения участников образовательного процесса.

Несмотря на подтвержденную применимость представленных алгоритмов в задачах базовой автоматизации, они не обеспечивают необходимый уровень гибкости и адаптивности, требуемый в современных условиях образовательного процесса. Кроме того, такие подходы практически не учитывают большое количество дополнительных параметров, включая предпочтения преподавателей, специфику аудиторий и механизмы эффективного разрешения возникающих конфликтов.

Прогресс в области интеллектуальных технологий расширяет возможности для качественного решения этой многокритериальной задачи. Указанные проблемы могут быть эффективно решены с помощью мультиагентного подхода. Мультиагентная система определяется как сеть слабо связанных между собой программных сущностей (агентов), специализирующихся на решении частных задач, которые существуют в общей среде и взаимодействуют между собой для достижения тех или иных целей системы. Взаимодействие может осуществляться агентами либо прямым образом – путем обмена сообщениями, либо некоторым косвенным образом, когда одни агенты воспринимают присутствие других агентов через изменения во внешней среде, с которой они взаимодействуют [3].

Применение данного подхода позволяет повысить гибкость процесса формирования расписаний, так как система обретает способность адаптироваться к изменяющимся ограничениям посредством интеграции новых агентов. Дополнительно достигается устойчивость системы, при которой выход из строя отдельного агента не влечет за собой прекращение ее функционирования в целом. При этом, учитывается распределенный характер данных, поскольку исходная информация рассредоточена между различными участниками процесса, в частности, на кафедрах, у преподавателей или в системе управления аудиторным фондом.

В разрабатываемой системе каждый агент соответствует определенной роли или сущности учебного процесса, действует автономно, опираясь на локальную информацию и собственные цели, а также взаимодействует с другими агентами для обеспечения глобальной согласованности расписания и повышения его качества.

Система организована по принципу децентрализованной или горизонтальной архитектуры: управляющие агенты взаимодействуют на одном уровне и являются равноправными. Агентами в данном случае являются сущности, представляющие отдельные кафедры высшего учебного заведения. Их главная цель – составление согласованного расписания для отдельной кафедры. На пути к ее достижению агенты проверяют наличие конфликтов у преподавателей, соблюдение норм по нагрузке и внутренних правил.

Отдельно в архитектуре системы предусмотрен уровень хранения ресурсов для агентов, на нем функционируют следующие сущности:

- группы. Хранят расписание конкретной группы и ее название;
- аудитории. Обладают информацией о расписании конкретной аудитории, ее номер, вместимость, принадлежность, тип и имеющееся оборудование;
- преподаватели. По своей структуре схожи с сущностями групп – хранят расписание конкретного преподавателя, его имя и уникальный идентификатор.

Архитектура взаимодействия агентов изображена на рисунке 1.

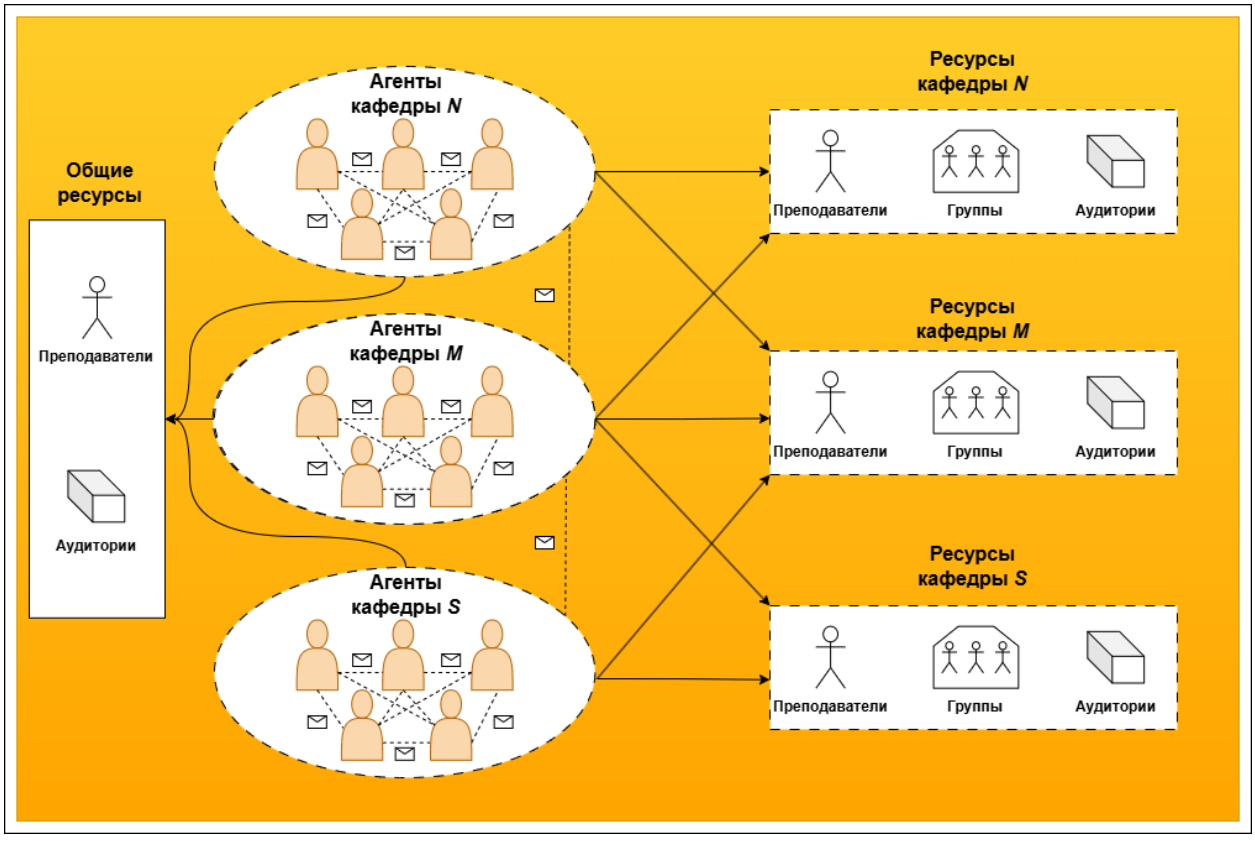


Рис. 1. Архитектура мультиагентной системы автоматизированного составления расписания

Направленными связями изображено использование ресурсов агентами – каждому агенту доступны ресурсы, относящиеся к его кафедре. Также он может претендовать на ресурсы других подразделений, если это разрешено правилами высшего учебного заведения.

Ненаправленные пунктирные линии со значком конверта показывают возможность коммуникации между сущностями. Как видно из рисунка 1, каждый агент имеет возможность общения с любым другим, независимо от кафедральной принадлежности, что позволяет распределять занятия максимально гибко и выгодно.

Средой, связывающей агентов, выступает шина данных, в которой при первом запуске системы каждый из них регистрируется и получает доступ к функции отправки сообщений. Принципиальным аспектом реализации шины является то, что агенты не имеют информации о друг друге – лишь при попытке назначить занятие в уже зарезервированный кем-то слот система связывает непосредственных участников процесса друг с другом. Этим подтверждается наличие одной из важнейших составляющих мультиагентной системы – слабосвязности.

Рабочий процесс агента может быть представлен следующим образом:

1. Алгоритмическое составление расписания своей кафедры имеющимися инструментами;

2. Анализ составленного расписания – перестановки распределенных занятий с целью максимизации учтенных предпочтений;

3. Фаза коммуникации – запросы на перестановку занятий в другой временной слот или обмен ими с другим агентам. Также со стремлением увеличить количество учтенных пожеланий преподавателей.

Чтобы расписание было допустимым, то есть возможным для реализации в реальности, необходимо учитывать ряд ограничений, связанных с доступностью ресурсов, временными рамками и логистическими условиями. Эти ограничения обеспечивают согласованность действий всех участников учебного процесса, исключают конфликты между занятиями, и позволяют эффективно использовать доступные преподавательские, аудиторные и временные ресурсы.

Ограничения (не допускают нарушения):

- преподаватель не может одновременно проводить более одного занятия;
- учебная группа не может посещать два занятия в одно и то же время, за исключением потоковых;

- аудитория не может быть занята двумя разными занятиями одновременно;
- общее количество часов по каждой дисциплине должно строго соответствовать учебному плану;
- тип занятия должен соответствовать назначению аудитории (например, лекции – в лекционных залах, лабораторные работы – в лабораториях);
- вместимость аудитории должна позволять разместить всех студентов группы;
- преподаватель может вести только те дисциплины, которые закреплены за ним;
- занятия не должны назначаться на выходные и праздничные дни, если это не предусмотрено спецификой учебного процесса;
- расписание должно укладываться в границы учебного семестра.

Соблюдение ограничений позволяет создать реализуемое расписание, но не учитывает более тонкие, хотя и не менее важные моменты – пожелания.

Учет пожеланий направлен на повышение удобства и сбалансированности расписания. Для этого каждому критерию назначается коэффициент значимости в диапазоне от 0 до 3, где 0 соответствует отсутствию важности, а 3 – максимально высокой желательности выполнения условия. При этом пожелания относятся к категории мягких ограничений и могут быть нарушены, если это необходимо для обеспечения корректности и выполнимости расписания.

Пожелания:

- минимизация количества "окон" в расписании;
- минимизация количества рабочих дней в неделю;
- максимизация количества пар в определенные дни недели;
- учет предпочтений преподавателей по времени (в какие дни, в какое время нежелательно ставить занятия).

Также пожелания играют еще одну важную роль – являются одной из главных метрик оценки качества формируемого расписания. Чем больше пожеланий будет учтено в итоге, тем расписание считается качественнее.

В дальнейшем результаты текущего исследования могут быть применены для создания мультиагентной системы автоматизации составления расписаний.

Список используемых источников

1. Гришин И. Ю. Новый подход к решению задачи составления расписания / И. Ю. Гришин, Р. Р. Тимиргалеева // NovaInfo.Ru. 2017. Т. 2. № 63. С. 283-287.

2. Самсонова Н. В. Составление расписания в высшем учебном заведении: математические методы и программные продукты / Н. В. Самсонова, А. Б. Симонов // E-Management. 2018. Т. 1. № 1. С. 60-69.

3. Городецкий В. И. Современное состояние и перспективы индустриальных применений многоагентных систем / В. И. Городецкий, О. Л. Бухвалов, П. О. Скобелев // Управление большими системами: сборник трудов. 2017. № 66. С. 94-157.

Статья представлена кандидатом технических наук, заведующим кафедрой ИУС СПбГУТ, доцентом В. Л. Литвиновым.

УДК 004.722.2

ИССЛЕДОВАНИЕ P2P-ПЕРЕДАЧИ ДАННЫХ ПОСРЕДСТВОМ ВЕБ-ПРИЛОЖЕНИЙ

Ю. Я. Перевозник (к.п.н., доцент кафедры СОД СПбГУТ)
Е. Г. Скрябин (студент группы ИСТ-222 СПбГУТ), skryabin.eg@sut.ru

Статья посвящена исследованию проблем, связанных с клиент-серверной архитектурой, анализу преимуществ и недостатков peer-to-peer (P2P) передачи по сравнению с клиент-серверной архитектурой, а также принципов и технологий реализации P2P-передачи данных в веб-среде. В статье описываются основы работы технологии WebRTC и этапы установления P2P-соединения с использованием WebRTC. Рассмотрены недостатки исследуемых подходов и технологий.

программное обеспечение, архитектура программного обеспечения, передача данных, сетевые технологии, распределенные информационные системы, веб-приложения, peer-to-peer, WebRTC

Передача информации в веб-среде традиционно основывается на клиент-серверной модели взаимодействия устройств, где обмен данными между пользователями осуществляется через центральный сервер. Такая архитектура удобна для управления, но создает узкие места: зависимость от третьей стороны, дополнительные задержки, риски утечки данных и рост инфраструктурных затрат. В последние годы все большую актуальность приобретает альтернативный подход – peer-to-peer (P2P) передача данных, при которой устройства пользователей обмениваются информацией напрямую [1]. Ключевой технологией, позволившей реализовать P2P-взаимодействие прямо в браузере без установки дополнительного ПО, стал стандарт WebRTC [2].

Peer-to-peer (одноранговая) сеть – это модель взаимодействия, при которой каждый участник (peer) может одновременно выступать и клиентом, и сервером. В контексте веб-приложений это означает, что браузеры пользователей устанавливают прямое соединение и обмениваются данными без необходимости постоянного взаимодействия с центральным сервером.

Сервер в такой системе все еще может использоваться, но его роль ограничивается служебными задачами:

- первичная координация соединения (сигналинг);
- аутентификация пользователей;
- обмен метаданными.

Основной поток данных – файлы, сообщения, медиаконтент – передается напрямую между устройствами пользователей.

P2P-передача данных имеет ряд преимуществ в сравнении с клиент-серверной архитектурой.

Ключевым преимуществом P2P является отсутствие третьей стороны, через которую проходит пользовательский контент. В классической клиент-серверной модели сервер хранит данные, передает их и потенциально имеет к ним доступ. Возникает критическая точка уязвимости: компрометация сервера приводит к утечке информации множества пользователей. Использование сервисов с центральным сервером требует доверия к провайдеру услуги. В P2P-модели данные передаются напрямую между участниками соединения, что снижает риски.

WebRTC дополнительно усиливает безопасность за счет обязательного шифрования трафика (DTLS и SRTP), что делает перехват данных в канале связи практически бесполезным без ключей сессии.

P2P-подключение имеет потенциально лучшую производительность и меньшие задержки при передаче полезных данных. Так как в клиент-серверной модели данные преодолевают минимум один дополнительный сетевой «хоп» через сервер, возникает потенциальное увеличение задержки и нагрузка на сеть, а также возможность перегрузки канала на серверной стороне. Данный критерий имеет особую значимость при передаче большого объема данных или потоковой передаче, например, аудио и видеозвонках или онлайн-играх.

Еще одно важное достоинство P2P – лучшая масштабируемость. Информационные системы на основе центрального сервера требуют вертикального или горизонтального масштабирования базовой инфраструктуры вместе с ростом числа пользователей. P2P-архитектура распределяет нагрузку на устройства клиентов. Рост числа участников автоматически увеличивает вычислительную мощность сети.

Облегченная масштабируемость приводит к потенциальному снижению инфраструктурных затрат на развитие системы. Сервер выполняет лишь координирующую роль. Поскольку основной трафик не проходит через сервер, снижаются расходы на увеличение производительности и объема хранилищ.

Также, P2P-сети обладают лучшей отказоустойчивостью. Центральный сервер – это единая точка отказа. Сбой работы сервера нарушает работу

всего сервиса. В P2P-архитектуре отказ одного узла затрагивает только соединения, связанные с ним, но не выводит из строя всю систему. Распределенный принцип сети повышает устойчивость к сбоям и сетевым атакам типа DDoS, направленным на конкретный узел.

Основой P2P-передачи в веб-среде является технология WebRTC.

WebRTC (Web Real-Time Communication) – это набор стандартов и API, позволяющих браузерам и мобильным приложениям устанавливать защищенные P2P-соединения для передачи аудио, видео и произвольных данных.

Процесс установления P2P-соединения с использованием WebRTC включает несколько этапов, описанных ниже [3].

1. Сигналинг. Два клиента (браузера) сначала взаимодействуют через сервер сигналинга. Они обмениваются SDP-описаниями (Session Description Protocol), содержащими информацию о поддерживаемых кодеках, типах соединений и параметрах сессии, и сетевыми кандидатами (ICE candidates). На этом этапе сервер лишь передает сообщения, необходимые для установки P2P-соединения, но не участвует в передаче пользовательских данных.

2. Обход NAT. Большинство устройств находятся за NAT и не имеют публичного IP-адреса. Для установления прямого соединения используется механизм ICE (Interactive Connectivity Establishment) [4], который собирает возможные сетевые адреса (кандидаты), проверяет различные пути соединения и выбирает наилучший маршрут.

Для этого применяются вспомогательные серверы:

- STUN – позволяет определить внешний IP и порт [5];
- TURN – используется как резервный ретранслятор, если прямое соединение невозможно [6].

3. Установление защищенного канала. После выбора маршрута между участниками устанавливается защищенное соединение. Безопасность обеспечивают протоколы DTLS (обмен ключами и шифрование произвольных данных) и SRTP (шифрование аудио и видео). Шифрование является обязательным, что повышает безопасность P2P-обмена.

4. Передача данных. После успешного завершения предыдущих шагов участники могут начать передачу «полезных» данных. Передача идет напрямую между браузерами, минуя сервер сигналинга.

Схема, отражающая принцип работы WebRTC представлена на рис. 1.

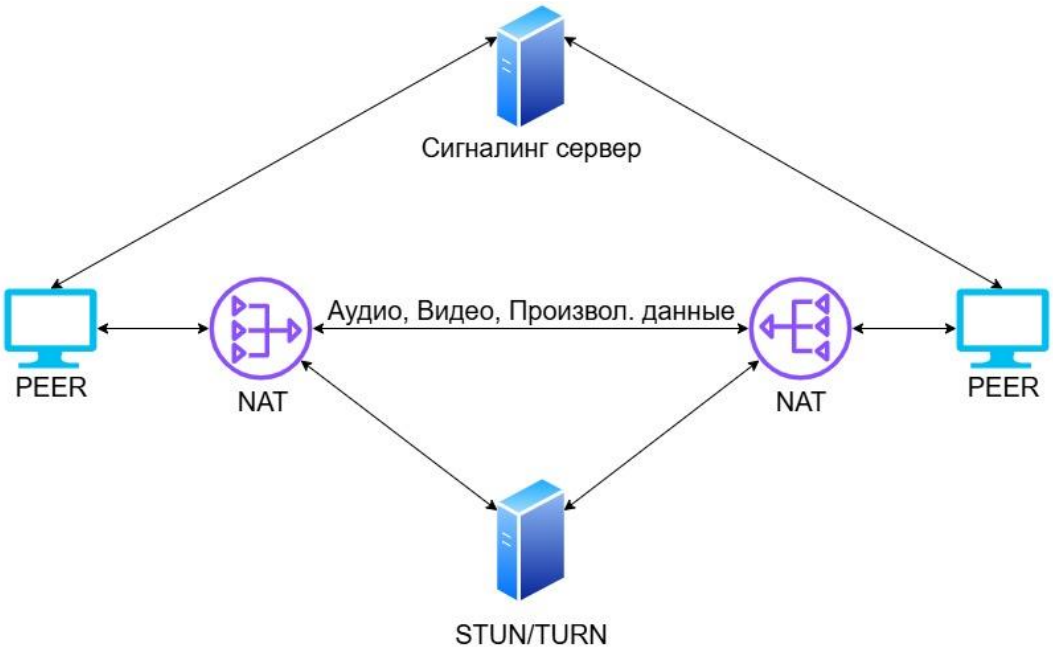


Рис. 1. Принцип работы WebRTC

Несмотря на преимущества, P2P и WebRTC имеют ряд технических вызовов:

- сложность обхода NAT и необходимость STUN/TURN-инфраструктуры;
- нестабильность соединений в мобильных сетях;
- ограниченные ресурсы пользовательских устройств.

Также, в некоторых случаях, например, с симметричным NAT, когда все запросы с одинаковыми локальными IP-адресом и портом источника, но различными IP-адресами назначения отображаются в отличающиеся внешние IP-адрес и порт источника, использование STUN невозможно, и полезные данные будут пересылаться через TURN-сервер, что возвращает централизованный элемент.

Целью данного исследования был анализ P2P-архитектуры и особенностей ее реализации в веб-среде, выявление преимуществ и недостатков такого подхода, а также сравнение с клиент-серверной архитектурой. Исследование показало: P2P-передача данных в веб-среде имеет достоинства и может использоваться для достижения определенных целей при разработке некоторых веб-приложений. Системы на основе P2P-передачи, также, имеют ряд недостатков и ограничений, обусловленные самой архитектурой и особенностями технической реализации, которые следует учитывать при выборе архитектурного подхода для веб-приложения.

Список используемых источников

1. Стин ван М., Таненбаум Э. С. Распределенные системы / пер. с англ. В. А. Яроцкого. М.: ДМК Пресс, 2021. 584 с.: ил.

2. H. Alvestrand. Real-Time Protocols for Browser-Based Applications: RFC 8825 IETF, January 2021. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc8825 (дата обращения: 25.12.2025).

3. WebRTC: Real-Time Communication in Browsers W3C, 13 March 2025. W3C Recommendation [Электронный ресурс]. URL: https://www.w3.org/TR/webrtc/ (дата обращения: 12.01.2025).

4. Keranen A., Holmberg C., Resenberg J. Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal. RFC 8445 IETF, July 2018. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc8445 (дата обращения: 12.01.2026).

5. Rosenberg J., Mahy R., Matthews P., Wing D. Session Traversal Utilities for NAT (STUN). RFC 5389 Network Working Group, October 2008. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc5389 (дата обращения: 13.01.2026).

6. R Mahy., Matthews P., Rosenberg J. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). RFC 5766 IETF, April 2010. Proposed Standard [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc5766 (дата обращения: 13.01.2026).

Статья представлена научным руководителем, доцентом кафедры СОД СПБГУТ кандидатом педагогических наук Ю. Я. Перевозником

УДК 004.853

ИССЛЕДОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ ФОРМИРОВАНИЯ ИНДИВИДУАЛЬНОЙ ТРАЕКТОРИИ РАЗВИТИЯ

О. В. Раковский (к.т.н., доцент, доцент кафедры ИУС СПбГУТ)
И. И. Турлыков (студент группы ИСТ-411м СПбГУТ), turlykov.ii@sut.ru

Интеллектуальные подходы к формированию индивидуальной траектории развития становятся все более популярными благодаря цифровой трансформации образования и возможности адаптировать обучение под уникальные особенности каждого человека. Их внедрение не требует радикальной перестройки учебного процесса, но при этом позволяет гибко учитывать темп, цели и уровень подготовки обучающегося. Появление разнообразных цифровых платформ и систем на базе искусственного интеллекта предоставляет свободу выбора и помогает экономить время и ресурсы.

индивидуальная траектория развития, интеллектуальные методы, персонализация, цифровое образование, адаптивное обучение, образовательные платформы

Цифровая эпоха предъявляет к образованию новые требования: современные обучающиеся ожидают индивидуального подхода, сопоставимого с тем, который предлагают рекомендательные сервисы в онлайн-среде. Интеллектуальные методы, основанные на анализе больших данных и технологиях искусственного интеллекта, позволяют гибко адаптировать содержание, темп и формат занятий под уникальные особенности каждого ученика [1, 2]. При этом их внедрение не требует кардинальной перестройки классического учебного процесса: достаточно интегрировать гибкие цифровые инструменты, учитывающие уровень подготовки, цели и предпочтения обучающегося [3]. Наличие разнообразных адаптивных платформ и образовательных систем на базе ИИ дает свободу выбора эффективных ресурсов и позволяет экономить время и силы как обучающихся, так и образовательных организаций.

Формирование индивидуальной траектории развития – это целенаправленный многоэтапный процесс создания персонального учебного маршрута. Он учитывает исходный уровень знаний, навыков и умений обучающегося, его цели, предпочтительный стиль обучения и темп усвоения материала. Процесс начинается с диагностики: на этом этапе с помощью тестов, анкет и аналитических инструментов выявляются сильные и слабые стороны ученика, его мотивация и интересы [2]. Результаты диагностики

помогают определить, с какого материала начать обучение и какие темы требуют наибольшего внимания. Затем проводится проектирование траектории: формируется индивидуальная программа, включающая подбор учебных модулей, их последовательность и сложность, а также способы контроля знаний.

Далее начинается реализация спроектированного плана. Учащийся последовательно проходит учебные модули через цифровую образовательную платформу: изучает тексты и видеоматериалы, решает практические задачи и тесты. При обучении используются разнообразные ресурсы, например тексты, видео, симуляторы и интерактивные задания, в тех форматах, которые наиболее эффективны для данного человека [4]. Одновременно система ведет мониторинг процесса: собираются данные о прогрессе – результаты контрольных работ, время выполнения заданий, активность в системе, например посещаемость и участие в форумах. Анализ этих данных позволяет определить, какие темы даются ученику труднее и где требуются дополнительные пояснения [1].

Корректировка траектории осуществляется на основе мониторинга. При должном усвоении материала раздела учеником, система ускоряет темп: программа предложит более высокую сложность заданий после определенного количества правильных ответов и пойдет по следующим темам. Выявление систематических ошибок приведет к добавлению дополнительных объяснений или к упражнениям для исправления проблемного навыка. Этапы мониторинга, проектирования и реализации создают циклический процесс, рис. 1: результаты одного из циклов обучения будут основой при формировании плана для следующего цикла, тем самым текущие потребности ученика реализуются непрерывной адаптацией траектории [3].

В персонализации ключевую роль играют интеллектуальные технологии. В реальном времени адаптивные обучающие системы анализируют поведение и ответы ученика и подстраивают учебный контент в данный момент: при решении студентом заданий без ошибок, система включит усложненные упражнения, а при трудностях выдаст дополнительные подсказки и примеры [1]. Большие объемы данных об успеваемости обрабатываются методами машинного обучения: скрытые закономерности выявляются алгоритмами, формируются персональные рекомендации и прогнозируется прогресс [2]. Сбор данных о поведении учащихся формируется образовательной аналитикой, примеров служит активность в ЛМС, траектории прохождения курсов и результаты тестов, и оптимизирует курс:

в учебную программу могут быть внесены изменения на основе ее выводов [3]. Для подбора наиболее релевантных материалов и курсов, включая предыдущие результаты, рекомендательные системы интегрируются с учебными платформами и используют цифровой профиль ученика [4].

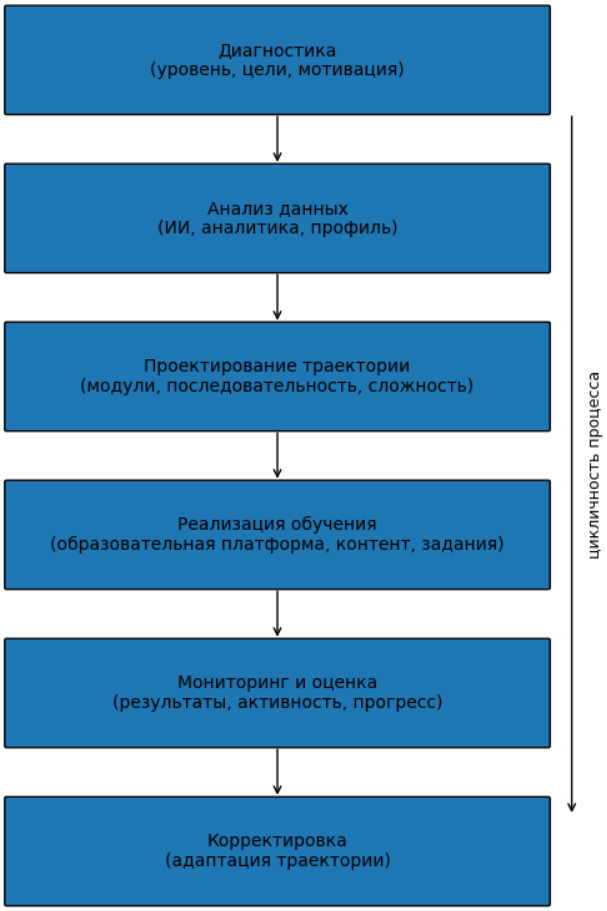


Рис. 1. Непрерывная адаптация траектории, цикл обучения

Очень важной частью для всего процесса являются специальные приемы для поддержания концентрации и мотивации. Внедряются игровые элементы геймификации, такие как таблицы лидеров, уровни, значки и баллы, в процесс образования, чтобы больше увлечь: визуальные награды и соревновательный характер мотивируют к активному участию учащихся [4]. Разбитие контента на очень короткие видеоролики или модули, по 5–10 минут, каждый из которых держит фокус на какой-то одной ключевой идее называется микрообучением; такой формат снижает информационную нагрузку и облегчает усвоение материала. Регулярное предоставление ученику данных о его успехах предполагает персонализированная обратная связь: комментарии преподавателя или автоматические подсказки в системе помогают видеть достигнутые результаты и своевременно корректировать ошибки [1]. Пройденный материал демонстрируется графиками и прогресс-барами при

помощи визуализации прогресса; видимый прогресс помогает планировать дальнейшие шаги и поддерживает мотивацию. Создают образовательное сообщество, такие как форумы, чаты, совместные проекты и наставничество, социальные механизмы: взаимопомощь и взаимодействие среди преподавателей и учащихся делают процесс обучения менее изолированным и укрепляют вовлеченность [3].

Заметные преимущества имеют интеллектуальные методы персонализации. Обучение происходит более адаптивно и эффективно: повышает качество усвоения знаний, студент проходящий учебный план, точно соответствующий его потребностям и уровню [1]. Устранения лишнего достигается за счет экономии времени: ученик фокусируется на областях вместо стандартного изучения всего курса, требующих развития, а вспомогательным материалом могут послужить знакомые темы. Поддерживает мотивацию и развивает самостоятельность гибкость системы: для каждого учебный опыт индивидуален. Однако существуют ограничения: ошибки на начальном этапе могут привести к неэффективному плану, и адаптивность зависит от точности диагностики. Требуется квалифицированные педагоги и надежная техническая инфраструктура для работы таких систем. Наконец, соблюдения норм конфиденциальности и этики, при анализе и сборе персональных данных учеников [5, 6]. Важно, остается значимой роль живого учителя: для глубокого понимания материала и эмоциональной поддержки по-прежнему важны наставничество и личное общение.

Таким образом, перспективное направление развития образования представляют собой интеллектуальные технологии формирования индивидуальной траектории. В дальнейшем образовательный процесс может расширять диагностические возможности, использование биометрических данных и учет эмоционального состояния обучающихся, внедрение обновленных форматов обучения, включая дополненную и виртуальную реальность [4]. При правильном направлении совершенствования алгоритмов аналитики и искусственного интеллекта: смогут работать с большим объемом разнотипных данных для более точного построения траекторий развития [2]. Не менее важно совершенствовать практическую реализацию – разрабатывать удобные платформы, повышать квалификацию педагогов и обеспечивать правовую и этическую безопасность применения данных технологий [5, 6]. В конечном итоге комплексное применение интеллектуальных методов может сделать образование более эффективным, доступным и мотивирующим для каждого учащегося.

Список используемых источников

1. Воронова Д. Ю. Этические аспекты использования искусственного интеллекта в образовании // Гуманитарий: актуальные проблемы гуманитарной науки и образования. 2026. [Электронный ресурс]. URL: https://giefjournal.ru/node/2407 (дата обращения: 13.01.2026).

2. Тупикова С. Е., Кучмина Е. Э. Правовые особенности внедрения искусственного интеллекта в образовательный процесс // Digital Humanities and Technology in Education. 2025. [Электронный ресурс]. URL: http://digitalmpgu.ru/wp-content/uploads/2025/05/1-2025-41-48.pdf (дата обращения: 13.01.2026).

3. Искусственный интеллект: воздействие на систему «образование» // AC Journal. 2024. URL: https://www.acjournal.ru/jour/article/viewFile/2829/2068 (дата обращения: 13.01.2026).

4. Персонализированное обучение на основе технологий искусственного интеллекта: насколько готовы современные студенты к новым возможностям получения образования // Вестник высшей школы. 2025. [Электронный ресурс]. URL: https://vovr.elpub.ru/jour/article/view/5367/0 (дата обращения: 13.01.2026).

5. Левин Б. А., Пискунов А. А., Поляков В. Ю., Савин А. В. Искусственный интеллект в инженерном образовании // Высшее образование в России. 2022. Т. 31. № 7. С. 79–95. DOI: 10.31992/0869-3617-2022-31-7-79-95.

6. Матузак А. Ф., Павлова О. Ю., Носова Л. С., Велиева Л. Ф., Салимова И. М. Роль искусственного интеллекта и цифровых технологий в высшем образовании // Russian Journal of Education and Psychology. 2025. Т. 16. № 2. С. 73–94. DOI: 10.12731/2658-4034-2025-16-2-731.

УДК 004.94:514.18

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ВИЗУАЛИЗАЦИИ СТЕРЕОМЕТРИЧЕСКИХ ЗАДАЧ: ОБЗОР И АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

Сатуев Э. А. (студент группы ИСТ-222 СПбГУТ), satuev.ea@sut.ru

В статье рассматривается предметная область обучения стереометрии с применением средств интерактивной 3D-визуализации на мобильных устройствах. Проведен анализ проблем, возникающих при традиционных методах преподавания данного раздела геометрии, и обоснована необходимость создания специализированного инструмента. Выполнен сравнительный анализ существующих программных продуктов по ключевым критериям: функциональности 3D-визуализации, образовательной направленности и доступности на мобильных платформах. Предложен подход к нативной разработке Android-приложения на языке Kotlin с использованием OpenGL ES 3.0 для рендеринга трехмерных объектов и архитектуры Clean Architecture + MVVM, позволяющего устранить выявленные недостатки аналогов.

стереометрия, 3D-визуализация, мобильное приложение, Android, Kotlin, OpenGL ES, образовательные технологии, геометрия

Стереометрия – один из ключевых разделов школьного курса геометрии, формирующий пространственное мышление, необходимое для последующего освоения таких дисциплин, как начертательная геометрия, компьютерная графика и инженерное проектирование [1]. Вместе с тем данный раздел традиционно считается одним из наиболее трудных для восприятия: учащиеся испытывают затруднения при мысленном оперировании трехмерными объектами, визуализации их сечений и взаимного расположения фигур в пространстве.

Традиционные методы преподавания стереометрии – статичные чертежи в учебниках и на доске – принципиально не способны передать динамическую природу трехмерных геометрических преобразований. В условиях активной цифровизации образования интерактивная 3D-визуализация выступает перспективным инструментом преодоления этих ограничений [2]. Особую роль приобретают мобильные приложения, обеспечивающие доступность обучающих инструментов в любое время и в любом месте – в соответствии с современными тенденциями персонализированного и мобильного обучения.

Цель настоящей работы – провести обзор и анализ существующих программных решений в области визуализации стереометрических объектов,

выявить их ключевые преимущества и недостатки, а также обосновать подход к разработке специализированного мобильного приложения, устраняющего выявленные пробелы.

Проблемы изучения стереометрии и потенциал 3D-визуализации

Сложности при освоении стереометрии носят комплексный характер и затрагивают как психолого-педагогическое, так и технологическое измерение учебного процесса. На психолого-педагогическом уровне ключевой проблемой является несформированность пространственного мышления: переход от планиметрии к стереометрии представляет качественный скачок в когнитивных требованиях, к которому значительная часть учащихся оказывается не готова [3]. Абстрактные концепции – такие как угол между скрещивающимися прямыми или перпендикулярность прямой и плоскости – требуют умения отвлечься от конкретного изображения и оперировать идеализированными моделями.

На дидактическом уровне доминирование статичной визуализации существенно ограничивает возможности восприятия. Двумерный способ представления трехмерных объектов в принципе не позволяет продемонстрировать непрерывность геометрических преобразований и динамику построения сечений. Классические физические модели многогранников, имеющиеся в арсенале учителей, зачастую не дают возможности производить с ними интерактивные действия.

На технологическом уровне существующие инструменты 3D-моделирования общего назначения (AutoCAD, Blender) избыточно сложны для учебных целей и не адаптированы под специфику образовательного процесса по стереометрии [4]. Описанное противоречие между динамической природой трехмерных геометрических объектов и статичными методами их представления создает объективную потребность в специализированных образовательных инструментах.

Интерактивная 3D-визуализация способна устранить перечисленные проблемы. Ее ключевые преимущества для образовательного процесса заключаются в следующем. Во-первых, она реализует принцип наглядности на качественно новом уровне, позволяя демонстрировать динамические геометрические преобразования в реальном времени. Во-вторых, возможность непосредственного взаимодействия с трехмерной моделью – ее вращения, масштабирования, построения сечений – способствует формированию адекватных пространственных представлений. В-третьих, интерактивный

формат работы повышает мотивацию и вовлеченность учащихся, преодолевая психологические барьеры, связанные с изучением абстрактных математических концепций.

Анализ существующих программных решений

Для определения требований к разрабатываемому приложению был проведен сравнительный анализ наиболее распространенных программных продуктов, применяемых для визуализации геометрических объектов в образовательном контексте. Критерии оценки: функциональность 3D-визуализации, специализация на задачах стереометрии, образовательная направленность, наличие и полнота мобильной версии, доступность (бесплатность) и интуитивность интерфейса. Результаты анализа представлены в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ программных продуктов для визуализации стереометрических объектов

Продукт	Тип	Возможности 3D	Специализация на стереометрии	Образовательная направленность	Мобильная версия	Бесплатность
GeoGebra	Онлайн-платформа и приложение	Полнофункциональная: сечения, поверхности, вращение тел	Средняя (часть общего функционала)	Высокая, интеграция с учебными программами	Да, но ограниченный функционал	Да
Desmos 3D	Онлайн-платформа и приложение	Базовая: построение поверхностей и графиков функций	Низкая (ориентация на алгебру)	Средняя, акцент на алгебре и функциях	Да	Да
Math3D	Онлайн-платформа	Продвинутая: параметрические поверхности, объемные тела	Средняя (для высшей школы)	Средняя, ориентация на высшее образование	Нет	Да
Geometry Pad	Мобильное приложение	Ограниченная: преимущественно 2D-геометрия	Низкая (фокус на планиметрии)	Высокая, ориентация на школьников	Да (iOS, Android)	Частично
Cabri 3D	Десктоп-приложение	Высокая: построение тел, сечений, измерение	Высокая (специализация на стереометрии)	Высокая, соответствие школьной программе	Нет	Нет (платное)

Проведенный анализ позволяет выделить три характерные группы решений. Первую группу составляют универсальные образовательные платформы (GeoGebra, Desmos 3D), предоставляющие широкий функционал, однако не специализированные на задачах стереометрии [5, 6]. GeoGebra, несмотря на богатые возможности 3D-визуализации, имеет существенное ограничение в мобильной версии и не предлагает специализированного инструментария именно для работы с геометрическими телами в контексте школьной программы. Desmos 3D ориентирован в первую очередь на алгебраическое представление функций и поверхностей, а не на интерактивную работу со стереометрическими объектами [6].

Вторую группу образуют специализированные математические визуализаторы для высшей школы (Math3D), предлагающие продвинутые инструменты, но рассчитанные на студентов вузов и не учитывающие специфику школьной программы по стереометрии. Третья группа – инструменты с частичным охватом предметной области: Geometry Pad хорошо адаптирован для мобильных устройств, однако его возможности ограничены преимущественно планиметрией. Cabri 3D обладает наиболее близкой к требуемой специализацией, однако является платным настольным приложением без мобильной версии [7].

Таким образом, анализ демонстрирует наличие незаполненной ниши: на рынке отсутствует бесплатное специализированное нативное мобильное приложение для Android, сочетающее полнофункциональную 3D-визуализацию стереометрических тел с интерфейсом, адаптированным для школьников.

Предлагаемый подход к разработке приложения

На основе выявленных пробелов в существующих решениях была определена концепция разрабатываемого приложения. Его отличительными особенностями являются: специализация исключительно на задачах школьной стереометрии; полнофункциональная нативная Android-реализация без ограничений базового функционала; интуитивный интерфейс на базе Jetpack Compose, адаптированный для аудитории школьников; интерактивные инструменты построения сечений и расчета параметров геометрических тел.

В качестве технологического стека для реализации приложения выбрана нативная разработка под Android с использованием языка Kotlin

и среды Android Studio. Такой подход обеспечит максимальную производительность на целевой платформе и прямой доступ к аппаратным возможностям устройства. Минимальная поддерживаемая версия платформы – Android 8.0 (API 26), что охватывает подавляющее большинство актуальных устройств.

Для рендеринга трехмерных объектов планируется использовать OpenGL ES 3.0 через компонент GLSurfaceView [8]. Данная технология предоставит прямой доступ к графическому процессору устройства, обеспечивая высокую производительность при отображении геометрических тел и построении сечений. OpenGL ES 3.0 был выбран в сравнении с Vulkan как более широко поддерживаемая технология, совместимая со всеми Android-устройствами начиная с API 26. Геометрические тела будут реализованы через программную генерацию мешей непосредственно в шейдерах, что позволит динамически обновлять форму объектов при изменении пользователем их параметров.

Архитектура приложения будет построена по принципу Clean Architecture в сочетании с паттерном MVVM. Такой подход обеспечит четкое разделение ответственности между слоями: слой представления будет реализован на Jetpack Compose и содержать только логику отображения UI-элементов поверх 3D-сцены; слой ViewModel будет управлять состоянием через Kotlin StateFlow и обрабатывать пользовательский ввод; слой доменной логики включит use cases для операций с геометрическими объектами, расчета параметров и построения сечений; слой данных будет отвечать за хранение и загрузку параметров геометрических тел. Управление зависимостями планируется осуществить посредством Dagger Hilt, асинхронные операции – на базе Kotlin Coroutines.

Управление трехмерной сценой планируется реализовать через стандартные жесты: смахивание для вращения объекта, жест «pinch» для масштабирования и двойное касание для сброса положения камеры. Элементы управления и информационные панели будут реализованы на Jetpack Compose и отображаться поверх GLSurfaceView, обеспечивая единый и современный визуальный стиль [9]. Реактивное управление состоянием через Kotlin Flows обеспечит мгновенное обновление интерфейса при любом изменении параметров отображаемых объектов. Ключевые характеристики разрабатываемого приложения в сравнении с лучшими аналогами приведены в таблице 2.

ТАБЛИЦА 2. Характеристики разрабатываемого приложения в сравнении с ключевыми аналогами

Характеристика	GeoGebra	Cabri 3D	Разрабатываемое приложение
Специализация на школьной стереометрии	Частичная	Высокая	Высокая
Полноценная мобильная версия (Android)	Ограниченная	Нет	Да (нативная)
Технология рендеринга 3D	WebGL / Canvas	Проприетарный движок	OpenGL ES 3.0
Построение сечений	Есть	Есть	Есть
Расчет параметров тел	Частичный	Есть	Есть
Современный UI (Jetpack Compose)	Нет	Нет	Да
Бесплатность	Да	Нет	Да

Разрабатываемое приложение призвано устранить выявленный разрыв между функциональными требованиями образовательного процесса по стереометрии и возможностями существующих инструментов. В отличие от GeoGebra, оно будет целиком сфокусировано на задачах стереометрии и обеспечит полноценный нативный Android-опыт без ограничений функционала. В отличие от Cabri 3D, оно будет доступно бесплатно и реализовано как нативное приложение с современным интерфейсом на Jetpack Compose и жестовым управлением, привычным для современных школьников.

Перспективы дальнейшего развития проекта включают расширение библиотеки геометрических объектов, добавление инструментов для работы с координатами в пространстве, интеграцию с образовательными платформами, а также поддержку технологий дополненной реальности средствами ARCore, что позволит создать еще более наглядную среду для изучения стереометрии.

Список используемых источников

1. Михайлова Л. В. Компьютерная визуализация данных. URL: https://scienceforum.ru/2016/article/2016025747 (дата обращения: 27.11.2025).

2. Голованов Н. Н. Геометрическое моделирование: учебник. М.: Издательский центр «Академия», 2011.272 с.

3. Ласло М. Вычислительная геометрия и компьютерная графика на C++. М.: Бином, 2004.

4. Боресков А. В., Шикин Е. В. Компьютерная графика. Полигональные модели.М.: «ДиалогМИФИ», 2001.

5. GeoGebra 3D Graphing Calculator. URL: https://www.geogebra.org/3d (дата обращения: 15.03.2026).

6. Desmos 3D. URL: https://www.desmos.com/3d (дата обращения: 15.03.2026).

7. Cabri 3D. URL: https://www.cabri.com (дата обращения: 15.03.2026).

8. Android Developers. OpenGL ES. URL: https://developer.android.com/guide/topics/graphics/opengl (дата обращения: 20.03.2026).

9. Android Developers. Jetpack Compose. URL: https://developer.android.com/jetpack/compose (дата обращения: 20.03.2026).

Статья представлена и. о. заведующего кафедрой СОД СПбГУТ, кандидатом технических наук, доцентом Ю. М. Бородянским.

УДК 004.891.2

ПСИХОМЕТРИЯ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: МОЖНО ЛИ АЛГОРИТМАМ ДОВЕРИТЬ ОЦЕНКУ ЛИЧНОСТИ

Д. А. Старков (студент группы МТД-2521 СПбГУТ), starkov.da@sut.ru

В данной статье рассматриваются различные методы психометрии, использующиеся для оценки кандидатов. Проведено исследование современных технологий искусственного интеллекта в HR-сфере, а также выявлены ключевые проблемы их использования. В результате обоснована концепция гибридных моделей, в которых ИИ выполняет первичную оценку, а финальное решение остается за менеджером по управлению персоналом.

психометрия, модели оценки, искусственный интеллект, оценка компетенций, управление персоналом, гибридные системы

В настоящее время мы живем в эпоху, где искусственный интеллект уже используется практически во всех сферах нашей жизни, он постоянно развивается и захватывает все новые и новые сферы нашей повседневности. Раньше казалось, что непосредственное оценивание личности кандидата, менеджером по управлению персоналом, никогда не будет заменено машиной. Однако, что же мы видим сейчас? ИИ это уже непросто «анализатор текста», а полноценный мощный инструмент, способный считывать эмоции и психологическое состояние по видеозаписи с голосом, после чего проводить различного рода анализы и выдавать собранную информацию о кандидате. Однако личность, все-таки нечто сложное и непостижимое, требующее для анализа таких человечески качеств, как эмпатия или, например страх, которых априори не может быть у машины. Таким образом, цель данной статьи заключается в рассмотрении методов психометрии, внедряемые в ИИ-системы и оценивании насколько они соответствуют требованиям объективности, научной обоснованности и этики [1-5].

Психометрия представляет собой науку, которая изучает, как измерять психические процессы и особенности человека. С помощью специальных тестов психологи определяют черты личности, способности, мотивацию и поведенческие модели. Это помогает понять, как внутренние характеристики человека влияют на его поведение и принятие решений [5]. В управлении персоналом она используется для перевода качественных характеристик личности в форму переменных, для удобного и качественного анализа, сравнения и интерпретации.

Качество любого психометрического инструмента определяется совокупностью критериев, среди которых ключевое значение имеют:

- надежность понимается как устойчивость измерительной процедуры к случайным погрешностям;
- валидность отражает степень соответствия измерительного инструмента измеряемому конструкту;
- стандартизация предполагает унификацию процедур проведения, обработки и интерпретации результатов.

В современной психометрике сложилось множество подходов к тому, как структурировать и оценивать личностные характеристики. Выделяют две самые популярные и большие модели, это диспозициональные и типологические [3]. Их основное различие заключается в том, что первые описывают личность через непрерывные черты на шкале, а вторые через четкие дискретные категории людей. В свою очередь, ниже представлена таблица (табл. 1), самых популярных и применяемых на практике моделей оценки персонала.

ТАБЛИЦА 1. Модели оценки персонала

Модель	Структура
Big Five (OCEAN)	Пять суперфакторов: открытость опыту, добросовестность, экстраверсия, доброжелательность, нейротизм [3]. Каждый фактор включает ряд более узких граней
16 PF	Шестнадцать биполярных факторов: замкнутость – общительность, конкретное мышление – абстрактное, эмоциональная нестабильность – стабильность
MBTI (Майерс-Бриггс)	Четыре биполярные шкалы: экстраверсия – интроверсия, сенсорика – интуиция, мышление – чувство, суждение – восприятие. Комбинации формируют 16 типов личности
DISC	Четыре поведенческих стиля: доминирование, влияние, стабильность, добросовестность. Результаты визуализируются в виде круговой диаграммы с комбинациями стилей
Hogan Assessment Systems	Трехуровневая структура: «светлая сторона» (повседневная личность, аналог Big Five), «темная сторона» (дезадаптивные черты, проявляющиеся в стрессовых ситуациях), «мотивы и ценности» (внутренние драйверы и предпочтения)

Все представленные выше модели имеют свою плюсы и минусы, различаются п остепени научной обоснованности и другому, однако на практике в основном выбор осуществляется по большей степени из-за традиций

компании или требований заказчика. В ИИ-системах в основном используется Big Five модель, так как ее черты образуют многомерное пространство с непрерывными значениями, которые удобны для алгоритмов и прогнозов.

В современных HR-платформах используется большое количество разных технологий, которые в совокупности образуют целый комплекс. Одним из самых распространенных направлений является обработка естественного языка [4]. Оно способствует семантическому и стилистическому анализу текста, а на основе собранной информации уже строятся предположения о личности кандидата. Данный инструмент ИИ наиболее понятен и развит в данный момент, так как дольше всех находится в использовании.

В настоящий момент активно развивается технология видеоинтервьюирования. Такой инструмент не только считывает то, что говорит кандидат, но и оценивает мимику, движения глаз, реакцию на вопросы и многие другие микровыражения. По заявлениям разработчиков, некоторые такие системы распознают до 1000 параметров лица. В дополнение к этому идут алгоритмы акустического анализа речи, которые могут точно определить: темп, интонации, паузы и многое другое, что в совокупности с анализом видеоряда может давать фантастические результаты по оценке компетенций кандидата.

Отдельную категорию составляют геймифицированные платформы [1]. В рамках такого подхода кандидат выполняет серию игровых заданий, а алгоритмы ИИ оценивают поведенческие метрики, такие как скорость реакции, импульсивность, склонность к риску и многое другое. Диагностика происходит исключительно в игровом формате без текстовых вопросов. Таким образом, кандидат погружается в процесс и забывает, что на самом деле проходит интервью, тем самым увеличивается шанс более точной оценки кандидата.

Совокупность всех вышеперечисленных технологий показывает развитие тренда на оценку по поведенческим и биометрическим данным, нежели по самоотчету кандидата. Однако, именно этот переход порождает комплекс проблем, связанных с обоснованностью, прозрачностью и этическими границами применения подобных систем. В первую очередь возникает вопрос психометрической валидности данных. В отличии от классической, где эксперты обосновывают каждый показатель теоретически и эмпирически, в ИИ-системах связь зачастую строится на корреляциях (ускорилась речь значит человек нервничает), что не всегда является правильным.

Еще одной не менее важной проблемой является, предвзятость данных и дискриминационный потенциал. Искусственный интеллект обучается людьми, у которых первоначально могут быть стереотипы, которые в дальнейшем перенесутся и на алгоритм. Культурные различие также могут мешать объективному оцениванию, например взгляд в глаза, в некоторых культурах признак уверенности, а в других враждебность. Все это мешает алгоритму объективно оценивать кандидатов и делает роль менеджера по управлению персоналом незаменимым.

В-третьих, проблема прозрачности. Модели глубокого обучения работают как «черный ящик», не давая доступа к логике решений. В свою очередь, в традиционной психометрии, выводы являются чуть ли не ключевой составляющей анализа.

И наконец, этическая сторона вопроса, которая вызывает особую озабоченность, так как сбор биометрических данных требует согласия, которое на практике часто оформляется формально, без разъяснения кандидату сути процедуры. Кроме того, алгоритмические системы, в отличие от классической психометрии, оптимизированы прежде всего на экономическую эффективность отбора, пренебрегая рисками ошибочной классификации и долгосрочными последствиями для карьеры кандидатов.

Перечисленные проблемы не означают отказа от ИИ в психометрической оценке компетенций, но требуют пересмотра самого подхода. Наиболее реалистичным сценарием выступают гибридные модели, где алгоритм выполняет первичную фильтрацию, а финальное решение остается за HR-специалистом, сохраняющим человеческое мышление. Также необходимо параллельно установить стандартизация прозрачности, обязывающую объяснять, какие именно признаки повлияли на результат. А на уровне компании грамотно доводить информацию до кандидатов, с правом на отказ от биометрического анализа или получение объяснений по результатам анализа. Все это в совокупности позволит, уменьшить все возможные риски, и использовать искусственный интеллект на максимум.

Исходя из всего вышесказанного, в настоящий момент методы психометрии, применяемые в ИИ-системах, не могут полностью обеспечить соблюдения всех необходимых требований при оценке кандидатов, однако нецелесообразно, игнорировать интеграцию данных областей. Оптимальным путем развития технологий для управления персоналом, являются гибридные модели, сочетающие все лучшее от алгоритмов и человеческого мыш-

ления. Только при таком подходе искусственный интеллект станет не проблемой на рынке подбора персонала, а будет надежным инструментом в руках профессиональных HR-менеджеров.

Список используемых источников

1. Геймификация для HR: мировые практики и советы по внедрению // topcareer URL: https://top-career.ru/blog/gamification_in_hr (дата обращения: 03.04.2026).

2. Диспозициональное направление в теории личности: Гордон Олпорт, Рэймонд-Кеттел и Ганс Айзенк // StudFiles URL: https://studfile.net/preview/3235081/ (дата обращения: 03.04.2026).

3. Модель Большая пятерка // Психологические тесты онлайн. URL: https://psytests.org/big5/bigfive.html (дата обращения: 04.04.2026).

4. Основы Natural Language Processing для текста // Хабр URL: https://habr.com/ru/companies/Voximplant/articles/446738/ (дата обращения: 04.04.2026).

5. Психометрия: что это такое и как ее использовать в работе психолога // ПЕДСОВЕТ: Журнал АккадемСити URL: https://pedsovet.org/article/psihometria-cto-eto-takoe-i-kak-ee-ispolzovat-v-rabote-psihologa (дата обращения: 04.04.2026).

Статья представлена научным руководителем, кандидатом педагогических наук, доцентом кафедры ИКД СПбГУТ, доцентом А. А. Шияном.

УДК 004.624

РАЗРАБОТКА КОНВЕЙЕРА ДЛЯ МАШИННОГО ОБУЧЕНИЯ ПО ПОДГОТОВКЕ И ВЕРСИОНИРОВАНИЮ ДАТАСЕТОВ С ИСПОЛЬЗОВАНИЕМ GIT И DVC

И. П. Тихиня (студент группы ИКТК-21 СПбГУТ) tihinya.ip@sut.ru
Р. И. Пупцев (старший преподаватель кафедры ИКС)
М.А. Шальнов (студент группы ИКТК-21 СПбГУТ)

В статье представлена архитектура и реализация конвейера подготовки данных на базе связки Git и DVC (Data Version Control). Предложенное решение обеспечивает детерминированную предобработку, автоматическое версионирование тяжелых файлов и прозрачное отслеживание зависимостей между этапами трансформации.

Data Version Control, Git, конвейер данных, версионирование датасетов, MLOps, воспроизводимость экспериментов

1. Введение

В условиях стремительного развития методов машинного обучения воспроизводимость экспериментов и управление жизненным циклом данных становятся критически важными. Традиционные системы контроля версий, такие как Git, оптимизированы для текстовых файлов и исходного кода, но неэффективны при работе с бинарными и тяжелыми артефактами. Это приводит к раздуванию репозиториев, потере истории изменений данных и невозможности гарантировать, что модель была обучена именно на зафиксированной версии датасета

Современные проекты в области Data Science и Machine Learning характеризуются высокой динамичностью: меняются источники данных, обновляются алгоритмы предобработки, корректируются гиперпараметры. Без системного подхода к версионированию всех этих компонентов возрастает риск потери воспроизводимости ранее полученных результатов, что снижает доверие к модельным решениям и усложняет их внедрение для решения реальных задач. Система версионирования позволяет обеспечить прозрачность, управляемость изменений и устойчивость развертывания моделей, что делает ее необходимым элементом архитектуры MLOps-пайплайнов [1].

Целью данной работы является разработка конвейера, который превращает сырые метеорологические данные и исторический каталог лавин в версионированный, готовый к обучению модели датасет. Главный инструмент – DVC, интегрированный с Git, что позволяет разделить хранение кода и тяжелых артефактов, сохраняя при этом полную воспроизводимость процесса [2].

2. Архитектура и структурная схема взаимодействия

Структурная схема репозитория демонстрирует последовательный поток данных от источников к целевому ML-репозиторию. Источниками выступают СУБД PostgreSQL (погодные данные) и внешний каталог лавин, изучаемой локации. Данные поступают в репозиторий предобработки, где набор скриптов объединен в DVC-пайплайн. Каждый этап принимает на вход зависимости (deps), выполняет преобразования и создает артефакты (outs). Происходит автоматическое хранение и отслеживание данных благодаря кэшированию выходных файлов, создаются .dvc-указатели и фиксируется состояние конвейера в dvc.lock. Git отслеживает только конфигурационные файлы и код. Взаимодействие элементов строго детерминировано: изменение на любом этапе автоматически пересчитывает хэши зависимых стадий, а DVC выполняет только те шаги, выходные хэши которых изменились.

3. Стадии конвейера предобработки

Пайплайн разбит на четыре логически изолированные стадии, каждая из которых решает конкретную задачу преобразования данных.

dvc.yaml - dvc.yaml file (schema.json)

```yaml
# ex_to_csv → convert_export_to_csv
# merge_true → merge_with_labels
# live_preprocess → build_features
stages:
  export_from_database:
    cmd: py src_preprocess/SuperExport.py src_preprocess/env data/raw/Khibiny_exported.csv
    always_changed: true
    deps:
      - src_preprocess/SuperExport.py
      - src_preprocess/env
    outs:
      - data/raw/Khibiny_exported.csv
  ex_to_csv:
    cmd: py src_preprocess/ExcToCsv.py data\raw\Result_Lavina_ExcToCsv.csv data/raw/Khibiny_exported.csv
    deps:
      - src_preprocess/ExcToCsv.py
      - data/raw/Khibiny_exported.csv
    outs:
      - data\raw\Result_Lavina_ExcToCsv.csv
  merge_true:
    cmd: py src_preprocess/MergeTrue.py data\raw\Result_Lavina_ExcToCsv.csv data\raw\Dataset_Raw_For_Prepare.csv
    deps:
      - src_preprocess/MergeTrue.py
      - data\raw\Result_Lavina_ExcToCsv.csv
    outs:
      - data\raw\Dataset_Raw_For_Prepare.csv
  live_preprocess:
    cmd: py src_preprocess/live_preprocess.py data\raw\Dataset_Raw_For_Prepare.csv data/processed/Khibiny_Dataset.csv
    deps:
      - src_preprocess/live_preprocess.py
      - data\raw\Dataset_Raw_For_Prepare.csv
    outs:
      - data/processed/Khibiny_Dataset.csv
```

Рис. 1. Стадии пайплайна в файле dvc.yaml

На рис. 1 представлены все стадии предобработки данных, которые на выходе дают готовый предобработанный датасет для дальнейшего его использования моделями машинного обучения.

Задачи решаемые пайплайном:

1. Экспорт сырых погодных данных из PostgreSQL. Скрипт подключается к БД, выполняет SQL-запросы с фильтрацией по временным окнам и географическим координатам. Результат выгружается в репозиторий.

2. Преобразование и стандартизация файла каталога лавин. Исторический каталог приводится к единой схеме: парсинг дат, нормализация единиц измерения, удаление дубликатов и некорректных записей.

3. Сопоставление каталога и погодных данных. Даты и координаты сходов лавин сопоставляются с ближайшими метеоданными. Результат: объединенный сырой датасет с размеченными лавинами по часам или дням, в зависимости от задачи.

4. Предобработка объединенного датасета. Финальная стадия включает обработку пропусков, учет дисбаланса классов (SMOTE или взвешивание), One-Hot Encoding категориальных признаков, масштабирование числовых данных. Итоговый файл экспортируется в DVC remote хранилище (заранее настроенное), и может быть запрошено из ML-репозитория с моделями.

4. Механизмы версионирования: dvc.yaml, dvc.lock и хеширование

Файл dvc.yaml выступает инструкцией пайплайна. В нем описываются стадии, команды их запуска, зависимости (deps) и выходные файлы (outs). После запуска команды dvc repro DVC выполняет все стадии последовательно, вычисляет хэши входных зависимостей и выходных файлов, и записывает их в dvc.lock. Данный файл содержит точные хэши всех зависимостей и выходов каждой стадии, выступая снимком состояния пайплайна. Если при повторном запуске хэши в dvc.lock совпадают с текущими, DVC пропускает выполнение стадии, что подтверждается консольным выводом на рис. 2 «Stage '...' didn't change, skipping» и экономит вычислительные ресурсы.

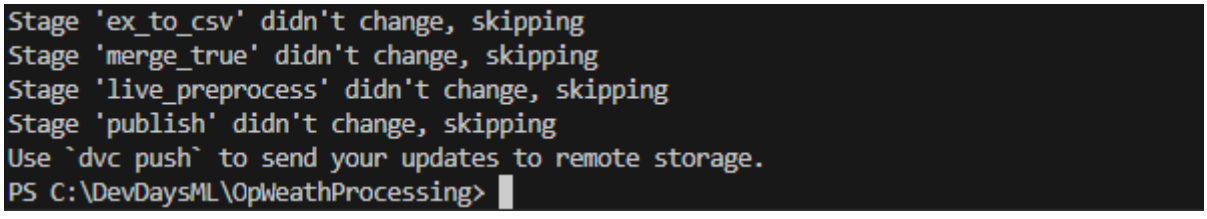


Рис. 2. Консольный вывод команды dvc repro при неизмененных хэшах в dvc.lock

DVC использует content-addressable storage. При добавлении файла вычисляется его криптографический хэш (по умолчанию MD5). Файл копируется в локальный кэш .dvc/cache/, где структура каталогов определяется хэшем: первые два символа формируют поддиректорию, остаток становится именем файла. Это предотвращает коллизии имен и ускоряет поиск. В репозитории Git хранится лишь легковесный .dvc-файл с хэшем (маловесной ссылкой на тяжелый файл), а не сам датасет. При dvc pull DVC по хэшу восстанавливает файл из кэша или удаленного хранилища. Таким образом, код и легкие конфигурации хранятся в Git, а тяжелые файлы находятся под управлением DVC, что позволяет репозиторию оставаться компактным при полной воспроизводимости [3].

5. Заключение и перспективы развития

Разработанный конвейер решает ключевые задачи data engineering: обеспечивает последовательную предобработку, автоматическое версионирование датасетов, отслеживание зависимостей и экономию ресурсов за счет механизмов кэширования и использования файлов .dvc. Интеграция Git и DVC гарантирует, что в любое время можно восстановить точную версию данных, на которой обучалась модель и экспериментировать с результатами предсказаний.

Следующим этапом разработки станет создание специализированного репозитория-поставщика данных. Механизм работы: каждые 15 минут опрашивать внешние источники, валидировать входящие данные и автоматически приводить поток к строго заданному формату, ожидаемому моделью на входе (те же признаки, порядок столбцов, типы данных, масштабирование) [4].

Список используемых источников

1. Scott Chacon, Ben Straub // Pro Git // Version 2.1.448, 2025-07-25 URL: https://git-scm.com/book/en/v2/ (дата обращения: 27.10.2025)

2. DVC Documentation. URL: https://dvc.org/doc/ (дата обращения: 20.05.2024).

3. Lakshmanan V., Robinson S., Munn M. Machine Learning Design Patterns. O'Reilly Media, 2020. 312 p.

4. Treveil M. et al. Data Management for Machine Learning with DVC and Git // Proc. of the Int. Conf. on MLOps. 2023. P. 112–119.

КИБЕРБЕЗОПАСНОСТЬ

УДК 004.75

АНАЛИЗ ВЛИЯНИЯ АРХИТЕКТУРЫ РАЗМЕЩЕНИЯ ИИ-НАГРУЗОК НА ДОСТУПНОСТЬ СЕРВИСОВ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

Т. А. Абзалов (студент группы ИБС-22 СПбГУТ), abzalov.ta@sut.ru

В работе рассматривается влияние архитектуры размещения ИИ-нагрузок на доступность сервисов в центрах обработки данных. Показано, что рост требований к памяти и подсистеме хранения может приводить к увеличению задержек и снижению устойчивости сервисов при нерациональном распределении ресурсов. Рассматриваются поэтапная подгрузка данных модели, выборочная активация параметров, уменьшение общего объема модели и квантование. Сопоставление выполнено по критериям, значимым для инфраструктуры ЦОД: выигрышу по памяти, влиянию на задержки, зависимости от локального накопителя, доступности сервисов и сложности внедрения.

центры обработки данных, ИИ-нагрузки, доступность сервисов, архитектура размещения, устойчивость сервисов, локальный накопитель; квантование

Современные центры обработки данных используются не только для размещения виртуальных машин, баз данных и прикладных сервисов, но и для выполнения задач искусственного интеллекта. Расширение применения ИИ-сервисов приводит к росту нагрузки на серверные узлы и повышает требования к вычислительным ресурсам, прежде всего к оперативной памяти и видеопамяти [1].

Для инфраструктуры ЦОД это означает не только увеличение вычислительной нагрузки, но и рост риска снижения устойчивости сервисов при нерациональном распределении ресурсов. Чем больше памяти требует модель, тем выше стоимость серверного узла и тем меньшее число сервисов может быть размещено на одном физическом сервере. Дополнительная нагрузка при этом ложится не только на вычислительную часть, но и на локальные накопители, сеть, питание и охлаждение. В результате задача раз-

мещения ИИ-нагрузок выходит за рамки простой оптимизации производительности и становится связанной с обеспечением устойчивой и предсказуемой работы сервисов [2, 3].

С точки зрения доступности критическим становится не только общий объем выделенных ресурсов, но и способ размещения модели на вычислительном узле. Перегрузка памяти, избыточные задержки при обращении к накопителю и неудачная архитектура выполнения модели могут приводить к увеличению времени отклика, снижению плотности размещения сервисов и, как следствие, к ухудшению доступности ИИ-сервисов в ЦОД. По этой причине технологии снижения потребления памяти целесообразно рассматривать не только как средство повышения эффективности, но и как один из факторов поддержания устойчивости сервисов.

Рассматриваемые подходы различаются механизмом работы и по-разному влияют на характеристики серверного узла. Поэтапная подгрузка данных модели предполагает, что часть параметров не хранится постоянно в RAM или VRAM, а извлекается по мере выполнения отдельных этапов вычислений. За счет этого уменьшается объем памяти, занятый моделью в каждый момент времени, но одновременно возрастает зависимость от характеристик локального накопителя. При недостаточной скорости чтения такой подход может приводить к росту задержки ответа и, следовательно, к снижению устойчивости сервиса под нагрузкой [4].

Выборочная активация параметров модели строится по другому принципу: при обработке запроса используется не вся модель целиком, а только необходимая часть параметров. Это позволяет уменьшить текущую нагрузку на память и вычислительные ресурсы. В отличие от поэтапной подгрузки такой подход в меньшей степени зависит от накопителя, однако требует более сложной архитектурной организации модели и ее исполнения. В условиях ЦОД это важно с точки зрения сопровождения и предсказуемости поведения сервиса при изменении нагрузки.

Подход, связанный с уменьшением общего объема модели, направлен на сокращение числа данных, которые требуется постоянно хранить и обрабатывать. Снижение требований к памяти в этом случае достигается без регулярного обращения к внешнему хранилищу, поэтому результат обычно оказывается более стабильным с точки зрения задержек. Вместе с тем выигрыш по памяти, как правило, ниже, чем в подходах, где часть данных модели выносится за пределы основной памяти [4].

Квантование основано на переводе параметров модели в формат с меньшей разрядностью. За счет этого уменьшается объем памяти, необходимый для хранения модели, и снижается нагрузка на подсистему памяти при вычислениях. Для ЦОД такой подход важен не только как способ экономии ресурсов, но и как средство повышения плотности размещения сервисов без существенного роста задержек. Ограничением при этом остается возможное влияние на точность результатов [5].

Сравнение перечисленных подходов имеет смысл только в привязке к параметрам, важным для доступности сервисов в инфраструктуре ЦОД. Поэтому для сопоставления выбраны следующие критерии: выигрыш по памяти, влияние на задержки, зависимость от локального накопителя, влияние на доступность сервисов и сложность внедрения. Под влиянием на доступность понимается то, насколько выбранный подход способствует сохранению устойчивой и предсказуемой работы сервиса при увеличении нагрузки и ограниченности ресурсов вычислительного узла.

ТАБЛИЦА 1. Сравнение подходов к размещению ИИ-нагрузок с точки зрения доступности сервисов в ЦОД

Подход	Выигрыш по памяти	Влияние на задержки	Зависимость от локального накопителя	Влияние на доступность сервисов	Сложность внедрения
Поэтапная подгрузка данных модели	высокий	возможно заметное увеличение	высокая	высокое при быстром накопителе	средняя
Выборочная активация параметров модели	средний или высокий	умеренные	низкая	среднее или высокое	высокая
Уменьшение общего объема модели	средний	низкие	низкая	среднее	средняя
Квантование	высокий	низкие или умеренные	низкая	высокое	средняя

Из таблицы 1 видно, что наибольший выигрыш по памяти дают поэтапная подгрузка данных модели и квантование. Однако для ЦОД важен не только объем сэкономленной памяти, но и то, как выбранный подход влияет на задержки, зависимость от локального накопителя и доступность сервиса.

Поэтому такие решения нужно оценивать не отдельно от инфраструктуры, а с учетом конфигурации серверного узла и характера рабочей нагрузки.

Для сервисов, где важна стабильная задержка ответа, предпочтительнее использовать квантование или умеренное уменьшение общего объема модели. Эти варианты не требуют постоянного обращения к локальному накопителю, поэтому время отклика меньше зависит от скорости чтения данных. Для интерактивных ИИ-сервисов это особенно важно, так как пользователь может заметить даже небольшой рост задержки, особенно если сервис используется часто или обрабатывает много запросов подряд [5].

Поэтапная подгрузка данных модели целесообразна прежде всего тогда, когда основное ограничение связано именно с объемом памяти. Например, если на одном серверном узле требуется разместить несколько экземпляров модели или увеличить число одновременно обрабатываемых запросов без перехода на более дорогое оборудование. При наличии быстрого NVMe-накопителя часть параметров можно вынести за пределы RAM или VRAM и подгружать их в процессе выполнения. В такой ситуации схема помогает экономнее использовать память. Но при недостаточной производительности локального накопителя эффект может оказаться обратным: экономия памяти будет сопровождаться нестабильным временем отклика и риском нарушения устойчивой работы сервиса.

Выборочная активация параметров является более сложным, но достаточно гибким вариантом. Она может быть полезна в многопользовательских сценариях, когда нагрузка меняется во времени и ресурсы приходится распределять между несколькими потоками запросов. С точки зрения доступности это помогает поддерживать работу сервиса при изменяющейся нагрузке. Основной недостаток заключается в более сложной реализации, настройке и дальнейшем сопровождении [4].

Для типовой инфраструктуры ЦОД наиболее практичным решением остается квантование. Оно не требует обязательного вынесения части параметров на накопитель, сравнительно проще внедряется и позволяет увеличить плотность размещения ИИ-сервисов на сервере. Это удобно при масштабировании уже работающего сервиса, когда требуется снизить требования к памяти без полной переработки модели и без существенного изменения логики ее выполнения.

По результатам сравнения можно сформулировать несколько практических правил выбора. Если главная проблема связана с нехваткой RAM или VRAM, в первую очередь стоит рассматривать поэтапную подгрузку

данных и квантование. Если для сервиса важна низкая задержка, более подходящими являются квантование и уменьшение общего объема модели, так как они меньше зависят от операций чтения с накопителя. Наличие быстрого NVMe-накопителя делает поэтапную подгрузку более оправданной. При высоких требованиях к простоте внедрения и сопровождения целесообразнее использовать квантование или прямое уменьшение объема модели.

При размещении ИИ-нагрузок в ЦОД нельзя ориентироваться только на расход памяти. Один и тот же вариант может хорошо работать на одном сервере и оказаться менее эффективным на другом, если отличаются объем доступной памяти, скорость накопителя или характер нагрузки. Способ оптимизации следует выбирать с учетом конкретных условий: доступного объема RAM или VRAM, допустимой задержки, наличия быстрого локального накопителя и числа обслуживаемых запросов. При проектировании инфраструктуры для ИИ-сервисов важно учитывать не только экономию ресурсов, но и устойчивость работы сервиса при реальной нагрузке.

Список используемых источников

1. Uptime Institute AI Infrastructure Survey 2025 [Электронный ресурс]. URL: https://nextdc.com/hubfs/Uptime%20Institute%20AI%20Infrastructure%20Survey%202025.pdf (дата обращения: 03.04.2026).

2. Тютляева Е. О., Одинцов И. О., Московский А. А., Мармузов Г. В. Тенденции развития вычислительных узлов современных суперкомпьютеров // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2019. Т. 8. № 3. С. 92–114. URL: https://cyberleninka.ru/article/n/tendentsii-razvitiya-vychislitelnyh-uzlov-sovremennyh-superkompyuterov (дата обращения: 03.04.2026).

3. Гуз И. Д., Острейковский В. А. Анализ эксплуатационной надежности оборудования центра обработки данных крупной компании // Надежность и качество сложных систем. 2019. № 4 (28). С. 87–93. DOI: 10.21685/2307-4205-2019-4-9.

4. Gemma 3n model overview [Электронный ресурс] // Google AI for Developers. URL: https://ai.google.dev/gemma/docs/gemma-3n (дата обращения: 03.04.2026).

5. Татарникова Т. М., Раскопина А. С. Анализ эффективности постобучающего квантования для оптимизации нейронных сетей // Наукоемкие технологии в космических исследованиях Земли. 2025. Т. 17. № 2. С. 4–10. DOI: 10.36724/2409-5419-2025-17-2-4-10.

Статья представлена научным руководителем, старшим преподавателем кафедры ИБКС СПбГУТ М. А. Скорых.

УДК 004.056.53

РАЗРАБОТКА ТРЕБОВАНИЙ К МЕТОДИКЕ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ ВЕБ-САЙТА НА СООТВЕТСТВИЕ 152-ФЗ

С. Алькаттан (аспирант группы 236А-25 СПбГУТ)
Г. Мано (студент группы ИКТБ-47м СПбГУТ)
А. В. Никифоров (студент группы ИКТБ-47м СПбГУТ),
nikiforov_av@sut.ru

Обеспечение защиты персональных данных на веб-сайтах – прямая обязанность операторов по 152-ФЗ. Практика показывает, что ручной контроль соблюдения норм закона неэффективен при масштабировании, а готовые программные решения фрагментарны. Цель данной работы – определить состав требований к методике автоматизированной проверки веб-ресурсов на соответствие законодательству о персональных данных. Изменения, касающиеся локализации баз данных, получения согласий, внешней аналитики и трансграничной передачи данных, требуют регулярного пересмотра критериев проверки.

152-ФЗ, персональные данные, информационная безопасность, автоматизированная проверка

Требования к методике автоматизированной проверки веб-сайтов на соответствие 152-ФЗ должны охватывать четыре категории: организационные меры, технические меры защиты, каналы передачи данных и периодичность контроля. Категории представляют собой укрупненные блоки оценки, а параметры – конкретные проверяемые признаки внутри каждого блока. В рамках организационных мер автоматизированная система должна проверять следующие параметры.

1. Политика обработки персональных данных. Документ должен быть размещен на сайте в виде отдельной страницы или файла для скачивания (PDF/HTML), доступного по прямой ссылке без необходимости авторизации. Содержание политики должно включать цели обработки, категории субъектов и перечень обрабатываемых персональных данных, правовые основания, перечень действий с персональными данными, сроки обработки и хранения, порядок уничтожения, сведения о трансграничной передаче, права субъектов и способы их реализации, а также меры по защите данных (статья 18.1, часть 2) [1, 2].

2. Сведения об ответственном за организацию обработки персональных данных. Назначение такого лица оформляется внутренним приказом

оператора; при автоматизированной проверке публичной части сайта целесообразно фиксировать наличие контактных данных или канала связи для обращений субъектов персональных данных в разделе политики конфиденциальности либо в разделе «Контакты» (статья 22.1, часть 1) [1].

3. Согласия на обработку персональных данных. Формы сбора данных должны содержать отдельное поле для выражения согласия. Текст согласия должен включать наименование оператора, цели обработки, перечень обрабатываемых персональных данных, перечень действий с персональными данными, срок действия согласия и порядок его отзыва. Должна быть предусмотрена возможность отзыва согласия через личный кабинет, специальную форму на сайте или по электронной почте (статья 9, части 1 и 4) [3].

4. Информирование субъектов. На сайте должна быть опубликована информация о порядке реализации прав субъектов персональных данных: доступа к своим данным, их уточнения, блокирования, уничтожения и обжалования действий оператора. Должны быть указаны контактные данные для направления запросов. При сборе данных через формы должно отображаться краткое уведомление о целях обработки и ссылка на полный текст политики (статья 18, часть 1) [1, 4].

Организационные требования должны дополняться техническими параметрами, обеспечивающими защиту персональных данных при передаче, хранении и обработке.

К ключевым техническим параметрам относятся следующие.

- Идентификация и аутентификация – использование защищенных механизмов входа, ограничение числа неудачных попыток авторизации и завершение сессии при длительной неактивности [5].
- Разграничение доступа – предоставление доступа только в пределах служебных обязанностей, разделение пользовательского и административного интерфейсов, исключение горизонтального расширения привилегий [2].
- Регистрация событий – журналирование входов и выхода, создания, изменения, удаления и экспорта данных, а также действий администраторов; записи журналов должны быть доступны для анализа и защищены от несанкционированного изменения [6].
- Защита каналов передачи – использование HTTPS/TLS на всех страницах, где собираются или передаются персональные данные, автоматическое перенаправление с HTTP и отсутствие смешанного содержимого [7, 3].

● Шифрование при хранении – защита баз данных и резервных копий с персональными данными криптографическими средствами, хеширование паролей и раздельное хранение ключевого материала [8, 9].

● Защита инфраструктуры – своевременное обновление программного обеспечения, применение средств фильтрации сетевого трафика и регулярное резервное копирование [10].

● Систематизация категорий требований, параметров проверки, требований к реализации и критериев соответствия приведена в таблице 1.

ТАБЛИЦА 1. Категории требований, параметры проверки и критерии соответствия

Категория	Параметр	Требование	Критерий соответствия
Организационные меры	– Политика обработки ПДн – Сведения об ответственном – Согласие на обработку – Информирование субъектов	– Политика доступна без авторизации – Указан канал связи – Согласие оформлено отдельным действием – Есть ссылка на политику	– Документ найден и содержит обязательные разделы – Контакты доступны пользователю – В форме есть чекбокс – Пользователь информирован о целях и правах
Техническая защита	– Идентификация и аутентификация – Разграничение доступа – Регистрация событий – Защита хранения данных	– Защищенные механизмы входа – Доступ ограничен ролями – Значимые действия журналируются – ПДн и резервные копии защищены	– Нет слабой аутентификации – Нет избыточных прав – Ведутся записи о входе и изменении данных – Пароли не хранятся открыто
Каналы передачи данных	– HTTPS – Версия TLS – HSTS – SSL/TLS-сертификат	– Страницы с формами работают по HTTPS – Используются актуальные TLS	– Есть редирект на HTTPS – Устаревшие протоколы отключены – Заголовок HSTS

Категория	Параметр	Требование	Критерий соответствия
	– Смешанное содержимое	– Включен HSTS – Сертификат действителен – Ресурсы не загружаются по HTTP	присутствует – Сертификат соответствует домену – Mixed content отсутствует
Периодичность контроля	– Плановая проверка – Внеплановая проверка – Актуализация критериев	– Планово: не реже раза в квартал – Внепланово: при изменениях сайта – Методика обновляется при изменении законодательства	– Периодичность закреплена – Определены триггеры запуска – Версия методики актуализируется

Наконец, требования к периодичности проверок на соответствие 152-ФЗ определяют регламент проведения контрольных мероприятий – базовая проверка должна выполняться не реже одного раза в квартал, а также инициироваться внепланово при существенных изменениях в функционале сайта, смене хостинга, изменении форм сбора данных или обновлении законодательства [5].

В ходе верификации методики была установлена корреляция между числом выполненных параметров и интегральной оценкой соответствия. Параметр здесь рассматривается как отдельный проверяемый признак внутри категории требований. Рисунок 1 иллюстрирует нелинейный характер этой взаимосвязи.

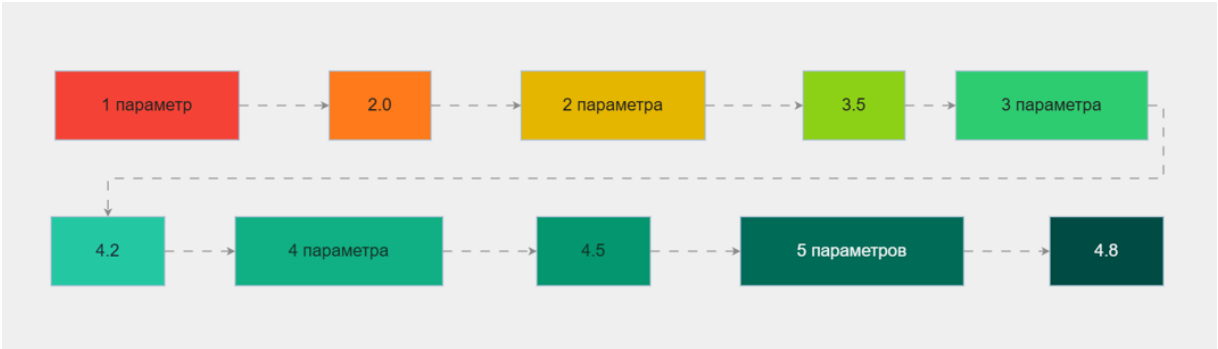


Рис. 1. Зависимость итогового балла соответствия от количества выполненных параметров

В работе сформированы требования к методике автоматизированной проверки веб-сайтов на соответствие 152-ФЗ и сгруппированы по четырем категориям: организационные меры, техническая защита, каналы передачи данных и периодичность контроля. Для каждой категории выделены параметры проверки: политика обработки ПДн, сведения об ответственном и формы согласия; механизмы аутентификации, разграничения доступа, регистрации событий и шифрования; конфигурация HTTPS/TLS и сертификата; регламент плановых и внеплановых проверок. Такое разделение категорий и параметров делает методику пригодной для программной реализации автоматизированного аудита и непрерывного мониторинга соответствия законодательству.

Список используемых источников

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261 (дата обращения 10.04.2026).

2. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке …» [Электронный ресурс] // Официальный сайт ФСТЭК. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения 10.04.2026).

3 Роль шифрования в защите персональных данных [Электронный ресурс] // B-152.ru. URL: https://b-152.ru/rol-shifrovaniya-v-zashhite-personalnykh-dannykh (дата обращения 10.04.2026).

4. Требования к политике обработки персональных данных: разъяснения Роскомнадзора [Электронный ресурс] // Роскомнадзор. URL: https://rkn.gov.ru/personal-data/ (дата обращения 10.04.2026).

5. Проверка сайтов на соответствие ФЗ-152: методические рекомендации [Электронный ресурс] // Regforum.ru. URL: https://regforum.ru/posts/2392_proverka-saytov-na-sootvetstvie-152-fz/ (дата обращения 10.04.2026).

6. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Багомедова А. Р., Ушаков И. А., Цветков А. Ю.// В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С. В. Бачевского. 2018. С. 58-63.

7. Метод обнаружения WLAN точек доступа нарушителя в распределенной ИСПДн // М. М. Ковцур, Д. В. Сахаров, Э. В. Бирих, В. Е. Дрепа // Электросвязь. 2024. № 12-2. С. 60-69. DOI 10.34832/ELSV.2024.61.12.008. EDN: SABMPS.

8. Емельянов Н. Р. Адаптация методологии защищенной разработки мобильных приложений для команд разного масштаба / Н. Р. Емельянов, М. М. Ковцур // Информационная безопасность регионов России (ИБРР-2025): Материалы XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2025. С. 468-469. EDN: HUMCJW.

9. Ковцур М. М. Организация защищенного взаимодействия распределенных сетевых устройств // М. М. Ковцур, А. А. Браницкий, Н. И. Казаков // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сборник материалов (тезисов) 51-й Международной конференции, Москва, 24–26 апреля 2023 года. Москва: ЗАО "Национальный институт радио и инфокоммуникационных технологий", 2023. С. 37-39. EDN: LJJMFV.

10. Виткова Л. А. Математическое моделирование защищенности объектов критической инфраструктуры / Л. А. Виткова, Д. А. Лебедева, Д. В. Сахаров // Региональная информатика и информационная безопасность: Сборник трудов XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2025. С. 125-127. EDN: DGBPXK.

Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом М. М. Ковцуром.

УДК 004.056

АНАЛИЗ МЕТОДОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ТИПОВЫХ АРХИТЕКТУРАХ ОБЛАЧНЫХ ИНФРАСТРУКТУР

С. О. Антипина (студент группы МЗС-2512 СПбГУТ), antipina.so@sut.ru
А. О. Манжула (студент группы ИКТБ-47м СПбГУТ), kamalova.ao@sut.ru
И. Е. Пестов (к.т.н., доцент кафедры ЗСС СПбГУТ)
П. Е. Шелкоплясова (студент группы МИБ-2512 СПбГУТ)

В этой статье рассмотрены типовые архитектуры облачных инфраструктур и некоторые алгоритмы шифрования, а также выполнен анализ исследования времени передачи данных в физической инфраструктуре и облачной инфраструктуре с использованием различных алгоритмов шифрования (Кузнечик, Магма, RSA-2048, AES-256) для защиты передаваемых данных. В результате выбран наиболее оптимальный алгоритм шифрования, который обеспечивает необходимую безопасность и не требует много времени для шифрования, дешифрования и передачи файла.

информационная безопасность, облачная инфраструктура, безопасность облаков, инфраструктура как сервис, криптография, алгоритмы шифрования

Облачная инфраструктура – это совокупность аппаратных и программных ресурсов, таких как серверы, хранилища данных и сетевое оборудование, которые используются для создания облачных вычислений [1].

Типовые архитектуры облачных инфраструктур

Облачные вычисления имеют три основные модели облачных сервисов:

- Infrastructure as a Service (далее – IaaS) – инфраструктура как услуга, например, виртуальные серверы и виртуальная сеть; клиент может устанавливать любое программное обеспечение и приложения [2, 3];
- Platform as a Service – платформа как услуга, например, веб-сервер или база данных; клиент управляет приложениями, операционной системой управляет провайдер;
- Software as a Service – программное обеспечение как услуга, например, электронная почта или иное офисное приложение; клиент пользуется приложением, базовыми настройками приложения управляет провайдер.

OpenStack – платформа облачных вычислений с открытым исходным кодом, которая поддерживает все типы облачных сред [4]. Управление происходит с помощью панели мониторинга, которая предоставляет администраторам контроль, а пользователям – возможность предоставлять ресурсы через веб-интерфейс.

OpenStack предоставляет решение IaaS с помощью различных дополнительных услуг. Каждая служба предлагает интерфейс прикладного программирования (API), который облегчает эту интеграцию.

Исследуемые алгоритмы шифрования

В данной статье используются следующие алгоритмы:

1. AES-256 – это симметричный алгоритм блочного шифрования, который работает с матрицей размером 4×4 байта (128-битный блок) и использует структуру, которая легко поддается оптимизации.

2. Кузнечик – российский стандарт симметричного блочного шифрования (ГОСТ Р 34.12-2015, ГОСТ 34.12-2018), использующий SP-сеть и предназначенный для защиты информации в системах с повышенными требованиями к криптостойкости [5].

3. Алгоритм Магма – стандартизированный алгоритм блочного шифрования, утвержденный в стандартах ГОСТ Р 34.12-2015 и ГОСТ 34.12-2018), предназначенный для обеспечения конфиденциальности информации в системах с повышенными требованиями к безопасности.

4. RSA-2048 – асимметричный алгоритм, который использует пару ключей (открытый и закрытый) для шифрования и расшифровки данных, в котором размер модуля составляет 2048 бит [6, 7].

Алгоритм RSA-2048 не предназначен для прямого шифрования файлов или трафика. Он медленный и его главная задача – обеспечить безопасный ключевой обмен (например, передать ключ для AES) и цифровые подписи. В облачных инфраструктурах он используется при установлении TLS-соединения [8], где сервер аутентифицируется с помощью RSA, а затем сессионный ключ для AES передается клиенту.

Алгоритмы AES-256, Магма и Кузнечик обеспечивают высокоскоростное шифрование всего последующего трафика или хранимой информации после того, как ключ безопасно передан (например, с помощью ассиметричного алгоритма RSA).

Проведение исследования времени передачи данных с использованием различных криптографических алгоритмов

Для исследования были развернуты похожие стенды на облачной инфраструктуре и на физической. Схема сети в физической инфраструктуре приведена на рис. 1, в облачной инфраструктуре аналогичный стенд был развернут на базе платформы OpenStack.

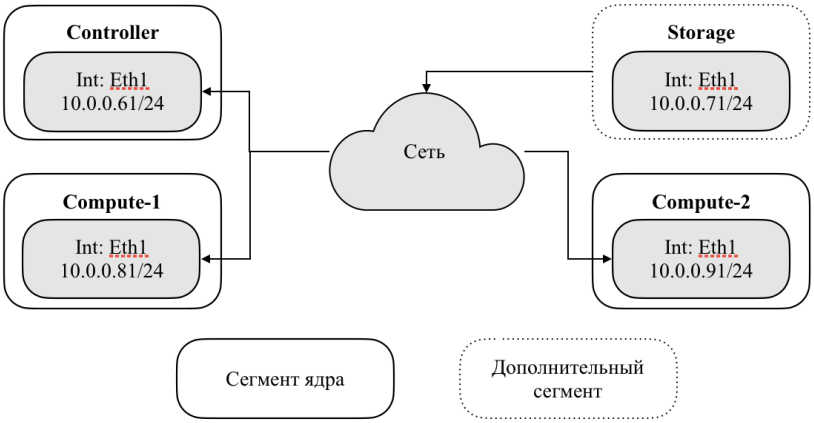


Рис. 1. Схема сети в физической инфраструктуре

Время передачи данных по сети (1) определяется суммой непосредственно времени передачи файла, времени шифрования и времени дешифрования файла.

$$T_{общ} = T_{шифр} + T_{сеть} + T_{расш} \quad (1)$$

где $T_{шифр}$ и $T_{расш}$ – время шифрования и время дешифрования, которые зависят от размера файла и вычислительной сложности используемого алгоритма, $T_{сеть}$ – время передачи данных по сети, $T_{общ}$ – общее время передачи данных от одной машины к другой.

Результаты исследования в облачной инфраструктуре – время передачи файла с одной виртуальной машины на другую – представлены в табл. 1.

ТАБЛИЦА 1. Полученные в результате исследования значения времени передачи данных в облачной инфраструктуре

Размер файла	Время передачи файла, с				
	Без шифрования	AES-256	Кузнечик	Магма	RSA-2048
100 МБ	4,2	5,3	7,8	6,1	485,1
500 МБ	20,1	26,8	38,5	29,9	2401,5
1 ГБ	41,5	54,1	78,3	61,4	4810,2

По полученным в результате исследования данным видно, что использование алгоритма RSA-2048 нецелесообразно, потому что время шифрования и дешифрования файла очень велико. Следовательно, можно предположить, что ассиметричные алгоритмы шифрования не подходят для данной задачи из-за высокой вычислительной сложности.

Для оптимизации времени передачи данных по сети и повышения защищенности этих данных был также рассмотрен гибридный формат шифрования, где алгоритм шифрования RSA-2048 используется для обмена ключами, а передача файла происходит с помощью симметричного алгоритма (например, Магма, Кузнечик и пр.).

При использовании гибридного подхода время передачи файла определяется вычислительной сложностью симметричных алгоритмов шифрования, а время на подтверждение связи по TLS становится незначительным по мере увеличения объема передаваемых данных. Таким образом можно получить оптимальное соотношение между безопасностью, производительностью и функциональной совместимостью.

В физической инфраструктуре каждый тест повторялся 20 раз, при этом первые 5 результатов отбрасывались для учета прогрева кэша файловой системы для обеспечения стабильность измерений. Результаты измерения времени передачи файла, а также производительности на физических серверах представлены в табл. 2.

ТАБЛИЦА 2. Время и производительность передачи данных на физическом оборудовании

Размер файла	Алгоритм шифрования	Среднее время передачи файла, с	Пропускная способность, МБ/с	Загрузка процессора (на ядро), %
100 МБ	AES-256	0,58	172,4	18
	Кузнечик	2,71	36,9	98
	Магма	1,45	69,0	75
	RSA-2048	2847	0,035	100
500 МБ	AES-256	2,52	198,4	19
	Кузнечик	12,35	40,5	99
	Магма	6,61	75,6	78
	RSA-2048	14215	0,035	100
1 ГБ	AES-256	4,93	208,1	20
	Кузнечик	24,88	41,1	100
	Магма	13,42	76,3	80
	RSA-2048	28430	0,035	100

Полученные результаты показывают, что пропускная способность увеличивается с увеличением размера файла. Это особенно заметно для алго-

ритма AES-256: 172 МБ/с для 100 МБ против 208 МБ/с для 1 ГБ. Это объясняется тем, что настройка каждого сеанса TLS имеет фиксированное значение: подтверждение связи (~0,105 секунды), настройка TCP-соединения и прочие временные затраты, связанные с обработкой каждого пакета на уровне записи TLS. Для файлов меньшего размера эта фиксированная стоимость составляет большую относительную часть общего времени передачи, снижая измеряемую пропускную способность. При больших и длительных передачах эти издержки становятся незначительными, что позволяет обеспечить максимальную устойчивую пропускную способность алгоритма.

Алгоритм RSA-2048 поддерживает постоянную пропускную способность (0,035 МБ/с) независимо от размера файла, что подтверждает линейную временную сложность O(n) для блочного шифрования. Каждая операция шифрования RSA-2048 полностью использует ядро центрального процессора, для достижения измеренной пропускной способности требуется одновременное использование 16 ядер. Время шифрования показывает, почему RSA-2048 никогда не используется для прямого шифрования файлов в производственных системах, и подтверждает эффективность гибридной модели шифрования.

Из табл. 2 видно, что наиболее производительный алгоритм – AES-256, а наименее – Кузнечик. Алгоритм AES-256 примерно в 5 раз быстрее алгоритма Кузнечик и в 2,7 раза быстрее алгоритма Магма при передаче файле размером 1 ГБ. Такая иерархия алгоритмов соблюдается для любых размеров файлов.

Заключение

Таким образом, исследование показывает, что, хотя виртуализация обеспечивает гибкость облачных вычислений, она сопряжена с определенными и поддающимися количественной оценке затратами на криптографические операции. Понимание этих затрат важно для создания облачных инфраструктур, которые не только масштабируемы и безопасны, но и способны обеспечивать высокопроизводительную обработку передаваемых данных.

Разница в производительности между асимметричным и симметричным алгоритмами обусловлена их вычислительной сложностью. Теоретическое соотношение вычислительной сложности может быть выражено согласно формуле (2).

$$\frac{\text{Сложность алгоритма } RSA{-}2048}{\text{Сложность алгоритма } AES{-}256} \approx \frac{20483}{128{*}14} \approx 4{,}8 * 10^6 \quad (2)$$

Это теоретическое соотношение соответствует наблюдаемой разнице в производительности (AES-256 работает в 5767 раз быстрее), учитывая оптимизацию реализации и аппаратное ускорение.

Эффективность гибридного шифрования ($O_{\text{гибрид}}$) можно оценить математически (3).

$$O_{\text{гибрид}} = \frac{1}{\frac{\text{T}_{RSA}}{T_{\text{д}}} + \frac{1}{\vartheta}} \quad (3)$$

где T_{RSA} – время подтверждения RSA-2048, $T_{\text{д}}$ – время шифрования данных с помощью симметричного алгоритма, ϑ – скорость симметричного алгоритма в сравнении с RSA-2048.

Для файла объемом 1 ГБ с шифрованием с помощью алгоритма AES-256 в физической среде эффективность гибридного шифрования можно высчитать по формуле (4).

$$O_{\text{гибрид}} = \frac{1}{\frac{0{,}105}{4{,}93} + \frac{1}{5767}} \approx 47 \quad (4)$$

Следовательно, гибридный подход примерно в 47 раз эффективнее, чем использование RSA-256 как для обмена ключами, так и для шифрования передаваемых данных.

Список используемых источников

1. Алехин Р. В., Красов А. В., Макарова А. Д., Орлов Г. А. Облачные сервисы. Принцип работы, классификация и модели обслуживания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 15–16 февраля 2022 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 70-74.

2. Бударный Г. С., Казанцев А. А., Красов А. В., Поляничева А. В. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): Сборник научных статей XI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 15–16 февраля 2022 года. Том 4. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 406-411.

3. Домбровский Р. М., Петрив Р. Б. Анализ уязвимостей ядра и оценка эффективности средств защиты операционных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024): Сборник научных статей XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург,

27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2024. С. 657-661.

4. Официальный сайт документации OpenStack: [Электронный ресурс]. Текст электронный. URL: https://docs.openstack.org/ocata/ru/install-guide-rdo/overview.html. (дата обращения: 16.01.2026).

5. Киясов М. Р. Шифрование / расшифрование данных файла на основе шифра «Кузнечик» в режиме гаммирования // Первый шаг в науку: материалы X Всероссийской научно-практической конференции: в двух томах, Луганск, 08 апреля 2025 года. Луганск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Луганский государственный педагогический университет", 2025. С. 83-87.

6. Спиридонова Г. О., Басаев А. А. Алгоритмы шифрования в современном мире: AES, RSA и другие // Научные исследования студентов и учащихся: Сборник статей XIV Международной научно-практической конференции, Пенза, 30 сентября 2024 года. Пенза: Наука и Просвещение (ИП Гуляев Г. Ю.), 2024. С. 32-34.

7. Ахмеров А. С., Резяпов И. Н. Сравнительный анализ алгоритмов асимметричного шифрования RSA и ECC // Мавлютовские чтения: материалы XV Всероссийской молодежной научной конференции: в 7 томах, Уфа, 26–28 октября 2021 года. Том 4. Уфа: Уфимский государственный авиационный технический университет, 2021. С. 326-330.

8. Носов М. В., Тезин А. В., Кирикова Ю. А. Основные подходы к обеспечению информационной безопасности в IP – сетях // Современные задачи и перспективные направления инновационного развития науки: Сборник статей по итогам Международной научно-практической конференции, Иркутск, 09 февраля 2023 года. Стерлитамак: Общество с ограниченной ответственностью "Агентство международных исследований", 2023. С. 105-108.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук И. Е. Пестовым.

УДК 004.056.5

МОДЕЛИ И АЛГОРИТМ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО АККАУНТА В СОЦИАЛЬНЫХ СЕТЯХ

С. В. Борисов (аспирант кафедры ЗСС СПбГУТ)
Г. А. Демидов (магистрант группы МЗС-2512 СПбГУТ),
demidov.ga@sut.ru
П. Ю. Егорова (студент группы ИКБ-22 СПбГУТ)

В условиях активного развития социальных сетей инфраструктура платформ ежедневно сталкивается с угрозами, связанными с аномальной активностью аккаунтов. В отличие от статических методов защиты, распространение угроз в сетях носит динамический характер, что делает традиционные средства фильтрации недостаточно эффективными для их своевременного выявления. Для решения данной задачи предлагается подход к выявлению аномальных аккаунтов в социальных сетях, основанный на совместном использовании эпидемиологических моделей и алгоритмов нейронных сетей, объединяющих макроуровневое прогнозирование и микроуровневую классификацию.

социальные сети, аномальное поведение, эпидемиологические модели, нейронные сети, информационная безопасность, выявление угроз, машинное обучение

Развитие социальных сетей сопровождается ростом угроз информационной безопасности, таких как распространение спама, фишинга и мошеннических схем [1]. Традиционные методы защиты часто оказываются недостаточными для своевременного выявления аномального поведения аккаунтов [2]. Актуальность работы обусловлена необходимостью разработки комплексных подходов, сочетающих макромоделирование угроз и микроанализ пользовательской активности [3].

Существующие методы включают использование эпидемиологических моделей, адаптированных для анализа распространения угроз в сетевых структурах, а также алгоритмы машинного обучения для классификации поведения отдельных узлов [4]. Эпидемиологические модели, изначально разработанные для биологических систем и компьютерных сетей, позволяют прогнозировать динамику заражения, тогда как нейросетевые алгоритмы выявляют отклонения в поведении конкретных пользователей [5, 6].

Эпидемиологические модели распространения в сетях

1. SIS-модель (Susceptible-Infected-Susceptible) предполагает бинарные состояния аккаунтов: «восприимчивые» (Susceptible) и «зараженные»

(Infected). Уязвимые узлы подвержены влиянию аномального поведения, а зараженные узлы выступают его распространителями. После применения мер защиты (блокировка, очистка) аккаунт возвращается в состояние восприимчивости. Модель применима для оценки скорости распространения спама или вредоносных ссылок и анализа эффективности мер сдерживания в условиях возможности повторного заражения [7].

2. SIR-модель (Susceptible-Infected-Removed) вводит третье состояние – «удаленные» (Removed), в которое переходят аккаунты после нейтрализации угрозы. Узлы в этом состоянии приобретают иммунитет и не могут быть повторно заражены или распространять угрозу [8]. Модель используется для анализа долгосрочных последствий атак, позволяя оценить предельное число зараженных аккаунтов до полной локализации эпидемии и долю узлов, оставшихся защищенными.

3. SEIR-модель (Susceptible-Exposed-Infected-Removed) дополняет структуру состоянием «латентное» (Exposed), характеризующим аккаунты, которые уже заражены, но еще не проявляют активной вредоносной деятельности. Данный подход актуален для моделирования атак с отложенной активностью, когда вредоносный код или аномальное поведение активируется с задержкой [9]. Модель позволяет прогнозировать начало массовой фазы распространения угрозы и планировать превентивные меры.

4. SIHR-модель (Susceptible-Infected-Hibernator-Removed) расширяет классическую структуру SIR добавлением состояния «спящий» (Hibernator), что учитывает временную неактивность пользователей. Аккаунты могут переходить в состояние неактивности добровольно или в результате временной блокировки, что снижает скорость распространения аномалий [10]. Однако при возвращении к активности такие узлы могут возобновить распространение угрозы. Использование модели SIHR позволяет прогнозировать динамику эпидемии с учетом цикличности пользовательской активности и разрабатывать адаптивные стратегии защиты.

5. SCWIEHR-модель, добавлены дополнительные классы пользователей: комментаторы, ожидающие, разоблачители и временно неактивные. Учтено повторяющееся выжидательное поведение, влияние платформенных алгоритмов и постоянный приток новых пользователей. Это позволяет более точно моделировать реальное поведение пользователей в социальных сетях [11].

Алгоритм выявления аномального поведения на основе нейронной сети

Для детектирования аномалий на уровне отдельных узлов применен алгоритм на основе многослойного перцептрона (MLP). Алгоритм анализирует вектор признаков пользовательской активности и выявляет статистически значимые отклонения от базового профиля. К признакам относятся временные метки активности, частота операций, типы используемых ресурсов и объем передаваемых данных [12].

Входной слой содержит 8 нейронов, соответствующих количеству анализируемых параметров поведения. Сеть включает два скрытых слоя (20 и 10 нейронов) для выделения нелинейных зависимостей. Выходной слой (1 нейрон) формирует вероятность принадлежности действия к классу аномалий. Обучение модели осуществлялось с использованием функции бинарной кросс-энтропии и оптимизатора Adam.

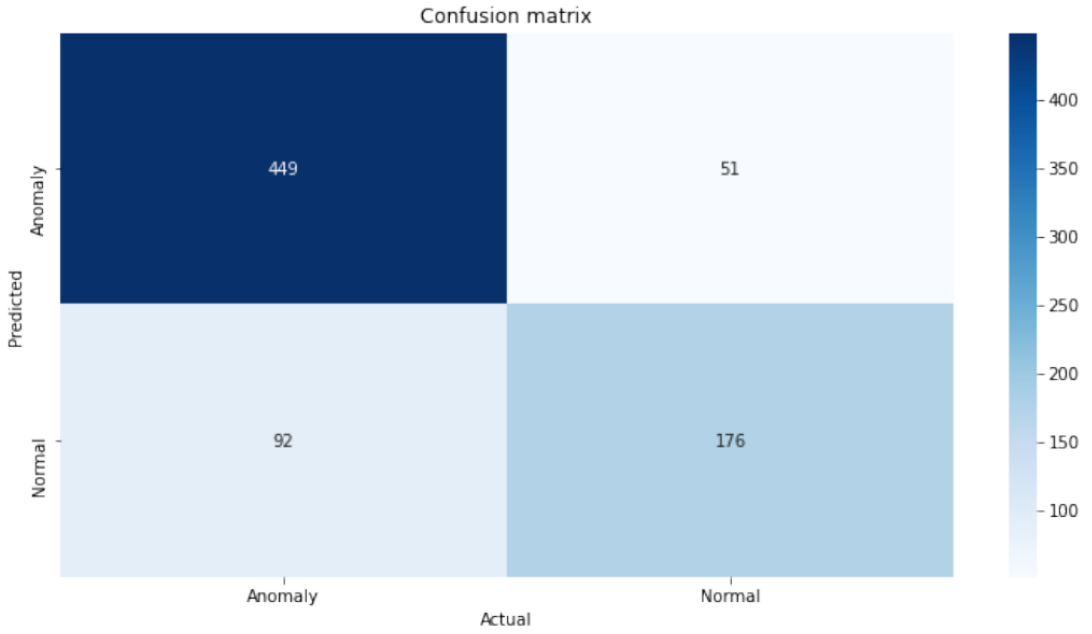


Рис. 1. Матрица 1-го и 2-го рода

В ходе экспериментальной проверки алгоритма достигнута точность классификации 78,52 %. Модель верно идентифицировала 449 случаев аномального поведения. При этом зафиксировано 51 ложное срабатывание (ошибка первого рода) и 92 пропуска целей (ошибка второго рода).

Полученные данные свидетельствуют о работоспособности метода для автоматического мониторинга, однако высокий уровень ошибок требует доработки. В частности, необходимо расширение обучающей выборки

и внедрение механизмов верификации сомнительных случаев. Алгоритм рекомендуется использовать как компонент многоуровневой системы защиты, требующий частичного ручного контроля на этапе внедрения.

Заключение

Предложенный подход к выявлению аномальных аккаунтов на основе комбинации эпидемиологических моделей и нейросетевых алгоритмов позволяет реализовать многоуровневую систему мониторинга безопасности социальных сетей. Применение модели SCWIEHR обеспечивает наиболее точное прогнозирование динамики угроз с учетом временной неактивности пользователей, а экспериментальная проверка классификатора на основе многослойного перцептрона (архитектура 8-20-10-1) подтвердила работоспособность метода с точностью 78,52 %. Наличие ошибок классификации обуславливает необходимость расширения обучающей выборки и разработки механизмов обратной связи, где параметры эпидемиологического моделирования корректируют пороги срабатывания нейросети, что станет предметом дальнейших исследований.

Список используемых источников

1. Котенко И. В., Хинензон А. В. Анализ алгоритмов обнаружения аномального поведения в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). 2020. С. 644-648.

2. Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Модель вредоносной информации и ее распространителя в социальных сетях // Защита информации. Инсайд. 2020. № 3. С. 66-72.

3. Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. № 4. С. 362-377.

4. Ляпушев В. Н. Поиск аномальных объектов в социальных сетях // Инновационные подходы в современной науке. 2020. С. 74-78.

5. Хачатрян М. Г., Чепик П. И. Обнаружение ботов в социальных сетях с помощью многослойного перцептрона // Политехнический молодежный журнал. 2019. № 4. С. 5-5.

6. Липатников В.А., Сахаров Д.В., Кузнецов И.А Управление безопасностью распределенной ивс на основе прогноза заражения компьютерным вирусом. // Электросвязь. 2017. № 1. С. 53-59.

7. Виткова Л. А., Чечулин А. А., Сахаров Д. В. Выбор мер противодействия вредоносной информации в социальных сетях // Вестник Воронежского института ФСИН России. 2020. № 3. С. 20-29.

8. Колесин И. Д., Житкова Е. М. Математическое моделирование распространения COVID-19 с учетом распределения бессимптомных случаев между действительно бессимптомными и предсимптомными // Математическая биология и биоинформатика. 2024. Т. 19. № 1. С. 52-60.

9. Тарутин А. Моделирование вирусных эпидемий // Инновации. Наука. Образование. 2021. № 27. С. 930-938.

10. Саенко И. Б., Хинензон А. В. Анализ метаданных социальных сетей для обнаружения аномального поведения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). 2021. С. 642-647.

11. Егорова П.Ю., Борисов С.В., Сахаров Д.В. Распространение слухов в социальных сетях на основе расширенной модели SCWIEHR // Защита информации. Инсайд. 2026. № 2 (128). С. 4-14.

12. Комашинский В. В., Скрылев А. О. Об интеллектуальном обнаружении аномального поведения пользователя в сети // Обработка, передача и защита информации в компьютерных системах'22. 2022. С. 256-260.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Д. В. Сахаров.

УДК 004.451:004.056.5

УСТОЙЧИВОСТЬ СЕРВЕРНЫХ ОС К SYN-FLOOD АТАКЕ

М. М. Ветров (студент группы ИБС-32 СПбГУТ), vetrov.mm@sut.ru
М. В. Мухина (студент группы ИКБ-32 СПбГУТ), mukhina.mv@sut.ru

В статье рассматривается актуальная проблема обеспечения доступности серверных систем при воздействии сетевого трафика типа SYN-flood. Проведено экспериментальное исследование устойчивости отечественной ОС Astra Linux 1.8 и зарубежной Windows Server 2025 в конфигурации «из коробки». В ходе работы выявлены критические различия в механизмах обработки полуоткрытых соединений и динамического управления очередью. Авторами предложены практические рекомендации по оптимизации параметров стека TCP/IP для повышения защищенности систем. Результаты подтверждают необходимость дополнительной настройки параметров ядра для отечественных систем в агрессивных сетевых средах.

сетевая безопасность, DDoS-атака, SYN-flood, Astra Linux, Windows Server 2025, TCP Syncookies

На сегодняшний день доступность сетевых ресурсов является критически важным аспектом функционирования информационных систем. Согласно статистике Cloudflare за 2-й квартал 2025 года, атаки типа SYN-flood составляют более 27 % от общего числа DDoS-атак на сетевом уровне. Проблема обусловлена дизайном протокола TCP и эксплуатацией механизма «трехэтапного рукопожатия» (3-way handshake) [1].

Актуальность исследования заключается в необходимости оценки защищенности современных ОС, используемых в государственном секторе, особенно в условиях импортозамещения [2], где Astra Linux становится основным стандартом [3].

Стандартное установление TCP-соединения включает три этапа: SYN, SYN/ACK и ACK. В случае SYN-flood атаки злоумышленник отправляет большое количество SYN-пакетов, часто с поддельными IP-адресами, игнорируя ответы сервера. как отмечается в классической работе К. Шобы [1], использование поддельных IP-адресов позволяет злоумышленнику эффективно обходить простейшие системы фильтрации. Сервер выделяет ресурсы (Task Control Block) и ожидает подтверждения, помещая соединение в очередь (backlog queue). При интенсивном потоке очередь переполняется, и сервер перестает принимать легитимные запросы. Для понимания критичности данной угрозы необходимо рассмотреть структуру блока управления передачей (TCB). На каждое новое соединение ОС выделяет в среднем от

280 до 500 байт оперативной памяти. При атаке интенсивностью 100 000 пакетов в секунду объем зарезервированной, но не используемой памяти начинает расти в геометрической прогрессии. Кроме того, процесс поиска и удаления устаревших записей из очереди по тайм-ауту (обычно 75 или 150 секунд) создает дополнительную нагрузку на планировщик задач операционной системы, что, в конечном итоге, приводит к деградации производительности всей сетевой подсистемы.

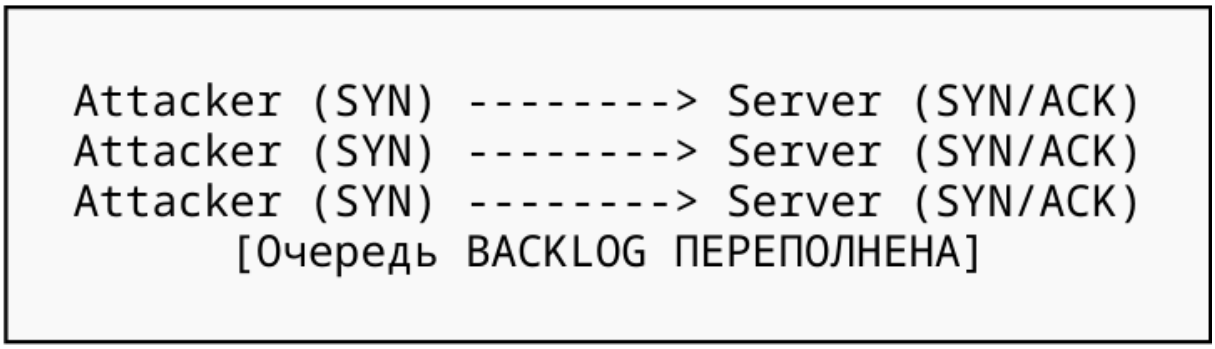


Рис. 1. Схема реализации атаки SYN-flood на очередь соединений

Существует два принципиально разных подхода к защите от SYN-flood [4; 5]. Первый – использование механизмов SYN-cookies. Суть метода заключается в том, что сервер не выделяет ресурсы под TCB сразу после получения SYN-пакета. Вместо этого он вычисляет криптографический хэш (cookie), который передается клиенту в поле порядкового номера (Sequence Number) пакета SYN-ACK. Ресурсы выделяются только после того, как клиент пришлет корректный ACK-пакет. Это позволяет серверу оставаться доступным даже при полностью заполненном бэклоге.

Второй подход, реализованный в современных версиях Windows Server [6], – динамическое регулирование размера очереди и сокращение времени жизни полуоткрытых соединений. Система в реальном времени анализирует скорость заполнения очереди и, при достижении критического порога, принудительно завершает старые неактивные сессии, освобождая место для новых запросов

Для проведения исследования был развернут стенд [7], включающий серверную среду и узел злоумышленника. В качестве атакующей платформы использовалась ОС Kali Linux с утилитой hping3. Объектами исследования выступили Astra Linux 1.8 (ядро 6.x) и Windows Server 2025 в конфигурации по умолчанию. Тестирование проводилось в три этапа: фоновое измерение задержек (ping), дозированная отправка SYN-пакетов (10-20

Mbps) и атака в режиме «наводнения» (flood mode). В ходе атаки фиксировались такие параметры, как время отклика (RTT), процент потери пакетов и загрузка ЦП.

В ходе эксперимента было зафиксировано резкое различие в поведении систем. Astra Linux 1.8 при интенсивности атаки в flood-режиме продемонстрировала 100 % потерю пакетов (packet loss) в течение первых секунд воздействия. Очередь backlog заполнилась мгновенно, что привело к невозможности установки новых соединений легитимными пользователями. Это подтверждается данными презентации, где при передаче 647473 пакетов было получено 0 ответов.

В свою очередь, Windows Server 2025 успешно противостоял атаке. Исследование показало, что система автоматически активирует механизмы SYN-cookies и динамического управления бэклогом при обнаружении аномального всплеска полуоткрытых соединений. Это позволило сохранить доступность сервера, хотя и привело к незначительному росту загрузки центрального процессора и увеличению RTT до 1.45 мс.

ТАБЛИЦА 1. Значения времени передачи кадра при различных соотношениях параметров

Параметр	Astra Linux 1.8 (Default)	Windows Server 2025 (Default)
Задержка (норма), мс	0,22	0,25
Задержка (атака), мс	Timed out	1,45
Потеря пакетов, %	100	0-2
Доступность сервиса	Отказ (DoS)	Работает

Анализ данных таблицы 1 показывает, что Windows Server 2025 демонстрирует более агрессивную политику защиты. В то же время атака на Astra Linux 1.8, что сетевой стек перестал обрабатывать входящие пакеты после переполнения очереди бэклога. Дополнительно было замечено, что при использовании отечественной ОС в режиме "из коробки" время ожидания ответа (RTT) для легитимного пользователя увеличивалось с 0.2 мс до 300 мс в первые минуты атаки.

Низкая устойчивость Astra Linux «из коробки» объясняется консервативными настройками стека TCP/IP. Для повышения защищенности систем на базе Linux необходимо применение технологий тонкой настройки параметров ядра. Ключевыми мерами являются включение net.ipv4.tcp_syncookies = 1 и увеличение размера tcp_max_syn_backlog.

Также рекомендуется использование Honeypot решений для раннего обнаружения и анализа действий злоумышленника в корпоративной сети [8].

Сопоставление результатов испытаний показывает, что устойчивость серверной ОС к SYN-flood определяется не только набором встроенных средств защиты, но и их исходной настройкой. В проведенном эксперименте Windows Server 2025 сохранила работоспособность сервиса при атаке, тогда как Astra Linux 1.8 в конфигурации по умолчанию столкнулась с переполнением очереди и потерей доступности. Поэтому для эксплуатации Astra Linux в условиях повышенной сетевой нагрузки целесообразно заранее формировать и проверять профиль защиты, включая параметры TCP-стека в /etc/sysctl.conf, а не ограничиваться стандартными значениями. Полученные результаты могут быть использованы при подготовке защищенных сегментов корпоративной инфраструктуры [9; 10]. В дальнейшем представляет интерес проверка поведения обеих систем при распределенной нагрузке, создаваемой бот-сетями, с оценкой не только доступности, но и времени восстановления сервиса.

Список используемых источников

1. Schuba C. L. Analysis of a Denial of Service Attack on TCP. West Lafayette: Purdue University, 1993.

2. Оптимизация структуры ИСПДн объектов КИИ на основе теории рисков / Э. В. Бирих, И. И. Фадеев, Е. Н. Николаев [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52, № 4. С. 49-62. DOI 10.21822/2073-6185-2025-52-4-49-62. EDN: PVMMFD.

3. Minyaev, A. A. The method and methodology of efficiency assessment of protection system of distributed information systems / A. A. Minyaev, A. V. Krasov, D. V. Saharov // 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020, Brno, 05–07 октября 2020 года. Brno: Institute of Electrical and Electronics Engineers, 2020. P. 291-295. DOI: 10.1109/ICUMT51630.2020.9222451. EDN: KAGNKZ.

4. Патент № 2490703 C1 Российская Федерация, МПК G06F 21/00. Способ защиты канала связи вычислительной сети: заявл. 04.06.2012: опубл. 20.08.2013 / А. Е. Балясов, В. В. Бухарин, Б. В. Голуб [и др.]; заявитель Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации. EDN: UPMQZZ.

5. Патент № 2472211 C1 Российская Федерация, МПК G06F 12/14. Способ защиты информационно-вычислительных сетей от компьютерных атак: № 2011147613/08: заявл. 23.11.2011: опубл. 10.01.2013 / В. И. Андрианов, В. В. Бухарин, А. В. Кирьянов [и др.]; заявитель Федеральное государственное военное образовательное учреждение высшего профессионального образования «ВОЕННАЯ АКАДЕМИЯ СВЯЗИ имени маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации. EDN: HIOVLT.

6. Катасонов, А. И. Эффективность встроенной защиты microsoft windows server от ddos-атак на основе TCP SYN / А. И. Катасонов, А. В. Красов, А. Ю. Цветков // Сборник статей Круглого стола «Безопасность в профессиональной деятельности»: Сборник статей Круглого стола «Безопасность в профессиональной деятельности», в рамках II Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики» ITES-2020, Санкт-Петербург, 27 марта 2020 года. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2020. С. 68-78. EDN: KITNAH.

7. Защищенная модель программно-определяемой сети в среде виртуализации KVM / Д. В. Сахаров, А. В. Красов, И. А. Ушаков, Г. А. Орлов // Электросвязь. 2020. № 3. С. 26-32. DOI 10.34832/ELSV.2020.4.3.004. EDN: IRRVAB.

8. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях / А. В. Красов, Р. Б. Петрив, Д. В. Сахаров [и др.] // Труды учебных заведений связи. 2019. Т. 5, № 3. С. 86-97. DOI: 10.31854/1813-324X-2019-5-3-86-97. EDN: VDCCKM.

9. Липатников, В. А. Управление безопасностью распределенной ИВС на основе прогноза заражения компьютерным вирусом / В. А. Липатников, Д. В. Сахаров, И. А. Кузнецов // Электросвязь. 2017. № 1. С. 53-59. EDN: XHDUPB.

10. Костарев, С. В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры / С. В. Костарев, В. А. Липатников, Д. В. Сахаров // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120-125. EDN: UHSQDF.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Д. В. Сахаровым.

УДК 004.056

МОНИТОРИНГ ДРЕЙФА ДАННЫХ И КОНЦЕПТУАЛЬНОГО ДРЕЙФА КАК ИНДИКАТОРОВ СНИЖЕНИЯ КИБЕРУСТОЙЧИВОСТИ ИИ-СИСТЕМ

Л. А. Виткова (к.т.н., доцент кафедры ЗСС СПбГУТ), vitkova.la@sut.ru
Е. А. Трофимов (студент группы ИКТБ 48М СПбГУТ), trofimov1.ea@sut.ru

В работе рассматриваются явления дрейфа данных и концептуального дрейфа в контексте обеспечения киберустойчивости искусственного интеллекта на этапе эксплуатации. Предлагается классификация типов дрейфа с точки зрения кибербезопасности, включающая разграничение естественных изменений распределения данных и индуцированных изменений, характерных для кибератак. Анализируются методы статистического обнаружения дрейфа: CUSUM, DDM и ADWIN. Проводится их сравнительная оценка по критериям адаптивности, вычислительной сложности и чувствительности к угрозам. Предложена двухуровневая схема мониторинга, интегрирующая обнаружение дрейфа с системой классификации инцидентов кибербезопасности.

дрейф данных, концептуальный дрейф, киберустойчивость, искусственный интеллект, мониторинг, CUSUM, DDM, ADWIN, кибербезопасность

Современные технологии искусственного интеллекта (далее ИИ) все чаще используются в составе критически важных бизнес-процессов и цифровых сервисов: от интеллектуальных помощников и рекомендательных систем до модулей принятия решений, систем обнаружений аномалий и средств автоматизации реагирования на инциденты.

Особенность ИИ систем заключается в том, что они принимают решения на основе данных и статистических закономерностей, а значит их поведение может существенно меняться при сдвигах распределения данных, изменения контекста, обновления инфраструктуры и появление новых сценариев использования. При этом атакующий может целенаправленно провоцироваться такие изменения, формируя входные воздействия, которые ухудшают качество модели, вызывают ошибочные решения или приводят к раскрытию информации. [1, 2].

Актуальность проблемы обусловлена широким внедрением ИИ в различные сферы, это подтверждается разработкой новых стандартов, к примеру ПНСТ 1046-2026 «Искусственный интеллект в критической информационной инфраструктуре. Общие положения». Снижение киберустойчивости, вызванное индуцированным дрейфом, может повлечь серьезные последствия. Стандарт вводит детализированные требования к мониторингу ИИ систем на этапе эксплуатации, предписывает организациям обеспечивать: непрерывный контроль работоспособности, производительности и безопасности системы [3].

Целью настоящей статьи является систематизация типов дрейфа с позиций киберустойчивости и сравнительный анализ методов их обнаружения применительно к задачам непрерывного мониторинга систем ИИ на этапе эксплуатации.

Классификация дрейфа с точки зрения кибербезопасности

Под дрейфом данных понимается изменение маргинального распределения входных признаков P(X) без обязательного изменения условного распределения P(Y|X). Концептуальный дрейф (concept drift) характеризуется изменением именно условного распределения P(Y|X), то есть изменением самого понятия, которое предсказывает модель [4].

С позиций кибербезопасности данные явления предлагается разграничить на естественные и индуцированные. Естественный дрейф обусловлен изменениями среды: сезонностью, сменой пользовательского поведения, обновлением программного обеспечения. Индуцированный дрейф является результатом преднамеренного воздействия злоумышленника и соответствует известным категориям атак на ИИ: отравлению данных (data poisoning), состязательным примерам (adversarial examples) и атакам на конвейер данных.

Тип дрейфа по временному характеру также коррелирует с классом угрозы. Внезапный дрейф, при котором распределение изменяется резко, характерен для атак типа data injection. Постепенный и инкрементальный дрейф соответствует продвинутым постоянным угрозам, при которых злоумышленник намеренно замедляет темп воздействия, чтобы обойти пороговые детекторы. Таблица 1 показывает, соответствие типов дрейфа к классам киберугроз.

ТАБЛИЦА 1. Соответствие типов дрейфа к классам киберугроз.

Тип дрейфа	Тип изменения	Вероятный класс атаки	Кибер-риск
Внезапный (abrupt)	P(Y|X) резко меняется	Data injection, adversarial examples	Высокий
Постепенный (gradual)	Медленное смещение	APT, скрытое отравление обучения	Высокий
Периодический (recurring)	Циклическое изменение	Как правило, не атака	Низкий
Инкрементальный	Плавное накопление	Slow poisoning	Средний

Методы обнаружения дрейфа

Метод CUSUM (Cumulative Sum Control Chart) основан на накоплении кумулятивной суммы отклонений наблюдаемой метрики от эталонного значения. Сигнал тревоги формируется при превышении накопленной суммой заданного порога. Метод обладает высокой чувствительностью к малым систематическим сдвигам, имеет вычислительную сложность O(1) и не требует разметки входных данных, что делает его применимым непосредственно к статистикам входного потока. Ограничение метода состоит в необходимости предварительного знания фонового распределения и низкой эффективности при многомерном дрейфе [5]. Существует open-source решение AIM-CU: A CUSUM-based tool for AI Monitoring.

Метод DDM (Drift Detection Method) отслеживает статистику частоты ошибок потокового классификатора, формируя двухуровневую систему оповещения: уровень предупреждения и уровень тревоги. Архитектура двух порогов органично вписывается в логику систем обнаружения вторжений (IDS) и допускает интеграцию в корпоративный центр мониторинга безопасности (SOC). Существенным ограничением является обязательное наличие разметки в режиме реального времени (ground truth), что нередко недостижимо в промышленных условиях [6].

Метод ADWIN (ADaptive WINdowing) использует адаптивное скользящее окно, автоматически сужаемое при обнаружении статистически значимого изменения среднего между подокнами. Метод обладает строгими теоретическими гарантиями на число ложных тревог, не требует разметки и адаптируется к скорости изменений, что делает его эффективным как против быстрых, так и против медленных атак. Вычислительная сложность O(log n) несколько выше, чем у CUSUM и DDM [7].

Сравнительный анализ методов

На основе анализа свойств рассмотренных методов составлена сравнительная таблица 2 по критериям, наиболее значимым для задач мониторинга киберустойчивости ИИ: наличие теоретических гарантий, требования к разметке данных, адаптивность к скорости дрейфа и чувствительность к различным классам угроз.

ТАБЛИЦА 2. Сравнительная характеристика методов обнаружения дрейфа.

Критерий	CUSUM	DDM	ADWIN
Тип обнаруживаемого дрейфа	Внезапный	Внезапный, постепенный	Все типы
Вычислительная сложность	O(1)	O(1)	O(log n)
Требует разметки (ground truth)	Нет	Да	Нет
Теоретические гарантии	Частично	Нет	Да
Адаптивность к скорости дрейфа	Нет	Нет	Да
Чувствительность к APT-атакам	Низкая	Средняя	Высокая

Метод ADWIN демонстрирует наиболее высокие характеристики по совокупности критериев, тогда как CUSUM рекомендуется для быстрого мониторинга статистик входного потока без разметки, а DDM – для потоковых классификаторов с доступным ground truth.

Схема мониторинга

На основе проведенного анализа предлагается схема мониторинга киберустойчивости систем ИИ, интегрирующая обнаружение дрейфа с логикой классификации инцидентов безопасности.

Метод CUSUM применяется к статистикам входных признаков для обнаружения дрейфа данных P(X). Параллельно метод ADWIN анализирует ошибки модели на предмет концептуального дрейфа P(Y|X). Результаты обоих методов поступают на этап корреляционного анализа, где оценивается совпадение дрейфов и их временной характер. Классификация инцидента производится по трем сценариям. Одновременное наличие обоих дрейфов с внезапным временным характером классифицируется как вероятный инцидент кибербезопасности и передается в SOC для расследования. Постепенный дрейф направляется на проверку конвейера данных и, при необходимости, инициирует процедуру дообучения модели. Изолированный дрейф P(Y|X) без изменения P(X) рассматривается как признак скрытой угрозы – отравления меток или компрометации модели – и инициирует аудит модели.

Параллельная архитектура мониторинга позволяет обнаруживать не только атаки через входной поток, но и воздействия, не затрагивающие распределение входных данных, что расширяет охват детектируемых угроз по сравнению с последовательной схемой.

В статье систематизированы типы дрейфа данных и концептуального дрейфа применительно к задачам мониторинга киберустойчивости систем ИИ. Установлена корреляция между временным характером дрейфа и классом киберугрозы. Проведен сравнительный анализ методов CUSUM, DDM и ADWIN, показавший преимущества метода ADWIN по критериям адаптивности и теоретической обоснованности. Предложена схема мониторинга, обеспечивающая переход от обнаружения факта дрейфа к классификации типа инцидента безопасности.

Список используемых источников

1. Testing the limits: exploring adversarial techniques in AI models // PeerJ Computer Science. 2026. № cs-3330. URL: https://peerj.com/articles/cs-3330/ (дата обращения: 10.03.2026).

2. HackedGPT: Novel AI Vulnerabilities Open the Door for Private Data Leakage / Tenable Research// Security Boulevard. 2025. 4 нояб. URL: https://securityboulevard.com/2025/11/hackedgpt-novel-ai-vulnerabilities-open-the-door-for-private-data-leakage/ (дата обращения: 10.03.2026).

3. ПНСТ 1046–2026. Искусственный интеллект в критической информационной инфраструктуре. Общие положения. Москва: Росстандарт, 2026.

4. Lu J., Liu A., Dong F., Gu F., Gama J., Zhang G. Learning under concept drift: a review// IEEE Transactions on Knowledge and Data Engineering. 2019. Vol. 31, N 12. P. 2346–2363. URL: https://arxiv.org/abs/2004.05785 (дата обращения: 10.03.2026).

5. Quantifying input data drift in medical machine learning models by detecting change-points in time-series data // Proceedings of SPIE. URL: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12927/129270E/Quantifying-input-data-drift-in-medical-machine-learning-models-by/10.1117/12.3008771.short (дата обращения: 10.03.2026).

6. Gama J., Medas P., Castillo G., Rodrigues P. Learning with drift detection // Advances in Artificial Intelligence. 2004. P. 286–295. URL: https://www.researchgate.net/publication/220974771_Learning_with_Drift_Detection.

7. McDiarmid drift detection methods for evolving data streams// arXiv. URL: https://arxiv.org/abs/1710.02030 (дата обращения: 10.03.2026).

Статья представлена научным руководителем, кандидат технических наук, доцент кафедры ЗСС Л. А. Витковой.

УДК 004.056.2

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ТОЧКАМИ ДОСТУПА ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ЦЕЛЕЙ

Д. Е. Гилева (студент группы ИКТЗ-25 СПбГУТ), gileva.de@sut.ru
Н. Ф. Махмутова (студент группы ИКТБ-47м СПбГУТ), mahmutova.nf@sut.ru

Точки доступа Wi-Fi являются ключевым элементом лабораторных стендов при подготовке специалистов в области беспроводных сетей, а также сетевых инженеров. В условиях учебного процесса часто возникает проблема переполнения конфигураций оборудования из-за создания студентами или обучающимся множества собственных сетей (SSID), что требует регулярного ручного вмешательства преподавателя или проводящего занятия.

автоматизация, точка доступа, SSH, Ansible, SNMP, Zabbix, лабораторный стенд, Wi-Fi, SSID, Python

В современных учебных лабораториях, где проводятся практические занятия по беспроводным сетям, активно используются точки доступа (ТД). В ходе выполнения лабораторных работ студенты или обучающиеся создают собственные Wi-Fi сети (SSID), что приводит к постепенному заполнению конфигурации ТД. При достижении лимита активных SSID новые сети не создаются, и работа студентов блокируется. В сложившихся условиях преподаватель вынужден вручную проверять состояние ТД, заходить в веб-интерфейс или консоль, оценивать количество SSID и при необходимости выполнять сброс конфигурации. Это отнимает значительное время и снижает эффективность учебного процесса. Автоматизация данных операций позволяет сократить временные затраты и исключить рутинные действия.

Рассмотрим несколько подходов решения данной проблемы. Первый метод предполагает разработку собственного программного модуля на Python, который подключается к ТД по SSH, выполняет команды управления и анализирует полученные данные. Основными преимуществами данного подхода являются полный контроль над логикой работы, возможность быстрой адаптации под конкретные задачи лабораторного стенда, минимальные требования к оборудованию (любой ПК с 512 МБ RAM и 10 МБ дискового пространства), а также отсутствие необходимости установки дополнительных сервисов. К недостаткам можно отнести необходимость владения навыками программирования на Python и отсутствие автоматического масштабирования на большое количество устройств [1, 2].

Второй подход основан на использовании Ansible – системы управления конфигурациями, работающей через SSH без установки агентов. Ansible позволяет описывать желаемое состояние оборудования в декларативных playbook-файлах на языке YAML. Преимуществами являются идемпотентность (повторное применение безопасно), возможность параллельного выполнения на множестве устройств и наличие большого количества готовых модулей. Однако данный подход требует изучения синтаксиса YAML, установки на управляющий ПК и, при необходимости решения нестандартных задач, написания собственных модулей [3].

Третий подход представляет собой связку системы мониторинга Zabbix и протокола SNMP. Zabbix собирает данные по SNMP, позволяет отслеживать состояние оборудования и выполнять автоматические действия при срабатывании триггеров. К преимуществам можно отнести централизованный мониторинг, визуализацию данных в виде графиков и автоматическое обнаружение устройств. Однако данный подход требует развертывания отдельного сервера (от 4 ГБ RAM и 10 ГБ диска), а SNMP предоставляет ограниченные возможности управления – преимущественно чтение данных, что затрудняет реализацию активного управления [2].

Для объективного сравнения подходов выделим критерии, отражающие специфику образовательной среды: простота внедрения, гибкость, автономность, требования к оборудованию. Результаты сравнения представлены в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ критериев методов автоматизации управления точками тоступа

Критерии	Программный модуль на Python через SSH	Ansible	Zabbix и управление через SNMP
Простота внедрения	Один файл, копировать и запустить	Требует установки Ansible, PIP, настройка окружения	Требуется установка Zabbix, сервер, база данных, агенты, настройка
Автономность	Работает на любом ПК	Нужен Ansible	Нужен сервер
Гибкость	контролируемый код, можно добавить любую функцию	Найти/написать модуль для сбора сведений, обновить playbook	Ограниченный набор предустановленных действий

Критерии	Программный модуль на Python через SSH	Ansible	Zabbix и управление через SNMP
Минимальные требования к ПК	• Любой ПК (от 512 МБ RAM) • Python 3.6+ (установлен) • Библиотека paramiko (apt install) • SSH-доступ к ТД	• ПК от 1 ГБ RAM • Python 3.8+ • Ansible (pip install) • SSH-доступ к ТД	• Сервер: 2+ ядра, 4+ ГБ RAM • PostgreSQL/MySQL • Zabbix Server • SNMP-доступ к ТД

Анализ таблицы 1 показывает, что для образовательных целей, где ключевыми требованиями являются вышеперечисленные аспекты, наиболее оптимальным является подход на основе Python-скрипта с использованием SSH.

На основе выбранного подхода разработан программный модуль на языке Python с использованием библиотеки paramiko для SSH-взаимодействия. Модуль построен по объектно-ориентированному принципу и включает класс APController, реализующий методы подключения к ТД, получения количества SSID, сброса конфигурации, управления радиоинтерфейсами и выполнения операций по расписанию. [1]

Для количественной оценки эффективности произведен расчет временных затрат на обслуживание лабораторного стенда за 1 день. Исходные данные: количество ТД – 3, количество проверок в день – 3 (при заполнении лимита), время ручной проверки – 5 мин, время ручного подключения – 1 мин, время ожидания сброса – 2 мин, время запуска скрипта – 0.5 мин. Результаты расчета представлены в таблице 2 [4].

ТАБЛИЦА 2. Результаты расчетов количественной оценки эффективности за 1 день

Показатель	Без автоматизации (ручное выполнение)	С автоматизацией (ручной ввод команд)	С автоматизацией (cron)
Затраты, мин	72	64,8	28,8
Экономия, мин	0	7,2	43,2
Выигрыш, %	0	10	60

При учете регулярных проверок (30 проверок в семестр) экономия составляет свыше 90 %, что подтверждает высокую эффективность разработанного решения.

Таким образом, проведенный сравнительный анализ показал, что для образовательных целей наиболее оптимальным является подход на основе Python-скрипта с использованием SSH. Разработанный модуль позволяет автоматически контролировать количество активных SSID, выполнять сброс конфигурации при превышении лимита и управлять радиоинтерфейсами по расписанию, что обеспечивает сокращение временных затрат преподавателя на обслуживание лабораторного стенда до 90 % в семестр.

Список используемых источников

1. Проничев В. Д. Автоматизированный анализ изменений в сетевых конфигурациях устройств на основе нейронных сетей / В. Д. Проничев, И. А. Ушаков // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024): Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах, Санкт-Петербург, 03–05 декабря 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025. С. 443-448. EDN: DDZZOT.

2. Платонов А. Е. Исследование нейросетевых технологий как технологии для автоматизированного реагирования на инциденты / А. Е. Платонов, М. М. Ковцур, А. А. Миняев // Информационная безопасность регионов России (ИБРР-2025): Материалы XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2025. С. 491-492. EDN: EYQUOZ.

3. Зебзеев Е. А. Разработка модуля Ansible для обнаружения нелегитимных беспроводных точек доступа в корпоративной сети / Е. А. Зебзеев, М. М. Ковцур, Т. В. Петрова // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 15–16 февраля 2022 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 478-483. EDN: ALZEMY.

4. Дрепа В. Е. Оценка времени для блокировки нелегитимных точек доступа в корпоративной сети / В. Е. Дрепа, М. М. Ковцур, Т. В. Петрова // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 2023 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. С. 423-427. EDN: YRFHCE.

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ИБКС, доцентом М. М. Ковцуром.

УДК 004.056.57

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К ОБНАРУЖЕНИЮ ДЛИТЕЛЬНЫХ СОЕДИНЕНИЙ В КАНАЛАХ УПРАВЛЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В. А. Горковенко (студент группы МЗС-2511 СПбГУТ),
gorkovenko.va@sut.ru

В статье проводится сравнительный анализ подходов к обнаружению длительных соединений (long connection) и периодических сигналов (beaconing) в каналах управления (C2) вредоносного программного обеспечения. Рассматриваются пять отечественных и зарубежных работ, опубликованных в период 2016–2025 годов. Анализ охватывает методологии обнаружения, анализируемые протоколы, используемые статистические параметры, методы HTTP-туннелирования и особенности работы с зашифрованным трафиком TLS. В результате исследования выявлен переход от сигнатурных методов к поведенческим и статистическим, а также определены перспективные направления для дальнейших исследований.

канал управления, C2, длительное соединение, long connection, beaconing, обнаружение аномалий, сетевой трафик, статистические параметры, HTTP-туннелирование, TLS

Современные кибератаки, особенно реализуемые с использованием моделей ransomware-as-a-service и целевых атак (APT), характеризуются активным применением каналов управления (Command and Control, C2) для поддержания устойчивой связи между атакующим и скомпрометированными хостами. Согласно исследованиям, протокол TLS активно используется злоумышленниками для сокрытия исходящих вредоносных коммуникаций, и в последние годы наблюдается устойчивая тенденция к росту его применения в C2-инфраструктурах.

Одним из ключевых демаскирующих признаков таких каналов является использование длительных соединений (long connection) – аномально продолжительных сетевых сессий, значительно превышающих по длительности типичные легитимные взаимодействия, а также периодических подключений (beaconing), реализуемых по принципу «keepalive» [1]. Сложность обнаружения long connection C2 обусловлена активным применением злоумышленниками методов маскировки, включая шифрование трафика, обфускацию, использование легитимных протоколов прикладного уровня (HTTP, DNS) и технологий туннелирования.

Целью настоящей работы является сравнительный анализ современных подходов к обнаружению длительных соединений в C2-каналах, представленных в отечественной и зарубежной научной литературе.

В работе Скорых М. А. [1] выделяются два основных демаскирующих признака C2-каналов. Первый признак – Long connection – представляет собой аномально длительные сетевые сессии, превышающие по длительности типичную легитимную пользовательскую активность. Данный признак характерен для таких инструментов, как Mythic, Havoc, Sliver, Stowaway. Второй признак – Beaconing – представляет собой периодические подключения агента вредоносного программного обеспечения к центру удаленного управления с постоянными интервалами времени. Данный признак присущ Havoc, Sliver, Cobalt Strike, Merlin, IBombShell, Metasploit, Pupy.

Авторы А. В. Козачок и Е. В. Кочетков [2] дополняют этот перечень, выделяя в качестве одного из ключевых признаков «устойчивую периодичность установления соединения с центром управления ботнет-сетью». Авторы предлагают оценивать данный признак через дисперсию интервалов между установлениями соединений: чем меньше дисперсия, тем выше вероятность наличия ботнет-клиента в сети.

Для проведения сравнительного анализа были отобраны пять работ, опубликованных в период 2016–2025 годов и непосредственно или косвенно затрагивающих проблематику обнаружения long connection C2. Характеристики выбранных статей представлены в таблице 1.

ТАБЛИЦА 1. Характеристика объектов сравнительного анализа

Автор(ы)	Название	Источник	Год
Скорых М. А.	Алгоритм обнаружения каналов управления вредоносного программного обеспечения в сетевом трафике с использованием статистических параметров	Сборник трудов конференции «Региональная информатика и информационная безопасность»	2025
Козачок А. В., Кочетков Е. В.	Обнаружение вредоносного программного обеспечения на основе выявления аномальной сетевой активности	Журнал Информационные системы и технологии	2016

Автор(ы)	Название	Источник	Год
Подшибкин А. С., Степанюк О. М.	Разработка и применение метода оперативного выявления HTTP-туннелирования в сетевом трафике информационно-телекоммуникационных систем	Журнал Известия Тульского государственного университета 2024	2024
Barradas D. et al.	Extending C2 Traffic Detection Methodologies: From TLS 1.2 to TLS 1.3-enabled Malware	RAID 2024	2024
Novo C., Morla R.	Flow-based detection and proxy-based evasion of encrypted malware C2 traffic	AISec 2020	2020

В работе Скорых М. А. [1] предлагается алгоритм, основанный на вычислении статистических параметров сетевого трафика с последующей проверкой на соответствие критериям аномальности. В качестве источника данных используется программное обеспечение Zeek, позволяющее получать детализированные журналы сетевых сессий (conn.log, http.log, ssl.log, weird.log). Алгоритм включает вычисление 15 статистических параметров, среди которых: максимальная длительность сессии, вариация длительности соединений, вариация межсессионных интервалов, асимметрия передаваемых байт и пакетов. Решение о наличии аномалии принимается на основе сравнения вычисленных значений с эмпирически заданными порогами и последующей интеграции с данными из внешних источников об индикаторах компрометации.

Авторы А. В. Козачок и Е. В. Кочетков [2] предлагают методику, базирующуюся на пяти признаках аномальной активности, среди которых особое место занимает устойчивая периодичность установления соединений. Авторы вводят формальные математические выражения для оценки каждого признака: отношение объема исходящего трафика к входящему, отношение количества SYN-пакетов к FIN-пакетам, а также математическое ожидание и дисперсию интервалов между установлениями соединений. На основе результатов проверки формируется бинарный вектор признаков, на основании которого администратор безопасности принимает решение о наличии вредоносной активности.

Авторы А. С. Подшибкин и О. М. Степанюк [3] разработали метод оперативного выявления HTTP-туннелирования, который позволяет обнаруживать beaconing по частоте POST-запросов на нестандартные порты. Инструментальная реализация на базе библиотеки Scapy позволяет не только обнаруживать подозрительные запросы, но и отслеживать частоту их поступления: превышение порога в несколько запросов в минуту классифицируется как подозрительная активность, что соответствует обнаружению периодических сигналов.

D. Barradas с соавторами [4] предлагают два метода обнаружения C2-трафика в TLS 1.3. Первый метод (C-Cert) основан на определении размера сертификата сервера. Несмотря на то, что в TLS 1.3 сертификаты передаются в зашифрованном виде, авторы разработали методику оценки их размера на основе анализа структуры handshake-сообщений. Второй метод (C-Behav) основан на изолировании последовательностей прикладных данных и анализе паттернов поведения приложения, что напрямую коррелирует с выявлением длительных соединений.

C. Novo и R. Morla [5] исследуют уязвимость детекторов, основанных на анализе сетевых потоков, к атакам уклонения. Авторы показывают, что изменение характеристик потока – в частности, искусственное увеличение его длительности – существенно снижает точность обнаружения. В работе используется набор числовых характеристик сетевых потоков, извлекаемых с помощью инструмента Tstat.

Различные подходы к обнаружению long connection C2 оперируют разными наборами протоколов и параметров. Сравнительный анализ представлен в таблице 2.

ТАБЛИЦА 2. Сравнение по анализируемым протоколам и параметрам

Автор(ы)	Скорых [1]	Козачок, Кочетков [2]	Подшибкин, Степанюк [3]	Barradas [4]	Novo, Morla [5]
Протоколы	HTTP, SSL, общий сетевой	HTTP, SSH, UltraVNC	HTTP	TLS 1.2, TLS 1.3	общий сетевой (TCP/IP)
Параметры	статистические (длительность, вариации, асимметрия)	порты, IP, URL	частота POST-запросов, нестандартные порты	размер сертификата, последовательности прикладных данных	характеристик и потоков (длительность, количество пакетов, байт, RTT)
Инструменты	Zeek	MITRE ATT&CK	Scapy	Joy	Tstat

Важной особенностью современных подходов является интеграция методов статистического анализа с данными из внешних источников об индикаторах компрометации. В работе М. А. Скорых [1] предусмотрен этап проверки сетевых артефактов (IP-адресов, доменных имен, отпечатков сертификатов) по базам данных известных вредоносных кампаний, что позволяет повысить достоверность обнаружения и снизить количество ложных срабатываний.

Авторы А. В. Козачок и Е. В. Кочетков [2] используют обращение к IP-адресам из «черных списков» как один из детерминированных признаков наличия ботнет-клиента. При обнаружении такого обращения делается однозначный вывод о вредоносной активности.

D. Barradas с соавторами [4] при формировании обучающих выборок используют SSL Blacklist – список сертификатов, заведомо связанных с ботнет-сетями, что позволяет точно маркировать вредоносный трафик.

Проведенный сравнительный анализ пяти актуальных работ позволяет сделать следующие выводы. Проблема обнаружения длительных соединений (long connection) и периодических сигналов (beaconing) в C2-каналах является актуальной и находит отражение как в отечественной, так и в зарубежной научной литературе. В русскоязычных исследованиях преобладают работы, предлагающие конкретные алгоритмы и инструментальные решения с использованием открытого программного обеспечения (Zeek, Scapy), тогда как в зарубежных – экспериментальные исследования, направленные на анализ уязвимостей существующих детекторов и адаптацию к новым версиям протоколов (TLS 1.3).

Ключевым трендом является переход от сигнатурных методов к поведенческим и статистическим, что обусловлено активным применением злоумышленниками шифрования и обфускации трафика. Вычисление статистических параметров сетевых сессий (длительность, вариация интервалов, частота запросов, асимметрия трафика) позволяет эффективно выявлять аномалии, характерные для long connection и beaconing.

Важным результатом зарубежных исследований является демонстрация уязвимости существующих детекторов к простым методам уклонения – в частности, к искусственному увеличению длительности потока, а также разработка методов адаптации обнаружения к TLS 1.3. Эти результаты подчеркивают необходимость постоянного совершенствования методов обнаружения с учетом эволюции протоколов и тактик злоумышленников.

Перспективным направлением дальнейших исследований является разработка гибридных моделей обнаружения, сочетающих статистический анализ с методами машинного обучения, а также адаптация существующих подходов к специфике российских информационно-телекоммуникационных систем и критической информационной инфраструктуры.

Список используемых источников

1. Скорых М. А. Алгоритм обнаружения каналов управления вредоносного программного обеспечения в сетевом трафике с использованием статистических параметров // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и XIV Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2025. С. 244–248.

2. Козачок А. В., Кочетков Е. В. Обнаружение вредоносного программного обеспечения на основе выявления аномальной сетевой активности // Информационные системы и технологии. 2016. № 5(97). С. 107–114. EDN: WXIKER.

3. Подшибкин А. С., Степанюк О. М. Разработка и применение метода оперативного выявления HTTP-туннелирования в сетевом трафике информационно-телекоммуникационных систем // Известия ТулГУ. Технические науки. 2025. Номер 2. С. 387-399.

4. Barradas D., Novo C., Portela B., Romeiro S., Santos N. Extending C2 Traffic Detection Methodologies: From TLS 1.2 to TLS 1.3-enabled Malware // Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024). ACM, 2024. P. 181–196. DOI: 10.1145/3678890.3678921.

5. Novo C., Morla R. Flow-based detection and proxy-based evasion of encrypted malware C2 traffic // Proceedings of the 13th ACM Workshop on Artificial Intelligence and Security (AISec 2020). ACM, 2020. P. 83–91. DOI: 10.1145/3411508.3421379.

Статья представлена научным руководителем, старшим преподавателем кафедры ИКБС СПбГУТ М. А. Скорых.

УДК 004.056.53

МЕТОДЫ ОГРАНИЧЕНИЯ ПОВЕРХНОСТИ АТАК В ИНФРАСТРУКТУРЕ ЦЕНТРА ОБРАБОТКИ ДАННЫХ, ОСНОВАННЫХ НА ШТАТНЫХ СРЕДСТВАХ АВТОМАТИЗАЦИИ ZABBIX

О. С. Грибов (студент группы ИБС-21 СПбГУТ), gribov.os@sut.ru

Современные центры обработки данных представляют собой сложную совокупность ИТ-инфраструктуры и инженерных систем, где обеспечение непрерывной доступности сервисов напрямую зависит от качества программно-аппаратного мониторинга. Система Zabbix занимает центральное место в управлении инфраструктурой предприятия, позволяя отслеживать состояние не только сетевого оборудования, но и вспомогательных устройств. Однако широкие возможности автоматизации и наличие штатных механизмов удаленного выполнения команд создают дополнительные риски безопасности. В статье рассматривается комплекс мер защиты, направленный на минимизацию поверхности атаки.

Zabbix, Zabbix агент, мониторинг инфраструктуры, удаленное выполнение кода, уязвимость, комплекс мер защиты, центр обработки данных, информационная безопасность

В условиях цифровой трансформации современные центры обработки данных функционируют как многокомпонентные системы, отказоустойчивость которых определяет стабильность критически важных сервисов. Для обеспечения оперативного контроля состояния ИТ-инфраструктуры обосновано применение специализированных платформ, в частности системы Zabbix, реализующей функции комплексного мониторинга.

Функциональная архитектура рассматриваемой системы обеспечивает сбор и анализ данных на нескольких уровнях. На аппаратном уровне посредством стандарта IPMI осуществляется агрегация показателей физического состояния компонентов: температурных режимов, параметров электропитания и интенсивности работы систем охлаждения. Подобная диагностика позволяет минимизировать риски возникновения аппаратных инцидентов. Системный уровень мониторинга включает регистрацию метрик производительности дисковых подсистем, аудит целостности файлов и контроль параметров идентификации узлов (время непрерывной работы, сетевое имя) [1].

Сетевой сегмент мониторинга характеризуется детальным анализом пропускной способности с дифференциацией входящих и исходящих потоков, а также верификацией состояния интерфейсов и протоколированием ошибок. На прикладном уровне система позволяет осуществлять мониторинг многих сервисов и аудит жизненного цикла сертификатов. Интеграция вспомогательного оборудования, включая источники бесперебойного питания, в единый мониторинговый контур обеспечивает целостность управления инфраструктурой [2, 3]. Централизация телеметрии и ее визуализация в реальном времени способствуют переходу к проактивному управлению инцидентами, позволяя идентифицировать аномалии в работе систем до наступления критических сбоев.

Гетерогенность контролируемой инфраструктуры и необходимость взаимодействия с широким спектром оконечных устройств обуславливают требования к высокой адаптивности и расширяемости системы мониторинга. В Zabbix реализация данных свойств обеспечивается механизмами внешних проверок и поддержкой интерпретируемых языков программирования (Ruby, Python, Perl, Shell) [4, 5, 6]. Однако наличие развитого инструментария автоматизации расширяет поверхность атаки и формирует дополнительные векторы компрометации информационной безопасности.

Анализ практики эксплуатации системы подтверждает, что штатный функционал автоматизации может быть использован для реализации деструктивных воздействий [7]. В частности, критическая уязвимость CVE-2013-3628, реализованная в рамках фреймворка Metasploit, позволяла авторизованному злоумышленнику осуществлять инъекцию и исполнение произвольного программного кода на стороне сервера мониторинга через локальный интерфейс 127.0.0.1, что фактически приводило к полной компрометации узла [8]. Аналогичные риски информационной безопасности характерны и для более современных версий системы: уязвимость CVE-2021-46088 открывает возможность удаленного выполнения команд на сервере приложений пользователем с административными привилегиями в интерфейсе Zabbix [9].

Вместе с тем, риски информационной безопасности не ограничиваются центральным узлом, архитектурные спецификации Zabbix позволяют масштабировать данные угрозы на всю ИТ-инфраструктуру организации. Архитектура системы базируется на взаимодействии центрального сервера и программных агентов, установленных на оконечных узлах. Основной де-

структивный потенциал заключается в функционале удаленного выполнения команд и возможности запуска произвольных сценариев. Активация параметра EnableRemoteCommands=1 для оперативного реагирования на инциденты позволяет агенту обрабатывать системные вызовы через ключ system.run []. В случае компрометации центрального сервера данный механизм фактически трансформируется в легитимный бэкдор [10], обеспечивающий злоумышленнику доступ к целевым хостам. Данный процесс проиллюстрирован на рис. 1.

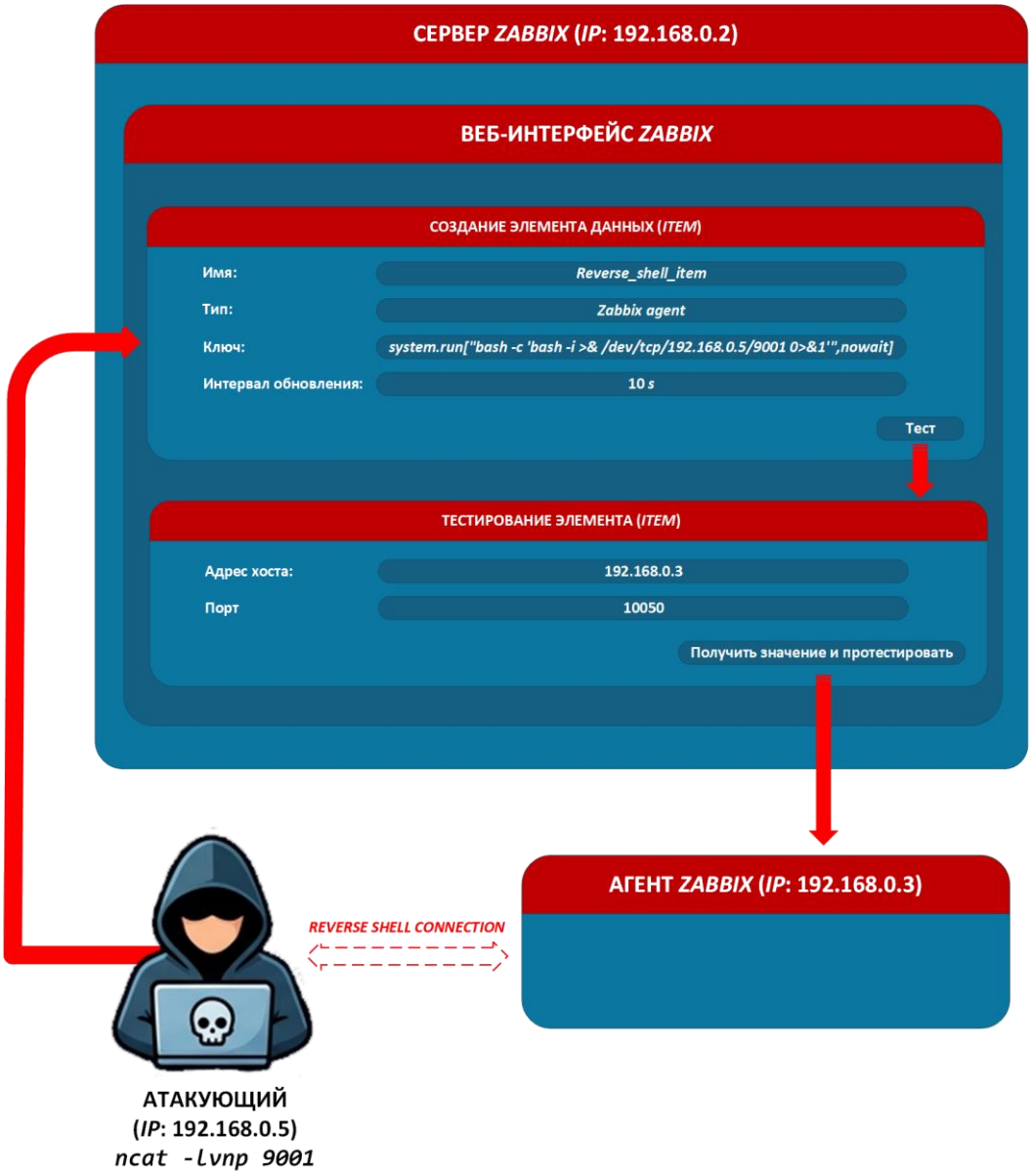


Рис. 1. Реализация Reverse Shell через функционал Zabbix

Анализ механизмов обеспечения безопасности инфраструктуры мониторинга указывает на критическую значимость комплексной защиты как

оконечных агентов, так и центрального сервера. Основополагающим методом предотвращения несанкционированного удаленного выполнения кода является реализация принципа минимизации функционала: параметр EnableRemoteCommands в конфигурационном файле zabbix_agentd.conf должен быть установлен в ноль по умолчанию. В условиях производственной необходимости автоматизации процессов следует исключить использование универсального ключа system.run [*], заменив его на механизмы формирования белых списков посредством директив AllowKey и DenyKey. Это позволяет жестко регламентировать перечень допустимых инструкций и пресечь возможность инъекции произвольного программного кода.

Техническая реализация данных мер должна сопровождаться соблюдением принципа наименьших привилегий [11, 12] на уровне операционной системы. Запуск процессов агента от имени суперпользователя root недопустим, использование выделенной учетной записи zabbix существенно ограничивает возможности злоумышленника по закреплению в системе в случае компрометации службы. Логическим дополнением выступает внедрение строгой ролевой модели доступа непосредственно в веб-интерфейсе системы. Разграничение прав операторов [13, 14] исключает техническую возможность модификации сценариев реагирования и создания вредоносных элементов данных через консоль управления.

Завершающим этапом формирования защищенного контура является сетевая изоляция: применение параметра Server для авторизации запросов только с IP-адреса управляющего узла [15] и корректная настройка межсетевых экранов. Ограничение входящего трафика на порт 10050 исключительно доверенными адресами сервера трансформирует сегмент мониторинга в закрытую систему, устойчивую к внешним вторжениям и рискам горизонтального перемещения [16] внутри корпоративной сети.

Список используемых источников

1. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. Исследование модели сети ЦОД на основе политик CISCO ACI // Защита информации. Инсайд. 2019. № 4 (88). С. 32-43.

2. Смушкин В. А. ZABBIX для мониторинга в IT-инфраструктуре [Электронный ресурс] // Форум молодых ученых: электрон. научн. журн. 2019. № 4 (32). С. 958–962. URL: http://forum-nauka.ru (дата обращения: 10.02.2026).

3. Сапожников К. Ю. Использование системы Zabbix для мониторинга сетеобразующего и вспомогательного оборудования предприятия // Индустриальная Россия: вчера, сегодня, завтра: материалы III междунар. науч.-практ. конф., Уфа, 11 авг. 2020 г. Уфа: НИЦ Вестник науки, 2020. С. 52–57.

4. Половинко Е. В., Половинко С. О. Программно-аппаратный мониторинг устройств локальной вычислительной сети как средство предотвращения нарушений информационной безопасности предприятия [Электронный ресурс] // Форум молодых ученых: электрон. научн. журн. 2019. № 11 (39). С. 345–349. URL: http://forum-nauka.ru (дата обращения: 10.02.2026).

5. Пестов И. Е., Короченцев А. Е. Управление системой мониторинга и решение простейших задач администрирования в центрах обработки данных с использованием искусственного интеллекта // Цифровое будущее науки и образования: тренды и перспективы: сб. науч. тр. Казань: Базис, 2024. С. 193–196.

6. Пестов И. Е., Виткова Л. А., Шемякин С. Н. Технологии обеспечения информационной безопасности больших данных: учеб. пособие. СПб.: СПбГУТ, 2025. 94 с.

7. Бирих Э. В., Рябов Е. Ю., Сахаров Д. В. Методология формирования модели угроз безопасности информационных систем // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С. В. Бачевского. 2017. С. 103-107.

8. CVE-2013-3628 Detail [Электронный ресурс] // National Vulnerability Database. URL: https://nvd.nist.gov/vuln/detail/CVE-2013-3628 (дата обращения: 14.02.2026).

9. CVE-2021-46088 Detail [Электронный ресурс] // National Vulnerability Database. URL: https://nvd.nist.gov/vuln/detail/CVE-2021-46088 (дата обращения: 14.02.2026).

10. Климов Р. А. Актуальные уязвимости систем мониторинга [Электронный ресурс] // Научно-исследовательская работа обучающихся и молодых ученых: материалы юбилейной 75-й Всерос. (с междунар. участием) науч. конф. обучающихся и молодых ученых. Петрозаводск: Изд-во ПетрГУ, 2023. С. 451–454. URL: https://elibrary.petrsu.ru/books/64653 (дата обращения: 11.02.2026).

11. Рекомендации по безопасности [Электронный ресурс] // Zabbix Documentation 6.4: руководство пользователя. URL: https://www.zabbix.com/ documentation/6.4/ ru/manual/installation/requirements/best_practices (дата обращения: 16.02.2026).

12. Андрианов В. И., Бухарин В. В., Кирьянов А. В., Липатников В. А., Санин И. Ю., Сахаров Д. В., Стародубцев Ю. И. Способ защиты информационно-вычислительных сетей от компьютерных атак // Патент на изобретение RU 2472211 C1, 10.01.2013. Заявка № 2011147613/08 от 23.11.2011.

13. Minyaev A.A., Krasov A.V., Saharov D.V. The method and methodology of efficiency assessment of protection system of distributed information systems // В сборнике: 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020. Brno, 2020. С. 291-295.

14. Костарев С. В., Липатников В. А., Сахаров Д. В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120-125.

15. Махмутова Н. Ф., Бирих Э. В., Сахаров Д. В., Кривец А. С., Дегтярев М. А. Исследование способов повышения безопасности корпоративных сетей // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51. № 3. С. 110-116.

16. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных // Санкт-Петербург, 2019.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Д. В. Сахаровым

УДК 004.7

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ПО УРОВНЯМ МОДЕЛИ OSI

Ю. В. Денисова (старший преподаватель кафедры СОД СПбГУТ)
А. Р. Кушнир (студент группы ИСТ-223 СПбГУТ), kushnir.ar@sut.ru

Современная цифровая инфраструктура организаций все в большей степени зависит от устойчивости сетевого взаимодействия, поэтому вопросы анализа угроз информационной безопасности на различных уровнях сетевой архитектуры имеют высокую практическую и научную значимость. По данным организации ENISA, сохраняется довольно высокий уровень активности атакующих. Заметную роль продолжают играть веб-угрозы, социальная инженерия, компрометация данных, нарушение доступности цифровых сервисов. Одновременно CISA указывает, что распределенные атаки типа DDoS остаются по-прежнему одними из наиболее распространенных способов нарушения сетевых ресурсов.

В этих условиях использование модели OSI, как аналитического инструмента, позволяющего систематизировать угрозы в зависимости от уровня сетевого взаимодействия и воздействия на информационную систему, приобретает особую ценность. Послойный подход помогает структурировать угрозы, сопоставлять им типовые механизмы реализации и выбирать меры защиты несмотря на то, что в современных сетях воздействие на информационную систему затрагивают несколько уровней одновременно.

информационная безопасность, модель OSI, сетевые угрозы, уровни OSI, кибербезопасность, сетевые атаки, защита информации

Модель OSI традиционно рассматривается, как универсальная схема, описывающая процессы сетевого взаимодействия на семи уровнях: физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном. Несмотря на то, что в современных сетях взаимодействие протоколов и сервисов довольно часто выходит за рамки одного уровня, данная модель сохраняет ценность в задачах классификации угроз и выборе защитных мер [1, 2]. NIST в актуальных документах по управлению киберрисками исходит из того, что защита информационной инфраструктуры должна строиться как многоуровневая система, в которой контроль взаимодействия сочетается с контролем доступа и мониторинга.

Использование модели OSI в контексте информационной безопасности позволяет соотнести тип угрозы с уровнем, на котором реализуется деструктивное воздействие. Такой подход важен при анализе сетевых атак, поскольку один и тот же инцидент может затрагивать различные компоненты инфраструктуры: каналы связи, маршрутизацию, прикладные сервисы. Для

каждого уровня можно выделить характерные уязвимости, типовые механизмы атак и соответствующие средства защиты [3, 4]. NIST подчеркивает роль фильтрации трафика и сегментации при снижении рисков сетевых инцидентов.

Следует учитывать, что в реальных условиях многие атаки имеют межуровневый характер. Например, нарушение маршрутизации может привести к перехвату или перенаправлению трафика, а компрометация прикладного сервиса способна стать основой для дальнейшего перемещения атакующего внутри сети. Из-за этого модель OSI нужно рассматривать не как жесткую техническую границу между уровнями, а как аналитическую основу для систематизации угроз в сложной сетевой среде [1, 2, 5]. ENISA в обзоре угроз 2025 года отмечает тенденцию к комбинированным и непрерывным кампаниям, которые воздействуют на устойчивость цифровой инфраструктуры сразу по нескольким направлениям.

В рамках прикладного анализа угроз нужно учитывать, что не все уровни модели OSI обладают одинаковой значимостью с точки зрения современных сетевых атак. Наиболее практическое значение имеют физический, канальный, сетевой и транспортный уровни, поскольку именно на них формируются базовые условия передачи данных, маршрутизации, установления соединений и устойчивости сетевого взаимодействия, а также именно в пределах этих уровней реализуются распространенные атаки.

Физический уровень связан с передачей сигналов по среде распространения и потому подвержен угрозам, связанным с физическим взаимодействием на элементы инфраструктуры. К этим угрозам относятся повреждение кабелей, отключение оборудования, несанкционированное подключение к сетевой среде, создание помех, нарушающих передачу сигнала. Для беспроводных сетей важное значение имеют перехват сигнала, подмена точки доступа и использование слабых параметров конфигурации беспроводной сети [6]. NIST указывает, что сети IEEE 802.11 обычно более уязвимы, чем проводные сегменты, из-за доступности радиосреды и распространенности небезопасных конфигураций.

Нарушения на физическом уровне способны привести не только к потере доступности, но и к созданию условий для дальнейших атак на вышележащие уровни. Например, несанкционированный физический доступ к сетевому устройству может позволить изменить его конфигурацию, подключить постороннее оборудование или организовать скрытое наблюдение

за трафиком. В связи с этим в качестве базовых мер защиты рассматриваются контроль физического доступа, резервирование критически важных компонентов, защита кабельной инфраструктуры, а также применение безопасных режимов настройки беспроводных сетей [4, 5]. Также рекомендации отдельно включают жесткую настройку параметров безопасности, мониторинг точек доступа и контроль подключаемых устройств.

Канальный уровень обеспечивает передачу кадров внутри локального сегмента сети. К его угрозам относятся действия, связанные с подменой адресной информации, несанкционированным включением узла в сетевой сегмент и атаками на механизмы коммутации. В локальных сетях к наиболее известным угрозам относятся MAC spoofing, атаки на ARP-механизмы, подключения неавторизованных устройств и эксплуатация ошибок конфигурации коммутаторов. В беспроводных сетях этот уровень связан с механизмами аутентификации и доступа к среде передачи [5].

Уязвимости канального уровня создают условия для перехвата трафика, обхода политик сегментации и распространения атаки внутри локальной инфраструктуры. В рамках современной практики защиты для снижения рисков применяются контроль доступа к портам, сегментация сети, использование защищенных беспроводных конфигураций, постоянный мониторинг сетевого сегмента и ограничение доверия к устройствам только на основании их нахождения внутри локальной сети [2, 6]. Этот подход соответствует принципам zero trust.

Сетевой уровень отвечает за логическую адресацию и маршрутизацию, поэтому именно на нем реализуется значительная часть критических сетевых атак. К числу основных угроз относятся IP spoofing, манипулирование маршрутами, перегрузка сетевой инфраструктуры, а также атаки, нарушающие корректную доставку пакетов. Существенную опасность представляют DDoS-атаки, направленные на исчерпание пропускной способности канала или ресурсов сетевых устройств [7].

Отдельную группу угроз сетевого уровня составляют атаки на механизмы маршрутизации. В глобальной инфраструктуре Интернета особую значимость имеют риски, связанные с BGP, поскольку нарушения обмена маршрутной информацией способны привести к перенаправлению, потере или перехвату трафика. В RFC 7454 рассматриваются меры защиты BGP-сессий и контроля распространяемой маршрутной информации, которая включает фильтрацию префиксов, ограничение аномальных маршрутов и защиту сеансового взаимодействия между маршрутами [8].

Также в качестве мер противодействия угрозам сетевого уровня применяются фильтрация трафика, межсетевые экраны, сегментация, контроль маршрутизации, механизмы VPN и криптографическая защита передачи данных. IPsec предоставляет сетевому уровню сервисы конфиденциальности, целостности и аутентификации, что делает его важным инструментом защиты при передаче информации через сеть [4, 9].

На транспортном уровне угрозы связаны прежде всего с нарушением установления и поддержания сетевых соединений. К таким угрозам относятся TCP flood, SYN flood, UDP flood, иные формы перегрузки транспортных механизмов, которые приводят к ухудшению доступности сервиса или отказу в обслуживании [7]. В ряде случаев транспортный уровень также становится объектом эксплуатации из-за некорректной обработки соединений, ошибок управления сессиями и отсутствия должной фильтрации трафика [4]. CISA относит подобные сценарии к числу практически значимых разновидностей DoS и DDoS воздействия.

Меры защиты на транспортном уровне включают ограничение аномальной активности, фильтрацию подозрительных соединений, настройку межсетевых экранов, использование систем обнаружения и предотвращение вторжений, а также применение криптографических протоколов поверх транспортного взаимодействия. Несмотря на то, что шифрование не устраняет возможность перегрузки транспортных соединений, оно снижает риски перехвата и модификации передаваемых данных [4]. RFC 8446 определяет TLS 1.3 как протокол, предназначенный для предотвращения прослушивания, подмены и фальсификации сообщений между приложениями.

ТАБЛИЦА 1: Основные атаки и степень риска

Название атаки	Степень риска
Физический уровень	
Повреждение кабельной инфраструктуры	Высокая
Отключение сетевого оборудования	Высокая
Несанкционированный физический доступ к устройствам	Высокая
Создание радиопомех в беспроводной среде	Средняя

Название атаки	Степень риска
Подмена беспроводной точки доступа	Высокая
Канальный уровень	
MAC spoofing	Средняя
ARP spoofing	Высокая
Атаки на механизмы коммутации	Высокая
Сетевой уровень	
IP spoofing	Высокая
DDoS атака на сетевую инфраструктуру	Высокая
Манипулирование маршрутами	Высокая
Перенаправление трафика	Высокая
Транспортный уровень	
SYN flood	Высокая
TCP flood	Высокая
UDP flood	Высокая
Нарушение установления соединений	Средняя

Для систематизации рассмотренных угроз целесообразно представить их в табличной форме с указанием степени риска. Оценка степени риска носит качественный характер и определяется потенциальным влиянием атаки на доступность, целостность и конфиденциальность сетевого взаимодействия.

Высокая – атака может привести к серьезному нарушению доступности, перехвату трафика или компрометации инфраструктуры;

Средняя – атака опасна, но обычно требует дополнительных условий или ограничена по последствиям;

Низкая – атака имеет локальный характер или сравнительно легко компенсируется стандартными мерами защиты.

Список используемых источников

1. NIST. The Cybersecurity Framework (CSF) 2.0. Gaithersburg: National Institute of Standards and Technology, 2024.

2. NIST. Zero Trust Architecture. SP 800-207. Gaithersburg: National Institute of Standards and Technology, 2020.

3. NIST. Guidelines on Firewalls and Firewall Policy. SP 800-41 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2009.

4. ENISA. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity, 2025.

5. NIST. Guidelines for Securing Wireless Local Area Networks (WLANs). SP 800-153. Gaithersburg: National Institute of Standards and Technology, 2012.

6. CISA. Understanding and Responding to Distributed Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency, 2024.

7. IETF RFC 7454. BGP Operations and Security. RFC Editor, 2015.

8. NIST. Guide to IPsec VPNs. SP 800-77 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2020.

9. IETF RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. RFC Editor, 2018.

Статья представлена кандидатом технических наук, доцентом кафедры СОД СПбГУТ, доцентом Ю. М. Бородянским.

УДК 004.057.8

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ МНОГОПОЛЬЗОВАТЕЛЬСКОГО ВЕБ-ПРИЛОЖЕНИЯ С СИНХРОНИЗАЦИЕЙ В РЕАЛЬНОМ ВРЕМЕНИ

В. Е. Дрепа (аспирант кафедры ИБКС СПбГУТ) drepa.ve@sut.ru
В. Е. Филимонов (студент группы Р4208 ИТМО),
vladislav2407@icloud.com

Представлены результаты экспериментального исследования производительности многопользовательского веб-приложения с синхронизацией в реальном времени. Разработан прототип графического редактора на основе React, Redux и WebSocket с применением Centrifugo. Проведена оценка задержек, масштабируемости и пропускной способности при различных уровнях нагрузки с использованием Playwright и Performance API. Результаты показали среднюю локальную задержку 22 мс и удаленную задержку 38 мс.

многопользовательские приложения, React, производительность веб-приложений, синхронизация реального времени, архитектура распределенных систем

Современные веб-приложения все чаще включают функциональность совместной работы, когда множество пользователей одновременно взаимодействует с общими данными [1]. Такие системы предъявляют специфические требования: минимальные задержки обновления интерфейса, эффективная синхронизация состояния между клиентами, корректная обработка конкурентных изменений [2]. В предыдущей работе [3] была представлена классификация архитектурных подходов к построению многопользовательских React-приложений и сформулированы критерии их эффективности. Однако практическая применимость различных решений требует экспериментального подтверждения с измерением реальных показателей производительности.

Реализованная архитектура представляет собой систему, где ответственность распределена между клиентским приложением, сервером реального времени и системой хранения. Клиентская часть использует React и Redux Toolkit для управления состоянием [4]. Данные организованы в нормализованном виде с применением плоских словарей, что обеспечивает константное время доступа $O(1)$. Серверная часть использует

Centrifugo – масштабируемый WebSocket-сервер с поддержкой модели публикации-подписки [5]. Каждому проекту соответствует отдельный канал, на который подписываются участники.

Синхронизация состояния реализована через WebSocket middleware, перехватывающий действия Redux и транслирующий их другим участникам (рисунок 1) [6]. Для обеспечения отзывчивости применяется паттерн оптимистичных обновлений: изменения применяются локально без ожидания подтверждения [7]. При конфликтах используется стратегия последнего писателя с детерминированным порядком доставки через Centrifugo. События с высокой частотой генерации буферизуются с интервалом 16-50 мс, что снижает нагрузку в 5-10 раз (рисунок 2) [8]. На стороне получателя применяется интерполяция координат для сглаживания обновлений.

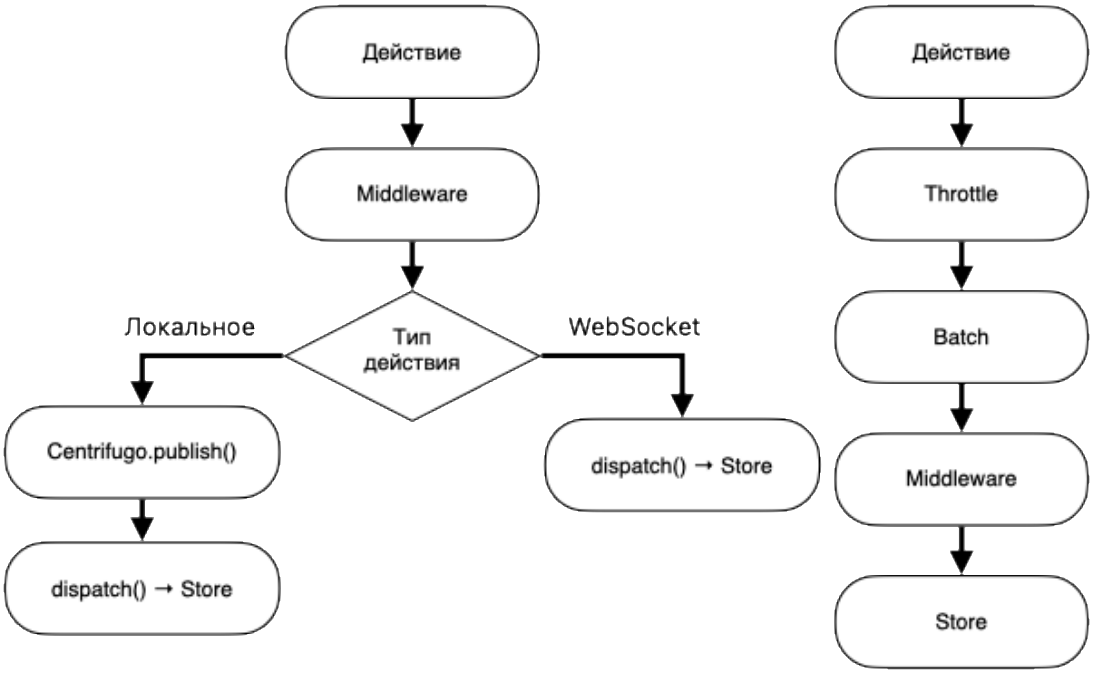


Рис. 1. Архитектура WebSocket middleware и поток данных

Тестирование выполнялось на MacBook Pro (M3 Pro, 18 ГБ ОЗУ) для клиента и удаленном сервере (2 ЦПУ 2.8 ГГц, 2 ГБ ОЗУ) для серверной части. Средний RTT составил 5,4 мс. Для автоматизации использовалась библиотека Playwright, каждый экземпляр браузера моделировал отдельного пользователя. Измерение выполнялось через Performance API браузера.

Оценивались следующие метрики: локальная задержка (действие → отображение), удаленная задержка (клиент → клиент), масштабируемость (1-10 пользователей), пропускная способность (операций/с) в режимах «burst» и «sustained», согласованность данных (сравнение итоговых состояний).

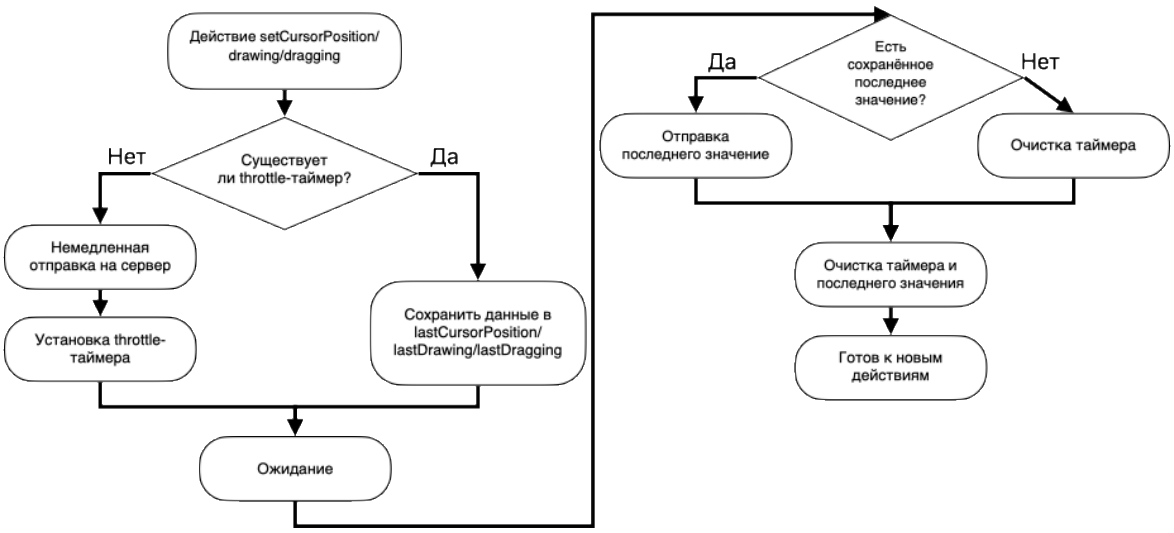


Рис. 2. Реализация тротлинга в middleware

Измерение локальной задержки показало среднее значение 22,0 мс при разбросе 21,1-23,1 мс (таблица 1), что значительно ниже порога восприятия ~100мс [9]. Удаленная задержка составила 38,1 мс при среднем RTT 5,4мс (таблица 2), что соответствует требованиям систем реального времени (100-150мс) [10]. Основная часть задержки (~33 мс) приходится на обработку данных и рендеринг, а не на сетевую передачу.

ТАБЛИЦА 1. Результаты измерения локальной задержки

Метрика	Значение, мс
Среднее	22,0
95-й перцентиль	22,9
99-й перцентиль	23,1
Минимум	21,1
Максимум	23,1

ТАБЛИЦА 2. Результаты измерения удаленной задержки

Метрика	Значение, мс
Среднее	38,1
95-й перцентиль	45,1
99-й перцентиль	48,6
Минимум	32,7
Максимум	48,6

Исследование масштабируемости (таблица 3) выявило линейный рост до 5 пользователей: задержка увеличилась с 26-27 мс (1-2 пользователя) до 62,9 мс (5 пользователей). При 8 пользователях средняя задержка достигла 121,1мс, при 10 – 202,7 мс. Характер роста приближается к $O(nlogn)$, что типично для централизованной координации [11]. Основная причина – квадратичный рост трафика: каждое действие транслируется всем участникам. Согласованность данных сохранилась во всех конфигурациях. Потребление памяти выросло незначительно: от 23,4 МБ до 32,5 Мб.

ТАБЛИЦА 3. Результаты тестирования масштабируемости

Пользователи	Средняя задержка, мс	95-й перцентиль, мс	Пропускная способность, оп./с	Память, Мб
1	26,9	29,1	2,0	23,4
2	26,3	32,7	4,0	26,3
5	62,9	124,1	9,99	31,8
8	121,1	231,5	15,63	32,0
10	202,7	507,3	15,36	32,5

Тестирование пропускной способности (таблица 4) показало 18,6 операций/с в режиме «burst» (185 операций за 10 с) и 15,1 операций/с в режиме «sustained» (452 операции за 30 с) без деградации. Эти значения превышают типичную интенсивность пользователя (5-10 операций/с).

ТАБЛИЦА 4. Результаты теста пропускной способности WebSocket

Режим	Длительность, с	Операции	Пропускная способность, оп./с	Средняя задержка, мс	95-й перцентиль, мс
Burst	10,00	185	18,61	22,05	22,80
Sustained	30,00	452	15,14	24,91	30,79

Нагрузочное тестирование Centrifugo (таблица 5) с 10-1000 клиентами показало стабильную задержку 1-2 мс без потерь сообщений. Пропускная способность составила 85-91 сообщений/с независимо от числа подписчиков. Centrifugo не является узким местом архитектуры.

ТАБЛИЦА 5. Результаты нагрузочного тестирования Centrifugo

Клиенты	Сообщений	Доставлено	Потеряно	Средняя задержка, мс	95-й перцентиль, мс	Пропускная способность, сообщ./с
10	2748	2748	0	1,53	2	85,83
25	2753	2753	0	1,52	2	86,00
50	2792	2792	0	1,39	2	87,23
100	2781	2781	0	1,11	2	86,90
200	2849	2849	0	1,05	1	89,00
500	2851	2851	0	1,04	1	89,07
800	2928	2928	0	1,11	2	91,46
1000	2802	2802	0	1,61	4	87,52

Экспериментальные данные подтверждают эффективность архитектуры для групп до 5-8 пользователей. Сетевая передача занимает ~14 % удаленной задержки (5,4 мс из 38,1 мс), основное время – клиентская обработка. Система демонстрирует линейную масштабируемость до 5 пользователей, при 8-10 – наблюдается деградация. Примененные оптимизации (тротлинг, нормализация состояния, мемоизация компонентов) дали суммарное ускорение ~60 % и снижение трафика в 5-10 раз.

Для масштабирования на большее число участников рекомендуется вынести обработку WebSocket-сообщений в Web Workers, внедрить виртуализацию рендеринга для проектов с тысячами объектов и рассмотреть переход от стратегии последнего писателя к алгоритмам операционных преобразований для более интеллектуального разрешения конфликтов.

Проведенное исследование подтвердило эффективность архитектуры многопользовательского веб-приложения на базе React, Redux и WebSocket с Centrifugo. Измеренные характеристики соответствуют требованиям систем реального времени. Выявлены границы применимости (оптимально для 5-8 пользователей) и предложены направления оптимизации для дальнейшего масштабирования.

Список используемых источников

1. Shneiderman B., Plaisant C., Cohen M., Jacobs S. Designing the user interface: strategies for effective human-computer interaction. Boston: Pearson, 2016. 560 с.

2. Kleppmann M. Designing Data-Intensive Applications. Sebastopol: O'Reilly Media, 2017. 590 с.

3. Филимонов В. Е., Махмутова Н. Ф., Киструга А. Ю. Исследование подходов к организации архитектуры многопользовательских React-приложений // Региональная информатика и информационная безопасность: сб. тр. Санкт-Петербургской междунар. конф. и XIV Санкт-Петербургской межрегион. конф., Санкт-Петербург, 29–31 окт. 2025. СПб. 2025. С. 269–272.

4. Redux Toolkit [Электронный ресурс]: документация. URL: https://redux-toolkit.js.org (дата обращения: 10.01.2026).

5. Centrifugo [Электронный ресурс]: документация. URL: https://centrifugal.dev/docs (дата обращения: 08.06.2025).

6. Ковцур М. М., Филимонов В. Е., Винников С. А., Щеголев Е. К. Сравнение библиотек WebSocket, Socket.IO и Centrifugo для многопользовательских веб-приложений // Вопросы науки. 2024. № 2. С. 27–30.

7. Saito Y., Shapiro M. Optimistic replication // ACM Computing Surveys. 2005. Т. 37. № 1. С. 42–81.

8. Fraser N. Differential Synchronization // Proceedings of the ACM Symposium on Document Engineering. 2009.

9. Nielsen J. Response times: the three important limits [Электронный ресурс]. URL: https://www.nngroup.com/articles/response-times-3-important-limits/ (дата обращения: 10.11.2024).

10. Pimentel V., Nickerson B. G. Communicating and Displaying Real-Time Data with WebSocket // IEEE Internet Computing. 2012. Т. 16. № 4. С. 45–53.

11. Ковцур М. М., Филимонов В. Е., Щеголев Е. К. Исследование подходов для реализации многопользовательского React-приложения на языке typescript // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сборник материалов (тезисов) 53-й Международной конференции, Москва, 22 апреля 2024 года. Москва: Национальный институт радио и инфокоммуникационных технологий, 2024. С. 58-61. EDN: DEPGAY.

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ИБКС СПбГУТ М. М. Ковцуром.

УДК 004.056.5

ОБНАРУЖЕНИЕ АТАК ТИПА УДАЛЕННОГО ВЫПОЛНЕНИЯ КОДА ПРИ ПОМОЩИ EBPF И IOB

А. Г. Дроботов (студент группы ИКТЗ-25 СПбГУТ), branickii1.aa@sut.ru

Атаки удаленного выполнения кода остаются одной из наиболее критичных угроз для современных распределенных IT-систем, особенно в контейнерных средах. Традиционные сигнатурные методы защиты неэффективны против бесфайловых RCE-атак и атак через цепочки поставок. В статье рассматривается подход к runtime-детектированию RCE-атак на основе технологии eBPF и поведенческих индикаторов IoB. Предложена архитектура системы, описаны eBPF-сенсор и IoB-правила для выявления reverse shell. Приведены результаты экспериментальной проверки на демонстрационном стенде.

RCE-атаки, eBPF, IoB, поведенческий анализ, reverse shell, MITRE ATT&CK, runtime-детектирование, системные вызовы

Современные ИТ-системы все чаще строятся на основе контейнерной виртуализации (Docker, Kubernetes). Это позволяет гибко масштабировать сервисы, однако порождает новые уязвимости. Атаки типа Remote Code Execution (RCE) занимают ведущие позиции в рейтинге OWASP Top 10 [1]. Особую опасность RCE представляет в контейнерных средах, где приложения часто запускаются с повышенными привилегиями: компрометация одного контейнера может привести к захвату всего хоста.

Дополнительную сложность создают бесфайловые RCE-атаки (вредоносный код выполняется только в памяти, не оставляя следов на диске) и supply chain-атаки (например, Log4Shell, Spring4Shell), при которых уязвимость внедряется через зависимости. Многие RCE-атаки не создают заметного сетевого шума, используя DNS-tunneling или уже установленные соединения, что делает их «тихими» и труднообнаружимыми для традиционных сигнатурных средств защиты (AV, IDS/IPS).

В связи с этим актуальной задачей является разработка систем поведенческого детектирования RCE-атак в реальном времени, работающих на уровне ядра операционной системы и не требующих модификации защищаемых приложений.

Для эффективного обнаружения RCE-атак в контейнерных средах предлагается использовать комбинацию двух технологий: eBPF (перехват системных вызовов на уровне ядра) и IoB (Поведенческие паттерны атак).

eBPF (Extended Berkeley Packet Filter) [2, 3, 4] – это технология ядра Linux, позволяющая выполнять верифицированные пользовательские программы в пространстве ядра без загрузки дополнительных модулей и без перекомпиляции ядра. Изначально eBPF применялся для фильтрации сетевых пакетов, однако сегодня его область применения охватывает трассировку, мониторинг производительности, безопасность и сетевое программирование.

Архитектура eBPF выглядит следующим образом (рис. 1):

- eBPF-программа – байт-код, написанный на ограниченном подмножестве C и скомпилированный с помощью LLVM/Clang.
- Verifier – статический анализатор, который проверяет программу перед загрузкой в ядро на отсутствие бесконечных циклов, безопасный доступ к памяти и корректность типов.
- JIT-компилятор – переводит байт-код eBPF в машинные инструкции целевой архитектуры для максимальной производительности.
- Хуки – точки в ядре, к которым можно прикрепить eBPF-программу: системные вызовы (tracepoints), kprobe/uprobe, сетевые интерфейсы (XDP).
- Карты – структуры данных для обмена информацией между eBPF-программой и пользовательским пространством (хеш-таблицы, массивы, очереди, стеки).

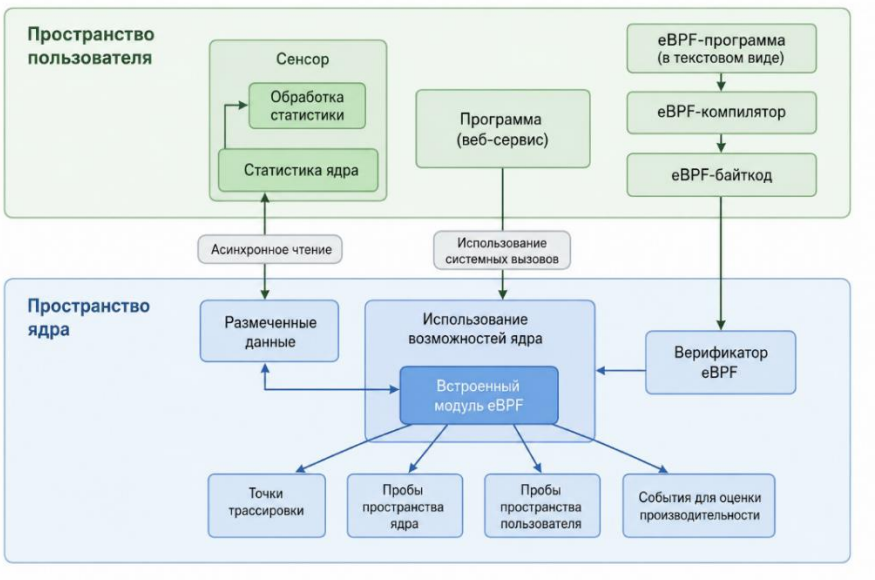


Рис. 1. Архитектура eBPF и взаимодействие основных компонентов

Для реализации сенсора в данной работе использовался bpftrace – высокоуровневый язык для однострочных сценариев и небольших программ

мониторинга. Альтернативными подходами являются библиотека BCC (BPF Compiler Collection) и современный libbpf.

Индикаторы поведения (IoB) необходимы для сбора и анализа цифровых следов пользователей, чтобы в реальном времени выявлять аномалии и автоматически адаптировать доступ к системе.

В рамках исследования выделены следующие поведенческие паттерны с привязкой к тактикам MITRE ATT&CK [5] (рис. 2):

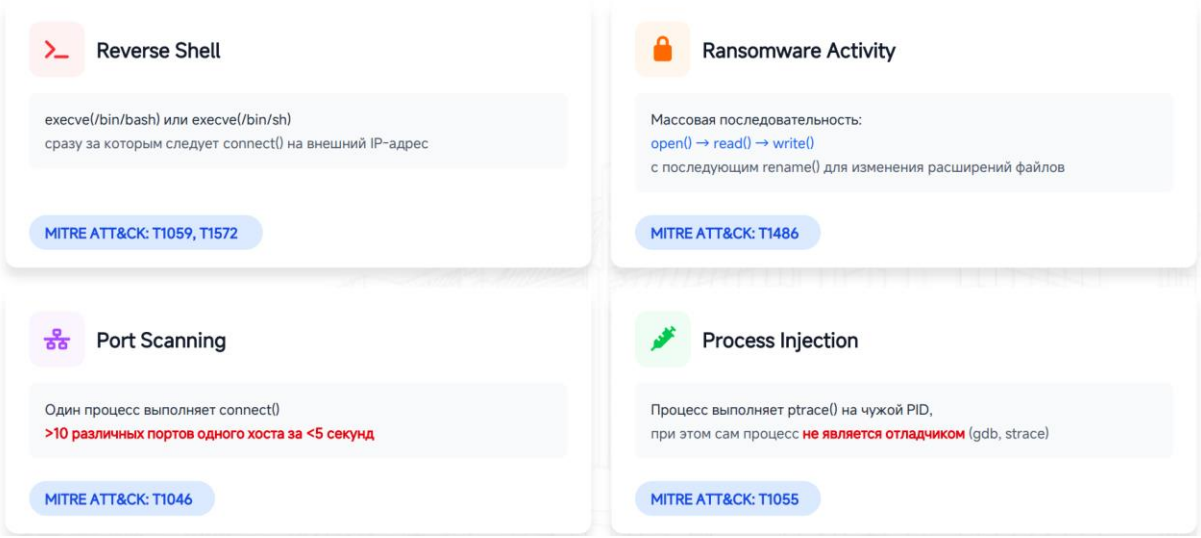


Рис. 2. Классические IoB-паттерны для детектирования атак

Для экспериментальной проверки предложенного подхода разработан демонстрационный стенд, архитектура которого представлена на рис. 3.

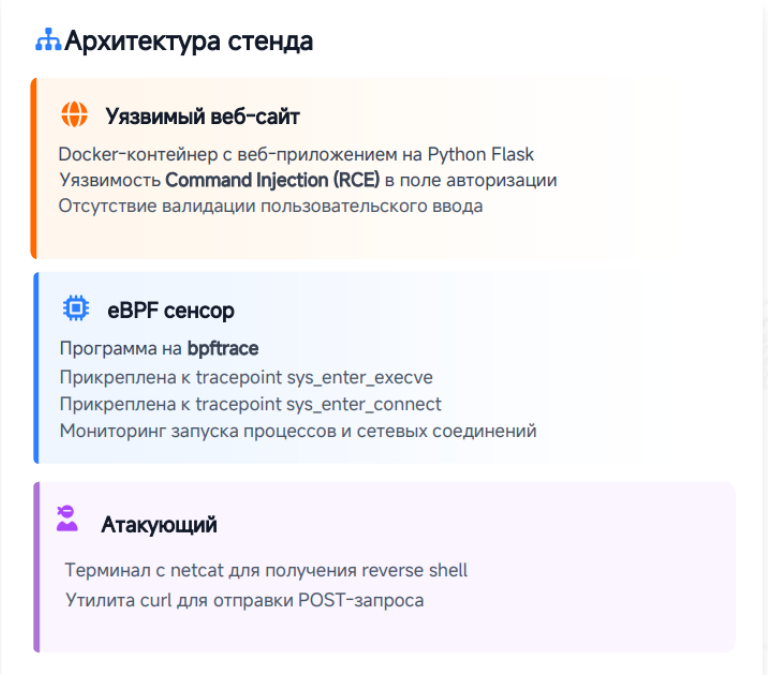


Рис. 3. Архитектура демонстрационного стенда

Сценарий атаки (результат представлен на рис. 4)

1. Атакующий запускает прослушивание порта 4444: **nc -lvnp 4444**
2. Отправляет HTTP POST-запрос через уязвимую форму: **username=admin; nc -e /bin/sh 192.168.1.100 4444**
3. Веб-приложение выполняет подстановку команды в контейнере.
4. eBPF-сенсор фиксирует IoB паттерн Reverce Shell:
- execve(/bin/sh) от процесса Python.
- connect(4444) на IP атакующего.
5. eBPF-сенсор выводит в системный журнал алерт.
6. Атакующий получает reverse shell, но факт атаки уже зафиксирован.

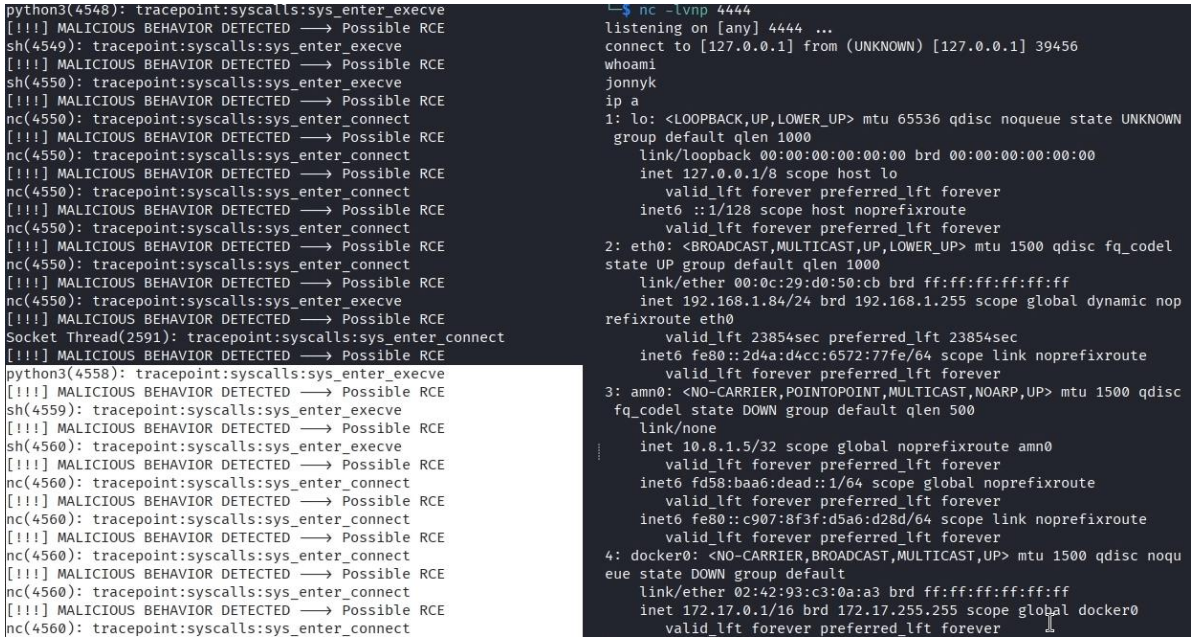


Рис. 4. Результат детектирования RCE-атаки

В результате злоумышленник получает доступ к системе, но его присутствие мгновенно обнаружено сенсором, что позволяет мгновенно отреагировать на сложившийся инцидент.

В статье рассмотрена актуальная проблема обнаружения RCE-атак в контейнерных средах. Предложен подход, основанный на комбинации технологии eBPF (перехват системных вызовов на уровне ядра) и поведенческих индикаторов IoB. Разработан демонстрационный стенд, включающий уязвимое веб-приложение на Flask, eBPF-сенсор на bpftrace и сценарий атаки типа reverse shell.

Выявлены основные ограничения текущей реализации (ложные срабатывания, отсутствие контекста, невозможность блокировки атак, сложность добавления правил) и предложены пути их устранения: интеграция с SIEM

для централизованного управления событиями ИБ и использование ML для уменьшения ложных срабатываний (рис. 5).

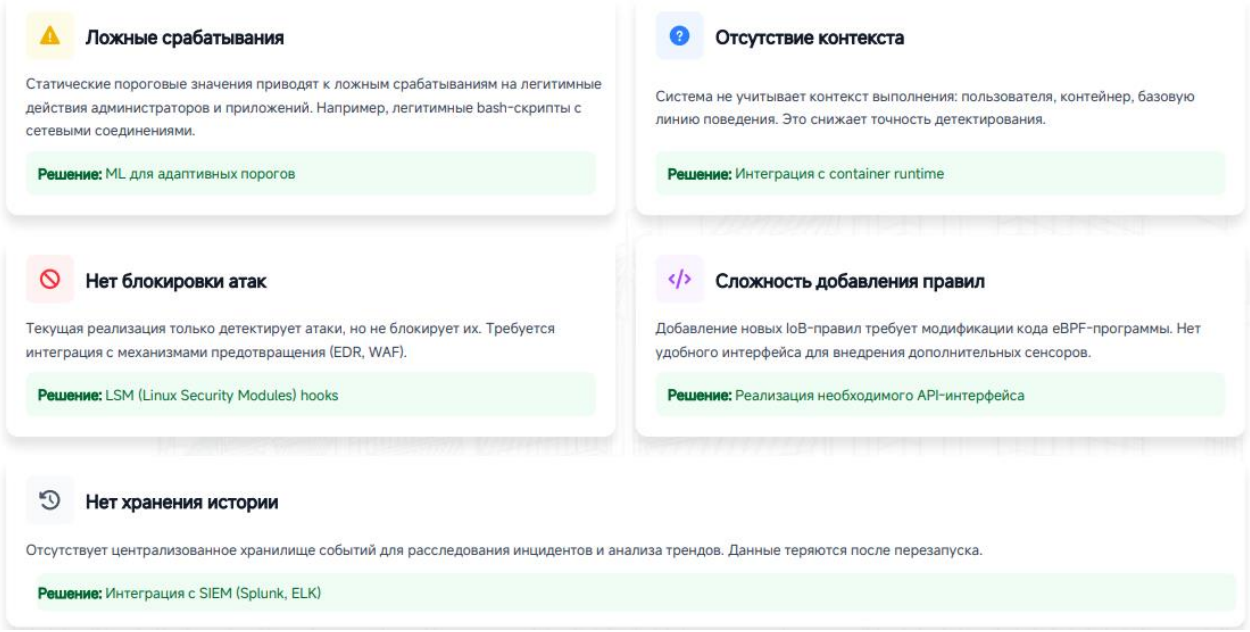


Рис. 5. Основные ограничения текущей реализации

Использование eBPF и IoB является перспективным направлением для построения систем runtime-безопасности в современных инфраструктурах.

Направление дальнейших исследований заключается в модификации существующего сенсора для уменьшения количества ложных срабатываний и интеграции моего сенсора с SIEM для централизованного управления журналами и облегчения расследований инцидентов ИБ.

Список используемых источников

1. OWASP Foundation. OWASP Top 10 – 2021. https://owasp.org/Top10/.
2. Linux Kernel documentation. BPF and XDP Reference Guide. https://docs.kernel.org/bpf/ (дата обращения: 10.03.2026).
3. Gregg B. BPF Performance Tools: Linux System and Application Observability. Addison-Wesley, 2019. 544 p.
4. Fleming M. BPF: A New Type of Software. ACM Queue, 2022. P. 45–68.
5. MITRE ATT&CK® Framework. https://attack.mitre.org/ (дата обращения: 10.03.2026).

Статья представлена научным руководителем, кандидатом технических наук, доцентом, доцентом кафедры ЗСС СПбГУТ А. А. Браницким.

УДК: 004.75

ПРОГНОЗИРОВАНИЕ ПОЛЬЗОВАТЕЛЬСКОГО ТРАФИКА БАЗОВОЙ СТАНЦИИ LTE С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ ARIMA ДЛЯ ЗАДАЧ КИИ

В. С. Елагин (к.т.н., и. о. декана факультета ИКСС СПбГУТ)
П. Д. Царев (студент группы МЗС-2512), carev.pd@sut.ru

В данной работе рассматривается задача прогнозирования пользовательского трафика базовой станции LTE с использованием математической модели ARIMA. В качестве исходных данных был сгенерирован временной ряд, имитирующий нагрузку на базовую станцию с антеннами MIMO 4×4 в условиях городской застройки. Прогнозирование выполнялось методом скользящего окна (rolling forecast), позволяющим учитывать динамику изменения нагрузки в реальном времени. Полученные результаты демонстрируют высокую точность модели и возможность ее применения в системах критической информационной инфраструктуры (КИИ) для предотвращения перегрузок и повышения надежности сети.

ARIMA, прогнозирование трафика, LTE, MIMO 4×4, временные ряды, скользящее окно, критическая информационная инфраструктура (КИИ)

Введение

Современные телекоммуникационные сети, особенно в условиях городской застройки, характеризуются высокой динамикой пользовательского трафика. Базовые станции стандарта LTE с использованием технологии MIMO 4×4 способны обеспечивать пропускную способность порядка 300–600 Мбит/с на сектор, однако фактическая нагрузка существенно изменяется в зависимости от времени суток и поведения пользователей. Современные телекоммуникационные сети, особенно в условиях городской застройки, характеризуются высокой динамикой пользовательского трафика. Базовые станции стандарта LTE с использованием технологии MIMO 4×4 способны обеспечивать пропускную способность порядка 300–600 Мбит/с на сектор, однако фактическая нагрузка существенно изменяется в зависимости от времени суток и поведения пользователей.

Теоретическая часть

Современные телекоммуникационные сети, особенно в условиях городской застройки, характеризуются высокой динамикой. В рамках данной работы был смоделирован недельный временной ряд пользовательского

трафика, отражающий: суточную цикличность (пики днем, минимумы ночью), увеличение нагрузки в выходные дни, случайные флуктуации. Далее данный ряд был обработан с использованием модели ARIMA для построения прогноза.

Модель ARIMA (AutoRegressive Integrated Moving Average) является одной из базовых моделей анализа временных рядов и описывается параметрами *(p, d, q), p* – порядок авторегрессии (AR), *d* – порядок дифференцирования, *q* – порядок скользящего среднего (MA).

Общий вид модели (1):

$$y_t = c + \sum_{i=1}^{p} \varphi_i \, y_{t-i} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j} + \varepsilon_t \,, \qquad (1)$$

где y_t – значение временного ряда, φ_i – коэффициенты авторегрессии, θ_j – коэффициенты скользящего среднего, ε_t – случайная ошибка.

Дифференцирование применяется для приведения ряда к стационарному виду (2):

$$y'_t = y_t - y_{t-1}. \qquad (2)$$

Для повышения точности прогнозирования был использован метод скользящего окна (rolling forecast). Суть метода в том, что модель обучается на имеющихся данных и выполняется прогноз следующего значения $\hat{y}_{t+1}$, в модель добавляется реальное значение y_{t+1}, далее процесс повторяется. Таким образом, модель постоянно адаптируется к новым данным, что особенно важно для повышения точности прогнозирования трафика.

Практическая часть

Ниже приведен фрагмент программной реализации на языке Python.

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
from statsmodels.tsa.arima.model import ARIMA

np.random.seed(42)

# ----------------------------
# 1. Генерация LTE трафика (неделя)
# ----------------------------
time = pd.date_range(start="2024-01-01", periods=24 * 7, freq="1h")

capacity = 600
base = 150
```

```
traffic = []

for t in time:
 hour = t.hour
 day = t.dayofweek

 daily = 200 * np.sin(2 * np.pi * (hour / 24 – 0.25)) + 200
 weekend = 100 if day >= 5 else 0
 noise = np.random.normal(0, 30)

 value = base + daily + weekend + noise
 value = max(20, min(capacity, value))

 traffic.append(value)

df = pd.DataFrame({"timestamp": time, "traffic": traffic})
df.set_index("timestamp", inplace=True)

# ----------------------------
# 2. Rolling прогноз на ВСЕМ ряде
# ----------------------------
order = (2, 1, 2)

history = []
predictions = []

for t in range(len(df)):

 # первые точки пропускаем (нужно накопить историю)
 if t < 10:
 predictions.append(np.nan)
 history.append(df ["traffic"].iloc [t])
 continue

 model = ARIMA(history, order=order)
 model_fit = model.fit()

 yhat = model_fit.forecast() [0]
 predictions.append(yhat)

 # добавляем реальное значение
 history.append(df ["traffic"].iloc [t])

# ----------------------------
# 3. График
# ----------------------------
plt.figure()

plt.plot(df.index, df ["traffic"], label="Реальный трафик")

plt.plot(df.index, predictions, linestyle='--', linewidth=2,
 label="ARIMA (скользящий прогноз)")
```

```
plt.legend()
plt.xticks(rotation=45)
plt.title("ARIMA прогноз трафика LTE (на всю неделю)")
plt.tight_layout()
plt.show()
```

В работе использовались следующие библиотеки: pandas – для работы с временными рядами, numpy – для генерации данных и вычислений, matplotlib – для построения графиков, statsmodels – реализация модели ARIMA. Библиотека statsmodels предоставляет удобный интерфейс для построения и обучения моделей временных рядов.

В рамках проведенного исследования были получены три уровня визуализации и прогнозирования пользовательского трафика базовой станции LTE. Первый график, см. рис. 1, отражает динамику нагрузки за недельный период. На нем отчетливо прослеживается суточная цикличность, а также увеличение трафика в выходные дни. Модель ARIMA демонстрирует способность описывать общий тренд и повторять структуру временного ряда, включая периоды роста нагрузки.

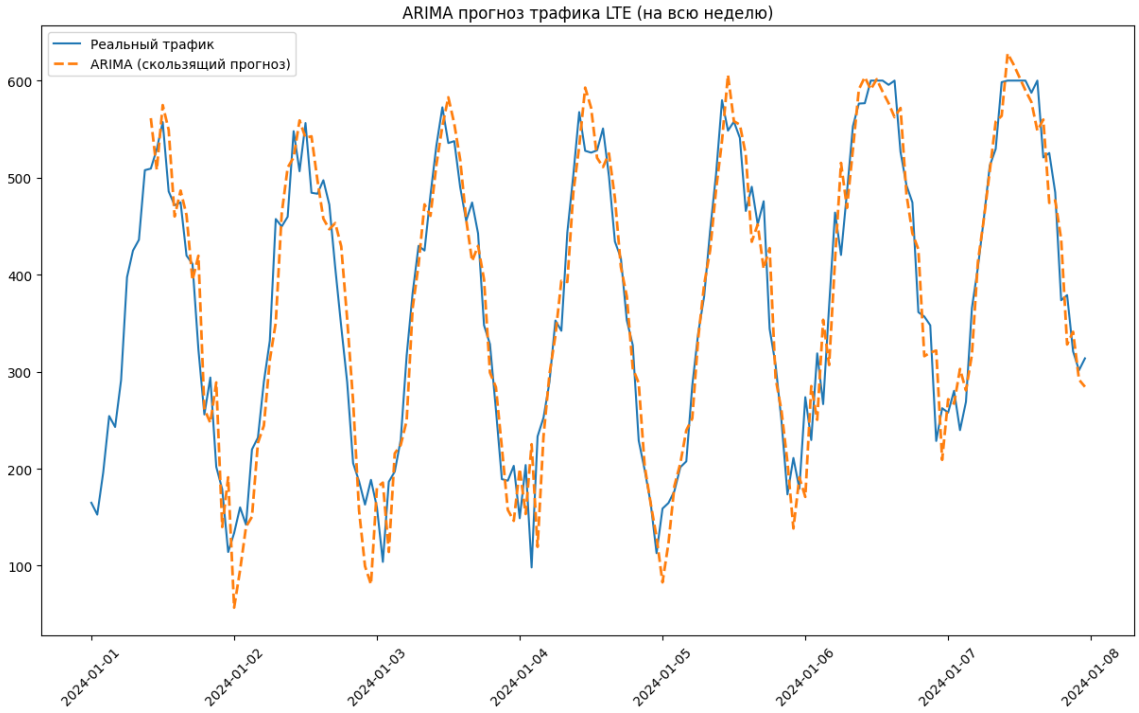


Рис. 1. Недельное прогнозирование при помощи ARIMA

Второй график, см. рис. 2, представляет более детализированный анализ для одного дня – воскресенья. В данном случае наблюдается более высокая загруженность сети по сравнению с будними днями, а также выраженные пики в дневное и вечернее время. Прогнозные значения,

полученные с использованием модели ARIMA, хорошо согласуются с фактическими данными и позволяют заранее выявить периоды максимальной нагрузки.

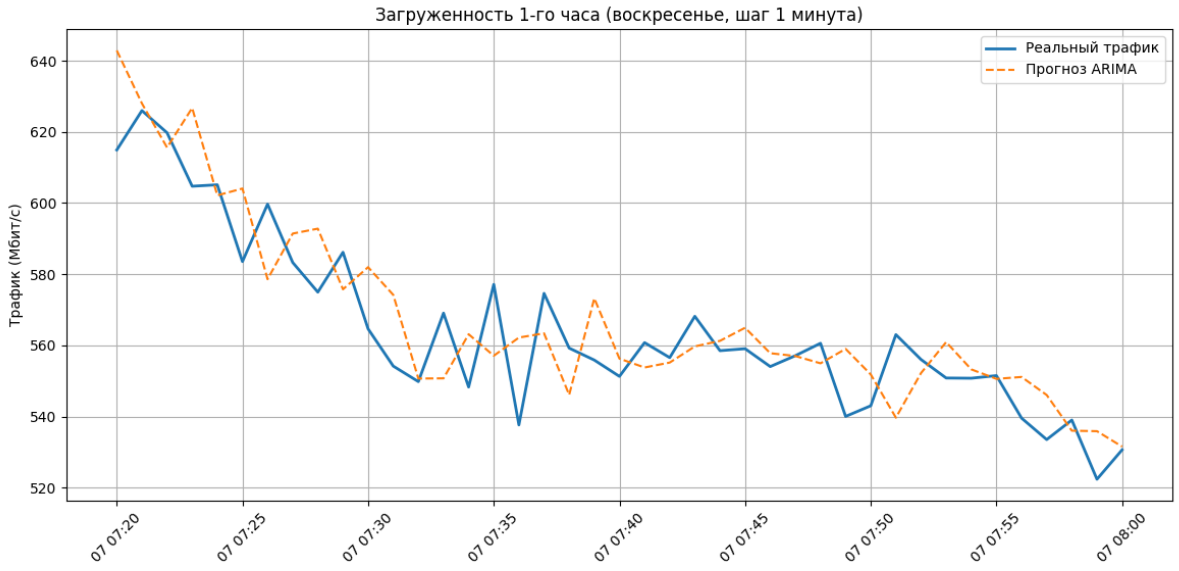


Рис. 2. Прогнозирование трафика в воскресенье при помощи ARIMA

Третий график, см. рис. 3, демонстрирует наиболее загруженный час в воскресенье с детализацией до одной минуты. С помощью такого анализа у нас появляется возможность выявлять разного рода всплески трафика. Таким образом, мы можем не допускать приближение к пиковым значениям трафика относительного общей емкости канала связи. Это важный вопрос особенно в рамках того, что базовые станции относятся к КИИ и их перегрузки критичны.



Рис. 3. Прогнозирование самого загруженного часа 7:20-8:00 при помощи ARIMA

Заключение

В ходе работы были получены графики временных рядов, на которых отображен пользовательский трафик с различными уровнями цикличности: неделя/сутки/час. На графиках видны тренды, в какой период времени происходит наибольшая загруженность канала: максимальные значения в дневное время и минимальные в ночное время. А самый высокий рост наблюдается в выходные дни, когда пользователи активно пользуются интернетом. Именно на последнем графике видно, что прогнозируется критическая загрузка под 600 Мбит/с. В ходе работы при помощи модели ARIMA получилось аппроксимировать временной ряд пользовательского трафика и повторять поведенческую характеристику графика, так же модель способна адаптироваться к входным изменяющимся параметрам при помощи метода скользящего окна, что позволяет поддерживать прогноз актуальным. Таким образом использование модели имеет прикладное значение в отношении КИИ.

Список используемых источников

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (последняя редакция). 26 июля 2017 года N 187-ФЗ.

2. Гребенщикова А. А. Обзор модели авторегрессии и проинтегрированного скользящего среднего Arima для прогнозирования сетевого трафика / А. А. Гребенщикова, В. С. Елагин // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ. 2022. Том 1. С. 266-271. EDN: PNYPJG.

3. Гребенщикова А. А. Модели авторегрессии и проинтегрированного скользящего среднего ARIMA для прогнозирования сетевого трафика // Электросвязь 2024. № 5. С. 39–46.

4. Гребенщикова А. А., Елагин В. С. Прогнозирование трафика трехмерной сети интернета вещей высокой плотности как многомерного случайного процесса // Текст научной статьи (специальность 2.2.15). Труды учебных заведений связи. 2024. Т. 10. № 4. С. 116–126. CyberLeninka URL: https://cyberleninka.ru/article/n/prognozirovanie-trafika-trehmernoy-seti-interneta-veschey-vysokoy-plotnosti-kak-mnogomernogo-sluchaynogo-protsessa (дата обращения: 27.03.2026).

5. Регуб А. В. Методика построения модели ARIMA для прогнозирования динамики временных рядов // Текст научной статьи (специальность «Математика»). Финансовый университет при Правительстве РФ. CyberLeninka URL: https://cyberleninka.ru/article/n/metodika-postroeniya-modeli-arima-dlya-prognozirovaniya-dinamiki-vremennyh-ryadov/viewer (дата обращения: 29.03.2026).

6. Соколова Э. С., Ляхманов Д. А. Анализ временных рядов технических параметров промышленных объектов // Текст научной статьи (специальность «Математика»). Нижегородский государственный технический университет им. Р. Е. Алексеева. CyberLeninka URL: https://cyberleninka.ru/article/n/analiz-vremennyh-ryadov-tehnicheskih-parametrov-promyshlennyh-obektov/viewer (дата обращения: 01.04.2026).

7. Прогнозирование временных рядов на Python // TimeWeb Cloud. URLhttps://timeweb.cloud/tutorials/python/prognozirovanie-vremennyh-ryadov-python-3 (дата обращения: 01.04.2026).

УДК 004.056

АНАЛИЗ DOS-АТАК, ПЕРЕХВАТА ВЫЗОВОВ И ФРОД–УГРОЗ В ИНФРАСТРУКТУРЕ SIP

В. С. Елагин (к.т.н., и. о. декана факультета ИКСС СПбГУТ)
Д. А. Черняков (студент группы МЗС-2512 СПбГУТ),
chernyakov.da@sut.ru

В статье рассматривается протокол IP-телефонии SIP, как основной протокол установления соединения в современных VoIP-сетях. Далее рассматриваются архитектурные и протокольные уязвимости, делающие SIP-системы подверженными атакам, типа отказ в обслуживании (DoS), нарушение конфиденциальности, компрометацию целостности и фрод. На основе анализа выявляются ключевые факторы, способствующие успешной реализации угроз.

SIP, VoIP, фрод, DoS, IP-телефония, переадресация, перехват звонка, MITM

Введение

Протокол инициализации сеанса связи SIP (Session Initiation Protocol) на протяжении последних двух десятилетий занимает центральное место в архитектуре современных систем голосовой связи. Будучи принятым в качестве стандарта IETF в марте 1999 года, он обеспечивает установление, управление и завершение мультимедийных сессий не только в корпоративных VoIP-сетях, но и в инфраструктуре крупных операторов связи. Гибкость, расширяемость и относительная простота реализации сделали SIP доминирующим протоколом сигнализации, вытеснившим устаревшие проприетарные решения.

Но, наряду с повсеместным внедрением протокола SIP появляются новые угрозы в области информационной безопасности, на которые нужно обратить должное внимание. Угрозы могут быть связаны с фродом, т.е. использованием услуг связи без их оплаты, DoS – атаками, а также с прослушиванием трафика. Целью данной статьи является систематизация и анализ уязвимостей протокола SIP, а также выявление основных угроз, реализуемых через его архитектурные недостатки. В статье рассмотрены как классические угрозы нарушения доступности и конфиденциальности, так и специфические сценарии фрода.

Архитектурные и протокольные уязвимости SIP

SIP представляет собой протокол прикладного уровня, работающий преимущественно поверх UDP или TCP. Его архитектура, основанная на текстовых сообщениях, обеспечивает гибкость, но одновременно создает ряд уязвимостей, которые могут быть использованы злоумышленниками [1].

Ключевая проблема протокола SIP заключается в том, что такие сообщения, как INVITE, REGISTER и BYE передаются в незашифрованном виде. Из-за этой особенности, злоумышленник, используя анализатор пакетов, может перехватить сигнальную информацию и извлечь из нее конфиденциальные данные, такие как номера абонентов, топологию сети или параметры сессии. В том случае, если для обмена сигнальными сообщениями используется протокол UDP, по определению не требующий установления соединения, существенно упрощается процесс подделка SIP-пакетов и проведение атак с подменой источника.

Приоритетными целями для атак являются SIP-серверы, SoftSwitch и SBC (Session Border Controller), т.к. вторжение в их работу или вывод из строя может нарушить работу всей сети. Также, большой проблемой является недостаточная фильтрация пакетов на границах систем, что в свою очередь может осложнить выявление аномальной активности на ранних этапах [2].

Основные угрозы безопасности в SIP-инфраструктуре

Выявленные уязвимости позволяют классифицировать атаки по характеру их воздействия.

1. Атаки типа DoS и Call Tampering:

Атаки на доступность являются наиболее эффективными из-за особенностей передачи голосового трафика. Даже относительно небольшое воздействие способно нарушить нормальную работу сервиса. Злоумышленник может организовать, например, массовую рассылку INVITE-запросов, что может привести к исчерпанию вычислительных ресурсов SIP-сервера и пропускной способности каналов связи. В результате атаки, легитимные запросы на установление соединения не могут быть обработаны, и услуга становится недоступной для обычных пользователей [3].

Другой вариант атаки на доступность – Call Tampering, при котором злоумышленник внедряется в существующий разговор, отправляя пустые

пакеты или поддельные сообщения, тем самым забивая медиапоток. Сервер, обрабатывая их, затрачивает дополнительные ресурсы, в результате чего возникают задержки, ухудшается качество связи, и вести беседу становится невозможно. Для тестирования уязвимостей к таким атакам могут использоваться специализированные инструменты вроде SIPp [4].

2. Угрозы типа MITM

Перехват вызова может быть реализован с помощью атаки MITM (Man-in-the-Middle. Суть атаки заключается в том, что злоумышленник подделывает MAC-адрес или DNS-запись, и далее, перенаправляет трафик через свои устройства. Инструменты вроде VoIP Hopper позволяют имитировать поведение IP-телефона для получения доступа к VLAN, выделенной для голосового трафика, собирая данные о сети, включая идентификаторы VLAN.

Получив возможность перехвата, злоумышленник может не только прослушивать разговоры, извлекая конфиденциальную информацию, но и собирать учетные данные пользователей. При отсутствии шифрования медиапотока (RTP), снифферы способны извлекать аудио из перехваченных пакетов и сохранять его, поддерживая широкий спектр кодеков, включая самый популярные G.711, GSM, G.729. Также известны случаи реализации SIP registration hijacking, когда злоумышленник, проведя DoS-атаку на клиента, регистрируется от его имени на АТС и пропускает весь трафик через зарегистрированное устройство [5].

3. Угрозы атак посредствам фрода

Также, атаки могут быть направлены на экономическую составляющую оператора связи. Наиболее опасными с такой точки зрения являются атаки, направленные на фрод, т.е. использование услуг связи без их оплаты. Примерами таких атак могут служить модификация запроса INVITE на SIP-trunk, имитация переадресации вызова с помощью ответа 302 на SIP-trunk и т.п.

Концепция первой атаки заключается в том, что злоумышленник перехватывает INVITE-сообщение от настоящего пользователя и модифицирует его таким образом, чтобы установить дополнительное соединение с выбранным абонентом за счет жертвы. Одновременно с этим, SoftSwitch, не получив ответа на перехваченный запрос, повторно отправляет INVITE и устанавливает легитимное соединение для настоящего пользователя. В результате, биллинг-система начисляет плату настоящему абоненту за два

одновременных соединения, хотя реально он участвует только в одном из них.

Цель второй атаки схожа с первой, но достигается за счет того, что инициирует вызов к абоненту-жертве, перехватывает входящий запрос INVITE и вместо того, чтобы пропустить его дальше, возвращает серверу ответ 302 Moved Temporarily. В этом ответе злоумышленник указывает номер абонента, с которым он действительно хочет соединиться. Сервер воспринимает ответ 302 как указание от самого абонента-жертвы выполнить переадресацию вызова и соединяет злоумышленника с нужным ему абонентом. В результате атаки, биллинг-система также начисляет настоящему абоненту двойную плату [6].

Вывод

В рамках работы было выявлено, что, несмотря на технологический прогресс, система сигнализации SIP остается подверженной атакам типа DoS, Call Tampering, MITM. Такая возможность существует, в основном, из-за архитектурных особенностей протокола, включая открытость сигнального трафика, использование UDP, допускающего спуффинг, и централизацию управления, создающую единые точки отказа.

Полученные результаты подтверждают необходимость дальнейшего изучения уязвимостей SIP и разработки эффективных подходов к их нейтрализации, поскольку надежная работа систем VoIP является критически важной как для бизнеса, так и для повседневной жизни пользователей.

Список используемых источников

1. Зубарев А. А. Современные проблемы защиты информации в телекоммуникационных системах на основе протоколов SIP / А. А. Зубарев // Проблемы естественных, математических и технических наук в контексте современного образования: Материалы Международной научно-практической конференции, Липецк, 24–25 октября 2024 года. Липецк: Липецкий государственный педагогический университет им. П.П. Семенова-Тян-Шанского, 2024. С. 253-257. EDN: BKVKDQ.

2. Морозов А. М. Анализ уязвимости сети SIP фрод-угрозам по результатам тестирования оборудования действующей сети / А. М. Морозов // Инженерный журнал: наука и инновации. 2013. № 2(14). С. 27. EDN: QZPWSN.

3. Юрченко Г. С. Безопасность сети VOIP / Г. С. Юрченко, Е. В. Глушко // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований: Материалы VI Всероссийской национальной научной конференции молодых ученых, Комсомольск-на-Амуре, 10–14 апреля 2023 года. Том Часть 2. Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2023. С. 412-415. EDN BGMYGS.

4. Яремчук С. Атаки на VoIP и методы защиты / С. Яремчук // Системный администратор. 2011. № 6(103). С. 62-64. EDN: RFVGQJ.

5. Крюков Ю. С. Безопасность VoIP-контента. Текущая ситуация, анализ угроз и тенденции рынка / Ю. С. Крюков // Защита информации. Инсайд. 2008. № 3(21). С. 83-91. EDN: TPHYOF.

Морозов А. М. Анализ уязвимостей сети SIP к угрозам фрода / А. М. Морозов // Электросвязь. 2013. № 7. С. 10-13. EDN: OSLMQK.

УДК 004.056.5

РАЗРАБОТКА ПОДСИСТЕМЫ БЕЗОПАСНОГО УПРАВЛЕНИЯ СЕКРЕТАМИ В ИНФРАСТРУКТУРЕ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ КОНФИГУРАЦИЯМИ

Н. Р. Калмыков (студент группы ИКБ-21 СПбГУТ), kalmykov.nr@sut.ru

В статье рассматривается разработка подсистемы безопасного управления секретами в инфраструктуре автоматизированного управления конфигурациями. Актуальность работы обусловлена тем, что в системах автоматизации конфиденциальные данные часто хранятся в конфигурационных хранилищах и передаются управляемым узлам без достаточной изоляции доступа. Это повышает риск компрометации учетных данных и последующего горизонтального перемещения внутри инфраструктуры. В качестве практического решения предлагается интеграция SaltStack, OpenBao и расширения salt-vault-ext, обеспечивающая выдачу ограниченных учетных данных и доступ к секретам на основе идентичности узла и его роли. Показано, что предложенный подход позволяет вынести секреты из pillar и реализовать принцип наименьших привилегий.

безопасное управление секретами, автоматизированное управление конфигурациями, SaltStack, OpenBao, AppRole, Saltext-vault, принцип наименьших привилегий

Введение

В условиях роста распределенных и динамически изменяющихся инфраструктур возрастает роль систем автоматизированного управления конфигурациями. Подобные системы позволяют централизованно применять состояния, управлять параметрами узлов и поддерживать воспроизводимость конфигураций. Вместе с тем именно автоматизация делает особенно чувствительной задачу безопасной доставки секретов. В роли таких секретов могут выступать пароли, токены, ключи доступа, параметры подключения к базам данных и иные конфиденциальные сведения, необходимые прикладным сервисам и инфраструктурным компонентам.

На практике чувствительные данные нередко хранятся в конфигурационных хранилищах или механизмах, подобных pillar в SaltStack. Такой подход удобен с точки зрения эксплуатации, однако не обеспечивает строгой изоляции доступа. Если секреты передаются в составе конфигурации в избыточном объеме, компрометация одного из узлов может привести к раскрытию данных, предназначенных для других компонентов инфраструктуры. Кроме того, использование статических секретов увеличивает

продолжительность окна компрометации и облегчает развитие атаки внутри инфраструктуры [1].

Целью работы является разработка подсистемы безопасного управления секретами в инфраструктуре автоматизированного управления конфигурациями. Для достижения поставленной цели необходимо решить следующие задачи: проанализировать ограничения традиционного хранения секретов в Salt-инфраструктуре; обосновать выбор специализированного хранилища секретов; разработать схему безопасной доставки секретов на управляемые узлы; реализовать разграничение доступа по идентичности узла и его функциональной роли.

Архитектура решения

В качестве среды автоматизации рассматривается SaltStack, использующий модель взаимодействия master-minion. Управляющий узел Salt Master хранит состояния, инициирует применение конфигурации и выступает центральной точкой управления. Управляемые узлы Salt Minion получают инструкции и выполняют конфигурационные операции. Для передачи параметров в Salt применяется механизм pillar, который удобен для централизованного задания переменных, но не является специализированным средством безопасного управления секретами [2].

Для устранения указанного ограничения в работе используется OpenBao как специализированное хранилище секретов. Выбор данного средства обусловлен поддержкой централизованного хранения, аудитом обращений, механизмом аутентификации AppRole, использованием сущностей Entity и их метаданных, а также возможностью применения шаблонных политик доступа. Концептуальной основой решения выступает принцип наименьших привилегий, согласно которому каждый узел должен получать только минимально необходимый набор секретов [3].

Практическая реализация построена на интеграции SaltStack, OpenBao и расширения salt-vault-ext. Общая схема работы заключается в следующем (рис. 1). В процессе выполнения состояния Salt Minion вызывает функцию чтения секрета. Вместо прямого обращения в OpenBao за долгосрочными учетными данными minion использует механизм peer_run для передачи запроса на Salt Master. Управляющий узел аутентифицируется в OpenBao по собственному AppRole и инициирует выпуск ограниченного secret_id для конкретного minion. При этом в OpenBao передаются метаданные

minion-id и roles. После этого minion получает ограниченные учетные данные, проходит аутентификацию по approle/login и получает токен, права которого вычисляются на основе шаблонных политик.

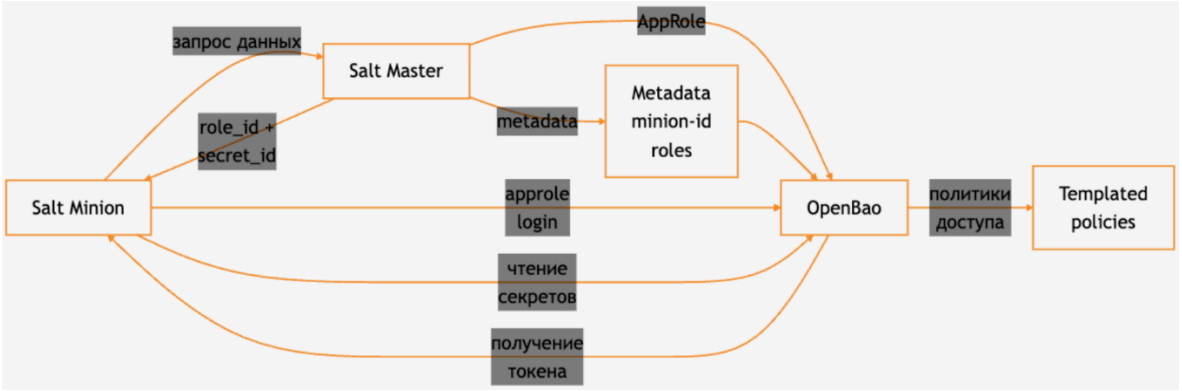


Рис. 1. Схема интеграции подсистемы безопасного управления секретами

Ключевую роль в предлагаемой подсистеме играет передача метаданных сущности. Значение minion-id используется для привязки узла к его собственным хостовым секретам. Значение roles отражает функциональную роль узла и применяется для выдачи доступа к секретам тех конфигурационных формул, которые относятся к данной роли. Такой подход позволяет отказаться от ручного дублирования секретов под каждый хост и одновременно сохранить адресность доступа.

Практическая реализация

На стороне Salt Master используется конфигурация, в которой определяются параметры аутентификации в OpenBao, выпуск AppRole-учетных данных для minion, а также набор передаваемых метаданных. В упрощенном виде соответствующая конфигурация может быть представлена следующим образом:

```
vault:
 auth:
 approle_mount: salt-masters
 method: approle
 metadata:
 entity:
 minion-id: '{minion}'
 roles: '{pillar [role]}'
peer_run:
 .*:
 - vault.generate_secret_id
```

Роль узла формируется на основе правила сопоставления идентификатора узла с набором характерных признаков. Полученная роль добавляется в pillar и затем используется расширение salt-vault-ext при формировании метаданных для OpenBao. На стороне OpenBao реализуются два AppRole-контура: один для Salt Master, второй для Salt Minion. Для minion используется шаблонная политика, ограничивающая доступ к путям, вычисляемым по метаданным Entity [4].

В такой реализации использование OpenBao в сочетании с salt-vault-ext позволяет реализовать адресную выдачу доступа без отказа от существующего процесса автоматизации. Minion получает доступ только к собственным хостовым секретам, к секретам своей роли и, при необходимости, к общим данным. При этом доступ к секретам других узлов и других ролей отсутствует.

Заключение

Таким образом, разработанная подсистема безопасного управления секретами в инфраструктуре автоматизированного управления конфигурациями обеспечивает выдачу ограниченных учетных данных и контролируемый доступ к конфиденциальной информации на основе идентичности и роли узла. Практическая значимость предложенного решения заключается в том, что оно позволяет вынести секреты из контура pillar в специализированное хранилище, ограничить объем данных, доступных каждому управляемому узлу, и реализовать принцип наименьших привилегий. Это снижает вероятность раскрытия чужих секретов и ограничивает возможности горизонтального перемещения злоумышленника внутри инфраструктуры.

Список используемых источников

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. Gaithersburg: NIST, 2020.

2. Salt Project Documentation. URL: https://docs.saltproject.io/ (дата обращения: 06.04.2026).

3. OpenBao Documentation. URL: https://openbao.org/docs/ (дата обращения: 06.04.2026).

4. Saltext-vault Documentation. URL: https://salt-extensions.github.io/saltext-vault/ (дата обращения: 06.04.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры ЗСС СПБГУТ А. Ю. Цветковым

УДК 004.738.5

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ РЕШЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ LORA / MESHTASTIC

Д. А. Красников (студент группы ИКТЗ-41м СПбГУТ) krasnikov.da@sut.tu
Т. Д. Любащенко (студент группы 236А-25 СПбГУТ)
М. А. Шахмоведев (студент группы МЗС-2512 СПбГУТ)

В работе проводится оценка производительности системы передачи данных на базе технологии LoRa с использованием платформы Meshtastic. Предложена методика экспериментальной оценки, основанная на анализе пропускной способности, задержки передачи и надежности доставки сообщений. Исследуется влияние параметров сети, числа узлов и типов трафика на характеристики системы. Отдельное внимание уделено оценке влияния механизмов шифрования на производительность передачи данных. Показано, что обеспечение безопасности приводит к дополнительным накладным расходам, влияющим на задержку и пропускную способность. Полученные результаты позволяют оценить компромисс между безопасностью и эффективностью передачи данных и определить особенности применения LoRa-сетей в задачах Интернета вещей.

LoRa, LPWAN, Meshtastic, Интернет вещей, mesh-сети, оценка производительности, пропускная способность, задержка, надежность передачи данных, криптографическая защита, беспроводные сети

В последние годы наблюдается активное развитие Интернета вещей, что приводит к росту требований к энергоэффективным беспроводным сетям. Одной из ключевых технологий в данном направлении является LoRa, обеспечивающая передачу данных на большие расстояния при низком энергопотреблении. Однако ее применение ограничивается низкой пропускной способностью, высокой задержкой передачи и регуляторными ограничениями.

Целью работы является оценка производительности системы передачи данных на базе LoRa при различных параметрах сети и режимах работы, включая использование механизмов шифрования.

Разрабатывается защищенная система передачи данных для IoT-устройств на базе LoRa [1] и платформы Meshtastic. Архитектура включает центральный узел и оконечные устройства, взаимодействующие по беспроводному каналу с поддержкой unicast-, broadcast- и клиент-центровой передачи [2]. Схематическое изображение разрабатываемой системы показано на рисунке 1.

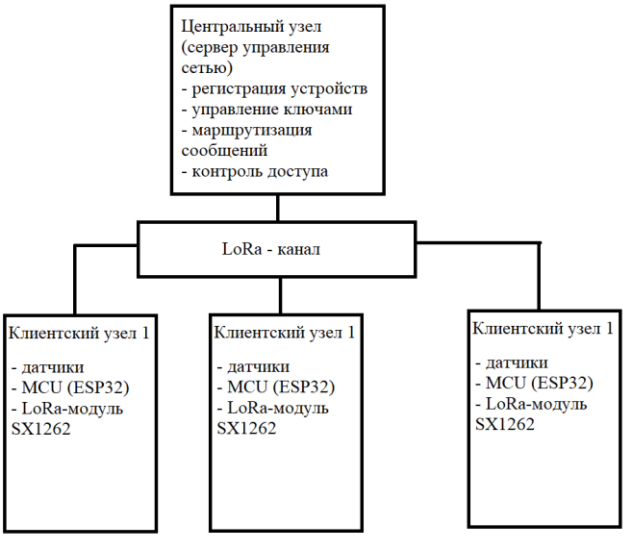


Рис. 1. Схематическое изображение разрабатываемой системы

Для количественного анализа используются следующие метрики:

- Пропускная способность (Throughput). Выражается формулой (1).

$$\text{Throughput} = \frac{\sum_{i=1}^{N} S_i}{T} \quad (1)$$

где S_i – размер i-го успешно доставленного сообщения (бит), N – количество успешно доставленных сообщений, T – общее время наблюдения (с).

- Задержка передачи (Latency)

$$Latency_{avg} = t_{receive} - t_{send}. \quad (2)$$

Среднее значение задержки:

$$Latency_{avg} = \frac{1}{N}\sum_{i=1}^{N}(t_{receive,i} - t_{send,i}), \quad (3)$$

где $t_{send,i}$ – момент отправки сообщения, $t_{receive,i}$ – момент получения сообщения.

- Доля успешно доставленных пакетов (Packet Delivery Ratio, PDR [3])

$$PDR = \frac{N_{received}}{N_{sent}} \quad (4)$$

где $N_{received}$ – количество полученных сообщений, N_{sent} – количество отправленных сообщений.

- Нагрузка на сеть

$$Load = N * \lambda, \quad (5)$$

где N – кол-во активных узлов, λ – интенсивность генерации сообщений (сообщений/с на узел).

● Влияние криптографических операций на время обработки сообщений

$$Overhead = \frac{T_{enc}+T_{dec}}{T_{total}}, \quad (6)$$

где T_{enc} – время шифрования, T_{dec} – время дешифрования, T_{total} – общее время обработки сообщения.

Пропускная способность определяется как отношение объема успешно переданных данных ко времени наблюдения. Задержка характеризует время передачи сообщения от отправителя к получателю. PDR отражает надежность передачи, а нагрузка на сеть определяется числом узлов и интенсивностью передачи сообщений [4].

Выбор метрик обусловлен ограничениями LoRa-сетей и необходимостью оценки эффективности, надежности и масштабируемости системы.

Сценарии тестирования предполагают экспериментальную оценку, проводящуюся при варьировании:

- числа узлов;
- параметров LoRa;
- типов передачи (unicast и broadcast);
- режимов работы с шифрованием и без него.

Сравнение выполняется по изменению задержки, пропускной способности, размера пакетов и вычислительной нагрузки.

Результаты экспериментов показывают, что увеличение числа узлов приводит к росту задержки передачи [5], что связано с увеличением числа ретрансляций и коллизий в сети.

Использование шифрования приводит к увеличению задержки передачи и снижению пропускной способности за счет роста размера пакетов и дополнительных вычислительных затрат. Результаты приведены в таблице 1.

ТАБЛИЦА 1. Влияние шифрования *на* задержку передачи

Режим	Средняя задержка (мс)
Без шифрования	240
С шифрованием	310

Также установлено, что широковещательная передача менее эффективна по сравнению с адресной из-за увеличения числа коллизий.

Таким образом, наблюдается зависимость характеристик системы от параметров сети и режима работы. В работе проведена оценка производительности системы передачи данных на базе технологии LoRa.

Показано, что внедрение механизмов безопасности приводит к снижению производительности, однако обеспечивает необходимый уровень защиты данных.

Полученные результаты подтверждают наличие компромисса между безопасностью и эффективностью передачи данных и могут быть использованы при проектировании IoT-систем.

Список используемых источников

1. Красников, Д. А. Практика построения устойчивой к атакам инфраструктуры на основе протокола lorawan / Д. А. Красников, М. М. Ковцур, А. В. Никифоров // Информационная безопасность регионов России (ИБРР-2025): Материалы XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2025. С. 481. EDN: WQKLKO.

2. Ковцур, М. М. Разработка концепции автономного модуля для радиообследования WLAN / М. М. Ковцур, Д. В. Сахаров // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025): Сборник научных статей, Санкт-Петербург, 17–21 февраля 2025 года. Санкт-Петербург: СПбГУТ, 2025. С. 414-418. EDN: OYKVDR.

3. Технологии защиты беспроводных сетей и мобильных приложений: Учебно-методическое пособие по выполнению лабораторных работ / М. М. Ковцур, И. А. Ушаков, А. И. Черкашин, Д. С. Левшун. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций имени профессора Бонч-Бруевича, 2025. 50 с. EDN: PCLUWP.

4. APPROACH TO DETECTION OF DENIAL-OF-SLEEP ATTACKS IN WIRELESS SENSOR NETWORKS ON THE BASE OF MACHINE LEARNING. Balueva A., Desnitsky V., Ushakov I. Studies in Computational Intelligence. 2020. Т. 868. С. 350-355.

5. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IoT-сети / Д. В. Сахаров, А. М. Гельфанд, А. А. Казанцев, И. Е. Пестов // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". 2020. № 2. С. 86-94. EDN: DLMENT.

Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом М. М. Ковцуром.

УДК 004.056

АНАЛИЗ ХАРАКТЕРИСТИК И ФУНКЦИЙ МЕЖСЕТЕВЫХ ЭКРАНОВ ВЕБ-ПРИЛОЖЕНИЙ

В. О. Мартыненко (студент группы МЗС-2512 СПбГУТ), martynenko.vo@sut.ru
А. Д. Николаев (студент группы МЗС-2512 СПбГУТ), nikolaev.ad@sut.ru
И. А. Терентьев (студент группы МЗС-2512 СПбГУТ), terentev.ia@spbgut.ru
И. А. Ушаков (к.т.н., доцент, заведующий кафедрой ИБКС СПбГУТ)

Межсетевые экраны уровня веб-приложений являются критически важным инструментом для защиты веб-ресурсов от целевых атак на прикладном уровне. Уход ключевых мировых вендоров с российского рынка в 2022 году создал условия для ускоренного импортозамещения и активного развития продуктов отечественных разработчиков. В данной статье представлен сравнительный анализ функциональных возможностей наиболее востребованных российских WAF-решений и признанных мировых лидеров отрасли.

межсетевой экран, WAF, межсетевой экран сетевых приложений, безопасность

Межсетевой экран веб-приложений (Web Application Firewall, (WAF)) является специализированным решением безопасности, предназначенным для защиты веб-ресурсов и API на прикладном уровне модели OSI. В отличие от традиционных средств защиты, WAF анализирует не просто заголовки пакетов, а логику HTTP/S-запросов, выступая защитным барьером между веб-сервером и потенциально опасным внешним трафиком. Он используется как наложенное средство защиты, располагающееся между перед основным приложением и проводящее анализ сетевого трафика, принимая в реальном времени решение о предоставлении доступа. Публикация ресурсов с помощью межсетевого экрана веб-приложений работает с помощью технологии reverse-прокси.

Современный WAF предлагает расширенный функционал, выходящий за рамки простого сигнатурного анализа. Он включает в себя поведенческий анализ пользователей, защиту от ботнет-активности, предотвращение атак из списка OWASP Top 10 (таких как SQL-инъекции и XSS), а также глубокую инспекцию зашифрованного SSL/TLS-трафика. Это позволяет обнаруживать аномалии, скрытые внутри ложно-легитимных запросов.

Традиционно признанными мировыми лидерами в сегменте WAF считались такие компании, как F5, Imperva и Akamai. Однако их уход с российского рынка в начале 2022 года радикально изменил рынок программного и аппаратного обеспечения информационной безопасности. Прекращение поддержки и облачных сервисов зарубежных вендоров создало критические риски для бизнеса, что открыло окно возможностей для отечественных разработчиков.

На сегодняшний день отечественные WAF-решения представлены как в виде программно-аппаратных комплексов (ПАК), так и в виде образов виртуальных машин, что позволяет гибко интегрировать их в любую инфраструктуру – от локальных серверных комнат до облачных сред.

Одни из лидирующих позиций на российском рынке занимают продукты компаний UserGate, Код Безопасности и Positive Technologies.

В таблице 1 приведены представители межсетевых экранов веб-приложений компании UserGate, поставляемые в виде ПАК, либо в виде образа виртуальной машины, предназначенного для развертывания в виртуальной среде. В конфигурации виртуальной машины межсетевой экран UserGate WAF поставляется с десятью Ethernet-интерфейсами, для ПАК предоставляется от 2 до 64 Ethernet-портов.

ТАБЛИЦА 1. Характеристики WAF UserGate [1]

Модель	D200	E1000	E3010	4 ядра (виртуальный)	8 ядер (виртуальный)
Сертификация	ФСТЭК № 3905	ФСТЭК № 3905	ФСТЭК № 3905	ФСТЭК № 3905	сертификат № 3905
RPS	1100	1750	3000	1000	2100
Технические характеристики	1xHDD, 1 Тб 1xCPU, 4 ядра, 2,4-3,4 ГГц 2xDDR4, ECC 16 Гб	1xHDD, 1 Тб 1xCPU, 4 ядра, 2,4-3,4 ГГц 2xDDR4, ECC 16 Гб	1xSSD, 1 Тб 1xCPU, 24 ядра, 2,85-4 ГГц 8xDDR4, 8Гб, ECC, REG	4 ядра от 2,5 ГГц ОЗУ: 8 Гб Накопитель 300 Гб	8 ядер от 2,5 ГГц ОЗУ: 16 Гб Накопитель 300 Гб

Как видно, из таблицы 1, все межсетевые экраны веб-приложений UserGate имеют сертификат ФСТЭК. Также можно увидеть, что по числу

обработки запросов в секунду, лидируют устройства серии E3010, обрабатывая до 3000 запросов в секунду. Виртуальные решения не отстают в производительности от ПАК, обрабатывая от 1000 до 2100 запросов в секунду.

Особенностью функционала данных межсетевых экранов веб-приложений является возможность создавать собственные правила анализа и фильтрации трафика, путем использования специализированного языка UPL. Так же одним из преимуществ WAF UserGate можно выделить наличие экосистемы, в которую входят NGFW, SIEM и LogAn и Management Center.

Межсетевой экран веб-приложений от компании Код безопасности имеет два варианта реализации. Первый вариант – отдельный продукт WAF. Второй вариант – TLS-сервер с функциями WAF.

Характеристики серий обоих вариантов реализации представлены в таблице 2.

ТАБЛИЦА 2. Характеристики WAF Континент [2]

Модель	WAF IPC-1000L	WAF IPC-3000L	TLS IPC-R1000	TLS IPC-R3000	TLS IPC-R550	TLS IPC-R50
Сертификация	-	-	ФСТЭК № 4259 ФСБ СФ/114-5391	ФСТЭК № 4259 ФСБ СФ/114-5391	ФСТЭК № 4259 ФСБ СФ/114-5391	ФСТЭК № 4259 ФСБ СФ/114-5391
RPS	1 000	3 000	60000	230000	30 000	17 000
Сетевые интерфейсы	8 x 1000BASE-T RJ45 8 x 1G SFP	1 x 1000BASE-T RJ45 4 x 10GB SFP+	8x 10/100/1000BASE-T RJ45 4x 10G SFP+	8x 10/100/1000 BASE-T RJ45 8x 10G SFP+	4x 10/100/1000 BASE-T RJ45 2x Combo 1G RJ45/SFP 2x 10G SFP+	4x 10/100/1000 BASE-T RJ45 1x 1G SFP

Как видно по таблице 2 межсетевой экран веб-приложений Континента способен обрабатывать от 1000 до 230000 запросов в секунду.

Однако межсетевые экраны веб-приложений как отдельный продукт у Кода безопасности не имеют лицензии ФСТЭК. В прошлом они имели лицензию ФСТЭК, но она истекла 2023 году и не была продлена. Сертификат

ФСТЭК и ФСБ имеет только TLS-сервер с функциями WAF. И его производительность колеблется от 15000 до 230000 RPS. Однако столько высокие показатели достигаются, только при работе с трафиком протокола HTTP. Если для соединения используется протокол HTTPS, производительность снижается и чем выше сложность расшифровки трафика, тем ниже будет производительность. Однако даже низко производительные WAF Континент при высокой сложности расшифровки обеспечивают обработку не менее 2000 запросов в секунду. Однако по мере увеличения сложности дешифрования трафика, значение производительности может опускаться еще ниже.

Особенностью функций межсетевых экранов данного производителя, является функция выдачи сертификатов административным пользователям приложений, которые WAF защищает. Это повышает безопасность защищаемых ресурсов, так как административным пользователям веб-приложений кроме логина и пароля необходимо еще иметь соответствующий сертификат.

Так же производитель данных межсетевых экранов веб-приложений, заявляет, что в них используются методы машинного обучения для анализаторов трафика.

Третьим производителем межсетевых экранов веб-приложений является компания Positive Technologies. Она предоставляет WAF в виде ПАК. Характеристики WAF от Positive Technologies представлены в таблице 3.

ТАБЛИЦА 3. Характеристики WAF Positive Technologies [3]

	PTAF-CH50	PTAF-CH100	PTAF-CH200-N1	PTAF-CH200-N2	PTAF-CH300
Сертификация	ФСТЭК № 3455	ФСТЭК № 3455	ФСТЭК № 3455	ФСТЭК № 3455	ФСТЭК № 3455
Максимальные значения параметров производительности для HTTP-трафика					
RPS	3700	22000	30000	40000	100000
Максимальные значения параметров производительности для HTTPS-трафика					
RPS	2300	13000	16000	20000	55000

Как видно из таблицы 3, самый производительный межсетевой экран веб-приложений у Positive Technologies – это межсетевой экран серии PTAF-CH300 способный обрабатывать до 100000 HTTP-запросов в секунду

и 55000 HTTPS запросов в секунду. Так же серии данных WAF имеют сертификат ФСТЭК.

ТАБЛИЦА 4. Сравнение характеристик WAF

	UserGate	Код безопасности	Positive Technologies
RPS	До 3000	До 230000	До 100000
Наличие виртуальных решений	+	-	+
Сертификация	ФСТЭК	ФСТЭК и ФСБ, но только у TLS	ФСТЭК

Как видно из таблицы 4, самым высокопроизводительным среди сертифицированных WAF является TLS IPC-R3000 от компании Код безопасности. Однако и стоимость приобретения и лицензии для такого устройства соответствует его характеристикам. Чем выше производительность – тем дороже стоимость ПАК или виртуального образа и лицензии.

TLS-сервера компании Континент и все серии кроме PTAF-CH50 у Positive Technologies подойдут среднему и крупному бизнесу, которому необходимо обеспечивать высокую производительность для доступа к своим ресурсам.

WAF компании UserGate и серия PTAF-CH50 у Positive Technologies подойдет для малого бизнеса, которому не требуется высокая производительность.

Однако межсетевые экраны от Кода безопасности имеют уникальные функции, такие как сертификация административных пользователей защищаемых веб-приложений и машинное обучение анализаторов трафика. В то время как WAF UserGate обладает возможностью гибкой настройки правил проверки и фильтрации путем возможности создания собственных пользовательских правил.

Также приобретая WAF Кода безопасности в случаях, когда необходимо наличие сертификата ФСТЭК, необходимо обращать внимание на приобретаемый продукт, так как не все реализации данной компании имеют данный сертификат.

Список используемых источников

1. UserGate. IT-компания производитель решений информационной безопасности [офиц. сайт]. URL: https://usergate.com (дата обращения: 25.03.2026).

2. Код безопасности. IT-компания производитель решений информационной безопасности [офиц. сайт]. URL: https://www.securitycode.ru (дата обращения: 27.03.2026).

3. Positive Technologies. IT-компания производитель решений информационной безопасности [офиц. сайт]. URL: https://ptsecurity.com (дата обращения: 28.03.2026).

Статья представлена научным руководителем, заведующим кафедрой ИБКС, СПбГУТ, кандидатом технических наук, доцентом И. А. Ушаковым.

УДК 004.056

СИСТЕМАТИЗАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ ЭМУЛЯТОРА И СРЕДСТВ ОТЛАДКИ В ВРЕДОНОСНОМ ПО ДЛЯ ANDROID

Д. Р. Мартыненко (студент группы ИКБ-21 СПбГУТ),
martynenko.dr@sut.ru

В последние годы наблюдается устойчивый рост числа вредоносных программ, ориентированных на мобильные платформы, среди которых операционная система Android занимает доминирующее положение. Широкое распространение данной платформы, а также разнообразие аппаратных конфигураций делают ее приоритетной целью для злоумышленников. В результате чего усложняются не только сами вредоносные программы, но и методы их сокрытия, направленные на противодействие средствам динамического анализа. В связи с этим, актуальна задача создания классификационной модели для анти-аналитических методов в вредоносном Android ПО.

Android, вредоносное ПО, динамический анализ, информационная безопасность

Мобильные устройства в последние годы все чаще становятся целью вредоносного программного обеспечения [1]. Наибольшее количество атак при этом направлено на платформу Android, которая из-за своей открытости и массового распространения особенно привлекает злоумышленников. Именно эти особенности делают ее одной из основных целей для разработки и распространения вредоносных программ.

Современные исследования показывают, что вредоносное программное обеспечение для Android активно эволюционирует, внедряя новые методы сокрытия своей активности и обхода средств анализа [2]. В частности, значительная доля вредоносных приложений использует анти-аналитические техники, направленные на обнаружение среды выполнения и инструментов анализа, таких как эмуляторы и отладчики.

Постановка задачи

Существующие исследования [2, 3] уделяют особое внимание техникам уклонения от анализа, включая обнаружение эмуляторов, динамическую загрузку и обфускацию кода. Подчеркивается, что злоумышленники активно адаптируют свои методы, что делает задачу анализа более сложной. Также отмечается рост использования нативного кода и системных вызовов для усложнения анализа и обхода инструментов мониторинга.

В связи с этим актуальной является задача разработки классификационной модели анти-аналитических техник в вредоносном Android ПО, основанной на разделении техник по уровням реализации и механизмам взаимодействия с системой. Полученные результаты могут быть использованы при создании и совершенствовании инструментов динамического анализа, а также в практической деятельности специалистов по информационной безопасности.

Динамический анализ Android приложений

Динамический анализ представляет собой метод исследования программного обеспечения, при котором изучается поведение приложения непосредственно в процессе его выполнения. В контексте операционной системы Android данный подход позволяет выявлять вредоносную активность, которая может быть скрыта или труднодоступной при статическом анализе.

Как правило, динамический анализ осуществляется в контролируемой среде, такой как эмулятор или песочница, либо на реальных устройствах. В процессе выполнения приложения фиксируются различные поведенческие характеристики, включая вызовы API, системные вызовы, изменения файловой системы и сетевую активность [4]. Для повышения глубины анализа применяются инструменты, такие как Frida [5], позволяющие перехватывать и модифицировать выполнение функций на уровне Java и нативного кода.

Несмотря на эффективность, динамический анализ имеет ряд ограничений, в частности, он зависит от условий выполнения приложения: если вредоносная логика активируется только при определенных обстоятельствах, например, при отсутствии взаимодействии пользователя с приложением, она может не проявиться в процессе анализа. Кроме того, современные вредоносные программы активно используют методы обнаружения средств отладки и эмуляции, направленные на выявление среды анализа и уклонение от наблюдения.

Основные категории анти-аналитических техник

Современное вредоносное программное обеспечение для Android использует широкий спектр методов, направленных на сокрытие вредоносной активности путем изменения логики выполнения программы в зависимости от условий среды ее выполнения. Основная цель таких техник заключается в том, чтобы вредоносная активность не проявлялась в ходе анализа.

В общем виде данные техники можно разделить на две категории:

1. Обнаружение эмулятора
2. Обнаружение отладки

Техники обнаружения эмулятора в контексте анти-аналитических механизмов можно условно разделить на поведенческие и основанные на анализе среды выполнения. Поведенческие методы ориентированы на выявление несоответствий в «естественном» поведении устройства: отсутствие пользовательской активности, нереалистичные паттерны взаимодействия, а также отсутствие сенсорных изменений, например, акселерометра или гироскопа [6]. Такие признаки характерны для эмуляторов и автоматизированных песочниц, где поведение устройства частично или полностью симулируется.

Вторая группа методов анализирует саму среду выполнения, опираясь на системные параметры и конфигурацию устройства, наличие специфичных файлов виртуализации, а также особенности аппаратного окружения. В совокупности эти подходы позволяют выявлять несоответствия между физическим устройством и эмулируемой средой.

Техники обнаружения отладки включают два основных направления: выявление отладчика и обнаружение других динамических инструментов. Обнаружение отладчика основано на проверке состояния процесса и системных признаков вмешательства, например, наличия подключенного отладчика через стандартные API [7] или анализа системных структур, указывающих на трассировку выполнения [8]. Такие методы направлены на выявление факта взаимодействия отладочных средств с процессом приложения.

Более сложный класс техник ориентирован на обнаружение динамических инструментов анализа, таких как Frida и ей подобных. Они работают за счет выявления следов инъекции в процесс, анализа загруженных библиотек, поиска характерных функций перехвата или проверки аномалий в адресном пространстве процесса. В совокупности такие методы позволяют вредоносному программному обеспечению определять факт анализа и изменять свое поведение.

Предлагаемая модель

В предлагаемой модели анти-аналитические техники разделяются по уровням реализации: в Java или в нативном коде, как показано в таблице 1.

ТАБЛИЦА 1. Классификация анти-аналитических техник вредоносного Android ПО с учетом уровня их реализации

Уровень реализации	Вид техники			
Java (Android API)	Обнаружение эмулятора		Обнаружение отладки	
	Поведенческие техники	Анализ системных параметров	Обнаружение отладчика	Обнаружение динамических инструментов
C/C++ (Системные вызовы)	Обнаружение эмулятора		Обнаружение отладки	
	Поведенческие техники	Анализ системных параметров	Обнаружение отладчика	Обнаружение динамических инструментов

Анти-аналитические техники, использующие Android API, преимущественно реализуются на языке Java. Хотя данные техники и могут быть реализованы в нативном коде, написанном на C или C++, они будут использовать Java Native Interface, который позволяет вызывать Java методы внутри нативного кода (рис. 1), в связи с чем, техниками, реализованными на уровне нативного кода, будут считаться те, что основаны на системных вызовах ядра Linux.

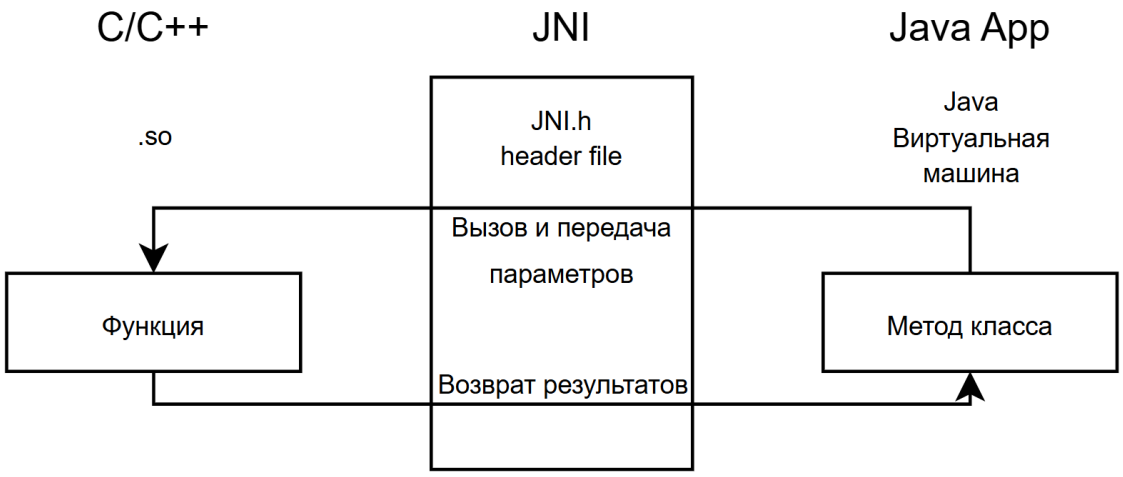


Рис. 1. Принцип работы Java Native Interface

Например, задержка выполнения вредоносного кода при помощи Android API может осуществляться через вызов «System. currentTimeMillis()», но при реализации подобной задержки в нативном коде, написанном на C или C++ может использоваться системный вызов «sleep()». Таким образом одна и та же техника может быть выполнена на разных системных уровнях,

что требует учета архитектурных особенностей приложения при анализе, а также при разработке инструментов для обнаружения и нейтрализации подобных методов.

Это подчеркивает необходимость разработки многоуровневых инструментов анализа, способных одновременно учитывать разные реализации анти-аналитических техник, что является ключевым фактором повышения эффективности обнаружения современных вредоносных программ.

Заключение

В ходе данного исследования была выполнена классификация существующих техник анти-анализа, выявлена сложность обнаружения многоуровневых техник, а также создана их систематизирующая модель.

Таким образом, исследование существующих подходов показывает, что они преимущественно ориентированы на функциональную классификацию анти-аналитических техник и не учитывают уровень их реализации. Предложенная модель классификации устраняет данный недостаток за счет разделения техник на уровень Android API и нативный уровень, что позволяет более точно описывать современные многоуровневые механизмы уклонения и повышает применяемость модели при анализе реального вредоносного программного обеспечения.

Практическая ценность данной модели заключается в том, что она отражает различия в сложности реализации и устойчивости техник к обходу. В частности, методы, реализованные на уровне Android API, как правило, проще в реализации, но легче обнаруживаются и обходятся при помощи инструментов динамического анализа. В тоже время техники, реализуемые в нативном коде, обеспечивают более глубокий контроль над процессом выполнения и существенно усложняют анализ за счет использования механизмов ядра операционной системы.

Список используемых источников

1. Dr. Web. Обзор мобильных угроз и вредоносного ПО [Электронный ресурс]. Режим доступа: https://news.drweb.ru/show/review/?lng=ru&i=15136 (дата обращения: 30.04.2026).

2. Faruki P., Bhan R., Jain V. и др. A Survey and Evaluation of Android-Based Malware Evasion Techniques and Detection Frameworks // Information. 2023. Т. 14, № 7. Ст. 374. DOI: 10.3390/info14070374.

3. Malware Analysis and Detection in Android Systems: A Comprehensive Review // Computers. 2025. Т. 14. № 11. С. 482. DOI: 10.3390/computers14110482.

4. Sutter T., Kehrer T., Rennhard M., Tellenbach B. Dynamic Security Analysis on Android: A Systematic Literature Review // IEEE Access. 2024. DOI: 10.1109/ACCESS.2024.3390612.

5. Selectel. Frida: реверс-инжиниринг приложений на Android [Электронный ресурс]. Режим доступа: https://selectel.ru/blog/frida-android/ (дата обращения: 30.04.2026).

6. Orange Cyberdefense. Reverse engineering of the Anubis malware [Электронный ресурс]. Режим доступа: https://www.orangecyberdefense.com/uk/insights/blog/career-1/cyberdefense/reverse-engineering-of-the-anubis-malware (дата обращения: 30.04.2026).

7. Java Debug Wire Protocol (JDWP) Specification [Электронный ресурс]. Oracle. Режим доступа: https://docs.oracle.com/javase/8/docs/technotes/guides/jpda/jdwp-spec.html (дата обращения: 30.04.2026).

8. OWASP Mobile Application Security Testing Guide (MASTG). Checking TracerPid [Электронный ресурс]. Режим доступа: https://mas.owasp.org/MASTG/knowledge/android/MASVS-RESILIENCE/MASTG-KNOW-0028/#checking-tracerpid (дата обращения: 30.04.2026).

9. Cyberly. How Frida detects and bypasses anti-debugging mechanisms in apps [Электронный ресурс]. Режим доступа: https://www.cyberly.org/en/how-does-frida-detect-and-bypass-anti-debugging-mechanisms-in-apps/index.html (дата обращения: 30.04.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры ЗСС СПбГУТ А. Ю. Цветковым.

УДК 004.056.5:004.91

СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Никифоров А. В. (студент группы ИКТБ-47м СПбГУТ)
Шахмоведев М. А. (студент группы МЗС-2512 СПбГУТ),
shahmovedev.ma@sut.ru

В статье выполнен структурированный анализ актуальных подходов и программно-технических решений, направленных на поддержание конфиденциальности и целостности данных в системах управления базами данных. Рассмотрены механизмы контроля доступа с применением ролевых схем, способы криптографической защиты, в том числе прозрачное шифрование массивов и динамическая маскировка сведений. Особое внимание уделено инструментам гарантии целостности на уровне транзакционных операций, контрольных сумм и систем аудита. Выполнено сопоставление реализации указанных механизмов в СУБД PostgreSQL, Oracle и MS SQL Server. Сформулированы предложения по формированию многоуровневой системы защиты информации.

информационная безопасность, СУБД, конфиденциальность, целостность данных, разграничение доступа, шифрование, аудит, ролевая модель

В условиях цифровой трансформации экономики наблюдается устойчивый рост объемов данных, обрабатываемых корпоративными информационными системами. Это обусловлено развитием облачных технологий, систем аналитики больших данных (Big Data), а также широким внедрением интернет-сервисов [1].

Дополнительным фактором является усиление регуляторного давления (например, требования по защите персональных данных и коммерческой тайны), что предъявляет повышенные требования к защищенности СУБД.

Анализ динамики интереса к тематике СУБД (рис. 1) демонстрирует выраженную сезонность и общий высокий уровень востребованности технологий управления данными [2].

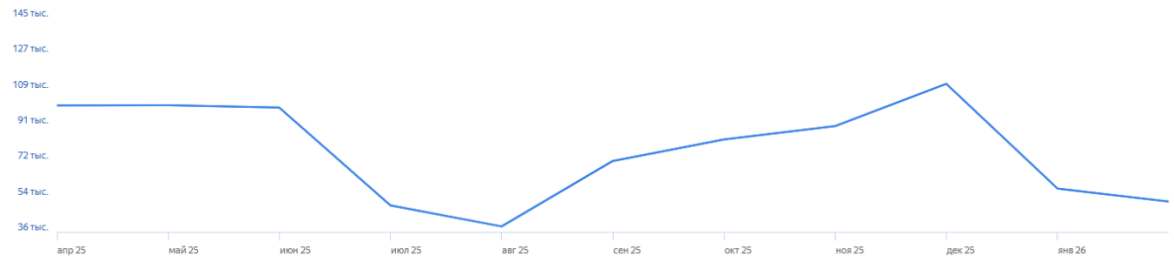


Рис. 1. Динамика популярности запросов, связанных с СУБД

Как видно из диаграммы, наблюдаются следующие тенденции:

- стабильный высокий интерес в первой половине года;
- снижение в летний период (что может быть связано с сезонным фактором);
- рост активности к концу года, достигающий пика в декабре;
- повторное снижение в начале следующего года.

Наблюдаемая динамика связана с циклическим характером внедрения ИТ-решений и модернизации инфраструктуры, в рамках которых системы управления базами данных выполняют одну из ключевых функций [3]. Это указывает на то, что обеспечение безопасности данных сохраняет высокую значимость и требует комплексной организации защитных механизмов.

Реализация защиты информации в СУБД строится на многоуровневом принципе организации (рис. 2).

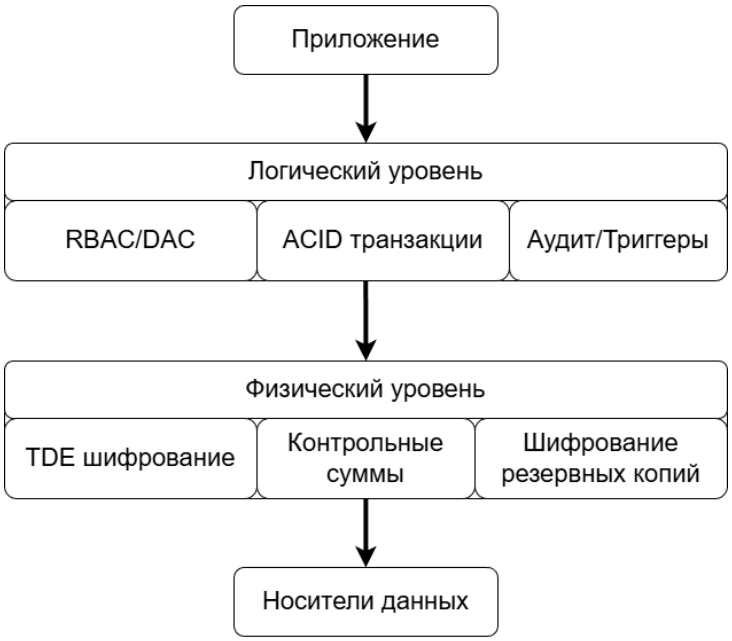


Рис. 2. Многоуровневая архитектура защиты данных в СУБД

Актуальные методы обеспечения безопасности данных в СУБД основаны на распределении средств защиты между несколькими архитектурными уровнями. Как правило, выделяют логический и физический уровни, а также связанные с ними сетевой и прикладной. Логический уровень обеспечивает контроль доступа, обработку транзакций и соблюдение правил взаимодействия с данными. Физический уровень ориентирован на сохранность информации на носителях и предотвращение повреждения либо несанкционированного получения данных.

Ключевым элементом обеспечения конфиденциальности в системах управления базами данных является система разграничения доступа, которая определяет правила взаимодействия субъектов (пользователей, процессов) с объектами (таблицами, представлениями, индексами и др.) [3]. В большинстве современных СУБД реализуются дискреционная и ролевая модели управления доступом, каждая из которых обладает своими преимуществами и ограничениями. Дискреционная модель (DAC) основывается на принципе владения объектами, при котором пользователь, создавший объект, получает полный контроль над ним и может делегировать права другим субъектам. Несмотря на гибкость, данный подход плохо масштабируется в условиях сложных корпоративных систем с большим числом пользователей и объектов, поскольку приводит к избыточному распределению привилегий и усложняет контроль их актуальности. Практика показывает, что именно ошибки конфигурации в рамках DAC часто становятся причиной утечек данных [4].

В связи с этим широкое распространение получила ролевая модель управления доступом (RBAC), в рамках которой права доступа агрегируются в роли, а пользователи получают доступ через назначение соответствующих ролей. Такой подход позволяет реализовать иерархии ролей, наследование привилегий и централизованное управление доступом, что существенно снижает административную нагрузку и повышает управляемость системы безопасности. RBAC дополнительно позволяет более жестко реализовывать принцип минимально необходимых привилегий (Least Privilege) и разграничение обязанностей (Separation of Duties), при котором критически важные полномочия не сосредотачиваются у одного пользователя. В корпоративной среде данная модель обычно интегрируется с централизованными каталогами пользователей, например LDAP или Active Directory, благодаря чему администрирование прав доступа осуществляется в рамках единой инфраструктуры организации.

Дальнейшее развитие механизмов контроля доступа связано с применением атрибутивных моделей (ABAC). В этом случае решение о предоставлении доступа формируется с учетом набора параметров: характеристик пользователя и объекта, а также условий среды – времени подключения, используемого устройства, местоположения или уровня доверия. Подобный подход особенно востребован в облачных и распределенных системах, где отсутствует жестко определенный сетевой периметр.

Вместе с тем использование ABAC сопровождается усложнением политики безопасности и увеличением вычислительных затрат.

Помимо логического разграничения доступа существенную роль играет криптографическая защита информации, предназначенная для предотвращения компрометации данных при получении доступа к носителям либо каналам передачи. Одним из наиболее распространенных механизмов считается Transparent Data Encryption (TDE), функционирующий непосредственно на уровне СУБД. Данная технология обеспечивает автоматическое шифрование файлов базы данных, журналов транзакций и резервных копий. Ее особенностью является отсутствие необходимости изменять прикладную логику, поскольку операции шифрования выполняются сервером в фоновом режиме. Как правило, защита ключей строится по иерархической схеме с разделением master key и database key, что упрощает централизованное управление ключевой инфраструктурой.

При этом TDE не решает проблему внутренних угроз. Пользователи с административными привилегиями либо злоумышленники, получившие доступ к учетным записям администраторов, могут взаимодействовать с уже расшифрованными данными в оперативной памяти. По этой причине в ряде систем применяется шифрование отдельных столбцов или шифрование на стороне приложения. В таком варианте данные преобразуются еще до передачи в СУБД, а ключи размещаются вне самой базы – например, в KMS-системах или аппаратных модулях HSM. Подобная архитектура обеспечивает более высокий уровень устойчивости к внутренним угрозам, однако усложняет реализацию приложений, требует механизмов распределения и регулярной ротации ключей, а также может ограничивать производительность и возможности индексирования.

Для дополнительной защиты конфиденциальной информации используется динамическое маскирование данных. Этот механизм позволяет отображать содержимое полей по-разному в зависимости от уровня доступа пользователя. В отличие от криптографических методов, маскирование не изменяет физически хранимые данные и применяется только при формировании результата запроса. Благодаря этому технология активно используется в тестовых, аналитических и разработческих средах, где требуется сохранить структуру базы данных без раскрытия чувствительной информации. В современных СУБД реализованы различные варианты маскирования: скрытие части символов, подмена значений, генерация псевдослучайных данных и использование заранее заданных шаблонов. Однако

само по себе маскирование не рассматривается как полноценный механизм криптографической защиты и применяется совместно с другими средствами безопасности.

Поддержание целостности данных в СУБД включает как контроль корректности операций, так и защиту информации от физических повреждений. На логическом уровне основой выступает транзакционная модель ACID. Свойство атомарности исключает частичное выполнение операций, что критично для финансовых и других высоконагруженных систем. Согласованность отвечает за соблюдение ограничений целостности, включая связи между таблицами, уникальность значений и прикладные правила обработки данных. Изоляция определяет порядок взаимодействия параллельных транзакций и реализуется через набор уровней изоляции, различающихся балансом между производительностью и строгостью консистентности. Во многих современных СУБД применяется механизм MVCC, основанный на хранении нескольких версий записей и позволяющий уменьшить количество блокировок при высокой параллельности операций. Надежность обеспечивает сохранение подтвержденных изменений даже после отказов оборудования или программных сбоев за счет журналирования и процедур восстановления [5].

На физическом уровне защита целостности достигается с помощью контрольных сумм страниц, предназначенных для обнаружения ошибок ввода-вывода, аппаратных неисправностей и повреждений носителей. Для восстановления состояния базы данных после аварий используется журналирование изменений по принципу Write-Ahead Logging: операции сначала фиксируются в журнале и только затем применяются к основным данным. Дополнительную устойчивость инфраструктуры обеспечивает репликация, при которой копии данных поддерживаются на отдельных узлах системы. В зависимости от архитектуры репликация может быть синхронной либо асинхронной.

Отдельное значение имеет аудит действий пользователей и процессов. Современные СУБД способны фиксировать широкий спектр событий: аутентификацию, изменение прав доступа, выполнение SQL-запросов и другие операции. Журналы аудита используются при расследовании инцидентов и анализе подозрительной активности, в том числе в интеграции с SIEM-платформами. Дополнительно применяются ограничения и триггеры, автоматически проверяющие корректность изменений непосред-

ственно на уровне базы данных. Такой подход снижает зависимость от прикладного слоя и способствует поддержанию целостности информации в распределенных системах.

В таблице 1 представлен сравнительный анализ рассмотренных механизмов в популярных СУБД.

Таблица 1. Сравнительная характеристика средств защиты в СУБД

Механизм защиты	PostgreSQL	Oracle Database	MySQL
Ролевая модель (RBAC)	Полная поддержка, гибкие иерархии	Полная поддержка, виртуальные привилегии	Ограниченная поддержка (с MySQL 8.0), иерархии отсутствуют, интеграция с AD через внешние плагины
Прозрачное шифрование (TDE)	Через расширения (pgcrypto)	Нативная поддержка, шифрование табличных пространств	Нативная поддержка (InnoDB tablespace encryption), шифрование БД и бэкапов
Маскирование данных	Через представления	Нативная поддержка (Data Redaction)	Нативная поддержка (Data Masking Functions)
Аудит	Расширение pgAudit	Unified Auditing, детальный контроль	Только в MySQL Enterprise Audit (коммерческая версия), в Community Edition – отсутствует

Сравнение популярных СУБД показывает разный уровень встроенной безопасности. Коммерческие Oracle Database предлагают широкий набор средств «из коробки» (аудит, маскирование, шифрование). Открытые PostgreSQL гибки, но требуют донастройки и расширений. Бесплатная версия MySQL имеет ограниченные возможности.

Проведенный анализ позволяет сделать вывод о том, что эффективная защита данных достигается только комплексным многоуровневым подходом (логические, криптографические, организационные меры). Выбор инструментов зависит от модели угроз, нормативных требований и баланса безопасности с производительностью.

Список используемых источников

1. Орлов С. А., Цилькер Б. Я. Технологии организации баз данных. СПб.: Питер, 2019. 432 с.

2. Галатенко В. А. Информационная безопасность баз данных: учебное пособие. М.: ИНТУИТ, 2017. 280 с.

3. Разработка методики внедрения машинного обучения для повышения информационной безопасности web-приложения / М. М. Ковцур, Д. И. Кириллов, А. В. Михайлова, П. А. Потемкин // Техника средств связи. 2020. № 4(152). С. 74-86. EDN ZNKWXK.

4. Коннолли Т., Бегг К. Базы данных: проектирование, реализация и сопровождение. М.: Вильямс, 2018. 1440 с.

5. Ковцур М. М. Разработка методики по оценке тестирования производительности базы данных / М. М. Ковцур, А. В. Михайлова, П. А. Потемкин // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции, Санкт-Петербург, 30 ноября – 02 2021 года. СПб.: СПбГУТ. 2022. С. 236-240. EDN: PVWORB.

Статья представлена кандидатом технических наук, доцентом кафедры ИБКС СПбГУТ М. М. Ковцуром.

УДК 004.02

АНАЛИЗ СТРУКТУРЫ ОСНОВНЫХ ФАЙЛОВ ВИРТУАЛЬНЫХ МАШИН В ЦИФРОВО-КРИМИНАЛИСТИЧЕСКОМ АСПЕКТЕ

А. У. Паскенова (студент группы ИБС-12 СПбГУТ), paskenova.au@sut.ru

В современном обществе виртуальные машины выступают основой IT-инфраструктуры. В условиях динамичного роста данных и развития технологических ресурсов, требующих высокой производительности, знание о б устройстве и взаимодействии файлов виртуальных машин становится актуальным как для предотвращения потенциальных угроз, так и для результативного цифрово-криминалистического расследования. В работе представлены основные типы файлов, их характеристики и влияние на производительность и безопасность виртуальных сред, что позволяет выделить важные аспекты для цифровых криминалистов, IT-специалистов и администраторов.

виртуальная машина, цифрово-криминалистический анализ, файловая структура, технологическая инфраструктура

Технология виртуализации в наши дни представляет собой одну из основополагающих составляющих успеха в работе с цифровой инфраструктурой. Основным элементом этой технологии выступают виртуальные машины (ВМ), предоставляющие возможность масштабирования, изолирования приложений, тестирования новых решений и проведения эффективного расследования инцидентов. Это особенно полезно в условиях, стремительно развивающихся технологий, нуждающихся в высокой производительности. Распространение виртуализации обязывает специалистов иметь глубокое понимание внутренней структуры файлов, которые лежат в основе функционирования виртуальных машин. Некорректная настройка данных файлов может привести к утрате конфиденциальной информации или нестабильной работе систем, что может обернуться существенными проблемами для предприятий разных сфер деятельности. Исходя из этого, детальное изучение основных видов файлов и их ролей является неотъемлемой частью процесса достижения успеха в деятельности цифровых криминалистов и системных администраторов.

Виртуальная машина является программной эмуляцией физического персонального компьютера (ПК), открывающей возможность запуска операционных систем и прикладного программного обеспечения в специально выделенной, изолированной среде. Гибкое распределение вычислительных

ресурсов, оперативность в развертывании и управлении – все это является ключевыми преимуществами виртуальных машин.

Сферы применения технологии виртуализации разнообразны. Эмуляторы ПК активно используются как в облачных технологиях, при тестировании нового программного обеспечения, так и в образовательных целях. Предоставляя возможность создания обособленных пространств для разработки и испытаний, виртуальные машины способствуют снижению потенциальных рисков при внедрении новых решений в эксплуатируемые рабочие информационные инфраструктуры.

Виртуализация также упрощает резервное копирование и восстановление систем.

Существуют три основных типа виртуальных машин:

● полноценные виртуальные машины. Данный тип ВМ использует гипервизоры, эмулирующие аппаратное обеспечение, что позволяет запустить различные ОС. Преимуществом является обеспечение высокого уровня изоляции и гибкости, недостатком – требование большого количества ресурсов;

● паравиртуальные машины. В отличие от предыдущего типа, требуют модификации гостевой ОС, для ее работы в среде виртуализации. Ввиду этого появляется возможность достижения более высокого уровня производительности по сравнению с полноценными виртуальными машинами, однако снижает уровень изоляции;

● контейнеры. Они представляют собой легковесную виртуализацию, где приложения работают в пределах общей операционной системы. Контейнеризация обеспечивает быстрое развертывание, масштабируемость и эффективное использование ресурсов, но с меньшей изоляцией по сравнению с полноценными виртуальными машинами [1].

Типы ВМ используют данные файлы по-разному. Полноценные виртуальные машины считывают свои параметры и ресурсы из файлов конфигурации и используют образ диска для полной эмуляции. Контейнеры, имея меньшую потребность в таких образах, лучше раскрывают возможности логирования и временных файлов для отслеживания изменений и состояния приложений в реальном времени.

Различные платформы виртуализации имеют свои особенности в структуре файлов, необходимых для функционирования виртуальных машин. Рассмотрим основные платформы виртуализации: VMware, Oracle

VirtualBox, Microsoft Hyper-V, KVM и проанализируем их файловую структуру.

VMware является одной из самых популярных платформ виртуализации и предоставляет инструменты для создания и управления виртуальными машинами. Структура виртуальной машины в VMware включает несколько ключевых компонентов:

● файлы образов дисков: основным форматом является VMDK, который хранит данные виртуального диска и может содержать как полностью развернутый, так и дифференциальный диск;

● файлы конфигурации: файл VMX содержит конфигурацию виртуальной машины, включая ее параметры. При старте ВМ данный файл загружается для инициализации необходимых ресурсов;

● логи: файлы логов регистрируют все действия и события, происходящие в процессе работы виртуальной машины, что позволяет администратору или цифровому криминалисту отслеживать историю выполнения и диагностировать возможные ошибки.

Файлы VMDK и VMX являются критическими для работы ВМ. Ошибка в одном из этих файлов приводит к сбою виртуальной машины или потере данных. Примеры использования таких файлов в администрировании могут варьироваться от восстановления из резервной копии образа диска до анализа журналов для устранения неполадок [2].

Oracle VirtualBox является бесплатной платформой для виртуализации, поддерживающей различные ОС. Структура файлов VirtualBox включает следующие элементы:

● VDI (Virtual Disk Image): основной формат файла виртуального диска, который хранит данные виртуальной машины. VDI поддерживает функции динамического выделения пространства и создания снимков;

● VBOX: файл конфигурации ВМ, хранящий количество выделенной памяти, процессоров и параметры сетевого адаптера. Данный файл записан в формате XML, что делает его удобным для редактирования;

● логи: VirtualBox создает файлы логов, содержащие информацию об операциях и событиях ВМ, позволяя администраторам и криминалистам отслеживать работу системы и диагностировать проблемы.

Microsoft Hyper-V выступает платформой виртуализации, встроенной в Windows Server и более новые версии Windows. Основные элементы структуры файлов Hyper-V включают:

● VHD и VHDX: форматы виртуальных жестких дисков. VHD имеет некоторые ограничения по размеру (до 2 ТБ), тогда как VHDX поддерживает более крупные образы и обеспечивает высокую производительность;

● конфигурационные XML-файлы: эти файлы служат для хранения настроек ВМ, обеспечивая их корректное функционирование;

● журналы учета событий: система Hyper-V фиксирует все происходящие события в журналы Windows, тем самым создает подробную хронологию рабочей сессии каждой ВМ. Это крайне важно для последующего проведения криминалистического анализа цифровых данных.

KVM (Kernel-based Virtual Machine) представляет собой комплексное решение для виртуализации, интегрированное в ядро операционной системы Linux. Файловая структура KVM имеет следующие ключевые компоненты:

● QCOW2 (QEMU Copy On Write): данный файл выступает в роли основного формата виртуального диска. Благодаря поддержке функций дедупликации и создания моментальных снимков (снапшотов), KVM позволяет сохранить состояние ВМ в определенный момент времени. Эта возможность имеет первостепенное значение для сбора и сохранения цифровых следов;

● файлы конфигурации: KVM допускает использование как XML-формата, так и обычных текстовых файлов для настройки. Это, в свою очередь, открывает широкие возможности для автоматизации процессов развертывания и управления с помощью разнообразных инструментов;

● логи и статистика: система KVM активно собирает информацию о работе ВМ в виде логов и статистических данных о производительности и действиях [3].

Анализ файловых структур виртуальных машин на различных платформах свидетельствует о схожести общих принципов работы при использовании многообразных форматов и схем организации. Понимание представленных структур поможет цифровым криминалистам в повышении уровня эффективности управления виртуальными средами и оперативном решении возникающих проблем при проведении расследования цифровых инцидентов. Сопоставление характеристик платформ открывает возможность выбора наиболее подходящего решения для конкретных задач.

Понимание данных различий играет важную роль не только в администрировании ВМ, но и при проведении цифрово-криминалистического анализа, поскольку знание специфики файловой структуры каждой платформы

позволяет провести восстановление и извлечение доказательств, идентификацию следов вмешательства, соблюдение юридических требований, оптимизацию ресурсов времени и проведение корректного анализа в целом. Все это способствует повышению доверия к процессу расследований, снижению риска упущения важных улик, укреплению правовой базы, что критично для выявления и предотвращения киберпреступлений.

В качестве примера рассмотрим платформу VMware, как одну из самых распространенных. В процессе работы цифровые криминалисты довольно часто сталкиваются с задачей извлечения данных из VMDK-файла, не запуская виртуальную машину, при помощи сторонних программно-аппаратных средств. Анализ VMX-файла предоставляет возможность установки параметров сети, объема выделенной на ВМ памяти, а также подключенные устройства, что может указывать на следы несанкционированного доступа и нарушения целостности конфигурации. Логи также являются неотъемлемой частью работы цифровых криминалистов. Временные метки, такие как моменты запуска, остановки и снимки экранов, могут стать основой для восстановления полной картины цифрового инцидента и последующего правового разбирательства [4].

Со стремительным развитием технологий виртуализация также продолжает эволюционировать. Новые файловые форматы и методы хранения данных обеспечивают более высокую производительность, надежность и безопасность. Ожидаются улучшения в области сжатия данных, поддержки облачных решений и активная интеграция искусственного интеллекта, что сделает виртуальные машины еще более эффективными и универсальными. Таким образом, внимание к деталям и детальное изучение файловой структуры, а также понимание ее значимости в управлении виртуальными машинами является одним из решающих факторов не только в повышении конкурентоспособности организаций и оптимизации IT-инфраструктуры, но и в обеспечении надежности, эффективности и точности цифровых криминалистических расследований.

Список используемых источников

1. Вехов В. Б., Зуев С. В. Цифровая криминалистика: учебник для вузов. 2-е изд., перераб. и доп. М: Юрайт, 2025. 490 с.

2. Шариков П. И., Красов А. В., Майоров А. В. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности // Вестник Дагестанского государственного технического университета. Технические

науки. 2025. Т. 52. № 1. С. 147–161. DOI: 10.21822/2073-6185-2025-52-1-147-161. EDN: AWEHRP.

3. Шариков П. И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов / П. И. Шариков // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 58-62.

4. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47-58.

Статья представлена научным руководителем, кандидатом технических наук П. И. Шариковым.

УДК 004.056.53

МЕТОДИКА ИДЕНТИФИКАЦИИ МНОГОЭТАПНЫХ КИБЕРАТАК НА ПРИКЛАДНЫЕ СЕРВИСЫ В ИНФРАСТРУКТУРЕ СЕТЕЙ 6G НА ОСНОВЕ АНАЛИЗА СЕТЕВОЙ ТЕЛЕМЕТРИИ

Д. А. Романова (магистрант группы МЗС-2512), romanova.da@sut.ru

С переходом к концепции граничных вычислений и децентрализации сетевых функций возрастает риск реализации сложных многоэтапных кибератак на периферийные узлы инфраструктуры. Традиционные прикладные сервисы, такие как веб-панели мониторинга и системы управления контентом, становятся критическими точками входа для реализации сложных многоэтапных воздействий. В данной статье на основе анализа сетевой телеметрии представлена методика идентификации цепочек кибератак в инфраструктуре 6G. Особое внимание уделяется необходимости комплексного мониторинга трафика для защиты целостности сервисных узлов и предотвращения несанкционированного доступа к данным в сетях связи будущего.

сети 6G, граничные вычисления, сетевая телеметрия, многоэтапные атаки, CMS, анализ трафика, инфраструктура связи

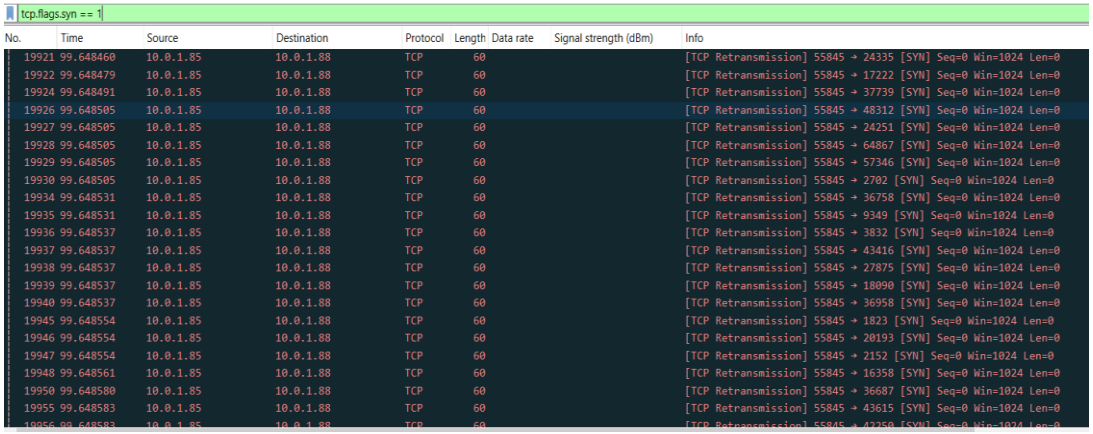
Современный этап развития инфокоммуникационных технологий характеризуется активным формированием архитектурных решений сетей шестого поколения. В отличие от предшествующих стандартов, экосистема 6G предполагает глубокое внедрение концепции граничных вычислений, где прикладные сервисы и сетевые функции выносятся на периферию сети для минимизации задержек [1]. Однако подобная децентрализация создает новые риски: периферийные узлы, зачастую работающие под управлением стандартных операционных систем и прикладного ПО, становятся первичными целями для реализации многоэтапных кибератак [2].

В условиях сверхвысоких скоростей передачи данных традиционные системы обнаружения вторжений могут демонстрировать недостаточную эффективность [3]. В этой связи фундаментальное значение приобретает ретроспективный анализ сетевой телеметрии в формате глубокого анализа пакетов (DPI). Детальное изучение дампов трафика позволяет восстановить полную хронологию инцидента в рамках модели Cyber Kill Chain [4].

Для верификации методики смоделирована атака на типовой Edge-узел под управлением CMS WordPress. Исследование базировалось на анализе дампов трафика с использованием ПО Wireshark. Методология включала сигнатурную идентификацию инструментов сканирования, декомпозицию полезной нагрузки HTTP-запросов и реконструирование интерактивных

TCP-сессий для выявления признаков повышения привилегий и эксфильтрации данных.

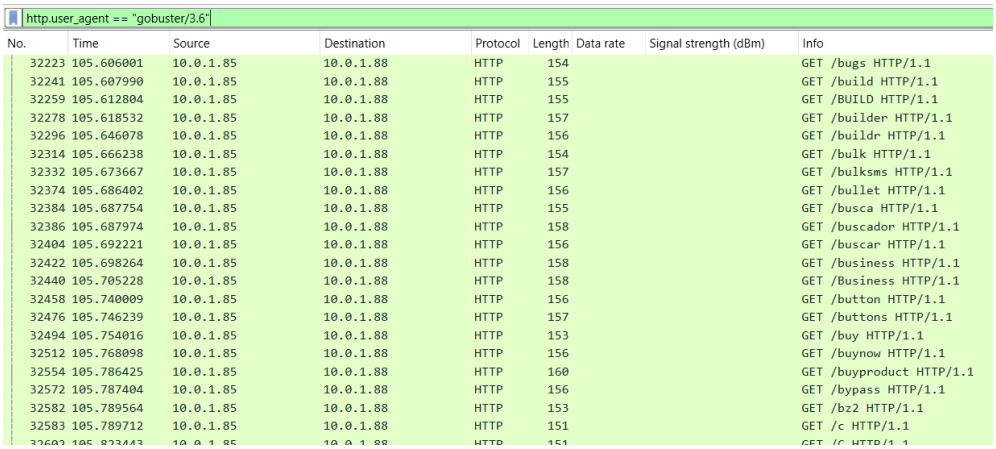
Начальная фаза атаки характеризовалась высокой активностью сканирующих утилит. Анализ телеметрии показал всплеск TCP SYN пакетов с адреса 10.0.1.85 на узел 10.0.1.88, что представлено на рисунке 1. Использование фильтра tcp.flags.syn == 1 позволило выявить работу сканера «masscan».


tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Length	Data rate	Signal strength (dBm)	Info
19921	99.648460	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 24335 [SYN] Seq=0 Win=1024 Len=0
19922	99.648479	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 17222 [SYN] Seq=0 Win=1024 Len=0
19924	99.648491	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 37739 [SYN] Seq=0 Win=1024 Len=0
19926	99.648505	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 48312 [SYN] Seq=0 Win=1024 Len=0
19927	99.648505	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 24251 [SYN] Seq=0 Win=1024 Len=0
19928	99.648505	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 64867 [SYN] Seq=0 Win=1024 Len=0
19929	99.648505	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 57346 [SYN] Seq=0 Win=1024 Len=0
19930	99.648505	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 2702 [SYN] Seq=0 Win=1024 Len=0
19934	99.648531	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 36758 [SYN] Seq=0 Win=1024 Len=0
19935	99.648531	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 9349 [SYN] Seq=0 Win=1024 Len=0
19936	99.648537	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 3832 [SYN] Seq=0 Win=1024 Len=0
19937	99.648537	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 43416 [SYN] Seq=0 Win=1024 Len=0
19938	99.648537	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 27875 [SYN] Seq=0 Win=1024 Len=0
19939	99.648537	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 18090 [SYN] Seq=0 Win=1024 Len=0
19940	99.648537	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 36958 [SYN] Seq=0 Win=1024 Len=0
19945	99.648554	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 1823 [SYN] Seq=0 Win=1024 Len=0
19946	99.648554	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 20193 [SYN] Seq=0 Win=1024 Len=0
19947	99.648554	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 2152 [SYN] Seq=0 Win=1024 Len=0
19948	99.648561	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 16358 [SYN] Seq=0 Win=1024 Len=0
19950	99.648580	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 36687 [SYN] Seq=0 Win=1024 Len=0
19955	99.648583	10.0.1.85	10.0.1.88	TCP	60			[TCP Retransmission] 55845 → 43615 [SYN] Seq=0 Win=1024 Len=0

Рис. 1. Применение фильтра tcp.flags.syn == 1

Последующая фаза брутфорса веб-директорий идентифицирована по полю User-Agent «gobuster» На рисунке 2 продемонстрировано, что идентификация инструмента проводилась по значению поля User-Agent: gobuster/3.6. Наличие множественных GET-запросов к несуществующим URL, таким как HTTP с последующим кодом ошибки 404 свидетельствует о подготовке к эксплуатации прикладного уровня.


http.user_agent == "gobuster/3.6"

No.	Time	Source	Destination	Protocol	Length	Data rate	Signal strength (dBm)	Info
32223	105.606001	10.0.1.85	10.0.1.88	HTTP	154			GET /bugs HTTP/1.1
32241	105.607990	10.0.1.85	10.0.1.88	HTTP	155			GET /build HTTP/1.1
32259	105.612804	10.0.1.85	10.0.1.88	HTTP	155			GET /BUILD HTTP/1.1
32278	105.618532	10.0.1.85	10.0.1.88	HTTP	157			GET /builder HTTP/1.1
32296	105.646078	10.0.1.85	10.0.1.88	HTTP	156			GET /buildr HTTP/1.1
32314	105.666238	10.0.1.85	10.0.1.88	HTTP	154			GET /bulk HTTP/1.1
32332	105.673667	10.0.1.85	10.0.1.88	HTTP	157			GET /bulksms HTTP/1.1
32374	105.686402	10.0.1.85	10.0.1.88	HTTP	156			GET /bullet HTTP/1.1
32384	105.687754	10.0.1.85	10.0.1.88	HTTP	155			GET /busca HTTP/1.1
32386	105.687974	10.0.1.85	10.0.1.88	HTTP	158			GET /buscador HTTP/1.1
32404	105.692221	10.0.1.85	10.0.1.88	HTTP	156			GET /buscar HTTP/1.1
32422	105.698264	10.0.1.85	10.0.1.88	HTTP	158			GET /business HTTP/1.1
32440	105.705228	10.0.1.85	10.0.1.88	HTTP	158			GET /Business HTTP/1.1
32458	105.740009	10.0.1.85	10.0.1.88	HTTP	156			GET /button HTTP/1.1
32476	105.746239	10.0.1.85	10.0.1.88	HTTP	157			GET /buttons HTTP/1.1
32494	105.754016	10.0.1.85	10.0.1.88	HTTP	153			GET /buy HTTP/1.1
32512	105.768098	10.0.1.85	10.0.1.88	HTTP	156			GET /buynow HTTP/1.1
32554	105.786425	10.0.1.85	10.0.1.88	HTTP	160			GET /buyproduct HTTP/1.1
32572	105.787404	10.0.1.85	10.0.1.88	HTTP	156			GET /bypass HTTP/1.1
32582	105.789564	10.0.1.85	10.0.1.88	HTTP	153			GET /bz2 HTTP/1.1
32583	105.789712	10.0.1.85	10.0.1.88	HTTP	151			GET /c HTTP/1.1

Рис. 2. Применение фильтра http.user_agent == "gobuster/3.6"

Злоумышленником реализована атака на критическую уязвимость плагина Elementor Pro. Телеметрия выявила несанкционированную регистрацию пользователя support с последующей аутентификацией, что показано на рисунке 3.

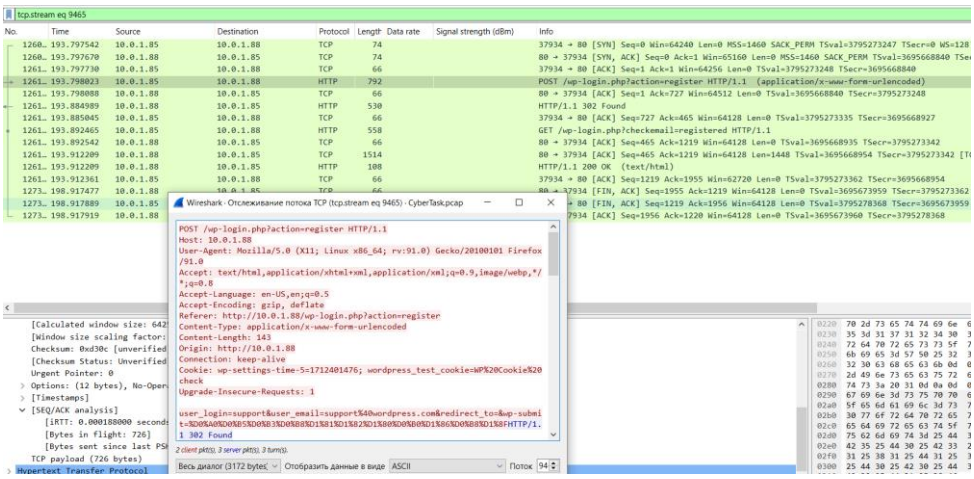


Рис. 3. Регистрация пользователя «support»

Извлечение файла из трафика подтвердило в полезной нагрузке PHP-скрипт, инициирующий соединение с центром управления по порту 4444. Последующий анализ показал загрузку модулей Meterpreter и использование утилиты socat на порту 443 для маскировки трафика под легитимную TLS-сессию, что фиксируется на рисунке 4. Это демонстрирует стремление маскировать атаку под стандартный веб-трафик сервисного узла 6G.

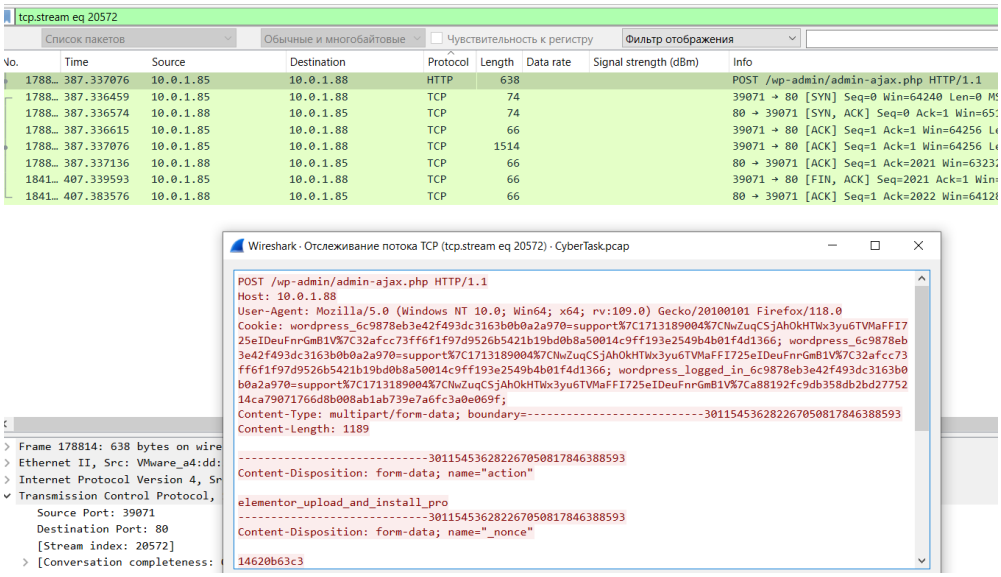


Рис. 4. Загрузка файла «elementor-pro.zip»

Критическим этапом стало локальное повышение привилегий через эксплуатацию некорректной конфигурации Linux Capabilities утилиты base64, что показано на изображении 5. Анализ TCP-потока выявил несанкционированное чтение файлов /etc/passwd и /etc/shadow. Финальная стадия включала в себя эксфильтрацию и заключалась в выгрузке зашифрованного архива pass.zip и GPG-контейнера через установленный веб-шелл семейства WSO, что представлено на рисунке 6.

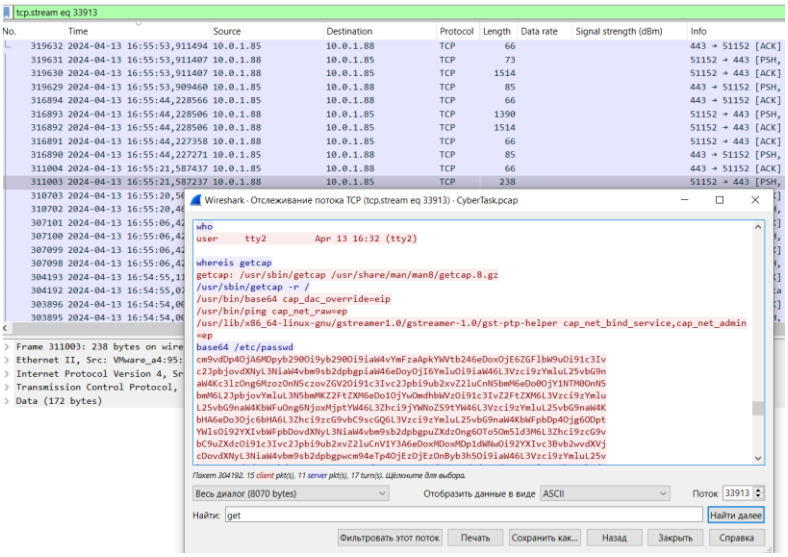


Рис. 5. Повышение привилегий

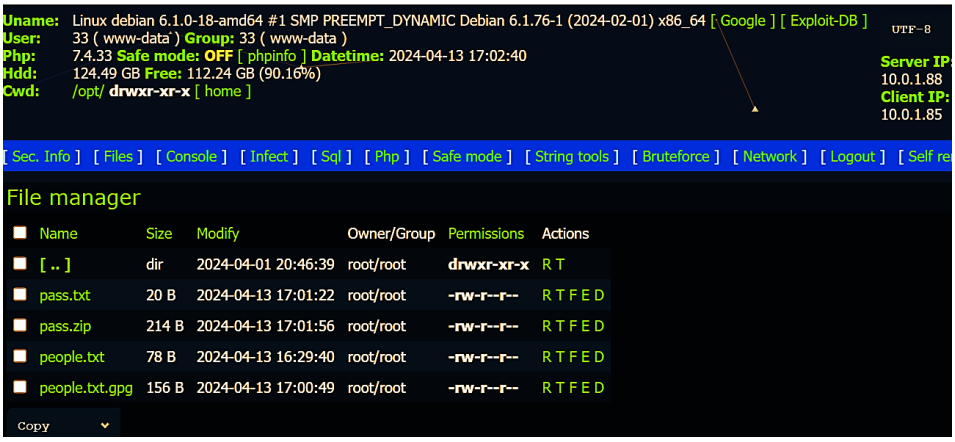


Рис. 6. Выгрузка зашифрованного GPG-контейнера с персональными данными пользователей

На основе проведенного анализа были сформированы ключевые индикаторы компрометации, позволяющие автоматизировать обнаружение подобных атак в высокоскоростных сегментах сетей 6G, представленные в таблице 1.

ТАБЛИЦА 1. Индикаторы компрометации сервисного узла

Тип индикатора	Значение	Описание
IP-адрес ЦУУ	10.0.1.85	Адрес атакующего узла
User-Agent	gobuster/3.6, sqlmap/1.6.8	Автоматизированные средства взлома
Сетевой порт	4444 (TCP)	Нестандартный порт C2-канала
Имя файла	wp-admin-support.php	Скрытый веб-шелл (WSO)

Результаты исследования показывают, что несмотря на новизну архитектур 6G, векторы атак на прикладном уровне остаются традиционными, что требует внедрения интеллектуальных систем мониторинга трафика на периферийных узлах связи [5]. Экспериментально было подтверждено, что методика анализа телеметрии позволяет идентифицировать все стадии многоэтапной атаки на граничные узлы сетей 6G. Результаты работы могут быть использованы для формирования баз сигнатур систем защиты нового поколения.

Список используемых источников

1. Мутханна А. С. А. Разработка и исследование комплекса моделей и методов интеграции граничных вычислений в сетях связи пятого и шестого поколений: диссертация на соискание ученой степени доктора технических наук / Мутханна Аммар Салех Али, 2023. 393 с. EDN: QFZHAN.

2. Заложук К. О. Исследование модели угроз для системы IOT умного города на примере интеллектуальной транспортной системы: угрозы безопасности и целостности данных / К. О. Заложук, М. В. Сомова // Перспективы цифровизации и технологические инновации: вызовы и возможности: Сборник статей по итогам Международной научно-практической конференции, Калуга, 19 января 2026 года. Стерлитамак: ООО "Агентство международных исследований", 2026. С. 77-81. EDN: TVHLEN.

3. Особенности классификации и фильтрации трафика сети передачи данных 6G / И. Г. Бужин, В. М. Антонова, Ю. Б. Миронов [и др.] // Труды МАИ. 2021. № 121. DOI 10.34759/trd-2021-121-12. EDN: XBAMMK.

4. Бойченко О. В. Модель многоступенчатой кибератаки Cyber Kill Chain / О. В. Бойченко // Дистанционные образовательные технологии:МАТЕРИАЛЫ VII МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ, Ялта, 20–22 сентября 2022 года. Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2022. С. 246-250. EDN: UGZVWV.

5. Лоскутова В. С. Анализ угроз безопасности в сетях 6G с применением моделей машинного обучения / В. С. Лоскутова // Профессиональный Вестник: Информационные технологии и безопасность. 2025. № 1. С. 3-9. EDN: QJQYUB.

Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук Д. В. Кушниром.

УДК 004.056

КОМБИНИРОВАННЫЙ ПОДХОД К АУДИТУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ИНТЕГРАЦИЯ СКАНЕРОВ УЯЗВИМОСТЕЙ И SIEM-СИСТЕМЫ

А. С. Сидельников (студент группы ИКТБ-48м СПбГУТ),
sidelnikov.as@sut.ru

В статье рассматривается проблема повышения эффективности аудита информационной безопасности организации за счет интеграции систем сканирования уязвимостей и SIEM-платформ. Цель исследования заключается в разработке комбинированного подхода, позволяющего объединить периодический контроль состояния инфраструктуры и непрерывный мониторинг событий безопасности. Предложена методика корреляции результатов сканирования уязвимостей с событиями SIEM-системы Wazuh. В качестве экспериментального стенда использована виртуальная инфраструктура на базе Ubuntu Server, Kali Linux и Wazuh OVA. Проведенные испытания показали возрастание полноты выявления инцидентов, снижение количества ложноположительных срабатываний и ускорение приоритизации рисков. Полученные результаты могут быть использованы при построении процессов внутреннего аудита ИБ в организациях малого и среднего бизнеса.

аудит информационной безопасности, сканирование уязвимостей, SIEM-система, Wazuh, мониторинг событий

Согласно аналитическим исследованиям, количество кибератак на корпоративную инфраструктуру ежегодно возрастает. По данным компании Positive Technologies за I-II кварталы 2025 года [1] в успешных атаках на организации был отмечен значительный рост интереса злоумышленников к вредоносному ПО. Благодаря способности быстро внедряться в атакуемые системы, подолгу оставаться в тени и давать злоумышленникам надежный контроль над взломанными ресурсами, это средство по-прежнему входит в число самых действенных при проведении кибератак [1-5]. Таким образом, возрастает значение регулярного аудита информационной безопасности.

Традиционные методы аудита информационной безопасности, основанные на периодических проверках, не позволяют своевременно выявлять возникающие угрозы, изменения конфигурации инфраструктуры и попытки эксплуатации уязвимостей. В условиях роста числа атак возникает необходимость перехода к непрерывному аудиту, основанному на автоматизированном сборе и анализе событий безопасности.

Целью работы является повышение эффективности аудита информационной безопасности за счет интеграции сканеров уязвимостей и SIEM-системы. В качестве SIEM-платформы рассмотрено решение Wazuh, предназначенное для централизованного сбора, хранения и корреляции событий безопасности [2].

Сканеры уязвимостей позволяют обнаруживать ошибки конфигурации, открытые сетевые сервисы, устаревшее программное обеспечение и иные потенциальные угрозы. Вместе с тем результаты сканирования отражают состояние инфраструктуры только на момент проверки. SIEM-система, напротив, обеспечивает постоянный анализ журналов событий, сетевой активности и действий пользователей, однако без дополнительных данных не всегда позволяет корректно определить приоритет угрозы.

Совместное применение указанных средств обеспечивает следующие преимущества:

- повышение полноты аудита за счет объединения статических и динамических данных;
- сокращение времени анализа инцидентов;
- приоритизацию событий безопасности с учетом обнаруженных уязвимостей;
- возможность автоматического запуска дополнительных проверок при выявлении подозрительной активности.

В качестве проверки комбинированного подхода был создан лабораторный стенд, состоящий из Ubuntu Server и Wazuh OVA, а также Kali Linux. Выбор Wazuh в качестве SIEM-системы основывался на ее доступности и широком выборе возможностей для обнаружения угроз [0]. В ходе работы было запущено сканирование портов тестового сервера утилитой Nmap. Сканирование осуществлялось с виртуальной среды Kali Linux с предустановленной утилитой Nmap и Wazuh Agent, в конфигурации которого создано правило (рис. 1).

В то же время на машине Wazuh OVA было установлено специальное оповещение (рис. 2) для дашборда Wazuh, в котором отображены все подробности о процессе сканирования.

```
<localfile>
  <log_format>full_command</log_format>
  <command>nmap -sV -F 192.168.0.154</command>
  <frequency>3600</frequency>
</localfile>
```

Рис. 1. Настройка правила обнаружения Nmap в Kali Linux

```
<group name="nmap_simple">
  <rule id="100500" level="7">
    <if_sid>530</if_sid>
    <match>nmap -sV -F 192.168.0.154</match>
    <description>Результат сканирования Nmap с Kali</description>
  </rule>
</group>
```

Рис. 2. Настройка корреляционного правила в Wazuh

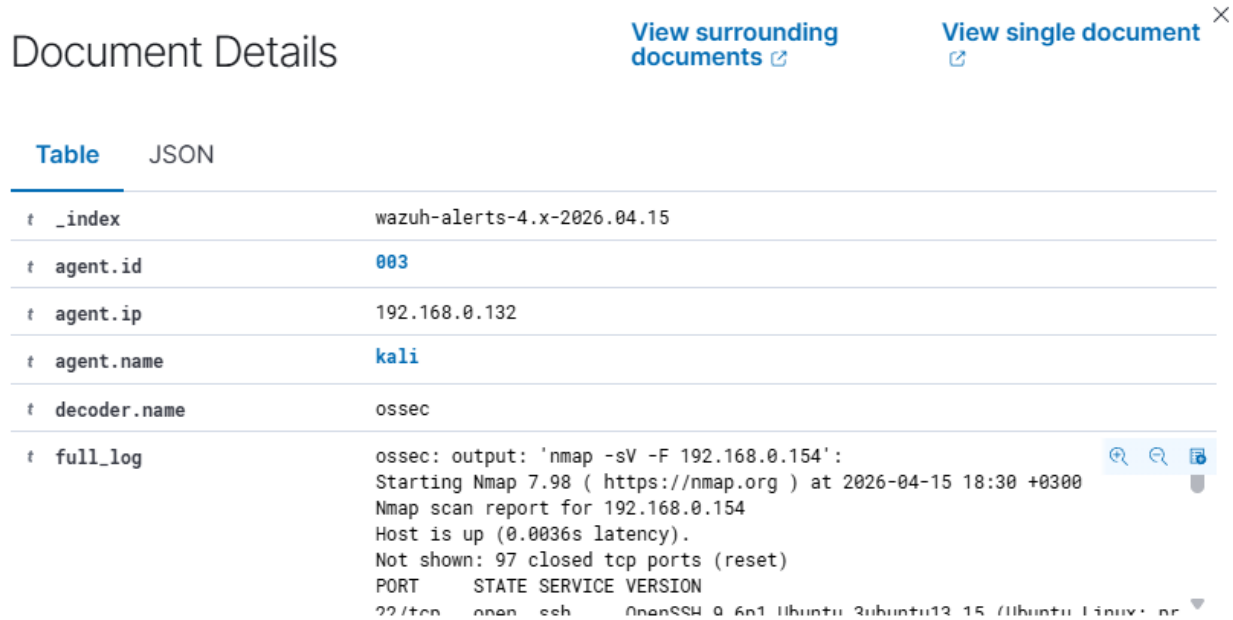


Рис. 3. Интерфейс оповещения о сетевом сканировании

В ходе эксперимента система Wazuh за короткое время зафиксировала обращения ко многим сетевым портам, по одному из которых сработало оповещение (рис. 3). Затем результаты сканирования были сопоставлены с данными о состоянии целевого узла. Это позволило определить, насколько событие критично, и точнее оценить риски.

Также нельзя не упомянуть, что платформа Wazuh поддерживает интеграцию со сканером уязвимостей OpenVAS, позволяя импортировать результаты проверок, в одном месте проанализировать все найденные уязвимости и использовать их при поиске взаимосвязей между событиями безопасности. Кроме того, система способна к обнаружению признаков SQL-инъекций, анализируя HTTP-заголовки и параметры запросов, что помогает эффективнее находить уязвимости в веб-приложениях.

Таким образом, проведенный эксперимент показал, что при объединении сканеров уязвимостей и SIEM-системы, можно перейти от периодических проверок к непрерывному мониторингу защищенности. Такой подход может быть применен в организациях малого и среднего бизнеса, не располагающих значительными финансовыми ресурсами.

Список используемых источников

1. Positive Technologies. Актуальные киберугрозы I–II кварталы 2025 года [Электронный ресурс]. Режим доступа: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (дата обращения: 11.04.2026).

2. Wazuh Documentation [Электронный ресурс]. Режим доступа: https://documentation.wazuh.com/ (дата обращения: 11.04.2026).

3. Stanković S., Gajin S., Petrović R. A review of Wazuh tool capabilities for detecting attacks based on log analysis //No Nama Agent Integrity File Added Delete Modified. 2022. Т. 1.

4. Greenbone Networks. OpenVAS Scanner Documentation [Электронный ресурс]. Режим доступа: https://www.greenbone.net/ (дата обращения: 11.04.2026).

5. Шарифов Р. Г. ЭФФЕКТИВНОСТЬ WAZUH ПРИ ОБНАРУЖЕНИИ АТАК В ЛВС // Информационная безопасность регионов России (ИБРР-2025). 2025. С. 508.

Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом И. Н. Бабковым.

УДК 004.056.5

КОНТЕЙНЕРИЗИРОВАННАЯ ПЛАТФОРМА ДЛЯ ПРАКТИЧЕСКОГО ИССЛЕДОВАНИЯ И ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА УЯЗВИМОСТЕЙ СМАРТ-КОНТРАКТОВ

А. А. Теровец (студент группы МЗС-2511 СПбГУТ), terovec.aa@sut.ru

В работе рассматривается специализированная локальная платформа для практического исследования уязвимостей смарт-контрактов в управляемой блокчейн-среде. Платформа реализована в виде преднастроенной виртуальной машины на базе Ubuntu, внутри которой развернут контейнеризированный учебно-исследовательский стенд. Стенд построен на основе локальной EVM-сети, корпуса преднамеренно уязвимых контрактов, сервисов публикации и верификации исходного кода, веб-приложения, обозревателя блоков и набора инструментов для разработки и взаимодействия с сетью.

В отличие от типовых учебных решений, сводящихся к разрозненным фрагментам кода или отдельным тестовым сценариям, предложенная платформа формирует единое воспроизводимое пространство, приближенное к условиям реальной эксплуатации смарт-контрактов. Практическая ценность решения состоит в том, что оно может использоваться не только как учебный стенд для лабораторных работ, но и как архитектурная основа для последующего построения универсальной системы автоматизированного и интеллектуального анализа смарт-контрактов.

смарт-контракты, контейнеризация, локальный блокчейн, информационная безопасность, интеллектуальный анализ

Уязвимости смарт-контрактов являются частным случаем более широкого класса угроз безопасности блокчейн-систем, включая проблемы криптографии, механизмов консенсуса и сетевого взаимодействия [1]. Практическое обучение безопасности смарт-контрактов требует среды, в которой уязвимости можно не только прочитать в исходном коде, но и воспроизвести в управляемом эксперименте. Это обусловлено широким распространением смарт-контрактов как основного механизма реализации логики в блокчейн-системах [2]. Использование публичных тестовых сетей неудобно по нескольким причинам, их состояние нестабильно, внешняя инфраструктура не контролируется, а раздельная настройка локальной сети, кошельков, обозревателей, среды разработки и инструментов тестирования отнимает значительное время. В результате существенная часть учебного процесса смещается в сторону администрирования, а не анализа атакующих сценариев.

Рассматриваемый проект решает эту проблему за счет преднастроенной виртуальной машины и контейнеризированной платформы, внутри которой уже собран полный исследовательский контур. Такой подход можно использовать не только для учебных задач, но и для экспериментальной работы: обучающийся получает готовую экосистему для практики, а исследователь – воспроизводимую среду для постановки и повторения атакующих сценариев, что особенно актуально в условиях наличия значительного числа рисков и угроз безопасности в децентрализованных приложениях [3, 4].

Цель работы состоит в создании воспроизводимой локальной платформы для практического изучения уязвимостей смарт-контрактов и подготовки архитектурной основы для последующего интеллектуального анализа контрактного кода и транзакционного поведения. Научно-практическая новизна решения заключается в объединении в едином контейнеризированном контуре локальной сети, сервиса деплоя, публикации и верификации исходников, обозревателя, контролируемого RPC-интерфейса и корпуса преднамеренно уязвимых контрактов.

Основой платформы является контейнеризированная инфраструктура, описанная в docker-compose.yml. В составе системы разворачиваются семь сервисов: geth, prefund, lab-deployer, webapp, sourcify, ots-bridge и explorer. Для пользователя это означает наличие полного контура работы: локальной сети, корпуса смарт-контрактов, пользовательского интерфейса, обозревателя блоков и механизма верификации исходного кода.

Доступ сервисам организован через разные точки входа. Веб-интерфейс работает на порту 8080, обозреватель блоков Otterscan доступен через 5100, Sourcify – 5555. Взаимодействие с локальными инструментами (MetaMask, Remix, локальные скрипты и др.) происходит с помощью RPC-контура реализованным на базе ots-bridge. Такое разделение позволяет изолировать друг от друга пользовательские и служебные функции.

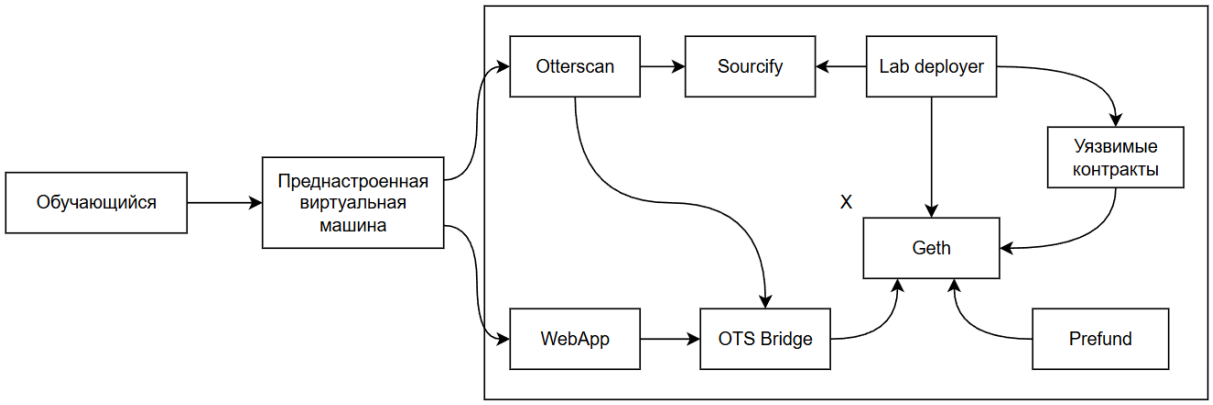


Рис. 1. Архитектура

Локальная сеть строится на базе Geth с chainId = 1337 и консенсусом Clique (Proof-of-Authority). Такой выбор обусловлен малым требованием к вычислительным ресурсам, а также стабильным временем генерации блоков. При запуске автоматически создаются три типа аккаунтов. Аккаунт валидатора и аккаунт студента, а также несколько вспомогательных (скрытых) адресов. Пользователь работает только с аккаунтом студента. Инфраструктура использует валидатор и скрытые аккаунты. Валидатор, который нужен чтобы создавать блоки, а скрытые аккаунты используются для развертывания контрактов и выступают как внешние симуляторы ликвидности.

Важная особенность проекта – автоматизированная подготовка среды. Когда сеть запущена в первый раз, сервис prefund переводит на аккаунт студента 10 ETH и задает повышенный уровень средств для скрытых аккаунтов. Это предотвращает ручное пополнение и позволяет сразу выполнять сценарии лабораторных работ.

Развертывание контрактов выполняется через сервис lab-deployer. Сервис автоматически собирает контракты и публикует их в сети, сохраняет ABI и манифест развертывания, а также отправляет исходный код контрактов в локальный Sourcify. Чтобы моделировать внешнюю ликвидность сервис lab-deployer, используя скрытые аккаунты, финансирует контракты определенной суммой ETH после того, как их исходный код опубликован в Sourcify. Суть механизма в том, что он объединяет байткод, abi, адрес и исходный код в единый наблюдаемый объект.

В стендовой архитектуре service ots-bridge всегда выступает промежуточным слоем. Он реализует методы ots_* и erigon_* для работы Geth под обозреватель Otterscan, поддерживает трассировку транзакций и также управляет внешним доступом к RPC. Также ots-bridge закрывает служебные вызовы к Geth. Это позволяет пользователю взаимодействовать с сетью с помощью знакомых инструментов, при этом предоставляя доступ только к аккаунту студента и сохраняя скрытые аккаунты защищенными и используемыми системой в сценариях лаборатории.

Реализация лабораторных сценариев представлена в формате capture the flag. Студенту нужно взломать web3 приложение. Эта часть реализована в виде легкого веб-приложения. Оно автоматически загружает текущие адреса контрактов, ABI развернутых контрактов, выполняется подключение к MetaMask, проверяется ожидаемая сеть и предоставляется базовый интер-

фейс для стандартных действий. Однако адреса контрактов не акцентируются на уровне интерфейса, с помощью этого поддерживается практика анализа через обозреватель, кошелек и инструменты разработки, а не через механическое копирование реквизитов.

Типовой сценарий взаимодействия с платформой требует уточнения с учетом фактической реализации репозитория. Во-первых, развертывание уязвимых контрактов выполняется не пользователем, а сервисом lab-deployer, который компилирует контракты, публикует их в локальной сети и передает исходные тексты и метаданные в Sourcify. Во-вторых, внешние пользовательские действия не направляются напрямую в Geth: все RPC-запросы от MetaMask, Remix, Hardhat, Foundry и браузерного интерфейса проходят через ots-bridge, который фильтрует разрешенные операции и оставляет доступной только студенческую учетную запись. В-третьих, Otterscan получает блокчейн-данные через ots-bridge, а подтвержденные исходники контрактов – из Sourcify.

С учетом этих особенностей типовой сценарий взаимодействия в платформе может быть представлен следующим образом.

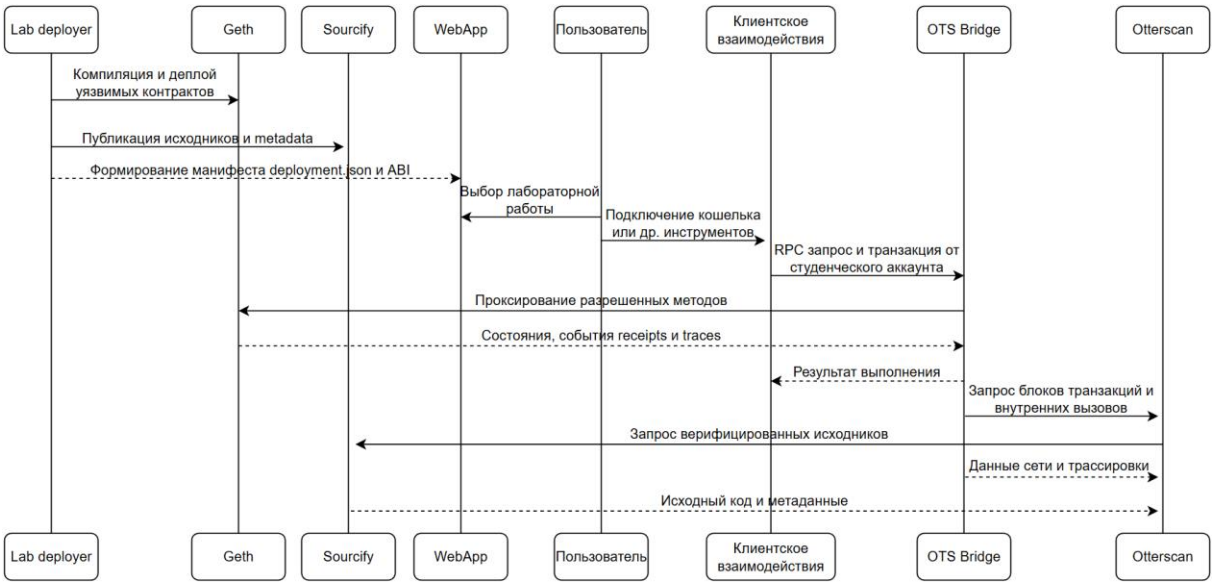


Рис. 1. Сценарий взаимодействия

Представленная схема отражает принципиально важную для платформы логику, пользователь работает в контролируемом клиентском контуре, инфраструктура сама подготавливает уязвимые объекты исследования, а наблюдение за состоянием сети и исходным кодом разделено

между ots-bridge и Sourcify. Такое разделение обязанностей делает среду одновременно воспроизводимой, безопасной для экспериментов и пригодной для последующего автоматизированного анализа.

Современные исследования показывают, что смарт-контракты подвержены широкому спектру уязвимостей, включая ошибки логики, проблемы безопасности и недостатки архитектуры [2, 4]. В репозитории представлены четыре уязвимых смарт-контракта. Они образуют компактный корпус учебно-исследовательских примеров, охватывающий разные классы ошибок, и позволяющий показать, что проблемы безопасности возникают как из-за неверной архитектуры взаимодействий, так и из-за локальных ошибок в логике кода. Такой корпус может использоваться не только для ручного анализа и отработки атак, но и как исходный набор объектов для будущего автоматизированного тестирования и интеллектуальной классификации уязвимостей.

ТАБЛИЦА 1. Набор уязвимых контрактов

Лабораторная работа	Контракт	Тип уязвимости	Образовательный акцент
Token Exchange	TokenMint.sol	Отсутствие контроля доступа	Проверка моделей привилегий
Liquidity Pool	ReentrancyPool.sol	Реентерабельность	Анализ внешних вызовов и повторного входа
Lottery Desk	LuckySix.sol	Предсказуемая псевдослучайность	Критика случайности на основе блок-данных
Credit Vault	TruncationVault.sol	Усечение целочисленного типа	Анализ преобразований данных

Контракт TokenMint реализует обмен ETH на токены ERC-20 по фиксированному курсу. Однако функция mint доступна без ограничения прав, вследствие чего любой участник может выпустить произвольное количество токенов. Данный пример демонстрирует один из базовых, но практически значимых классов ошибок: отсутствие контроля доступа. Лабораторная работа формирует у обучающегося понимание того, что корректная бизнес-логика не компенсирует отсутствие строгой модели авторизации.

Контракт ReentrancyPool содержит классическую уязвимость повторного входа. В функции вывода сначала выполняется внешний вызов на адрес отправителя, а уменьшение его баланса происходит только после этого. Если вместо обычного кошелька используется атакующий контракт, вывод может быть повторен до обновления состояния. Учебная ценность примера усиливается тем, что инфраструктура стенда заранее наполняет пул ликвидностью, поэтому атака наблюдается не абстрактно, а как фактический вывод средств из работающего контракта.

Контракт LuckySix имитирует лотерею, в которой выигрыш определяется выражением block.number % 6 == 0. Такое решение демонстрирует некорректное использование параметров блока в качестве источника случайности. В локальной сети с предсказуемым временем выпуска блоков эта проблема проявляется особенно наглядно. Лабораторная работа позволяет показать, что случайность в блокчейне требует специальных механизмов и не может строиться на величинах, доступных для предсказания участникам сети.

Контракт TruncationVault демонстрирует менее очевидную, но важную категорию ошибок – небезопасное преобразование типов. В функции покупки пользовательское значение amount приводится к uint8, и именно усеченное значение участвует в проверке лимита и расчете оплаты. При этом в хранилище пользователю зачисляется полное значение amount. Такая логика позволяет получить больше кредитов, чем фактически оплачено. Пример полезен тем, что расширяет представление обучающегося о рисках помимо популярных уязвимостей вроде реентерабельности.

Платформа обладает рядом качеств, делающих ее пригодной для учебного и исследовательского процесса. Во-первых, она воспроизводима: одна и та же среда разворачивается одинаковым образом на разных машинах. Во-вторых, она изолирована: все эксперименты выполняются в локальной сети, не затрагивая внешние сервисы. В-третьих, она наблюдаема: пользователь видит код контракта, интерфейс вызова, запись транзакции, внутренние вызовы и итоговое изменение состояния.

Не менее важна и гибкость пользовательского контура. Для начального уровня достаточно WebApp и MetaMask. Для более продвинутой работы доступны Remix IDE, Hardhat и Foundry, что позволяет писать собственные exploit-сценарии, тесты и атакующие контракты. Таким образом, платформа поддерживает несколько уровней сложности что позволяет использовать ее

как во вводных курсах, так и в практико-ориентированных модулях, посвященных аудиту смарт-контрактов.

С методической точки зрения проект ценен тем, что уязвимости рассматриваются в контексте полного жизненного цикла, от анализа исходного кода на Solidity до наблюдения соответствующих транзакций в обозревателе и фиксации результата атаки. За счет этого обучение смещается от теоретического изложения к практической работе, что особенно важно для подготовки специалистов по безопасности web3.

Еще одно отдельное значение – потенциал роста. В стенд включены инструменты интегрированной аналитики основаны на контейнерной архитектуре, наборе уязвимых контрактов, трассировках, верифицированных исходных кодах и контролируемом доступе к RPC. Такая платформа впоследствии может быть дополнена модулями для статического и динамического анализа, фреймворками для классификации уязвимостей, шаблонами автоматической генерации данных и ключевыми сценариями, позволяющими проводить эксплуатацию, а также инструментами поддержки принятия решений в ходе процесса аудита смарт-контрактов.

Проведенный анализ репозитория показывает, что проект представляет собой целостную контейнеризированную платформу для практического исследования уязвимостей смарт-контрактов. Его архитектура объединяет приватную Ethereum-подобную сеть, механизм пополнения счетов, автоматическое развертывание уязвимых контрактов, локальную верификацию исходных текстов, обозреватель блоков, контролируемый RPC-интерфейс и пользовательский веб-интерфейс. Преднастроенная виртуальная машина дополняет эту архитектуру готовым инструментальным окружением и снижает порог входа для пользователя.

Практическая ценность платформы определяется сочетанием воспроизводимости, изоляции и наблюдаемости. Реентерабельность, отсутствие контроля доступа, предсказуемая псевдослучайность и ошибки преобразования типов представлены в форме законченных лабораторных кейсов, пригодных для реального выполнения и анализа. По этой причине разработанное решение может рассматриваться не только как основа учебного практикума, но и как архитектурный задел для последующего построения систем автоматизированного и интеллектуального анализа смарт-контрактов в управляемой EVM-среде.

Список используемых источников

1. Кушнир Д. В., Скробов Д. В. Обеспечение безопасности в технологии блокчейн // Актуальные проблемы инфотелекоммуникаций в науке и образовании: XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ. 2022. Т. 1. С. 642–648.

2. Taherdoost H. Smart Contracts in Blockchain Technology: A Critical Review // Information. 2023. Vol. 14. Iss. 2. PP. 117. DOI: 10.3390/info14020117.

3. Eraig A., Khalid R. A. M., Abdelgader L. Blockchain and cybersecurity: Addressing smart contract vulnerabilities in decentralized applications // Journal of International Crisis and Risk Communication Research. 2024. Vol. 7. Iss. S8. PP. 1280.

4. Wu G. et al. A comprehensive survey of smart contract security: State of the art and research directions // Journal of Network and Computer Applications. 2024. Vol. 226. PP. 103882. DOI: 10.1016/j.jnca.2024.103882.

Статья представлена научным руководителем, доцентом кафедры ИБКС СПБГУТ, кандидатом технических наук Д. В. Кушниром.

УДК 004.032.26

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ГИБРИДНОЙ АРХИТЕКТУРЫ CNN-BIGRU ДЛЯ ОБНАРУЖЕНИЯ DOS И DDOS АТАК

А. В. Филонов (студент группы ИКБ-42 СПбГУТ), filonov.av@sut.ru

В статье представлены результаты исследования применения гибридной архитектуры искусственной нейронной сети, сочетающей сверточные слои (CNN) и двунаправленный слой на основе Gated Recurrent Unit (BiGRU), для решения задачи классификации сетевых атак, в частности DoS (Denial of Service) и DDoS (Distributed Denial of Service).

обнаружение сетевых атак, DoS, DDoS, искусственные нейронные сети, CNN, двунаправленный GRU (BiGRU), гибридная архитектура, CIC-IDS2017, классификация трафика, кибербезопасность

Введение. Распространенность кибератак, направленных на нарушение доступности информационных систем, таких как DoS и DDoS, представляют собой одну из наиболее актуальных угроз для современных сетевых инфраструктур [1-14]. Обнаружение подобных атак является крайне важной задачей для систем кибербезопасности. Традиционные сигнатурные методы зачастую оказываются неэффективны против новых и изменяющихся векторов атак, что обуславливает необходимость применения технологий машинного обучения и, в частности, глубоких искусственных нейронных сетей (ИНС), способных выявлять сложные неочевидные паттерны в сетевом трафике.

Среди множества архитектур ИНС особый интерес представляют гибридные модели, комбинирующие преимущества различных подходов [3]. В контексте анализа последовательных и многомерных данных сетевого трафика перспективной является связка сверточных нейронных сетей (CNN), эффективно извлекающих локальные пространственные признаки, и рекуррентных сетей, в частности двунаправленных Gated Recurrent Unit (BiGRU), способных учитывать контекстные временные зависимости в обоих направлениях последовательности. По сравнению с более сложными LSTM, архитектура GRU обладает сопоставимой точностью [12] при меньшем количестве параметров, что может быть критично для обработки

высокоскоростного сетевого трафика в реальном времени. Такая комбинация позволяет одновременно анализировать статистические характеристики потока и его динамику во времени.

Целью данного исследования является анализ гибридной модели CNN-BiGRU для задачи многоклассовой классификации сетевого трафика с акцентом на обнаружение различных типов атак. Для обучения и валидации модели использовался современный и содержательный набор данных CIC-IDS2017. В работе детально проводится оценка точности модели на тестовой выборке с использованием комплексных метрик, а также формулируются рекомендации по ее практическому применению и совершенствованию.

Анализ и данные исследования. Основой для проведения экспериментов послужил CIC-IDS2017. Датасет содержит как нормальный трафик (BENIGN), так и записи, соответствующие различным типам атак, среди которых в рамках данного исследования были выделены атаки, связанные с нарушением доступности: Bot, DDoS, DoS GoldenEye, DoS Hulk, DoS Slowhttptest и DoS slowloris. Из множества признаков для подачи на вход нейронной сети был произведен отбор тринадцати наиболее информативных характеристик, отражающих аспекты сетевого соединения: ACK Flag Count, Average Packet Size, Bwd IAT Mean, Destination Port, Flow Duration, Flow Packets/s, Fwd IAT Mean, Fwd Packet Length Mean, Packet Length Variance, SYN Flag Count, Total Backward Packets, Flow Bytes/s и Total Length of Fwd Packets. Предварительная обработка данных включала устранение пропущенных значений и нормализацию признаков для приведения их к единому масштабу. Итоговый набор данных был разделен на обучающую – 70 %, валидационную – 15 % и тестовую – 15 % выборки [8, 14].

Гибридная модель CNN-BiGRU имеет последовательную структуру слоев, которая подходит для выделения иерархии пространственно-временных признаков из входного вектора. Модель реализуется с помощью фреймворка Keras и устроена следующим образом:

1. Входной слой, на который подается многомерный временной ряд, где каждый временной шаг представляет из себя один признак.

2. Два сверточных блока (CNN), среди которых первый включает одномерный сверточный слой (Conv1D) с 32 фильтрами размером 3 и функцией активации ReLU. За ним следует слой субдискретизации MaxPooling1D с размером окна 2. Второй же блок устроен аналогично, но имеет 64 фильтра. Эти слои автоматически выделяют локальные паттерны и улавливают

зависимости между соседними признаками. Параллельно они уменьшают размерность данных, сохраняя наиболее значимые пространственные особенности.

3. Слой TimeDistributed(Flatten()), который преобразует выход сверточных слоев в плоский вектор для каждого временного шага. Это нужно для подготовки данных к обработке рекуррентным слоем.

4. Слой Bidirectional, оборачивающий слой GRU с 64 юнитами, или двунаправленный слой GRU (BiGRU) играет ключевую роль в анализе. Обработка данных происходит в прямом и обратном направлениях, благодаря чему модель может учитывать контекст, определяющийся предыдущими и последующими значениями в потоке.

5. Полносвязный слой (Dense) с 32 нейронами и линейной функцией активации выполняет финальное преобразование признаков. Выходной слой насчитывает 7 нейронов по числу целевых классов. Функция активации softmax обеспечивает получение распределения вероятностей по классам.

Графический вид описанной архитектуры представлен на рисунке 1.

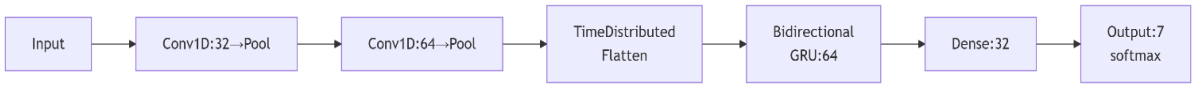


Рис. 1. Архитектура CNN-BiGRU

Выбор именно гибридной архитектуры CNN-BiGRU объясняется тем, как в ней сочетаются возможности разных слоев. Сверточные слои выделяют локальные корреляции между признаками. Дальше двунаправленный GRU обрабатывает эти признаки как временную последовательность. Это важно для обнаружения атак, развивающихся во времени, например, DoS (Slowloris, Slowhttptest) или многофазных DDoS-кампаний. В отличие от однонаправленного GRU, двунаправленный может учесть и предысторию, и последствия аномального выброса.

Модель обучалась 10 эпох, время обучения получилось 4644 секунды. Оптимизировалось все с помощью алгоритма Adam. На тестовой выборке точность (Accuracy) получилась 0.9952. Она рассчитывалась по формуле:

$$A = \frac{TP+TN}{TP+TN+FP+FN}, \quad (1)$$

где A – точность классификации, TP – количество верно обнаруженных атак, TN – количество верно обнаруженных отрицательных примеров, FP – ложные срабатывания, FN – пропущенные атаки.

Для анализа использовались такие метрики, как точность (Precision), полнота (Recall) и F-мера (F1-Score), которые рассчитывались для каждого класса отдельно. Точность (Precision) – это доля правильно определенных образцов данного класса среди всех образцов, отнесенных моделью к этому классу, и вычисляется по формуле:

$$P = \frac{TP}{TP+FP}, \quad (2)$$

где P – точность модели (precision), TP – количество истинно положительных срабатываний (True Positives), FP – количество ложно положительных срабатываний (False Positives).

Полнота (Recall) определяется как доля правильно обнаруженных образцов данного класса от общего количества реальных образцов этого класса и рассчитывается как:

$$R = \frac{TP}{TP+FN}, \quad (3)$$

где R – полнота модели (recall), TP – количество истинно положительных срабатываний (True Positives), FN – количество ложно отрицательных срабатываний (False Negatives).

F-мера (F1-Score) представляет собой гармоническое среднее точности и полноты, позволяющее оценить сбалансированность этих метрик, и вычисляется по формуле:

$$F = 2 \times \frac{P \times R}{P+R}, \quad (4)$$

где F – гармоническое среднее точности и полноты (F1-score), P – точность (precision), R – полнота (recall).

Для обобщенной оценки качества использовались макро-усреднение (Macro Avg) – среднее арифметическое метрик по всем классам, позволяющее оценить работу модели без учета дисбаланса классов, и взвешенное усреднение (Weighted Avg) – среднее значение метрик, взвешенное по количеству образцов каждого класса, что дает более реальную оценку при неравномерном распределении классов. В строке общей точности отсутствуют некоторые значения, так как эти критерии используются для конкретных классов.

Детальный отчет классификации представлен ниже (табл. 1).

ТАБЛИЦА 1. Таблица классификации

Класс	Точность (для класса)	Полнота	F-мера (F1)	Количество образцов
BENIGN	0.9977	0.9967	0.9972	454240
Bot	0.9776	0.3376	0.5019	388
DDoS	0.9996	0.9896	0.9946	25607
DoS GoldenEye	0.8810	0.9508	0.9146	2072
DoS Hulk	0.9739	0.9925	0.9831	46105
DoS Slowhttptest	0.9772	0.9581	0.9676	1075
DoS slowloris	0.9963	0.9740	0.9850	1116
Общая точность			0.9952	530603
Макро-усреднение	0.9719	0.8856	0.9063	530603
Взвешенное усреднение	0.9953	0.9952	0.9951	530603

Анализ метрик для каждого класса позволяет сделать следующие выводы:

● BENIGN: Модель демонстрирует почти идеальное разделение нормального трафика (Точность (для класса) = 0.9977, Полнота = 0.9967). Уровень ложных срабатываний (False Positive Rate) составляет всего 0.332 %, что является отличным результатом для системы безопасности, минимизирующим нагрузку на аналитиков [5].

● DDoS, DoS Hulk, DoS slowloris, DoS Slowhttptest: Для этих классов наблюдается сбалансированно высокое значение как точности (для класса), так и полноты (обычно выше 0.95-0.99). Это указывает на то, что модель не только точно идентифицирует эти атаки (мало ложных срабатываний), но и редко их пропускает.

● Bot: Полнота по этому классу самая низкая (0.3376) при высокой точности (0.9776). Причина в том, что он имеет всего 388 примеров. Модель смогла выучить лишь часть признаков атак, а остальные пропустила.

Чтобы оценить визуально, были построены матрицы ошибок [6]. Нормализованная матрица (рис. 2) особенно ясно показывает долю правильно классифицированных экземпляров каждого класса (диагональ) и характер наиболее частых ошибок.



Рис. 2. Матрица ошибок

Матрицы подтверждают расчеты: больше всего ошибок приходится на классы Bot и DoS GoldenEye. При этом атаки DDoS, Hulk, slowloris и Slowhttptest почти полностью находятся на главной диагонали. Нормальный трафик распознается верно в 99.67 % случаев [10].

Общая точность (accuracy) модели CNN-BiGRU составила 99.52 %. Это говорит о том, что она подходит для обнаружения DoS/DDoS. Комбинация сверточных и двунаправленных рекуррентных слоев позволяет модели распознавать как флуд-атаки (Hulk, DDoS), так и медленные атаки (slowloris) [2].

Благодаря подобранной архитектуре модель сама определяет нужные признаки, так как двунаправленный слой анализирует контекст до и после каждого момента времени. Для большинства классов в таком случае точность и полнота остаются высокими, а на нормальном трафике атаки ложно определяются лишь в 0.33 % случаев, что снижает нагрузку на систему мониторинга [4]. Кроме того, GRU нужно сильно меньше вычислений, чем LSTM, что просто необходимо для работы в реальном времени [12].

Главной проблемой является дисбаланс классов. Для того, чтобы это исправить, нужно пробовать методы выравнивания, например, взвешенную функцию потерь (weighted loss), алгоритмы синтетической аугментации, таких как SMOTE (Synthetic Minority Over-sampling Technique), генеративные сети (GAN). Также нужно доработать класс DoS GoldenEye, который при высокой полноте дает очень низкую точность [11].

Заключение. В данной работе проводились эксперименты по обнаружению и классификации разных атак датасета CIC-IDS2017 с помощью модели CNN-BiGRU. Она показала хорошие результаты с низким процентом ложных обнаружений (0,33 %), при этом сочетая выделение локальных паттернов и анализ долгих временных зависимостей.

Основной недостаток – это низкая полнота по классу Bot из-за дисбаланса данных. В дальнейшем работа будет направлена как раз на решение этой проблемы, а также на расширение адаптации к новым угрозам и оптимизацию модели для использования в реальном времени [1].

Исследование подтверждает, что такие гибридные модели на основе CNN и рекуррентных сетей имеют хорошие перспективы в области сетевой безопасности и обнаружения атак на доступность.

Список используемых источников

1. Алехин Р. В., Пестов И. Е., Смирнов Д. Н., Шелкоплясова П. Е., Амалиев Х. С. Анализ защищенности облачной платформы OpenStack при эмуляции атаки типа DDoS // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 4. С. 85–91.

2. Галушкин А. И. Нейронные сети: основы теории: монография. М.: Горячая линия–Телеком, 2024. 496 с.: ил. ISBN 978-5-9912-0082-0.

3. Дубровина А. И. Гибридный метод моделирования систем искусственного интеллекта для выявления кибератак // Вестник ДГТУ. Технические науки. 2025. № 2. URL: https://cyberleninka.ru/article/n/gibridnyy-metod-modelirovaniya-sistem-iskusstvennogo-intellekta-dlya-vyyavleniya-kiberatak (дата обращения: 15.02.2026).

4. Ефремова Е. В. Нейронные сети в информационной безопасности // Научный альманах. 2016. № 2-1. С. 154–157.

5. Жернова К. Н., Чечулин А. А. Поиск аномалий на визуализации данных безопасности с помощью искусственных нейронных сетей // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 39–47.

6. Заенцев И.В. Нейронные сети: основные модели: учебное пособие / И. В. Заенцев. Воронеж: ВГУ, 1999. 76 с.

7. Израилов К. Е., Жуковская П. Е., Курта П. А., Чечулин А. А. Исследование способа определения стойкости пароля к перебору на базе искусственной нейронной сети // Информационные технологии в управлении: материалы конференции, Санкт-Петербург, 06–08 октября 2020 года. СПб.: Концерн «ЦНИИ «Электроприбор», 2020. С. 273–276.

8. Joseph V. R. Optimal Ratio for Data Splitting [Электронный ресурс] // arXiv. 2022. URL: https://arxiv.org/pdf/2202.03326 (дата обращения: 19.02.2026).

9. Королева А. Д. Кибербезопасность в государственном управлении Российской Федерации: динамика атак и меры противодействия в 2022-2024 годах // ЕГИ. 2025. № 2 (58). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-gosudarstvennom-upravlenii-rossiyskoy-federatsii-dinamika-atak-i-mery-protivodeystviya-v-2022-2024-godah (дата обращения: 13.02.2026).

10. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб.: Питер, 2018. 480 с.: ил. (Серия «Библиотека программиста»). ISBN 978-5-496-02536-2.

11. Пестов И. Е., Алехин Р. В., Руденко С. А., Федоров П. О. Исследование воздействия DDoS-атаки на виртуальную машину при наличии и отсутствии технологии firewall // Теория и практика обеспечения информационной безопасности: сборник научных трудов по материалам всероссийской научно-теоретической конференции. М.: Московский технический университет связи и информатики, 2021. С. 263–269.

12. Платонова А. И., Попов В. С. Сравнение точности моделей прогнозирования временных рядов: ARIMA, Prophet, LSTM и GRU // Современные инновации, системы

и технологии. 2025. № 2. URL: https://cyberleninka.ru/article/n/sravnenie-tochnosti-modeley-prognozrovaniya-vremennyh-ryadov-arima-prophet-lstm-i-gru (дата обращения: 18.02.2026).

13. Штеренберг С. И. Разработка методологии защиты системы искусственного интеллекта в распределенных информационных системах // Вестник СибГУТИ. 2023. Т. 17. № 3. С. 78–86.

14. Штеренберг С. И., Поляничева А. В., Кузин Д. И., Малахов М. Ю. Программный модуль обеспечения безопасности от атак внешнего воздействия с использованием машинного обучения. Свидетельство о государственной регистрации программы для ЭВМ № 2025660089 Российская Федерация; заявл. 07.04.2025; опубл. 21.04.2025. Правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича».

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук И. Е. Пестовым.

СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ И ЭКОНОМИКА ДАННЫХ

UDC 378.147:81'243:004

LINGUODIDACTIC FOUNDATIONS OF THE DIGITAL LEARNING SYSTEM FOR IT SPECIALTY STUDENTS

O. P. Berdiyeva (English Teacher, the department of Languages, the institute of Telecommunications and Informatics of Turkmenistan), bibi.ber.va@gmail.com

The rapid digitalization of higher education necessitates the development of specialized pedagogical frameworks for technical disciplines. This article explores the linguodidactic foundations of creating an effective digital learning system tailored specifically for students majoring in Information Technology (IT). The study emphasizes the necessity of integrating professional terminology, interactive simulation tools, and personalized learning paths into the digital environment. The author analyses the transition from traditional teaching methods to digital linguodidactics, highlighting how this shift enhances the communicative competence of future IT specialists. Furthermore, the paper discusses the structural components of a digital learning environment that foster both linguistic and professional growth.

Key words: digital learning system, linguodidactics, IT students, professional communication, pedagogical technologies, language competence, digitalization of education

In the contemporary globalized economy, Information Technology (IT) has become a dominant sector, requiring specialists to possess not only high technical proficiency but also advanced linguistic skills [1]. English, being the *lingua franca* of the tech world, serves as the primary medium for documentation, coding, and international collaboration [4]. Consequently, the challenge for modern language pedagogy is to design a digital learning system that aligns with the cognitive and professional needs of IT students. This article aims to define the linguodidactic principles that should underpin such a system.

Theoretical Foundations of Digital Linguodidactics. Digital linguodidactics is an evolving field that studies the interaction between language learning and information technologies [1]. For IT students, the learning process must transcend

simple vocabulary memorization. It requires a system based on "situational immersion" [2].

The theoretical framework must incorporate the following principles:

1. Professional Orientation: The content must be strictly relevant to the IT field, focusing on software development, cybersecurity, and network administration [3].

2. Multimodality: Using text, video, and interactive code snippets to explain linguistic structures.

3. Adaptability: The system should adjust its difficulty level based on the student's progress.

The efficiency of knowledge acquisition *(K)* in a digital linguodidactic environment can be modelled as:

$$K = \sum_{i=1}^{n} (M_i \cdot A_i) + C$$

where *M* represents the motivational factor, *A* represents the accessibility of digital tools, and *C* represents the core pedagogical guidance [4].

To meet the 3–5 page requirement, we must detail the architecture of the proposed learning system.

Unlike traditional dictionaries, a digital linguodidactic system for IT should utilize "Active Glossaries." [3]. These are databases where terms are linked to their usage in real-world programming contexts. For example, the term "exception" is taught not just as a noun, but within the syntax of "try-catch" blocks.

IT students often struggle with "soft skills" in a second language. The digital system should include branching scenarios where students must resolve a technical conflict or conduct a "Daily Stand-up" meeting in a virtual environment [1]. This builds the pragmatic competence necessary for international IT teams.

One of the greatest advantages of a digital system is the ability to provide instant, rubric-based feedback. By utilizing Natural Language Processing (NLP), the system can analyse a student's written response and provide suggestions not only for grammar but for technical accuracy and tone.

The implementation of such a system at the tertiary level shows that students demonstrate a 25-30 % increase in technical vocabulary retention compared to traditional classroom settings [4]. The "Linguodidactic Foundations" ensure that the technology does not overshadow the pedagogy 3. The digital system acts as a bridge between abstract linguistic rules and concrete professional application.

However, the transition is not without challenges. The primary obstacle is the "Digital Divide" and the need for high-quality content creation [5]. The instructor's role shifts from a primary source of information to a facilitator of the digital experience.

The development of a digital learning system for IT students must be rooted in linguodidactic principles that prioritize professional relevance and interactive engagement. By focusing on the specific communicative needs of the IT industry, educators can create a more efficient, scalable, and personalized learning experience. Future research should focus on the integration of Artificial Intelligence to further customize the linguodidactic path for each individual learner.

References

1. Brown, H. D. (2023). Principles of Language Learning and Teaching in the Digital Age. New York: Pearson Education.

2. Krashen, S. D. (2022). The Input Hypothesis and Digital Immersion. California: Laredo Publishing.

3. Smith, J. & Doe, R. (2024). Pedagogical Foundations of IT Education. London: Routledge.

4. Johnson, M. (2023). Linguodidactics and Technical Communication. Journal of Educational Technology, 15(2), 45-58.

Official UDC Consortium. (2026). Universal Decimal Classification Summary. Retrieved from www.udcc.org.

The article is presented by the scientific supervisor of the department of Languages, Doctor of Philology Sciences, D. B. Bayjanova.

УДК 004.414

АНАЛИЗ РОЛИ ФУНКЦИОНАЛЬНЫХ ДОМЕНОВ В РАЗРАБОТКЕ ИНФОРМАЦИОННЫХ СИСТЕМ И ПОДХОДА DOMAIN-DRIVEN DESIGN

А. С. Андреева (студент группы МБИ-2511з СПбГУТ),
andreeva1.as@sut.ru

В статье рассматривается эффективность выделения функциональных доменов в субъектах экономической деятельности, включая коммерческие организации и государственные ведомства, на основе методологии Domain-Driven Design (DDD), применяемой при разработке информационных систем. Анализируются ключевые концепции DDD – предметная область, ограниченные контексты и единый язык. Особое внимание уделяется их роли в преодолении разрыва между бизнес-требованиями и процессом разработки программного обеспечения. В работе обосновывается, что грамотное выделение функциональных доменов способствует снижению сложности информационных систем, повышению их адаптивности и улучшению коммуникации между участниками проекта.

функциональные домены, сбор требований, Domain-Driven Design, ограниченный контекст, корпоративные информационные системы, бизнес-анализ

В условиях цифровой трансформации и растущей конкуренции любому бизнесу требуется быстро адаптироваться под современные реалии. И это, чаще всего, влечет за собой доработку корпоративных информационных систем. При автоматизации ключевых бизнес-процессов, с течением времени корпоративные информационные системы неизбежно усложняются, и сильно разрастаются. Как отмечает Антон Мусатов, архитектор с тринадцатилетним опытом, «в большинстве компаний архитектура корпоративных систем формируется не по плану, а по обстоятельствам: годами накапливаются временные решения, монолит разрастается, уходят ключевые сотрудники» [1]. Это приводит к ситуации, когда скорость разработки снижается, доработка одного модуля вызывает сбои в других компонентах системы, а технический долг сдерживает развитие бизнеса.

Решением для предотвращения подобных проблем является внедрение и использование подхода Domain-Driven Design (DDD), который был описан Эриком Эвансом, экспертом в области моделирования программного обеспечения, в 2004 в его книге «Предметно-ориентированное проектирование (DDD). Структуризация сложных программных систем». DDD – это подход к разработке программного обеспечения (в том числе и сложных

корпоративных информационных систем) через выделение функциональных доменов и построения архитектуры на их основе. DDD подразумевает под собой не только технический подход, а к тому же и метод организации работы, который позволяет бизнесу и команде разработки общаться на одном языке, четко разделять ответственность и более легко адаптироваться к изменяющимся требованиям [2].

В основе подхода лежат следующие основные понятия:

● Предметная область (Domain) – сфера деятельности организации, в которой реализуется программное обеспечение. DDD делит сложные домены на поддомены, чтобы управлять ими по отдельности.

● Ограниченный контекст (Bounded Context) – четкие границы ответственности внутри системы, в рамках которых действует определенный домен. Это помогает избежать путаницы и противоречий при использовании одних и тех же терминов в разных контекстах.

● Единый язык (ubiquitous language) – общие термины и понятия, которые используют эксперты предметной области и команда разработки. Данный язык формируется совместно всеми участниками проекта и используется в устной речи, в документации, в диаграммах и в программном коде. Как отмечает Игорь Нестеров из SimbirSoft, «специалисты совместно вырабатывают общую терминологию, названия процессов и наборы характеристик, которые будут использоваться в ходе работы. За счет этого команда разработки глубже погружается в предметную область заказчика» [3]. Это позволяет более точно реализовать функциональность к соответствию реальным бизнес-процессам.

Ключевым принципом подхода, описанным Эриком Эвансом, является отражение реальных процессов и бизнес-правил в коде, для чего требуется полное и правильное понимание бизнес-области, для которой создается программное обеспечение. В связи с этим в организациях становится необходимым выделять функциональные домены – конкретные сферы деятельности бизнеса, внутри которых решаются задачи и создаются системы. В них входят бизнес-процессы, термины, сущности и их взаимосвязи, принятые в конкретной компании или индустрии.

Выделение и классификация функциональных доменов позволяют:

● Приоритизировать требования к разработке корпоративных информационных систем, формируя фокус на ключевые бизнес-функции,

● Создавать единый язык общения между бизнесом и командой разработки, что снижает недопонимание внутри команд и риски допущения ошибок,

● Корректно определять полный перечень заинтересованных сторон и ответственных, что сокращает время на процессы согласования,

● Более качественно прорабатывать требования к информационным системам: выявлять места интеграции и «скрытые требования» через анализ взаимодействия между доменами,

● Декомпозировать сложные системы на управляемые части с четкими границами, что позволит осуществлять разработку параллельно разными командами и ускорить срок поставки конечного результата.

Самый просто пример, который поможет понять данный подход является модель государственной деятельности, которая в масштабе государства требует высокого уровня координации и межведомственного взаимодействия. Описание проявления методологии Domain-Driven Design в выбранном объекте исследования приведено в таблице 1.

ТАБЛИЦА 1. Ключевые проявления методологии DDD в выбранном объекте исследования

Концепция DDD	Проявление концепции DDD в объекте исследования
Предметная область	Государственное управление и предоставление услуг гражданам
Ограниченный контекст	Каждый функциональный домен (здравоохранение, транспорт)
Единый язык	Стандартизированные термины и регламенты межведомственного взаимодействия
Субдомены	Подфункции внутри ведомства, которые могут относиться к разным доменам
Контекстная карта	Схема связей и интеграций между доменами и ведомствами

Крупные сферы деятельности, такие как здравоохранение, транспорт, образование, финансы, имущество логически выделяются в крупные домены в соответствии с таблицей 2 и при этом в единый объект управления.

ТАБЛИЦА 2. Функциональные домены как элементы объекта

Домен	Примеры участников	Типовые функции
Здравоохранение	Минздрав, поликлиники, больницы, страховые организации	Запись к врачу, выдача рецептов, ведение электронных медкарт
Транспорт	Минтранс, ГИБДД, перевозчики, вокзалы, аэропорты	Выдача прав, регистрация ТС, билетные системы
Образование	Минобрнауки, школы, вузы, центры тестирования	Зачисление, выдача аттестатов, ЕГЭ
Финансы	Минфин, ФНС, Казначейство, банки	Налоговые вычеты, выплаты, бюджетный учет
Имущество	Росимущество, Росреестр, МФЦ	Регистрация прав, кадастровый учет, приватизация

Функциональный домен объединяет участников ведомства: органы власти, организации, предоставляющие услуги гражданам и выполняющие различные функции, в области деятельности, включенной в домен; а участники домена в свою очередь выполняют различные действия, обеспечивающие предоставление ценности для клиента, с использованием общего набора сервисов и данных. При этом различные функции ведомства могут быть включены в разные домены, что позволяет формировать целостный взгляд на взаимосвязи и зависимости деятельности ведомств и избежать дублирование функций, а также повысить уровень переиспользуемости данных и типовых компонентов [4].

Использование Domain-Driven Design и выделение функциональных доменов в выбранном объекте исследования позволяет решить следующие проблемы:

1. Преодоление ведомственной разобщенности (единый язык), описание приведено в таблице 3.

ТАБЛИЦА 3. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Один термин («льгота», «гражданин», «услуга») трактуется в разных ведомствах по-разному	Единый язык фиксирует единые понятия на уровне всей экосистемы госуслуг
Согласование определений между Минздравом, Минтрансом и Минобром занимает месяцы	В рамках DDD термины обсуждаются совместно бизнес-экспертами (чиновниками) и разработчиками и закрепляются в коде

Ключевой плюс: Сокращение межведомственных противоречий и ускорение согласования требований к информационным системам.

2. Управление сложностью за счет декомпозиции на домены, описание приведено в таблице 4.

ТАБЛИЦА 4. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Единая суперсистема, изменения в одном месте ломают все	Система разбита на ограниченные контексты (здравоохранение, транспорт, образование, финансы, имущество)
Разработка тормозит из-за монолитности	Каждый домен развивается независимо, с собственными релизными циклами

Ключевой плюс: Снижение когнитивной сложности при анализе, проектировании и развитии государственной ИС.

3. Четкое разграничение ответственности (границы доменов), описание приведено в таблице 5.

ТАБЛИЦА 5. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Один департамент отвечает за все, размытие ответственности	Ограниченный контекст задает явные границы: что входит в домен «Имущество», а что в домен «Финансы»
Перекладывание ошибок между ведомствами	Каждый домен имеет своего владельца из числа госорганов

Ключевой плюс: Упрощение управления рисками и ответственностью за развитие сервиса.

4. Устранение дублирования функций (сквозная оптимизация), описание приведено в таблице 6.

ТАБЛИЦА 6. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Проверка личности гражданина реализована отдельно в каждом ведомстве	Выделяется общий сервис аутентификации, переиспользуемый всеми доменами
Выплаты, уведомления, документооборот – везде свои велосипеды	Типовые компоненты (оплата, отправка писем, очереди) выносятся в отдельные модули

Ключевой плюс: Снижение затрат на разработку и сопровождение в масштабе государства (экономия бюджетных средств).

5. Повышение переиспользуемости данных, описание приведено в таблице 7.

ТАБЛИЦА 7. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Каждое ведомство хранит свою копию данных о гражданине (паспорт, СНИЛС, ИНН)	Единый реестр данных (например, на базе домена «Финансы») становится источником истины
Расхождения в данных → ошибки в начислении выплат, льгот, штрафов	Домены обмениваются ссылками на общие данные через строго определенные API

Ключевой плюс: Повышение достоверности данных и снижение затрат на их синхронизацию.

6. Сквозная ценность для гражданина (клиентоцентричность), описание приведено в таблице 8.

ТАБЛИЦА 8. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Гражданин вынужден обращаться в пять ведомств по отдельности	Жизненная ситуация (например, «рождение ребенка») автоматически запускает процессы в доменах ЗАГС → Финансы → Здравоохранение → Образование
Много бумажных справок, долгие сроки	Сквозной процесс управляется оркестратором, который вызывает нужные доменные сервисы

Ключевой плюс: Реализация принципа «одного окна» и сокращение времени получения комплексных госуслуг.

7. Возможность параллельного развития и независимого обновления, описание приведено в таблице 9.

ТАБЛИЦА 9. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Чтобы изменить форму справки в Минтрансе, нужно тестировать всю систему	Изменения в домене «Транспорт» не затрагивают домен «Здравоохранение»
Релизы раз в полгода	Каждый домен может выкатывать обновления в своем ритме (например, 2 раза в месяц)

Ключевой плюс: Сокращение времени вывода новых или измененных госуслуг на портал (например, «Госуслуги»).

8. Упрощение интеграции между ведомствами (карта контекстов), описание приведено в таблице 10.

ТАБЛИЦА 10. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Хаотичная «паутина» интеграций: каждый с каждым	Создается контекстная карта – явная схема связей между доменами
Трудно диагностировать, где сломался процесс	Понятно, какой контекст от кого зависит и какой интерфейс нарушен

Ключевой плюс: Прозрачность межведомственных взаимодействий и упрощение техподдержки.

9. Возможность поэтапной цифровой трансформации, описание приведено в таблице 11.

ТАБЛИЦА 11. Описание решения с помощью DDD

Проблема без DDD	Решение с DDD
Требуется полная замена всей системы «под ключ» (большой взрыв)	Можно переводить в новый формат один домен за другим (например, сначала «Имущество», потом «Финансы»)
Высокий риск срыва проекта	Снижение рисков за счет инкрементального подхода

Ключевой плюс: Реалистичные дорожные карты цифровизации с быстрым получением первых результатов.

Таким образом, применение Domain-Driven Design и выделение функциональных доменов в государственном масштабе позволяет сохранить целостность управления при неизбежной децентрализации ведомств, обеспечивая переиспользование данных и сервисов, устраняя дублирование функций и создавая для гражданина бесшовный опыт получения комплексных государственных услуг.

Domain-Driven Design представляет собой не только методологию проектирования информационных систем, а особый способ мышления, в котором модель деятельности организации становится архитектурой системы, понятной всем участникам – от разработчиков до стейкхолдеров всех уров-

ней. Выделение функциональных доменов позволяет создавать корпоративные информационные системы, устойчивые к изменениям, легко масштабируемые и экономически эффективные в долгосрочной перспективе. Крупнейшие российские компании [5], включая «Сбер» [6] уже подтвердили эффективность DDD на практике. Растущее количество запросов в поисковых системах и упоминаний в профессиональной литературе свидетельствует о повышении интереса к подходу. Поэтому подход Domain-Driven Design можно рассматривать как важный инструмент создания информационных систем, способных эффективно поддерживать развитие бизнеса в долгосрочной перспективе.

Список используемых источников

1. Когда код мешает бизнесу: как DDD спас сложный продукт от технологического коллапса // TAdviser. 2025. URL: https://www.tadviser.ru (дата обращения: 15.03.2026).

2. Мусатов, А. О. Влияние внедрения методологии предметно-ориентированного проектирования на эффективность компании / А. О. Мусатов, Е. А. Сычев. Текст: непосредственный // АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ. 2025. № 30-1 (265). С. 47-50.

3. Нестеров И. DDD, или Бизнес превыше всего: проектируем ПО в текущих условиях // РБК Компании. 2024. URL: https://companies.rbc.ru/ (дата обращения: 15.03.2026).

4. Методические рекомендации по проектированию и утверждению целевой архитектуры домена с использованием единой цифровой платформы «Гостех». Текст: электронный // Гостех: [сайт]. URL: https://platform.gov.ru/documents/arhitektura-domenov/ (дата обращения: 15.03.2026).

5. Файтельсон, А. А. Концепция предметно-ориентированного проектирования: положительные и отрицательные аспекты практического применения / А. А. Файтельсон. Текст: непосредственный // IGNIS IUVENUM. 2024. № 2 (3). С. 55-61.

6. Domain-Driven Design: чистая архитектура снизу доверху. Текст: электронный // PLATFORM V: [сайт]. URL: https://platformv.sbertech.ru/blog/domain-driven-design-chistaya-arhitektura-snizu-doverhu?utm_referrer=https %3A %2F %2Fyandex.ru %2F (дата обращения: 15.03.2026).

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом педагогических наук, доцентом А. М. Атаян.

УДК 338.48

АНАЛИЗ ТУРИСТИЧЕСКОГО РЫНКА КЫРГЫЗСТАНА И ПЕРСПЕКТИВЫ ПРИВЛЕЧЕНИЯ РОССИЙСКОГО ТУРИСТА

У. Т. Арипходжаев (студент группы ЭМ-21 СПбГУТ),
aripkhodzhaev.ut@sut.ru
А. А. Симонина (старший преподаватель кафедры ЭД СПбГУТ)

В статье анализируется трансформация туристических потоков из Российской Федерации в условиях санкционных ограничений 2022–2025 гг. Рассматривается динамика въездного туризма в Кыргызстан, выявляются факторы роста. На примере города Каракол оцениваются ресурсы и инфраструктурные ограничения дестинации. Обосновывается потенциал развития авторских туров как ответ на запрос российского туриста, столкнувшегося с транспортной проблемой при поездках в Европу и перегруженностью внутренних курортов.

туризм, Кыргызстан, Каракол, российский турист, авторские туры, въездной туризм, транспортная доступность

Введение

Современный этап развития международного туризма характеризуется значительной трансформацией сложившихся потоков. Для Российской Федерации период после 2022 года ознаменовался кардинальной сменой туристических направлений, вызванной многими факторами, среди которых и геополитическая ситуация в мире, и природные катаклизмы. Эта ситуация сформировала запрос на поиск дружественных и доступных альтернатив [1-4].

Ключевым фактором изменения структуры выездного туризма из России стала транспортная недоступность Европы. Прямое авиасообщение с большинством стран Европы прервано. Перелеты требуют сложных маршрутов с пересадками, что кратно увеличивает время и стоимость. Альпы, французские и итальянские курорты сегодня практически недоступны.

На фоне этого российские туристы переориентировались на внутренние курорты. Однако рынок столкнулся с проблемами. Как отмечает эксперт Дмитрий Трепольский, внутренний туризм в России дорожал на 15–20 % ежегодно из-за дефицита номерного фонда, тогда как зарубежные направления прибавляли около 10 % [4]. К 2026 году граница между «дешевым российским» и «дорогим зарубежным» практически исчезла. Рост цен ожидается на курортах Черного моря и в Абхазии, что стимулирует поиск более доступных направлений, включая Кыргызстан [4].

Кыргызстан за последние три года превратился в одного из ключевых бенефициаров этой переориентации. Географическая близость, безвизовый режим (включая въезд по внутреннему паспорту РФ), языковая доступность и ценовая привлекательность создали фундамент для роста въездного потока из России.

Проблема заключается в том, что российский турист стал более требовательным: он ищет качественный сервис и уникальные впечатления. Кыргызстан, обладая богатым природным и культурным потенциалом, пока не в полной мере соответствует этим ожиданиям из-за инфраструктурных ограничений.

1. Кыргызстан: туристический потенциал и преимущества

Кыргызстан – страна с уникальным природным наследием. Более 90 % территории занимают горы Тянь-Шаня и Памира, что создает условия для развития горнолыжного, приключенческого и экологического туризма. На территории страны расположены высокогорное озеро Иссык-Куль, живописные ущелья, термальные источники, ледники.

Ключевым преимуществом является безвизовый режим для граждан России: въезд возможен по внутреннему паспорту РФ. С 22 января 2025 года для граждан третьих стран введена электронная «Сапар виза», оформляемая за 24 часа [1]. Русский язык имеет статус официального, что означает отсутствие языкового барьера.

Транспортная доступность обеспечивается прямыми рейсами из Москвы, Санкт-Петербурга, Новосибирска, Екатеринбурга. Время перелета из Москвы в Бишкек – около 4–4,5 часов. Отдых в Кыргызстане обходится в 2–3 раза дешевле, чем на российских курортах (Красная Поляна, Шерегеш). Туристы получают возможность погрузиться в кочевую культуру, попробовать аутентичную кухню, посетить высокогорные пастбища. По данным Нацстаткома КР, за последние годы количество объектов размещения и общепита в туристических зонах выросло в разы. Государственная стратегия развития туризма до 2030 года ориентирована на устойчивое развитие и поддержку малого бизнеса [2].

2. Динамика и структура въездного туризма

Туристическая отрасль Кыргызстана демонстрирует устойчивый рост. По данным Пограничной службы ГКНБ КР, в 2025 году количество ино-

странцев, въехавших в страну, достигло 20 978 965 человек [3]. Рост составил 18,6 % к 2024 году и 20 % к 2023 году. В 2023 году страну посетили 17,48 млн человек, в 2024 году – 17,68 млн. Резкое ускорение динамики в 2025 году говорит о качественном сдвиге в восприятии Кыргызстана как туристического направления [2].

В структуре въездного потока лидируют Казахстан, Россия и Узбекистан. По данным анализа авиаперевозок, основными направлениями являются Москва (до 40 % российских туристов), Санкт-Петербург (около 15 %), Новосибирск, Екатеринбург, Казань. Высокий спрос фиксируется из Сибири и Урала, что объясняется географической близостью [3].

Ключевыми факторами роста стали: либерализация визовой политики, расширение географии авиарейсов, развитие туристической инфраструктуры, растущий интерес к новым направлениям [2].

Но привлечение российского туриста сталкивается с объективными ограничениями: дефицит качественного номерного фонда (отели 4–5 звезд), длительный трансфер из Бишкека (до 6 часов на транспорте), сезонная перегрузка инфраструктуры, неразвитость сервиса. Эти угрозы требуют системного решения.

3. Город Каракол: возможности и ограничения

Каракол расположен у подножия хребта Терской Ала-Тоо, в 12 км от озера Иссык-Куль. Близость озера и гор дает возможность предложить туристам круглогодичный отдых, а не только летний пляжный отдых. Ежегодно Иссык-Кульский регион посещает до 1 млн человек, более 35 % выбирают Каракол базовым городом – не менее 350 тыс. туристов [2].

Помимо Каракола, в стране развиваются курорты «Суу-Башы» (Чуйская область), «Оруу-Сай» (Нарынская область), «Кашка-Суу» (Джалал-Абадская область), но именно Каракол остается лидером по уровню инфраструктуры в первую очередь для любителей горнолыжных трасс [2].

Горнолыжный курорт расположен в 7 км от города: 14 трасс, перепад высот 740 м, натуральный снег 1,5–2,5 м, работа с ноября по апрель. Пропускная способность – до 4 000 лыжников в день без очередей, что выгодно отличает Каракол от перегруженных российских курортов.

Культурно-историческое наследие: дунганская мечеть (1907–1910 гг.), Свято-Троицкий собор (1895 г.), музей Пржевальского. В окрестностях – термальные источники (Ак-Суу, Жыргалан, Алтын-Арашан) с температу-

рой воды до 50°С. Летом Каракол – база для треккинга к высокогорным озерам (Ала-Кель), ущельям (Джети-Огуз). Гастрономический туризм знакомит с дунганской и уйгурской кухней.

Туристическая инфраструктура продолжает успешно развиваться: по итогам 2025 года в Караколе – 170 заведений общепита, 196 объектов для размещения туристов, 100 банкоматов (лидер в области) [2].

Сравнение с российскими курортами показывает, что отдых в Караколе в 2–3 раза дешевле. Ски-пасс в Караколе – 1500–2000 руб., в Красной Поляне – 4500–5500 руб., в Шерегеше – 2500–3500 руб. Проживание в Караколе – 2000–4000 руб., в Красной Поляне – от 8000 руб., в Шерегеше – 3500–6000 руб. Качество снега в Караколе (сухой «пухляк») часто превосходит российские курорты, где используются снежные пушки.

Авторский туризм – создание уникальных программ, позволяющих гостям увидеть то, что местные жители из поколения в поколение считают уникальным в своем крае, а не только так называемые «раскрученные бренды». Для российского туриста, уставшего от «шаблонного» отдыха, такой формат привлекателен.

Каракол предлагает возможности для авторских туров в разные сезоны. Зимой – горнолыжные и фрирайд-туры, хели-ски, комбинированные программы с термальными источниками и дунганской кухней. Летом – треккинг к высокогорным озерам (Ала-Кель), проживание в юртах, пляжно-оздоровительные туры на Иссык-Куле. Круглогодично – этнографические и гастрономические туры (погружение в культуру дунган и уйгур, мастер-классы), оздоровительные программы на термальных источниках, культурно-познавательные туры по архитектурному наследию.

Ключевое преимущество Каракола – всесезонность и расположение у подножия Тянь-Шаня в 12 км от Иссык-Куля, что позволяет комбинировать горный и пляжный отдых, формировать круглогодичные программы.

При всех преимуществах Каракол сталкивается с вызовами. Инфраструктура города, рассчитанная на 70–90 тыс. жителей, испытывает перегрузку в пик сезона: проблемы с вывозом мусора, нехватка мощностей, ограниченность транспорта. По уровню сервиса Каракол уступает российским курортам. Эти ограничения и проблемы и пути их решения заложены в генеральный план развития города до 2050 года и стратегию развития туризма до 2030 года [2].

Кроме инфраструктурных проблем, существуют также проблемы информированности россиян об отдыхе в Кыргызстане. Если для жителей Казахстана и Узбекистана это направление давно стало традиционным, то российский турист зачастую ничего о нем не слышал. Поэтому для привлечения россиян необходим комплекс маркетинговых инструментов: цифровой маркетинг (сайт, соцсети, таргетированная реклама), сотрудничество с блогерами, партнерство с российскими турагентствами, создание уникального контента, программ лояльности.

Заключение

Кыргызстан обладает конкурентными преимуществами для привлечения российских туристов: безвизовый режим, языковая доступность, транспортная доступность, ценовая привлекательность.

Город Каракол – перспективная всесезонная дестинация, сочетающая горнолыжный курорт, культурное наследие, термальные источники и треккинговые маршруты. Ценовая доступность (в 2–3 раза ниже российских аналогов) – ключевое преимущество. Развитие авторских туров в Караколе способно предложить российскому туристу уникальное сочетание доступности, аутентичности и качества природных условий. Всесезонность позволяет формировать стабильный турпоток в течение года, а реализация таких проектов соответствует государственной стратегии развития туризма Кыргызстана до 2030 года [2].

В России сформировался запрос на новые туристические направления: транспортная недоступность Европы, рост цен и перегруженность внутренних курортов создают благоприятные условия для вывода новых туристических продуктов [4]. Однако Кыргызстан сталкивается с инфраструктурными ограничениями: дефицит качественного номерного фонда, неразвитость сервиса и с недостаточной информированностью потенциальных туристов о возможности отдыха в Кыргызстане. Эти вызовы требуют решения и в Кыргызстане уже многое делается для успешного развития туризма.

Список используемых источников

1. В Киргизии вводят новый тип визы [Электронный ресурс] // Большая Азия. 2025. 14 января. URL: https://bigasia.ru/v-kirgizii-vvodyat-novyj-tip-vizy/ (дата обращения: 21.03.2026).

2. Национальный статистический комитет Кыргызской Республики. Туризм в Кыргызстане. Статистический сборник [Электронный ресурс]. Режим доступа: https://www.stat.gov.kg/ru/publications/sbornik-turizm-v-kyrgyzstane/ (дата обращения: 10.03.2026).

3. Данные Пограничной службы ГКНБ Кыргызской Республики за 2023–2025 гг. [Электронный ресурс]. Режим доступа: https://knews.kg/2026/01/23/pogransluzhba-po-itogam-2025-goda-v-kyrgyzstane-zafiksirovan-sushhestvennyj-rost-chisla-inostrantsev-vezzhayushhih-v-stranu/ (дата обращения: 10.03.2026).

4. Отдых внутри страны дорожает быстрее: заграница неожиданно стала равной альтернативой [Электронный ресурс] // Правда.ру. 2026. 23 января. URL: https://www.pravda.ru/travel/2330782-travel-cost-parity/ (дата обращения: 21.03.2026).

УДК 005.31

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ СЕРВИСНОЙ КОМПАНИИ ПРИ ПЕРЕХОДЕ НА ОТЕЧЕСТВЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

А. М. Атаян (к.п.н., доцент, доцент кафедры ЭД СПбГУТ)
Л. А. Марченко (студент группы МБИ-2511 СПбГУТ),
marchenko.la@sut.ru

В статье рассматриваются теоретические и практические аспекты миграции закупочных процессов из ERP-системы Microsoft Dynamics AX (Axapta) в системы 1С ДО и 1С ERP. Анализируются различия в архитектуре систем, особенности трансформации бизнес-процессов закупок, а также типовые проблемы, возникающие при переходе. Предлагается методология поэтапной миграции с учетом управления мастер-данными, интеграции и адаптации процессов.

бизнес-процесс, закупочный процесс, импортозамещение, Axapta, 1С:ДО, 1С:ERP

Актуальность исследования обусловлена возрастающей необходимостью перехода предприятий с зарубежных ERP-систем, таких как Microsoft Dynamics AX (Axapta), на отечественные решения, в частности 1С:ERP. Это связано с экономическими, технологическими и регуляторными факторами, включая снижение зависимости от иностранных поставщиков программного обеспечения, оптимизацию затрат на сопровождение систем и необходимость соответствия локальным требованиям учета и отчетности.

Особую значимость приобретает перевод закупочных процессов, поскольку они напрямую влияют на устойчивость цепей поставок, эффективность использования ресурсов и финансовые результаты предприятия. Неправильно реализованная миграция может привести к сбоям в операционной деятельности, что подчеркивает необходимость научного подхода к данному процессу.

В условиях импортозамещения предприятия все чаще переходят с зарубежных ERP-систем на локальные решения. Одним из распространенных направлений является миграция с Axapta (Microsoft Dynamics AX) на платформу 1С:ERP [1-5].

Axapta представляет собой комплексную ERP-систему, ориентированную на управление финансами, цепями поставок и производством. Однако в ряде стран предприятия переходят на 1С ввиду более низкой стоимости владения, локализации и гибкости настройки.

Закупочные процессы являются критически важным элементом ERP и требуют особого внимания при миграции, так как напрямую влияют на операционную эффективность предприятия.

Закупочный процесс – это совокупность множества подпроцессов, последовательность и состав которых регламентируется как действующим законодательством, так и внутренними регламентами предприятия. В рамках описанных правил необходимо определить основные параметры, в число которых входят:

- планируемая сумма закупки;
- номенклатура закупки;
- планируемые даты поставок и оплат;
- количество подходящих контрагентов и наличие недавних договоров с ними;
- наличие закупки в годовом плане закупок;
- прочие факторы.

Поскольку вышеописанные факторы способны повлиять на течение процесса и значительно удлинить его, в рамках данной работы будет описан только перенос согласования и утверждения расходного договора.

В рамках сервисной компании закупочные процессы обретают особую роль, поскольку от эффективности их исполнения будет зависеть результат, оказывающий влияние не только на саму компанию, но и на конечного получателя услуг и его эффективность. Например, сроки проведения закупочного процесса по строительным материалам окажут влияние на скорость проведения ремонтных работ в производственном помещении получателя услуг, от чего будет зависеть время простоя производства.

Для описания процесса согласования расходных договоров в Axapta был использован раздел «Конфигурации документооборота» в модуле «Договоры с поставщиками». Настройки были осуществлены с помощью стандартных средств системы.

При переносе в 1С по ряду причин было принято решение разделить создание и течение процесса между системами: заведение карточки договора происходит в 1С ERP, а течение процесса – в 1С Документооборот. Таким образом, удалось приблизить формат настроек условий назначения шагов к тому, который реализован в Axapta, и добиться максимальной гибкости в настройках карточки договора. Из минусов данного подхода можно отметить необходимость в интеграции систем: во-первых, требуется возможность просмотра текущего статуса согласования из 1С:ERP, а во-вторых, для соблюдения условий назначения шагов необходимо передавать

из ERP в ДО минимального набора реквизитов, участвующих в маршрутизации. При этом, при необходимости добавления в условия назначения нового реквизита, требуется реализовывать доработку по его передаче в 1С:ДО.

Основной целью переноса маршрутов из Axapta в 1С выступало импортозамещение, однако, во многих моментах 1С способна предложить более обширный функционал. Одним из самых ярких моментов выступает техническая реализация параллельных шагов: в Axapta для обозначения параллельности роли в одном шаге прописывалось общее условие назначения нескольких шагов, что исключает возможность назначения шагов по-отдельности. Была необходимость прописывать общие условия на параллельном шаге, индивидуальные на отдельных и на каждом из шагов взаимоисключающие условия во избежание дублирования согласующих. Т.е. для двух ролей, которые в зависимости от условий должны вставать либо параллельно, либо последовательно, была необходимость прописывать 3 шага. В 1С стандартный функционал позволяет избежать данных проблем за счет обозначения параллельности/последовательности шагов на этапах.

Так же переход на 1С позволил реализовать автоматическое заполнение реквизита «Форма договора», отвечающего за формат согласуемого договора. По задумке, еще на этапе внедрения реквизита в карточку договора в Axapta, пользователь должен был выбирать «Форму договора» в зависимости от способа создания файла: если был выбран типовой шаблон договора, то выбиралась «Типовая» форма, позволяющая убрать из маршрута согласования сотрудников, отвечающих за проверку составленного договора на корректность. На практике данная форма выбиралась некоторыми сотрудниками для ручного сокращения маршрута согласования. В 1С удалось решить эту проблему за счет генерации файла договора: Типовые шаблоны были загружены в систему, а необходимые для заполнения поля договора автоматически подтягивают информацию из реквизитов договора. Таким образом, сохраняется уверенность в отсутствии корректировок в договоре со стороны инициатора. Было введено ограничение на ручное заполнение поля «Форма договора». По умолчанию проставляется значение «Нетиповая», однако в случае добавления в карточку договора файла способом «Из типовых шаблонов», данное значение автоматически меняется на «Типовая».

Несмотря на множество преимуществ, переход на 1С сопровождается сложностями, к числу которых относятся:

1) Отсутствие функционала «Пропуск с учетом будущих шагов». Годы развития процесса в рамках Axapta повлекли за собой адаптацию условий под технические возможности старой системы, что привело к сложностям описания ввиду отсутствия аналогичного функционала в 1С:ДО. «Пропуск с учетом будущих шагов» позволял в реальном времени проанализировать маршрут процесса и исключить текущий шаг, если ответственный за него пользователь планируется к назначению далее по маршруту. Т.к. в целевой системе аналогичного функционала нет, появилась необходимость в ручном прописывании условий исключения на текущем шаге, если планируется назначение того же исполнителя в рамках одного из последующих шагов. При этом, условия исключения на текущем шаге будут обратными от условий назначения на последующих шагах, чтобы исполнитель не назначался на ранних шагах только в том случае, если будет назначен по условиям на последующих.

2) Функционал своевременного возврата на доработку с параллельного шага. По умолчанию в 1С:ДО возврат на доработку с параллельного шага при вынесении отрицательного вердикта осуществляется только после полного завершения шага (согласования всеми назначенными в рамках шага согласующими), что некорректно с точки зрения бизнес-логики, т.к. если договор уже некорректен по определенным причинам, нет смысла тратить время на его согласование другими сотрудниками.

3) Переобучение персонала. Данный пункт касается как технических специалистов, отвечающих за администрирование системы, так и рядовых пользователей. Поскольку интерфейсы и функционал систем разительно отличается, требуется комплекс мероприятий в виде обучающих конференций, тренингов и курсов для подготовки персонала к переходу на новую систему. При этом действует правило: чем больше влияние конкретного сотрудника на систему, тем больше времени требуется на его переобучение. Если деятельность сотрудника в системе ограничивается заведением договоров, то достаточно ознакомить с интерфейсом и новым функционалом (если таковой имеется). Если же речь идет про штатного программиста, то обучение новому языку программирования может растянуться на месяцы.

4) Выбор некомпетентного подрядчика. Зачастую, при переходе на новую систему компания предпочитает не найм персонала для организации миграции, а привлечение стороннего подрядчика, что позволяет рассчитывать на более качественный результат. Однако, поскольку рынок организаций, оказывающих услуги по настройке 1С, крайне разнообразен, велик риск остановить свой выбор на некомпетентном подрядчике. Во избежание

подобных ситуаций следует принимать решение, основываясь не только на стоимости услуг, но и на отзывах (как других компаний, так и внутренних сотрудников, обеспечивающих формирование и передачу технического задания).

5) Сложно предусмотреть все. В сложных системах, внедренных на крупных предприятиях, реализованы сотни функций, которые влияют на конечную производительность конкретных пользователей. При этом, как правило, в проработке технического задания для новой системы участвуют только разработчики и аналитики, которые при всей своей компетентности не могут знать тонкости работы всех сотрудников предприятия. Из-за этого во время внедрения новой системы в промышленную эксплуатацию на команду разработчиков может обрушиться множество обращений от пользователей с ошибками разного калибра. Во избежание этого следует предусмотреть этап промышленного тестирования, в рамках которого пользователи смогут ознакомиться с функционалом новой системы и передать пожелания по ее улучшению в разработку без вынужденных остановок основной деятельности.

Таким образом, если заблаговременно проработать все проблемные моменты перехода из Axapta в 1С, итоговая реализация позволяет повысить эффективность за счет экономии времени (табл. 1).

ТАБЛИЦА 1. Преимущество 1С в сравнении с Axapta

№	Преимущество 1С в сравнении с Axapta	Объем уменьшения трудозатрат, час	Частота использования преимущества
1	Автоматическая генерация файлов договоров по шаблонам	От 0,5 до 3	При заведении каждого договора
2	Строка поиска в шапке программы, осуществляющая поиск по всей системе (актуально для новых пользователей)	От 0,05 до 0,5	При поиске чего-либо в системе
3	Скорость работы системы	От 0,05 до 0,2	Регулярно
4	Возможность самостоятельного добавления согласующих, не предусмотренных маршрутом	От 0,5 до 3	Редко
5	Прочий функционал	От 0,05 до 0,5	Регулярно

В зависимости от функциональных обязанностей сотрудника, его опыта и времени работы в системе, экономия времени после перехода в 1С может составлять от нескольких минут до нескольких часов в неделю, что

в долгосрочной перспективе повышает эффективность на уровне конкретных отделов и всей компании.

Так же стоит отметить, что 1С обладает более проработанным UI, что благоприятно сказывается на погружении в систему для новых сотрудников.

Повышение эффективности бизнес-процессов при переходе на отечественное программное обеспечение – это важная цель, которую ставит перед собой множество предприятий в условиях стремительно изменяющегося рынка, ухода иностранных поставщиков или роста штата сотрудников. По сравнению с Microsoft AX, 1С обладает более обширным функционалом, что позволяет ускорить запуск и течение производственных процессов, что приводит к повышению эффективности всей компании. Так же возможность детальной настройки процессов без необходимости в написании кода позволяет снизить затраты на создание и доработку маршрутов обработки/согласования.

Список используемых источников

1. 1С:Документооборот 8// 1С:Предприятие 8. Официальный сайт. URL: https://v8.1c.ru/doc8/ (дата обращения: 04.04.2026).

2. 250 преимуществ «1С:Документооборота 8» // 1С:Предприятие 8. Официальный сайт. URL: https://v8.1c.ru/doc8/250-preimushchestv-1s-dokumentooborota-8/ (дата обращения: 04.04.2026).

4. АХАРТА vs 1С // Блог компании ERP-системы. URL: https://habr.com/ru/sandbox/112362/ (дата обращения: 04.04.2026).

5. Сравнение 1С и Аксапты // ООО «Инфостарт». Официальный сайт. URL: https://infostart.ru/pm/703444/ (дата обращения: 04.04.2026).

6. Долганова, О. И. Моделирование бизнес-процессов: учебник и практикум для вузов / О. И. Долганова, Е. В. Виноградова, А. М. Лобанова; под редакцией О. И. Долгановой. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2026. 245 с. ISBN: 978-5-534-17914-9.

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом педагогических наук А. М. Атаян.

УДК 005.5+004.8

ИССЛЕДОВАНИЕ ИНСТРУМЕНТОВ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОБОСНОВАНИЯ РАЗРАБОТКИ ИИ-АССИСТЕНТА БИЗНЕС-АНАЛИТИКА В БАНКЕ

Л. А. Басиева (студент группы БИМ-41з СПбГУТ), basieva.la@sut.ru

В условиях цифровой трансформации российского банковского сектора особую значимость приобретает автоматизация рутинных операций бизнес-аналитиков, выступающих ключевым звеном между бизнес-заказчиками и ИТ-разработкой. В статье представлены результаты применения классических инструментов принятия решений (SWOT-анализ, SMART-критерии, сценарный анализ, экспертные методы) для обоснования разработки персонального ИИ-ассистента.

бизнес-аналитика, инструменты принятия решений, искусственный интеллект, SWOT-анализ, SMART-критерии, ИИ-ассистент

Современные подходы к внедрению ИИ требуют системного анализа как внутренних факторов (готовность организации, наличие данных, компетенции), так и внешних условий (рыночные тренды, регуляторные ограничения, технологические возможности) [1]. Бизнес-аналитики играют ключевую роль в цифровой трансформации, выступая связующим звеном между бизнес-заказчиками и ИТ-подразделениями. Их работа связана с высокой нагрузкой по документированию требований, протоколированию встреч, анализу и согласованию. Как отмечается в исследовании Х. А. Магомедовой, решения на базе ИИ позволяют проводить сбор и анализ данных, на основе которых можно принимать решения в режиме реального времени [2]. Однако для того, чтобы эти возможности были реализованы, требуется качественная работа бизнес-аналитиков на этапе формализации задач.

Анализ деятельности отдела бизнес-аналитики ПАО «СОВКОМБАНК» показал, что специалисты тратят до 40-50 % рабочего времени на рутинные операции: документирование, протоколирование встреч, согласование требований. Основные функции бизнес-аналитика включают сбор и анализ требований, документирование, моделирование бизнес-процессов, коммуникацию и фасилитацию, а также поддержку разработки и тестирования.

В таблице 1 представлена классификация основных артефактов, создаваемых бизнес-аналитиками в процессе работы, с указанием средних временных затрат на их подготовку.

ТАБЛИЦА 1. Классификация создаваемых артефактов бизнес-аналитика

Тип документа	Назначение	Средняя частота создания (на 1 сотрудника)	Среднее время подготовки (на 1 сотрудника)
Бизнес-требования	Описание потребностей бизнеса и ожидаемых результатов	8-10 в месяц	8-12 часов
Протоколы встреч	Фиксация решений, договоренностей, задач	40-50 в месяц	1-2 часа
Пользовательские сценарии	Приложение к бизнес-требованиям	15-20 в месяц	2-3 часа
GAP-анализ	Описание процессов в формате AS-IS/TO-BE	3-5 в месяц	4-8 часов
Дорожные карты	Планирование и структурирование проекта	1-2 в месяц	2-3 часа

Наиболее перспективными направлениями автоматизации являются анализ записей встреч, генерация черновиков документов, проверка полноты требований и поиск релевантной информации.

Для выявления конкретных задач, подлежащих автоматизации, была сформирована экспертная группа из семи ключевых специалистов отдела. Экспертный метод состоит из нескольких различных методов, среди которых выделяют метод мозгового штурма, метод «Делфи» и др. [3]. С участием данной группы проведен мозговой штурм, в результате которого сгенерировано 16 уникальных предложений, систематизированных по пяти тематическим категориям: анализ встреч и коммуникаций; создание и оформление документации; анализ и доработка требований; поддержка принятия решений; обучение и адаптация новых сотрудников. По итогам экспертного голосования определены приоритетные задачи для реализации в минимально жизнеспособном продукте: генерация черновика бизнес-требований по промту, подготовка дорожной карты, анализ задач в low-code платформе, формирование краткого описания для согласования, создание инструкций и дайджестов.

Применение инструментов принятия решений сыграло ключевую роль в структурировании и обосновании полученных результатов. В таблице 2 представлена матрица SWOT-анализа проекта создания ИИ-ассистента, позволяющая системно оценить внутренние и внешние факторы, влияющие на успех внедрения. В контексте ИИ-проектов SWOT-анализ помогает идентифицировать ключевые факторы успеха и потенциальные риски на ранних этапах планирования [4].

ТАБЛИЦА 2. Матрица SWOT-анализа проекта создания ИИ-ассистента

Сильные стороны (Strengths)	Слабые стороны (Weaknesses)
1. Наличие сильной экспертизы в отделе 2. Поддержка руководства банка 3. Доступ к современной LLM (DeepSeek) 4. Высокая мотивация команды	1. Отсутствие опыта промпт-инжиниринга 2. Риск неполного понимания контекста моделью 3. Необходимость интеграции с существующими системами 4. Возможное сопротивление сотрудников изменениям
Возможности (Opportunities)	Угрозы (Threats)
1. Масштабирование решения на другие отделы 2. Создание корпоративной базы знаний 3. Повышение качества и унификации документации	1. Риски утечки конфиденциальных данных 2. Неточность генерации («галлюцинации» модели) 3. Быстрое изменение технологий

SWOT-анализ выявил сильные стороны проекта (наличие экспертизы, поддержка руководства) и ключевые угрозы (риски утечки данных, неточность генерации). С помощью SMART-критериев сформулированы измеримые цели: сокращение времени подготовки черновика бизнес-требований на 40 %, протоколов встреч – на 50 %, достижение точности выделения требований не менее 85 %. Для проектов в области искусственного интеллекта использование SMART-критериев позволяет увязать технологические инициативы с измеримыми бизнес-результатами [1]. Сценарный анализ (когнитивное моделирование) позволил идентифицировать критические факторы успеха проекта: качество данных, вовлеченность пилотной группы, стабильность систем. По мнению исследователей, когнитивное моделирование включает в себя совокупное влияние вешней среды организации на факторы, которые остаются за пределами формальной структуры модели [5].

Методы групповой экспертной оценки особенно эффективны при решении задач альтернативной классификации, многокритериального выбора и оценки эффективности в условиях неопределенности [3]. В рамках разработки ИИ-ассистента для бизнес-аналитиков перечисленные методы использовались для определения списка задач, подлежащих автоматизации, классификации и определения их приоритета, а также для оценки ожидаемой эффективности от внедрения ассистента.

На основе проведенного анализа была разработана модель ИИ-ассистента для определения границ минимально жизнеспособного продукта и описания ключевых сценариев использования, включая автоматическую запись совещаний и создание черновика бизнес-требований.

Результаты исследования могут быть использованы при внедрении ИИ-ассистентов в работу бизнес-аналитиков в организациях финансового сектора. Дальнейшие этапы работы включают создание системы, обучение сотрудников, сбор обратной связи и количественную оценку эффективности внедрения.

Список используемых источников

1. Павлов А. А. Интеграция искусственного интеллекта в систему стратегического управления организацией: методология и практика // Вестник Евразийской науки. 2025. Т. 17. № S3. EDN: PQDTSJ. URL: https://www.elibrary.ru/item.asp?id=82687075 (дата обращения: 28.05.2026).

2. Магомедова Х. А. Общие вопросы внедрения решений на базе технологии искусственного интеллекта в отечественный бизнес // УЭПС: управление, экономика, политика, социология. 2021. № 2. С. 11-16. EDN: VASSNN. URL: https://www.elibrary.ru/item.asp?id=47766765 (дата обращения: 28.05.2026).

3. Демидова Л. А. Интеллектуальные методы принятия решений на основе данных группового экспертного оценивания / Л. А. Демидова, А. Н. Пылькин. Москва: Горячая линия – Телеком. 2017. 238 с. URL: https://www.techbook.ru/book.php?id_book=912 (дата обращения: 28.05.2026).

4. Amplayo, R. K. Risk Management Strategy for Generative AI in Computing Education: How to Handle the Strengths, Weaknesses, Opportunities, and Threats? / R. K. Amplayo [et al.] // International Journal of Educational Technology in Higher Education. 2024. Vol. 21, Article 61. URL: https://link.springer.com/article/10.1186/s41239-024-00494-x (дата обращения: 28.05.2026).

5. Авдеева З. К., Коврига С. В., Макаренко Д. И. Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями) // Управление большими системами: сборник трудов. 2007. № 16. С. 26-39. EDN: HVGOCJ. URL: https://www.elibrary.ru/item.asp?id=9288111 (дата обращения: 28.05.2026).

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом педагогических наук, доцентом А. М. Атаян.

УДК 339.9

ТРАНСНАЦИОНАЛЬНАЯ КОРПОРАЦИЯ INDITEX НА МИРОВОМ РЫНКЕ FAST FASHION

Е. И. Бородич (студент группы М-2511 СПбГУТ), borodich.ei@ sut.ru

В статье представлен комплексный анализ деятельности транснациональной корпорации Inditex как мирового лидера индустрии быстрой моды. Рассмотрена уникальная бизнес-модель данной компании, сочетающая вертикальную и горизонтальную интеграцию. Проведено сопоставление масштабов бизнеса с экономиками отдельных государств. Особое внимание уделено двойственной роли корпорации в глобальной экономике и ее адаптации к вызовам устойчивого развития.

транснациональная корпорация, мировой рынок одежды, быстрая мода, Inditex, устойчивое развитие

Актуальность темы продиктована трансформацией глобальных потребительских привычек и изменением структуры международной торговли под влиянием цифровизации и ESG-повестки. Inditex представляет собой показательный кейс для изучения, поскольку демонстрирует способность удерживать лидерство в условиях разрыва традиционных логистических цепочек и санкционного давления на мировых рынках. Опыт построения комбинированной стратегии управления поставками содержит готовые решения для менеджмента компаний, стремящихся к операционной гибкости.

Испанская корпорация Inditex S.A. (Industria de Diseño Textil Sociedad Anónima) со штаб-квартирой в г. Артейхо (Галисия) сохраняет централизованное управление в регионе своего основания. Контрольный пакет акций остается в руках основателя Амансио Ортеги. Под управлением Inditex сосредоточено восемь основных брендов: флагманская Zara, премиальный Massimo Dutti, молодежные Pull&Bear, Bershka и Stradivarius, спортивное и домашнее направления Oysho и Zara Home. У компании более 5 800 магазинов в 213 странах и практически все точки являются ее собственностью [1]. Таким образом, Inditex избегает франчайзинга в пользу прямого управления розничными точками для сохранения тотального контроля над клиентским опытом.

В основе операционной эффективности Inditex лежит концепция fast fashion, доведенная до технологического совершенства. В отличие от клас-

сического fashion-ритейла с полугодовым циклом планирования, корпорация сократила путь от эскиза до появления изделия в торговом зале до 15 дней. Этот результат достигается за счет четырех компонентов.

Во-первых, уникальная система обратной связи – менеджеры магазинов ежедневно передают агрегированные данные о спросе и клиентских предпочтениях в аналитический центр.

Во-вторых, производственная сеть намеренно диверсифицирована: более 60 % продукции отшивается на мощностях, приближенных к штаб-квартире (Португалия, Марокко, Турция), что минимизирует транспортные издержки.

В-третьих, логистический хаб в Сарагосе функционирует как «сердце» системы, обеспечивая двухразовую в неделю отгрузку товаров по всему миру строго в соответствии с текущим спросом. Искусственное поддержание дефицита (малые партии коллекций) стимулирует частоту визитов покупателей до 17 раз в год, что в четыре раза превышает среднеотраслевой показатель.

В-четвертых, вещи завозятся малыми партиями в магазины, что подталкивает покупателей к немедленной покупке.

Проведенный анализ позволяет классифицировать Inditex как корпорацию с раздельным типом интеграции, комбинирующую признаки вертикальной и горизонтальной. Вертикальный контроль распространяется на всю цепочку создания продукта – от дизайнерских бюро и пошивочных центров до розничной полок, исключая оптовых посредников. Горизонтальная составляющая реализуется через мультибрендовую архитектуру, при которой различные марки используют общую инфраструктуру управления и аналитики больших данных.

С точки зрения стратегического поведения компания придерживается модели, условно обозначаемой как «муравей»: высокая стабильность, четкая централизация ключевых решений и одновременно способность быстро адаптироваться к локальным изменениям спроса.

Ретроспективный анализ статистической отчетности за период 2010–2025 гг. демонстрирует непрерывность роста [1]. Даже в условиях пандемийного 2020 года корпорация сумела компенсировать падение офлайн-трафика взрывным ростом электронной коммерции. По итогам 2025 финансового года онлайн-канал сгенерировал 10,7 млрд евро, обеспечив 27 % от совокупной выручки в 39,86 млрд евро [2]. Мобильные приложения и сайты брендов работают в тесной связке с физическими магазинами, а компания

экспериментирует и с дополнительными форматами – примером является запуск платформы перепродажи одежды Zara.

Расчет индекса транснационализации (соотношение зарубежных активов, продаж и персонала к общим показателям) подтверждает глобальный характер деятельности Inditex. Подавляющая часть бизнеса сосредоточена за пределами страны базирования. Масштаб операций – оборот корпорации (около 38 млрд долл. США) превосходит номинальный валовой внутренний продукт Исландии, Кипра, Албании и Багамских островов [1, 3].

Inditex уверенно входит в число ведущих fashion-ритейлеров планеты. В рейтинге Fortune Global 500 компания занимает вторую строчку в Европе по объему продаж среди розничных сетей и входит в топ-3 глобальных игроков fashion-индустрии [4]. В списке Forbes Global 2000 ее позиции отражают высокую инвестиционную привлекательность [5]. Отдельного внимания заслуживает 57-е место в авторитетном рейтинге Corporate Knights Global 100, что свидетельствует о заметном прогрессе в реализации экологической повестки [6].

Основные конкуренты: шведская H&M, японская Fast Retailing (владелец Uniqlo), американская Gap Inc., а также частично люксовый гигант LVMH и спортивный бренд Nike в смежных категориях. Признаки олигопольного сговора на рынке отсутствуют ввиду высокой фрагментации отрасли, однако имеет место феномен ценового лидерства, при котором изменения в ценовой политике Inditex, вызванные объективными издержками, принимаются рынком как индикативный сигнал.

Для экономики Испании корпорация выполняет функцию национального экономического драйвера. Прямая занятость на территории страны превышает 16 500 человек, а с учетом мультипликативного эффекта в смежных отраслях число поддерживаемых рабочих мест достигает 180 000 [1].

В глобальном масштабе Inditex кардинально изменила ландшафт потребительского поведения, сделав элементы высокой моды массово доступными. Вместе с тем именно масштаб деятельности заставляет компанию играть роль первопроходца в преодолении негативных последствий модели fast fashion. Стратегия устойчивого развития, включающая переход на переработанные и экологичные ткани, сокращение водного следа и публичную ESG-отчетность, становится неотъемлемой частью корпоративного управления и примером для всей индустрии.

Проведенное исследование подтверждает, что Inditex – образец того, как глобальный бизнес может сочетать жесткий контроль с цепочками поставок с мгновенной реакцией на спрос. Финансовая устойчивость, подкрепленная цифровизацией и омниканальной моделью продаж (интеграция онлайн и офлайн платформ), позволяет корпорации превосходить по экономическому весу бюджеты суверенных государств. Двойственность положения – одновременное выполнение роли драйвера потребления и вынужденного флагмана экологизации отрасли – определяет вектор стратегического развития компании на ближайшие десятилетия. Опыт Inditex демонстрирует, что в современных условиях ключевым фактором успеха транснационального бизнеса становится не только скорость, но и способность к системной адаптации под новые глобальные вызовы.

Список используемых источников

1. Официальный сайт Inditex [Электронный ресурс]. URL: https://www.inditex.com (дата обращения: 25.04.2026)

2. Ритейлер Inditex увеличил чистую прибыль в 2024 фингоду на 9 % [Электронный ресурс] // Информационная группа «Интерфакс». URL: https://www.interfax.ru/business/1013172 (дата обращения: 25.04.2026).

3. GDP (current US$) [Электронный ресурс] // The World Bank. URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD (дата обращения: 16.03.2026).

4. Fortune Global 500 Ranking (2025) [Электронный ресурс]. URL: https://fortune.com/ranking/global500 (дата обращения: 16.03.2026).

5. Forbes Global 2000 (2025) [Электронный ресурс]. URL: https://www.forbes.com/lists/global2000 (дата обращения: 16.03.2026).

6. Corporate Knights Global 100 [Электронный ресурс]. URL: https://corporateknights.com/rankings/global-100-rankings/ (дата обращения: 16.03.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры ЭД СПбГУТ, кандидатом экономических наук Т. И. Ююкиной.

УДК 338.467.6

КАК КИТАЙСКИЕ БЕСПЛАТНЫЕ GACHA-ИГРЫ ФОРМИРУЮТ СВЕРХДОХОДНУЮ БИЗНЕС-МОДЕЛЬ

Ю. А. Виноградова (студент группы ИСТ-331 СПбГУТ),
vinogradova.iua@sut.ru

В работе исследуется экономическая логика монетизации в китайских free-to-play gacha-играх. Предлагается интерпретация данной модели как вероятностного ценообразования: пользователь приобретает не сам цифровой актив, а шанс его получить. На основе методов теории вероятностей и поведенческой экономики оценивается ожидаемая стоимость получения редкого игрового объекта с учетом механизма гарантии (pity system). Показано, что сочетание случайностной природы покупки, цифрового характера продукта и поведенческих факторов приводит к высокой концентрации доходов и значительной маржинальности. Полученные результаты могут быть использованы при анализе цифровых платформ и проектировании моделей монетизации.

бизнес-модель, gacha-игры, вероятностное ценообразование, внутриигровые покупки, цифровые активы, маржинальность, китайский рынок.

В современной цифровой экономике наблюдается парадокс: продукты, распространяемые бесплатно, способны приносить существенную выручку. Наиболее заметно это проявляется в играх, работающих по модели free-to-play. В отличие от классической схемы с фиксированной ценой входа, здесь пользователь получает бесплатный доступ, а доход формируется за счет добровольных покупок внутри игры. Объектом анализа данного исследования являются gacha-игры, так как этот жанр является наиболее развитым направлением данной модели, получившим широкое распространение в Китае, и занимающим лидирующие позиции на мировом рынке. Так, в 2025 году только мобильный сегмент принес 55 % всей глобальной выручки, а доходы достигают сотни миллионов долларов ежегодно. Визуализация распределения доходов самых прибыльных проектов за 2025 год представлена на рисунке 1. Китай при этом остается одним из крупнейших рынков по объему потребительских расходов [1].

Ключевая особенность gacha-игр – механизм случайного получения объектов. Пользователь не приобретает игровой предмет напрямую, а оплачивает попытку его получения. Можно сказать, что в таком случае предметом сделки является не сам товар, а вероятность получения. Это принципиально отличает данную модель от традиционных рыночных механизмов и позволяет рассматривать ее как форму вероятностного ценообразования.

В такой системе цена перестает быть фиксированной величиной и становится случайной переменной, зависящей от вероятности успеха и поведения пользователя. Исследования показывают, что подобные механики стимулируют повторные траты. Это связано, в частности, с эффектом преследования потерь и рядом когнитивных искажений, характерных для азартных практик [2].

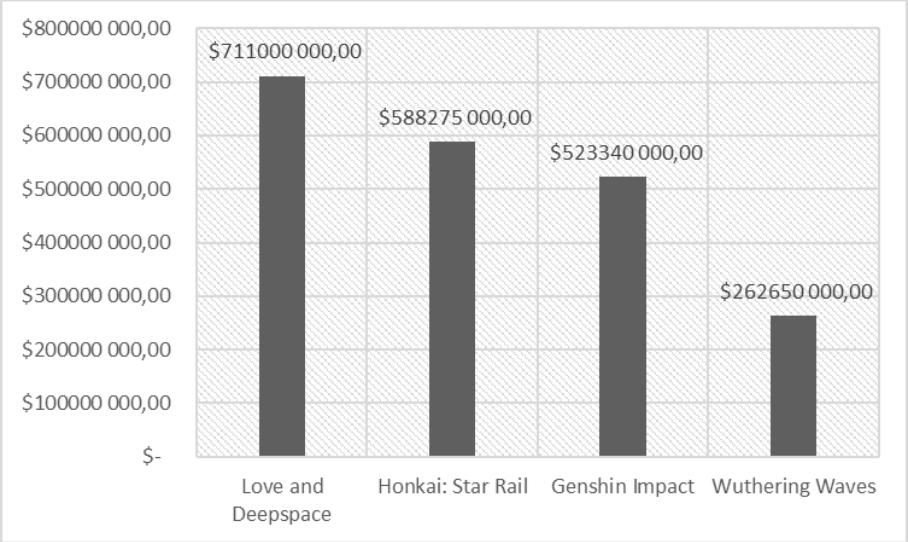


Рис. 1. Доходы мобильных gacha-игр за 2025 год

Игровые объекты в gacha-играх отличаются от обычных товаров. Были выделены следующие два вида ассетов – продаваемые напрямую за фиксированную цену и участвующие в вероятностной модели получения. Зачастую ко второму виду относятся персонажи, оружие и др. Они имеют следующие характеристики: нематериальны, практически не имеют предельной стоимости воспроизводства и приобретают ценность за счет искусственно заданной редкости. В таких условиях стоимость объекта определяется через математическое ожидание затрат на его получение. Это позволяет интерпретировать персонажа как вероятностный цифровой актив.

С точки зрения теории вероятностей процесс получения редкого персонажа в простейшем случае описывается геометрическим распределением с вероятностью успеха p в одной попытке. Тогда математическое ожидание числа попыток равно:

$$E(X) = \frac{1}{p}, \quad (1)$$

Например, при заданном значении $p = 0{,}006$ математическое ожидание составляет:

$$E(X) = \frac{1}{0{,}006} \approx 167 \text{ попыток}, \quad (2)$$

Однако в играх зачастую используется механизм гарантии (pity system), ограничивающий максимальное число попыток и увеличивающий вероятность успеха после серии неудач. В попытке формализации данного механизма можно представить распределение усеченным, а математическое ожидание определить суммой:

$$E(X) = \sum_{k=1}^{N} k \cdot P(X = k), \quad (3)$$

где N – максимальное число попыток до гарантированного получения персонажа. Так, с учетом механизма гарантии, среднее число попыток может снизиться до диапазона 120–160.

Далее ожидаемая стоимость получения персонажа определяется как:

$$C = E(X) \cdot c, \quad (4)$$

где c – стоимость одной попытки. При $c \approx 2$ USD и $E(X) \approx 150$ получаем:

$$C \approx 150 \cdot 2 \approx 300\, USD, \quad (5)$$

Для конкретизации полученных расчетов рассмотрим практическую реализацию вероятностной модели на примере игры Genshin Impact, являющейся одним из наиболее успешных проектов в жанре gacha.

Для начала стоит отметить, что в игре используется многоуровневая система валют. Основной донатной валютой являются «кристаллы сотворения», которые при покупке конвертируются во внутриигровую валюту «примогемы». Примогемы, в свою очередь, используются для совершения попыток получения персонажей. Стоимость одной попытки составляет 160 примогемов.

Система монетизации включает несколько пакетов кристаллов различного объема. При первом пополнении каждого пакета игрок получает удвоенное количество валюты, тогда как при последующих покупках предоставляется стандартный бонус меньшего размера. Таким образом, фактическая стоимость примогемов существенно зависит от истории покупок пользователя.

Рассмотрим стоимость полного набора донатных пакетов. При использовании всех бонусов первого пополнения суммарный объем приобретаемой валюты составляет 26160 примогемов при общей стоимости 18908 руб.,

а в случае отсутствия бонусов аналогичный объем валюты требует существенно больших затрат, что приводит к росту средней стоимости одной попытки. Таким образом, полный набор с бонусами дает возможность получить 163 попытки, что сопоставимо с теоретической оценкой математического ожидания, полученной ранее, и это не обычное совпадение, а скорее продуманный мотивационных ход со стороны разработчиков.

Далее рассмотрим стоимость получения персонажа при различных сценариях. Максимальное количество попыток, необходимое для гарантированного получения ограниченного по времени персонажа, составляет 180. В этом случае стоимость при наличии бонусов составляет 22246 руб., тогда как при их отсутствии она возрастает до 34478 руб. Таким образом, разница достигает более 50 %, что подтверждает значительное влияние бонусной системы на фактическую цену.

Средний сценарий, соответствующий 150 попыткам, демонстрирует аналогичную зависимость. При использовании бонусов стоимость составляет 17518 руб., тогда как без бонусов – 28794 руб. В более благоприятном сценарии (75 попыток) затраты снижаются до 8520 руб. с бонусами и 14279 руб. без них. Представление данного распределения представлено в таблице 1.

ТАБЛИЦА 1. Распределение цен попыток при различных соотношениях параметров

Кол-во попыток	Гарантия	Стоимость, руб.	
		Двойной бонус	Стандартный бонус
180	100 %	22246	34478
150	100 % (pity system)	17518	28794
75	50 % (pity system)	8520	14279

Полученные результаты демонстрируют, что фактическая стоимость цифрового актива является функцией не только вероятности его получения, но и структуры ценовой дискриминации, встроенной в систему монетизации. Бонусы первого пополнения снижают барьер входа и стимулируют начальные покупки, тогда как последующие транзакции становятся менее выгодными, увеличивая среднюю стоимость получения персонажа.

Таким образом, даже в рамках одного проекта наблюдается широкий диапазон фактических цен – от 8 000 до 34 000 руб. за один и тот же цифро-

вой актив. Это подтверждает ключевой тезис о вероятностной природе ценообразования, при которой итоговая цена определяется комбинацией случайных и поведенческих факторов.

Более того, данная модель усиливает эффект ценовой дискриминации: пользователи, совершающие большее количество попыток, фактически платят более высокую цену за тот же результат. Это позволяет разработчикам извлекать дополнительный доход за счет различий в поведении и платежеспособности аудитории.

Таким образом, реальная цена значительно превышает воспринимаемую стоимость отдельной транзакции, что создает эффект «размытой цены».

Экономическая эффективность модели можно описать через стандартные метрики цифровой индустрии. Средний доход на пользователя (ARPU) определяется:

$$ARPU = \frac{R}{U}, \tag{6}$$

где R – общая выручка, U – общее число пользователей. Средний доход на платящего пользователя:

$$ARPPU = \frac{R}{U_p}, \tag{7}$$

где U_p – число пользователей, совершающих покупки. Коэффициент конверсии (доля платящих пользователей) определяется:

$$CR = \frac{U_p}{U}, \tag{8}$$

Примерная доля платящих пользователей в мобильных free-to-play играх составляет около 1,5-3,5 %, в зависимости от жанра и региона, при этом в жанре RPG (к которому относятся большинство gacha-игр) этот показатель может достигать 4-5 %. Можно заметить, что значение коэффициента конверсии все равно остается низким, что указывает на высокую зависимость модели от платящей аудитории. При этом средний доход на платящего пользователя в успешных gacha-проектах может составлять 40-70 USD в месяц и более [3].

Характерной особенностью является высокая концентрация доходов. Около 2-5 % пользователей могут генерировать от 50 до 70 % всей выручки [4]. Их вклад можно выразить как:

$$S_w = \frac{R_w}{R}, \quad (9)$$

где R_w – выручка от высокоплатящих пользователей.

Для иллюстрации рассмотрим отдельный пример. Пусть в игре 1 млн пользователей, из которых 3 % являются платящими (U_p = 30 тыс.). При среднем значении ARPPU = 50 USD месячная выручка составит:

$$R = 30000 \cdot 50 = 1500000\ USD$$

Если при этом 5 % платящих пользователей (1,5 тыс. человек) обеспечивают 50 % (750 тыс. USD) выручки, то их вклад в среднем составляет 500 USD на человека, что демонстрирует высокую концентрацию доходов и объясняет устойчивость модели даже при низкой конверсии.

Таким образом, сочетание вероятностной модели ценообразования и неравномерного распределения расходов пользователей позволяет free-to-play gacha-играм достигать высокой прибыльности, несмотря на бесплатный доступ к продукту.

Дополнительное влияние оказывают поведенческие факторы: эффект потерь, склонность к завершению начатых действий и влияние ограниченных по времени предложений. Такие механики могут рассматриваться как «хищнические» схемы монетизации, поскольку они эксплуатируют когнитивные искажения пользователей, сходные с механизмами, используемыми в азартных играх [2].

С экономической точки зрения такая модель может быть интерпретирована как форма скрытой ценовой дискриминации: один и тот же цифровой актив обходится различным пользователям в разные суммы в зависимости от их поведения и случайных факторов. Это позволяет разработчикам извлекать большую долю потребительского излишка по сравнению с традиционными моделями ценообразования [5].

Высокая прибыльность также объясняется масштабируемостью цифровых товаров. После разработки персонажа его дальнейшее воспроизводство не требует затрат, что обеспечивает высокую маржинальность, которая оценивается в 30-50 %. Даже с учетом комиссий платформ и расходов на маркетинг такие проекты способны демонстрировать значительную рентабельность [1, 3].

Несмотря на экономическую эффективность, данная модель сталкивается с рядом ограничений. Во-первых, необходимость постоянного обнов-

ления контента приводит к росту издержек разработки. Во-вторых, существует риск обесценивания ранее полученных активов, что может снижать доверие пользователей. В-третьих, усиливается регуляторное давление, связанное с необходимостью раскрытия вероятностей и ограничением механик, сходных с азартными играми [2].

Институциональные факторы играют важную роль. В Китае введенные в 2021 году ограничения на игровое время для несовершеннолетних повлияли на структуру спроса, а в странах ЕС обсуждается правовой статус loot box-механик. Эти регуляторные изменения могут существенно трансформировать бизнес-модели gacha-игр в будущем. В России также обсуждаются регуляторные инициативы. Однако на текущий момент эти обсуждения не привели к блокировкам или запретам, и вопрос остается открытым для дальнейшего диалога между индустрией и регуляторами.

Подводя итог, gacha-игры можно рассматривать как специфическую форму цифровой экономики, где стоимость формируется не через фиксированную цену, а через вероятность получения актива. Вероятностная модель ценообразования позволяет дифференцировать фактические затраты пользователей, снижать воспринимаемую цену и обеспечивать высокую концентрацию доходов. Сочетание этих факторов объясняет способность бесплатных игр генерировать значительные доходы и подтверждает устойчивость данной модели в рамках цифровых платформ.

Список использованных источников

1. Newzoo. Global Games Market Report 2025. URL: https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2025 (дата обращения: 24.03.2026).

2. King, D. Predatory monetization schemes in video games / D. King, P. Delfabbro // Addiction. 2019. Vol. 114, N 4. PP. 604-606.

3. Sensor Tower. State of Gaming 2026: Mobile, PC, & Console Trends [Электронный ресурс] / Sensor Tower. 2026. URL: https://sensortower.com/report/state-of-gaming-2026 (дата обращения: 24.03.2026).

4. Drummond, A. Video game loot boxes are psychologically akin to gambling / A. Drummond, J. D. Sauer // Nature Human Behaviour. 2018. Vol. 2. N 8. PP. 530-532.

5. Varian, H. R. Intermediate Microeconomics: A Modern Approach / H. R. Varian. 9th ed. New York: W. W. Norton & Company, 2014. 832 p.

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом экономических наук, доцентом А. В. Исаковым.

УДК 32:659.4

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В ПОЛИТИЧЕСКИХ АНТИКРИЗИСНЫХ КОММУНИКАЦИЯХ

Л. В. Володина (к.ф.н., доцент, доцент кафедры СПН СПбГУТ)
Д. Ш. Парашов (студент группы РСО-41м СПбГУТ), parashov.ds@sut.ru

Данная работа посвящена анализу современных тенденций политических антикризисных коммуникаций в контексте глобальных вызовов 2024–2026 годов. Исследуется трансформация коммуникационных стратегий государств в условиях вооруженных конфликтов, нестабильности и цифровизации. Особое внимание уделено антикризисным коммуникациям в рамках ирано-американо-израильского конфликта 2025–2026 годов как ключевому кейсу современной дипломатии. Выявлен переход от реактивных моделей к проактивным стратегиям управления общественным мнением и международными отношениями в условиях непрерывной турбулентности.

антикризисные коммуникации, политический кризис, цифровая дипломатия, управление репутацией, ирано-израильский конфликт

Введение

В 2025 году индекс глобальных политических рисков Coface поднялся до 41,1 % – исторического рекорда [1]. Турбулентность слилась с нашими реалиями: вооруженные конфликты, и информационные войны требовали от государств перехода от тактических действий к стратегии непрерывного антикризисного общения. Ярче всего это было проиллюстрировано конфронтацией Ирана, США и Израиля 2025-2026 годов, где традиционная дипломатия стыковалась с цифровым противоборством [2].

Цель исследования – выявить ключевые трансформации стратегий политических антикризисных коммуникаций на основе анализа теоретических моделей, цифровых вызовов и конкретного кейса.

Теоретические рамки: от реактивности к проактивности

Сегодняшние антикризисные коммуникации представляют собой систему информационного взаимодействия государства с обществом и внешним миром, позволяющую противодействовать кризису, минимизировать его последствия и восстанавливать доверие. В зависимости от типа кризиса (конфликтного; консенсусного; полемического) в них применяются различные модели: традиционная (централизованная), партисипативная (диалоговая) и переговорно-диалоговая [3].

Главная тенденция – переход на проактивную модель непрерывных коммуникаций. Кризис перестал быть исключением. Государства выстраивают постоянную готовность, превентивное информирование и накапливают «доверительный капитал» в мирное время. Эффективность измеряется по четырем параметрам: доступность информации, снижение тревожности, учет общественных угроз и политическое выравнивание [3].

Цифровая трансформация – двусторонняя улица

Социальные сети изменили все. Современные платформы обеспечивают мониторинг в реальном времени, непосредственный диалог с обществом и контроль над нарративом. Но вместе с ними возникли и риски: скорость появления дезинформации превышает скорость ее опровержения, эхокамеры блокируют альтернативные мнения [4].

В современном арсенале для борьбы с этими угрозами имеется все: безопасные площадки, виртуальные координационные центры, системы оповещения и инструменты управления репутацией. Цифровизация важна, но требуется аккуратность: малейшая неточность или несогласованность перечеркнет все усилия.

Кейс: ирано-американо-израильское кризис 2025 – 2026 годов

Противостояние стало кульминацией противостояний вокруг Ирана. Ход событий: июнь 2025 г. – 12-дневная война, Израиль атакует объекты Ирана, США отвечают ударом. 28 февраля 2026 г. совместные атаки США и Израиля, после которых последовал ответ Ирана.

Стратегия Израиля: упреждающее обоснование («превентивный удар»), союзнические рамки, четкая цель (не допустить ядерное оружие Ирана) и временная определенность. Стратегия США: постепенное наращивание вовлеченности (от дипломатии к удару и полномасштабной операции), юридическое обоснование через ООН, фреймирование через ядерную угрозу. Стратегия Ирана: нарратив жертвы агрессии, символическое именование операций, апелляция к исламской солидарности и акцент на стойкость. Гибель аятоллы Хаменеи стала вызовом, но дала возможность мобилизации через мученичество.

Сравнительная эффективность: Анализ показал, что высокая доступность информации и политическое выравнивание являются ключевыми факторами эффективности кризисных коммуникаций. В свою очередь, рост

неопределенности и информационные ограничения внутри страны существенно снижают способность государства управлять тревожностью населения. Главный вывод: успех антикризисных коммуникаций в современных конфликтах требует четкой координации действий, ясной артикуляции целей и полной согласованности всех используемых каналов связи [5].

Ключевые тенденции и перспективы

С помощью теории, цифровых вызовов и кейса можно выделить пять тенденций:

1. Проактивность – неизменная готовность вместо разовых реакций.

2. Гибридизация каналов – единое сообщение через ТВ, соцсети, мессенджеры и брифинги.

3. Прозрачность как императив – открытость (в сбалансированности с безопасностью) накапливает доверие.

4. Партисипативность – вовлечение граждан может быть эффективным в естественных и техногенных кризисах (катастрофы, пандемия), но ограничено в конфликтах.

5. Устойчивость к перманентной нестабильности – быстрая адаптация, готовые сценарии, распределенная ответственность.

Перспективы: внедрение ИИ и больших данных для мониторинга, персонализация коммуникаций.

Заключение

Ирано-американо-израильский конфликт 2025–2026 годов подтвердил, что цифровая трансформация стала неотъемлемой частью современных политических кризисов. Успех антикризисных коммуникаций в условиях глобальной турбулентности определяется сочетанием оперативного реагирования и стратегического планирования. Эффективное управление информационными потоками выступает важным условием сохранения устойчивости политических институтов и общественного доверия.

Список используемых источников

1. Coface. World Economic Outlook: Political Risk Index 2025 // Coface Economic Publications. 2025. URL: https://www.coface.com/news-economy-and-insights/2025-political-and-social-risk-a-record-level-a-new-norm-for-businesses

2. Coombs, W. T. Ongoing Crisis Communication: Planning, Managing, and Responding / W. T. Coombs. 6th ed. Thousand Oaks: SAGE Publications, 2023. 256 p. ISBN 978-1-5443-3871-2. URL: https://studentebookhub.com/wp-content/uploads/2024/ preview/ 9781071816646.pdf (дата обращения 10.03.2026).

2. Heath, R. L. Handbook of Risk and Crisis Communication / R. L. Heath, H. D. O'Hair. 2nd ed. New York: Routledge, 2010. 712 p. ISBN 978-1-032-14473-7.URL: https://www.taylorfrancis.com/books/edit/10.4324/9781003070726/handbook-risk-crisis-communication-robert-heath-dan-hair (Дата обращения: 17.06.2026)

3. Vosoughi, S. The Spread of True and False News Online / S. Vosoughi, D. Roy, S. Aral // Science. 2018. Vol. 359, Iss. 6380. P. 1146–1151. DOI: 10.1126/science.aap9559. URL: https://www.science.org/doi/10.1126/science.aap9559

4. Nye, J. S. The Future of Power / J. S. Nye. New York: PublicAffairs, 2011. 320 p. ISBN: 978-1-58648-891-8.

УДК 329.17

НЕОНАЦИСТСКИЕ ОСНОВЫ БАТАЛЬОНА «АЗОВ»

А. Б. Гехт (к.и.н., доцент, зав. кафедрой ИиРВ СПбГУТ)
О. А. Ухалов (студент группы ЗР-21 СПбГУТ), uhalov.oa@sut.ru

В статье анализируется понятие денацификации, его исторические корни и применение в контексте специальной военной операции на Украине. Рассматриваются предпосылки использования данного термина, связанные с утверждением о присутствии неонацистской идеологии в украинских вооруженных формированиях. Особое внимание уделяется идеологическим основам бригады «Азов» – неонацистского формирования, история которого восходит к движению «Патриот Украины» и Социал-национальной партии. Анализируются программный документ «Право нации», публицистика лидера, а также визуальная символика подразделения, включая использование руны «Вольфсангель». Проводятся параллели между идеологией «Азова» и классическим национал-социализмом, что позволяет квалифицировать ее как разновидность современного неонацизма.

специальная военная операция, денацификация, нацистская идеология

Прошло уже 4 года с начала специальной военной операции, и ее основной целью были заявлены денацификация и демилитаризация на территории Украины. В данной статье мы разберем предпосылки денацификации и идеологические основы неонацистской бригады «Азов»*.

Что же такое денацификация? Это комплекс мероприятий, направленных на очищение послевоенного германского и австрийского общества, культуры, прессы, экономики, образования, юриспруденции и политики от влияния нацистской идеологии. Использование этого термина в контексте специальной военной операции базируется на утверждении, что на территории Украины присутствует неонацистская идеология, представленная рядом организаций и вооруженных формирований такими как «Азов», «Сич»*, «Правый сектор»* и другими.

* Здесь и далее упоминание организаций осуществляется в информационных целях в рамках научного исследования. Деятельность Украинского военизированного националистического объединения «Азов» признана террористической и запрещена на территории Российской Федерации (Решение Верховного Суда РФ от 02.08.2022 № АКПИ22-411С, вступило в силу 10.09.2022).

* Деятельность Общественной организации «СИЧ-С14» признана экстремистской и запрещена на территории РФ (Решение ВС РФ от 08.09.2022)

* Деятельность Украинского военизированного объединения «Национально-освободительное движение «Правый сектор» и его структурных подразделений признана экстремистской (с 17.11.2014) и террористической (с 23.01.2025 № АКПИ24-1079с) и запрещена на территории Российской Федерации.

Особое место в статье займет анализ идеологических основ бригады «Азов». Это неонацистское формирование стало одним из самых массовых, получило официальный статус в силовых ведомствах и располагает собственным тяжелым вооружением. Актуальность исследования заключается в том, чтобы через призму «Азова» продемонстрировать наличие неонацистских взглядов в вооруженных формированиях Украины.

История бригады «Азов» начинается задолго до событий специальной военной операции. Ее корни уходят в организацию «Патриот Украины», которая, в свою очередь, вышла из Социал-национальной партии Украины (СНПУ). Позже партия сменила вектор на более умеренный, сменила название на ВО «Свобода», но радикальное крыло осталось в структуре «Патриот Украины». Эта организация была зарегистрирована в Харькове в 2006 году и выполняла функции силового крыла Социал-национальной Ассамблеи.

Лидером организации был Андрей Билецкий*, выбравший себе соответствующее прозвище «Белый вождь». Идеологический стержень движения был закреплен в программном документе «Право нации», представленном в сентябре 2006 года. Уже в названии и тексте документа прослеживаются отсылки к нацистской риторике: слово «нация» всегда пишется с латинской буквой N. Некоторые пункты документа открыто демонстрируют национальное превосходство украинцев над другими народами. Вот несколько отрывков в переводе на русский язык: «*Единый расовый тип Нации растворяется под воздействием чужерасового элемента. Для утверждения Права Нации приемлемы любые методы... оправдывает любые... насилие и жестокость». «Нация имеет право улучшать свое здоровье через расовое, евгеническое и экологическое законодательство»* [1]. Из этих отрывков видны классические неонацистские взгляды от превознесения одного этноса над другими до призывов к евгенике. Пункт о «расовом законодательстве» напрямую перекликается с Нюрнбергскими расовыми законами 1935 года в Германии, где государственный аппарат использовался для «улучшения нации» путем искусственного отбора и изоляции «нежелательных элементов». Заканчивается документ такими словами: «*На утверждение Права Нации отдаем свои жизни, имущество и кровь*». Из этих слов можно сделать вывод, что лидеры готовы пойти на любые жертвы ради своей идеологии.

Андрей Билецкий является автором сборника националистических статей «Слово Белого вождя», в данном сборнике отражена позиция Билецкого

* А. Е. Билецкий включен в Перечень террористов и экстремистов (Росфинмониторинг, запись № 3187).

и его нацистские взгляды, разберем ключевые цитаты, чтобы продемонстрировать идеологическую предвзятость автора: *«Социальность для нас это особая форма экономического и политического устройства Нации... Она включает третий путь в экономике, авторитарность власти... Таким образом, название Социал-Национализм четко определяет комплекс наших идей»* [2]. В этом отрывке прослеживается параллель с идеологией немецких национал-социалистов, ведь концепция «третьего пути» была отличительной чертой Третьего рейха. По сути, это та же идеология, где просто местами переставлены слова, вместо «национал-социализма» предлагается «социал-национализм», но суть авторитаризма и расового государства остается неизменной. Более показателен следующий отрывок: *«Украинский социал-национализм считает Украинскую Нацию кровнорасовой общностью. Полевые антропологические исследования профессора Дяченко показали, что украинцы сохраняют все основные черты кроманьонского населения Украины, то есть существуют как неизменный расовый тип как минимум 40 тысяч лет. Раса есть все для нациообразования. Раса – это основа...»* [3]. В этом тексте проглядывается сходство с мифами о «древней арийской нации», популярными во времена Третьего рейха. Попытка доказать «древность» и «чистоту» нации через псевдонаучные антропологические исследования – это инструмент нацистской пропаганды 30 – 40-х годов. Утверждение, что «раса есть все», полностью копирует тезисы Гитлера о том, что культура и государство являются лишь следствием расовой природы народа, а не языка или религии.

Идеологическая составляющая подкрепляется и визуальной атрибутикой. Эмблема бригады «Азов», известная как «Идея Нации», представляет собой стилизованное изображение двух зеркально отраженных рун, напоминающих немецкую руну «Вольфсангель». Исторически этот символ использовался в геральдике Германии, а в годы Второй мировой войны он был отличительным знаком 2-й танковой дивизии СС «Рейх». Использование символики «Идеи Нации» украинскими неонацистами – это выбор, показывающий лояльность к эстетике и идеологии национал-социализма.

В заключение хочется отметить, что бригада «Азов» представляет собой не просто вооруженное подразделение, а носитель неонацистской идеологии. Разбор программных документов, публицистики лидеров и визуальной символики показывает преемственность с идеями национал-

социализма. Таким образом, рассмотрение бригады «Азова» в контексте денацификации обусловлено не только текущими боевыми действиями, но и глубокими идеологическими корнями организации.

Список используемых источников

1. Право нації: программные принципы ВГО «Патриот Украины» [Электронный ресурс]. URL: https://web.archive.org/web/20110824034104/http://patriotukr.org.ua /index.php? rub=doc (дата обращения: 02.04.2026).

2. Білецький А. Чому соціальний націоналізм? // Слово Белого вождя: сборник статей. С. 24.

3. Білецький А. Мова і раса – первинність питання // Слово Белого вождя: сборник статей. С. 29.

Статья представлена научным руководителем, заведующим кафедрой ИиРВ, доцентом, кандидатом исторических наук А. Б. Гехтом.

УДК 339.118:316.77

ВЛИЯНИЕ КОРОТКИХ ВИДЕОРОЛИКОВ НА ПОТРЕБИТЕЛЬСКОЕ ПОВЕДЕНИЕ В СОВРЕМЕННЫХ РЕАЛИЯХ

Д. А. Гриценко (студент группы РСО-2524 СПбГУТ), gritsenko.da@sut.ru
М. М. Заляжный (студент группы РСО-2523 СПбГУТ), zaliazhnyi.mm@sut.ru

Данная статья предусматривает исследование влияния коротких видеороликов (таких как Wibes, YouTube Shorts, TikTok) на трансформацию потребительского поведения в современных реалиях. Анализируются ключевые механизмы воздействия краткого формата контента на принятие решений о покупке, включая снижение когнитивной нагрузки и активизацию эмоционального отклика. Особое внимание уделяется изменению структуры внимания аудитории и формированию новых паттернов взаимодействия с организациями.

короткие видео, трансформация потребительского поведения, клиповое мышление, маркетинговые коммуникации, цифровая среда, интернет-коммуникации, социальные сети

Современный этап развития информационного общества характеризуется фундаментальной трансформацией способов потребления контента. Характерный рост объемов информации привел к дефициту главного ресурса – человеческого внимания. В этих условиях цифровые коммуникации используют инструменты, способные захватить и удержать внимание аудитории за минимальное время. Одними из подобных стали короткие видеоролики, распространенные платформой TikTok и впоследствии интегрированные во все крупнейшие социальные сети (Wibes, YouTube Shorts, VK Клипы и другие).

Феномен «клипового мышления», долгое время обсуждавшийся преимущественно в психолого-педагогическом дискурсе, сегодня стал объективной реальностью для маркетологов и создателей контента. Современный потребитель перегружен рекламными сообщениями, его внимание фрагментировано, а способность к длительной концентрации неуклонно снижается. Ответ цифровой среды – распространение формата коротких видео, которые адаптированы к новым когнитивным условиям.

В последние годы наблюдается стремительный рост популярности платформ, предлагающих контент в формате коротких видеороликов. По-

добный формат интернет-коммуникаций стал значительной частью цифрового потребления, оказывая значительное влияние на различные аспекты жизни, включая потребительское поведение. Особую актуальность приобретает исследование механизмов этого влияния в условиях современной рыночной среды, характеризующейся высокой конкуренцией и цифровой трансформацией. Целью настоящей статьи является анализ влияния коротких видеороликов на потребительское поведение в современных реалиях. Объектом исследования выступает современное потребительское поведение, а предметом исследования является влияние коротких видеороликов на потребительское поведение в современных реалиях.

Как было упомянуто ранее, короткие видеоролики – одна из технологий интернет-коммуникаций, так как они позволяют передавать различные послания целевым и потенциальным аудиториям. Помимо вышеперечисленного, подобный формат контента включает в себя следующие преимущества: эмоциональная связь, удобство просмотра, низкие затраты на производство посланий, высокая скорость распространения информации. Подобные преимущества повышают влияние коротких видеороликов на потребительское поведение.

Согласно статистике VK Клипы и Anketolog.ru, 89 % россиян используют короткие видео как один из основных источников информации [1]. Исследователи нашли связь между просмотром подобных видео и потребительскими привычками пользователей: 42 % опрошенных несколько раз в месяц покупали товары после того, как смотрели короткие видео с этими товарами, сообщили в пресс-службе ВКонтакте. Также 73 % опрошенных отметили, что короткие видео в целом вдохновляют их на изменения в жизни и побуждают к активным действиям. Из этого следует вывод, что контент в данном формате обладает достаточной силой убеждения.

Одним из достоинств клипового мышления является правило, которое работает по принципу «8 секунд»: если за этот временной период информация не заинтересовала пользователя, то он ее пропустит и, скорее всего, забудет [2]. Подобный формат мышления также сильно повлиял на смысловое восприятие. Мозг уже не улавливает подробностей и деталей, а формирует общую картину, которая дает лишь представление об основных пунктах или действиях. С точки зрения работы с большими массивами информации – это может быть полезно, но не более.

«В 2004 году мы выяснили, что средняя продолжительность концентрации внимания на любом экране составляет две с половиной минуты. В 2012

году этот показатель снизился до 75 секунд. В последние несколько лет он составляет около 47 секунд, а медиана – всего 40 секунд», – об этом рассказала Глория Марк, психолог из Калифорнийского университета, в подкасте Speaking of Psychology [3], что показывает влияние информационного шума и ухудшение когнитивных способностей у людей.

В TikTok распространяется множество видеороликов, где молодые люди показывают свой «марафон без гаджетов». Они снимают на камеру, как сидят и ничего не делают, отключив все цифровые раздражители. Например, ролик 19-летней студентки колледжа по имени Кейт [4]. В октябре больше 10 млн просмотров в социальной сети набрало видео, где она просто сидит без дела 15 минут. К шестому дню она уже держалась 20 минут. Подобные тренды демонстрируют влияние коротких видеороликов и скроллинга в целом, если речь идет о 20-ти минутах, не говоря уже о потребительском поведении.

Согласно данным, опубликованным на ресурсе DataReportal [5], в конце 2025 года аудитория TikTok в Российской Федерации, достигшая возраста 18 лет и старше, составляла 66,7 миллиона пользователей. Несмотря на то, что платформа позволяет осуществлять таргетинг рекламы на пользователей в возрасте от 13 лет, предоставляемые рекламными инструментами аналитические данные ориентированы исключительно на аудиторию в возрасте 18 лет и старше. Если рассматривать общую популяцию интернет-пользователей в стране, независимо от возраста, то охват рекламой TikTok составлял 49,2 %.

Но период с конца 2024 по конец 2025 года ознаменовался значительным ростом потенциального охвата рекламы TikTok в Российской Федерации – на 10,2 миллиона пользователей, что составило +18,0 %. Более того, этот показатель увеличился на 2,20 миллиона пользователей (или +3,4 %). Необходимо учитывать, что рекламные аудитории не всегда полностью отражают общую пользовательскую базу платформы, и статистика охвата рекламой (ориентированная на совершеннолетних пользователей) может отличаться от динамики общей пользовательской базы. Данный феномен полезен для маркетологов, рекламщиков и специалистов по связям с общественностью, так как они могут встраивать короткие ролики в повседневную жизнь человека, которая, во многом, состоит из них.

Проведенное исследование позволяет утверждать, что клиповое мышление, будучи продуктом цифровой эпохи, представляет собой уникальный

феномен, активно распространяющийся как отдельная технология интернет-коммуникаций. Изучение статистических данных и различных трендов показало, что влияние коротких видеороликов является неотъемлемым в современных реалиях.

Список используемых источников

1. Исследование VK Клипов и Anketolog.ru: 89 % россиян считают короткие видео одним из основных источников информации // ВКонтакте. Пресс-центр. 31.01.2025. URL: https://vk.com/press/clips-research-information (дата обращения: 03.03.2026).

2. Федорова, Е. Клиповое мышление, или Феномен XXI века / Е. Федорова // Витебские вести. 2022. URL: https://vitvesti.by/index.php/obshestvo/klipovoe-myshlenie-ili-fenomen-xxi-veka.html (дата обращения: 04.03.2026).

3. DataReportal. Digital 2026: Russian Federation // DataReportal. 2026. URL: https://datareportal.com/reports/digital-2026-russian-federation (дата обращения: 29.03.2026).

4. No screens, no distractions, no mercy. Inside Gen Z's 'rawdogging boredom' challenge // Yahoo Lifestyle Canada. 2025. URL: https://ca.style.yahoo.com/no-screens-no-distractions-no-mercy-inside-gen-zs-rawdogging-boredom-challenge-090010836.html (дата обращения: 04.03.2026).

5. Марк Г. Почему наша концентрация внимания сокращается = Why our attention spans are shrinking, with Gloria Mark, PhD / Глория Марк // Speaking of Psychology: подкаст / American Psychological Association. 2023. 23 марта. URL: https://www.apa.org/news/podcasts/speaking-of-psychology/attention-spans (дата обращения: 04.03.2026).

Статья представлена научным руководителем, деканом факультета СТЭД СПбГУТ, кандидатом политических наук, доцентом Д. В. Шутманом.

УДК 339.138

ОСОБЕННОСТИ ВОСПРИЯТИЯПОЛЬЗОВАТЕЛЬСКОГО ПОКОЛЕНИЯ Z И ALPHA

Р. А. Жадан (ассистент, заместитель зав. каф. по цифровым коммуникациям СПбГУТ)
Е. В. Петрова (студент группы РСО-42 СПбГУТ), petrova.ev@sut.ru

Данная работа посвящена исследованию особенностей восприятия пользовательского контента поколениями Z и Alpha, формирующими актуальные модели цифровой коммуникации. Анализируются ключевые факторы, влияющие на доверие, интерес и вовлеченность представителей этих поколений, включая аутентичность, визуальную привлекательность, краткость и интерактивность материалов. Поколение Z проявляет критичность, ценит реалистичность и социальную значимость UGC, тогда как поколение Alpha ориентируется на высокую динамику, игровые форматы и персонализированный опыт. Показано, что различия в медиапривычках и цифровой социализации определяют разные механизмы воздействия пользовательского контента, что необходимо учитывать брендам и медиаплатформам при разработке коммуникационных стратегий.

пользовательский контент, новые медиа, контент-маркетинг, поколения Z и Alpha

В эпоху цифровой трансформации восприятие контента коренным образом изменилось. Традиционные рекламные модели теряют эффективность, а ключевым фактором успеха становится аутентичность, источник которой – сам потребитель. По прогнозам WPP Media, в 2025 году на пользовательский контент придется более половины глобальной рекламной выручки, что знаменует переход инициативы от профессионального продакшена к «любителям»[1]. Рынок UGC-платформ оценивается в 9,85 млрд долларов, 92 % пользователей доверяют рекомендациям сверстников больше, чем брендам, а 79 % отмечают влияние UGC на покупки[2].

Особый интерес представляют поколения Z и Alpha, которые не только активно потребляют, но и создают пользовательский контент. Их медиаповедение и особенности восприятия требуют отдельного изучения, поскольку именно эти поколения формируют будущие тренды цифровой коммуникации [1]. Цель исследования – выявить особенности восприятия

[1] Буйлова В. «Любители» обгонят профессионалов по рекламным доходам – WPP Media // Adindex. 2025. 11 июн. URL: https://adindex.ru/news/tendencies/2025/06/11/334266.phtml (дата обращения: 15.04.2026).
[2] ВКонтакте изучила медиапривычки четырех поколений пользователей – альфа, зумеров, миллениалов и поколения X – и обнаружила заметный разрыв в способах потребления контента // Комсомольская правда. 2026. 02 https://www.kp.ru/daily/27756/5204288/ (дата обращения: 15.04.2026).

пользовательского контента поколениями Z и Alpha и определить их влияние на современные маркетинговые стратегии.

Поколение Z (рожденные примерно в 1997–2012 гг.) и поколение Alpha (с 2013 г.) являются «цифровыми аборигенами» – они выросли в среде, где интернет, социальные сети и мобильные устройства всегда были доступны. Однако, согласно исследованию ВК (2026), их стратегии потребления контента существенно различаются: Alpha выбирает «короткие сессии» (48 %) и лидирует в потреблении музыки, тогда как Z предпочитает длинные ролики и распаковки[2]. Ключевая мировоззренческая установка поколения Z – социальные сети как первичный источник информации.

По данным АРИР, зумеры составляют основу аудитории инфлюенс-маркетинга (36 %), но поколение Alpha активно наращивает присутствие (17 %)[3]. При этом исследователи отмечают парадокс: молодые потребители демонстрируют высокую покупательскую активность, но крайне низкую лояльность к брендам. Это создает новые вызовы для маркетологов.

Мотивация к созданию пользовательского контента принципиально различается у двух поколений. Поколение Z, выросшее в условиях экономической нестабильности, прагматично: они ориентированы на личный бренд и карьеру. Для них создание контента стало не подработкой, а трамплином для карьеры и рядовой профессиональной компетенцией. Поколение Alpha, напротив, руководствуется игровой логикой: 47 % представителей Alpha активно создают контент (у Z – только 22 %)[4]. Alpha «оживляет культуру через ремикс», рассматривая создание контента как игру и самовыражение, а не как инструмент достижения карьерных целей.

Восприятие UGC также имеет поколенческие различия. Для Z, с его финансовой тревожностью, обзоры и распаковки снижают риски перед покупкой. Они доверяют «равным для равных» – контенту, созданному похожими на них людьми, а не брендами. Для Alpha более значимы визуальные и игровые элементы: челленджи, AR-маски, короткие динамичные видео. Ключевым форматом для обоих поколений выступает короткое вертикальное видео, что требует от брендов адаптации к алгоритмической логике платформ [2].

---

[3] Ибушева М. Ключевыми платформами для работы с блогерами в 2026 году станут Telegram, и YouTube // Likeni.ru. 2025. 14 ноя. URL: https://www.likeni.ru/events/klyuchevymi-platformami-dlya-raboty-s-blogerami-v-2026-godu stanut-telegram-tiktok-i-youtube/ (дата обращения: 15.04.2026).

[4] Артемова А. Как молодежь меняет digital-культуру. Исследование ВКонтакте // Likeni.ru. 2025. 28 мар. URL: https://www.likeni.ru/events/kak-molodezh-menyaet-digital kulturu-issledovanie-vkontakte/ (дата обращения: 15.04.2026).

Обращение к пользовательскому контенту во многом обусловлено кризисом доверия к традиционной рекламе. По словам К. Никифоровой, UGC стал «инфраструктурой доверия» [3]. Потребитель ориентируется на чужой опыт, доверяя рекомендациям других больше, чем прямой рекламе. Согласно данным Influencer Marketing Hub, 72 % потребителей считают отзывы убедительнее бренд-контента[5].

Для поколений Z и Alpha этот фактор имеет особое значение. Пользовательский контент воспринимается ими как объективный, поскольку он неподконтролен бренду. Как подтверждают Усман и Виджая, UGC влияет на восприятие бренда именно через доверие. Присутствие бренда в UGC становится для молодых пользователей индикатором подлинности. Бренд, который обсуждается в сообществе, получает социальное признание. Для самого пользователя публикация контента о бренде – это акт самопрезентации, который, в свою очередь, усиливает его лояльность.

Эффективность UGC в восприятии поколений Z и Alpha объясняется следующими факторами:

- релевантность («равные для равных») – контент создается людьми из той же социальной среды;
- горизонтальные связи – доверие выстраивается не искусственно, а через сверстников;
- социальное доказательство – UGC является наглядным подтверждением качества или популярности продукта.

Анализ современной маркетинговой практики позволяет выделить ключевые факторы, определяющие успешность UGC в восприятии поколений Z и Alpha. Рассмотрим показательные кейсы.

Кейс Fresh Bar (2025): танцевальный челлендж в TikTok с Диларой Зинатуллиной и AR-маской. Результаты: 99,5 млн органических просмотров, 200 000 видео, 250 000 участников офлайн, +45 % подписчиков Telegram за две недели[6]. Кейс демонстрирует эффективность «повода для участия» с бесшовным переходом из интернета в реальную жизнь.

Кампания Rhode Beauty Хейли Бибер – ставка на культуру челленджей TikTok и формат «Get Ready With Me». Хэштеги #RhodeLips и #PeptideLipShape вызвали волну UGC, продукт стал «движением», собрав

[5] 5Шведова В. Социальные доказательства в емейл-маркетинге: от доверия к продажам // EMAILMATRIX. 2025. 23 сен. URL: https://emailmatrix.ru/blog/social-proof-email/ (дата обращения: 16.04.2026).

[6] 6От AR-масок до фестивалей: Fresh Bar построил воронку вовлечения для поколения Z // sostav.ru. 2025. 21 ноя. URL: https://www.sostav.ru/blogs/284292/71629 (дата обращения: 16.04.2026).

миллионы просмотров. Эксперты отмечают: «звездная мощь в сочетании с понятным контентом вдохновила высокую вовлеченность»[7].

Обобщение кейсов позволяет выделить факторы успеха UGC для восприятия поколениями Z и Alpha:

1. Вирусный потенциал – простота воспроизведения (Fresh Bar: простой танец, амбассадор-участник).

2. Алгоритмическая поддержка – короткие форматы с высоким удержанием получают преимущество в рекомендательных системах.

3. Низкий порог участия – AR-маска с 4 наклонами головы вовлекает даже неактивных пользователей.

4. Интеграция онлайн и офлайн – челлендж + фестивали создают целостный опыт.

5. Ко-креация – диалог с подписчиками и создание контента на основе их идей.

Однако восприятие UGC поколениями Z и Alpha сопряжено и с рисками. Утрата контроля над сообщением – ключевая проблема: негативный пользовательский контент распространяется так же вирусно, как и позитивный. Кейс Beauty Bomb показывает, что минимизировать риски можно через «вовлеченную модерацию» (диалог с сообществом). Без ресурсов на модерацию риск репутационных потерь крайне высок.

Особенности восприятия UGC поколениями Z и Alpha требуют пересмотра традиционных маркетинговых подходов:

1. От контроля – к диалогу. Бренды должны отказаться от монополии на высказывание и стать платформой для историй пользователей.

2. От профессионального продакшена – к экосистеме UGC. «Сырой», непрофессиональный контент воспринимается как более аутентичный.

3. Учет поколенческих различий. Для Z важны прагматичные обзоры, снижающие риски покупки; для Alpha – игровые механики и визуальные эффекты. Интеграция онлайн и офлайн. Молодые пользователи ценят бесшовный переход между цифровой и физической средой.

4. Баланс творчества и модерации. Необходимо выстраивать работу с комьюнити, поощрять ко-креацию, но при этом управлять репутационными рисками.

Пользовательский контент трансформируется в фундаментальный принцип отношений с аудиторией, особенно при работе с поколениями Z

[7] Лучшие примеры кампаний с участием влиятельных лиц в сфере красоты // Ecommerce Fastlane. 2025. 14 окт. URL: https://ecommercefastlane.com/ru (дата обращения: 19.04.2026).

и Alpha. Восприятие UGG этими поколениями характеризуется высоким доверием к «равным», низкой лояльностью к традиционной рекламе, предпочтением коротких вертикальных форматов и игровых механик. Бренды, создающие пространства для ко-креации и учитывающие поколенческие особенности восприятия, получают стратегическое преимущество. UGC становится мощным инструментом в современной маркетинговой модели, в которой пользователь выполняет функцию не только потребителя, но и соавтора.

Список используемых источников

1. Амзин А., Галустян А., Гатов В., Кастельс. М, Кульчицкая Д., Лосева Н., Паранько С., Паркс М., Силантьева О., Хаак В. Как новые медиа изменили журналистику. 2016 // под науч. ред. С. Балмаевой и М. Лукиной. Екатеринбург: Гуманитарный университет. С. 230.

2. Малков А. В. Трансформация моделей межличностного взаимодействия в условиях информатизации системы профессионального образования // Философия образования. 2012. № 4 (43). С. 82–88.

3. Никифорова К. UGC как инфраструктура доверия в цифровых продуктах // РБК Компании. 2026. 21 янв. URL: https://companies.rbc.ru/news/JJaaxtQKej/ugc-kak-infrastruktura-doveriya v-tsifrovyih-produktah/ (дата обращения: 16.04.2026).

УДК 330.16

РОЛЬ НЕМАТЕРИАЛЬНОГО ПООЩРЕНИЯ В ПОВЫШЕНИИ ВОВЛЕЧЕННОСТИ СОТРУДНИКОВ И СТУДЕНТОВ В ЭФФЕКТИВНОСТИ ТРУДОВОЙ И ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: АКЦЕНТ НА ПОКОЛЕНИЕ Z

О. П. Заболотник (студент группы РСО-33 СПбГУТ), posokhova.op@sut.ru
О. А. Посохова (преподаватель кафедры ЭД СПбГУТ)

В статье рассматривается роль нематериального поощрения в повышении вовлеченности сотрудников и студентов в эффективности трудовой и образовательной деятельности. Актуальность исследования обусловлена структурной трансформацией рынка труда и изменением доминирующих мотивационных паттернов в условиях цифровой экономики. Вступление поколения Z в профессиональную среду совпало с глобальной пандемией и массовой дистанциализацией трудовых процессов, что радикально изменило механизмы социализации в организациях. В условиях, когда организации вынуждены конкурировать за таланты в условиях «Большой отставки», непонимание специфики трансформации нематериальных стимулов приводит к снижению вовлеченности и росту текучести кадров среди молодых специалистов. Исследование механизмов «дезинтеграции» классического одобрения и формирования новых регуляторных практик представляет собой приоритетную задачу современного менеджмента.

поколение Z, нематериальное поощрение, трансформация рынка труда

Одной из основных особенностей текущего социально экономического контекста является повсеместное снижение концентрации внимания, вызванное условиями интенсификацией информационных потоков и цифровой нагрузки. В современных экономических реалиях и демографической ситуации особую значимость приобретает проблема повышения вовлеченности как сотрудников компаний, так и обучающихся студентов, что требует постоянной актуализации, поиска и применения инструментов мотивации в соответствии с чувствительностью аудитории к инструментам поощрения.

Актуальность исследования обусловлена структурной трансформацией рынка труда и изменением доминирующих мотивационных паттернов в условиях цифровой экономики. Вступление поколения Z в профессиональную среду совпало с глобальной пандемией и массовой дистанциализацией трудовых процессов, что радикально изменило механизмы социализации в организациях.

Традиционно зачастую ранее доминировал подход, в рамках которого финансовые стимулы рассматривались как ключевой инструмент мотивации людей, обеспечивающий достижение организационных целей и повышение производительности.

Цель исследования заключается в теоретическом обосновании и эмпирическом описании трансформации нематериальной мотивации особенно в контексте цифровой социализации поколения Z, выявлении специфических механизмов признания, альтернативных традиционным формам социального поощрения.

Понимание тонких различий в том, как различные поколения воспринимают внутренние и внешние вознаграждения, становится все более важным, так как многие компании стремятся максимизировать вовлеченность и удержание сотрудников. Упоминания и опыт работы с поколением зумеров отмечает тренд на частные увольнения. Ощутимое количество сотрудников увольняются в первый год работы. Значимыми мотивами отмечаются: преувеличенные ожидания относительно труда при недостаточном уровне оплаты труда и склонность к быстрой потере интереса к выполнению деятельности (около 80 % случаев смены работы). Кроме того, в 56 % случаев причиной является повышенная эмоциональная чувствительность [1].

В научной литературе указывается, что различия в мотивационных установках отличаются, в частности, более старшие возрастные группы в большей степени ориентированы на стабильность и устойчивость условий труда, тогда как молодые поколения придают большее значение нематериальным аспектам деятельности.

Согласно предыдущим исследованиям, миллениалы часто руководствуются чувством цели и стремлением к личностному развитию, рассматривая свою работу как способ воплотить свои идеалы и внести значимый вклад в общество.

Поколение миллениалов, как правило, рассматривают обучение как средство самосовершенствования и осмысленности труда, они часто ценят возможности, которые соответствуют их целям личного развития [2].

Особое внимание в рамках исследования уделяется именно представителям поколения Z, так как данная когорта сейчас активно выходит на рынок труда зачастую одновременно находясь и в роли обучающегося сегмента аудитории. В силу демографических причин именно это поколение

сейчас имеет влияние на трансформационные изменения рынка труда и образовательных проектов.

Современные исследования показывают, что для поколения Z характерна ориентация на такие мотивационные факторы, как саморазвитие, соответствие деятельности личным ценностям и смысловая изобретательность труда, что демонстрирует смещение в сторону внутренних форм мотивации [2]. Отмечается, что, когда сотрудники чувствуют, что их работа имеет моральную целостность, они становятся более мотивированными внутренне. Для поколения Z получение внутренних вознаграждений означает не только чувство компетентности, но обеспечение того, чтобы их труды создавали благотворное социальное воздействие. Внутреннее вознаграждение и восприятие моральной значимости труда рассматриваются как факторы, способствующие повышению вовлеченности и потенциально влияющие на удержание сотрудников поколения Z [3].

Таким образом, внутренние преимущества максимизируются, а более активное и заинтересованное отношение к обучению формируется, когда организации создают среду, в которой приоритет отдается обучению как для профессионального, так и для личностного развития.

Также авторы хотят отметить, что в эпоху нарастающего влияния развития цифровых экосистем и платформенной экономики наблюдается постепенное размывание границ между трудовой и образовательной деятельностью. Значительная часть современных организаций и особенно образовательных учреждений все активнее интегрируют элементы обучения в рабочие процессы, а также внедряют игровые механики и цифровые инструменты вовлечения, характерные для пользовательских платформ. В результате формируется единое поведенческое пространство, в котором деятельность индивида – независимо от ее формального статуса (работа или обучение) – строится на сходных мотивационных принципах.

Данная трансформация усиливает значимость нематериальных форм поощрения, таких как признание достижений, система цифровых рейтингов, бейджей, уровней, обратная связь и возможности самореализации. Использование геймификации и элементов микрообучения способствует поддержанию устойчивого интереса и вовлеченности, компенсируя снижение концентрации внимания и формируя внутреннюю мотивацию к продолжительной активности.

Работники поколения Z имеют иные взгляды на обучение и работу, чем предыдущие поколения. Следует отметить, что поколение Z с детства получало регулярные поощрения как в игровом, так и образовательном формате, что сформировало ожидания регулярных поощрений, как часть жизненной естественной парадигмы. Таким образом, нематериальные стимулы становятся универсальным инструментом повышения эффективности как трудовой, так и образовательной деятельности в условиях цифровой среды.

Отмечая зарубежный опыт, также необходимо отметить феномен великой отставки (великого увольнения), термин, введенный психологом и профессором менеджмента в Техасском университете Энтони Клотцем в 2021 году, когда он предсказал трендовую ситуацию, что COVID-19 приведет к тому, что люди массово будут уходить с работы [4]. Ключевыми факторами роста добровольных увольнений называются следующие: профессиональное выгорание, переоценка жизненных приоритетов, неудовлетворенность условиями труда и организационной культурой, а также недостаточное внимание со стороны работодателей к нематериальным аспектам мотивации, включая признание, обратную связь и возможности развития. Подобные процессы массовых увольнений сотрудников приобретают характер устойчивой тенденции, наблюдаемой в ряде стран, и отражают трансформацию трудовых установок в современных условиях. Вышеуказанные процессы могут трансформироваться в вызовы для работодателей, так как увольнения сотрудников увеличивают траты на привлечение и адаптацию новых специалистов. Сравнительный анализ показывает, что представители поколения X и миллениалы характеризуются более длительной занятостью в одной организации в среднем в 1,5–2 раза дольше, чем поколение Z [5].

Таким образом, наблюдаемые изменения на рынке труда отражают трансформацию мотивационных установок, в рамках которой нематериальные факторы приобретают все большее значение по сравнению с традиционными экономическими стимулами.

Понимание мотивации различных поколения имеет важное значение для создания позитивной и продуктивной рабочей среды. В реалиях смещения акцента в сторону внутренних мотивационных факторов – таких как саморазвитие и субъективная значимость труда – возрастает роль образовательных и организационных механик, способных использовать данные для установки и интегрировать их в практику управления персоналом.

Предварительные наблюдения авторов в образовательной практике указывают на ощутимую значимость нематериальных стимулов для поддержания интереса и активности студентов, что требует дальнейшего системного изучения.

Список используемых источников

1. Официальный сайт Коммерсантъ. Текучесть среди молодых специалистов поколения Z выше, чем у предыдущих поколений [Электронный ресурс]. URL: https://www.kommersant.ru/doc/7460137 (дата обращения: 26.04.2026).

2. Salvadorinho J., Ferreira C., Teixeira L., Hines P., Kumar M. From Gen Z to Boomers: Motivational drivers shaping Industry 5.0 and the future of work // Futures. 2025. URL: https://www.sciencedirect.com/science/article/pii/S0016328725001934 (дата обращения: 26.04.2026).

3. Krishna S., Agrawal S. Creative Performance of Millennials and Generation Z: What Matters More, Intrinsic or Extrinsic Rewards? // Administrative Sciences. 2024. Vol. 15, № 1. Art. 11. DOI: 10.3390/admsci15010011. [Электронный ресурс]. URL: https://www.researchgate.net/publication/387593152_Creative_Performance_of_Millennials_and_Generation_Z_What_Matters_More_Intrinsic_or_Extrinsic_Rewards

4. Официальный сайт РБК. Что такое «великое увольнение» и почему на Западе все чаще бросают работу. [Электронный ресурс]. URL:https://trends.rbc.ru/trends/education/62a489ee9a79475904a01ad1 (дата обращения: 22.04.2026).

5. Поколение Z на старте карьеры: что ожидать работодателям? // Finance: Theory and Practice. URL: https://finance-man.ru/index.php/journal/article/view/1646 (дата обращения: 26.04.2026).

Статья представлена научным руководителем, преподавателем кафедры ЭД СПбГУТ О. А. Посоховой.

УДК 330.34

ЦИФРОВЫЕ ЭКОСИСТЕМЫ КАК НОВАЯ ЭКОНОМИЧЕСКАЯ МОДЕЛЬ РАЗВИТИЯ КОМПАНИЙ

К. Э. Ильина (студент группы ИСТ-311), ilyina.ke@sut.ru

В статье рассматриваются цифровые экосистемы как новая модель развития компаний в условиях цифровизации экономики. Анализируются причины перехода бизнеса от традиционной модели специализации к экосистемному подходу, экономические преимущества данной модели, а также риски для бизнеса и потребителей. Рассматриваются примеры российских компаний, развивающих собственные цифровые экосистемы.

цифровая экономика, цифровые экосистемы, платформенная экономика, сетевые эффекты, конкуренция, цифровые платформы

Введение

В последние десятилетия мировая экономика переживает масштабную цифровую трансформацию. Развитие интернет-технологий, распространение смартфонов и рост объемов данных изменили структуру рынков и способы взаимодействия компаний с потребителями. Все больше экономической активности переносится в цифровую среду.

Одним из наиболее заметных явлений современной экономики стало формирование цифровых экосистем. Крупные компании все чаще выходят за пределы своей первоначальной специализации и объединяют различные сервисы в рамках единой цифровой платформы. В таких системах пользователь может получать доступ сразу к нескольким видам услуг – например, финансовым сервисам, медиаконтенту, электронной коммерции или транспортным приложениям.

Сущность цифровых экосистем

Понятие «цифровая экосистема» активно используется в современной экономической литературе, однако единого универсального определения данного термина не существует. В наиболее общем смысле цифровая экосистема представляет собой совокупность взаимосвязанных продуктов и сервисов, объединенных под единым брендом и функционирующих на основе общей технологической платформы.

Экосистема является многосторонней цифровой платформой, в рамках которой взаимодействуют несколько групп участников: пользователи, компании-партнеры и владелец платформы. Пользователи получают доступ к широкому спектру товаров и услуг в одной цифровой среде. Компании-партнеры могут использовать платформу как дополнительный канал продаж и продвижения своих продуктов. Владелец платформы, в свою очередь, получает доход от транзакций, рекламы, подписок и использования различных сервисов.

Развитие экосистем сопровождается сетевыми эффектами. Сетевой эффект возникает в ситуации, когда ценность платформы увеличивается по мере роста числа ее пользователей. Чем больше людей пользуются платформой, тем привлекательнее она становится для других пользователей и партнеров. Это приводит к ускоренному росту экосистемы и усилению ее позиций на рынке.

Еще одной важной особенностью экосистем является ориентация на пользователя. Компании стремятся создать такую цифровую среду, в которой клиент сможет решать как можно больше повседневных задач. Широкий набор сервисов внутри платформы позволяет удерживать пользователя и увеличивать время его взаимодействия с системой.

Классическая экономическая теория и переход к экосистемной модели

В основе традиционной экономической теории лежит идея специализации. Еще Адам Смит показал, что разделение труда повышает производительность. Позднее Давид Рикардо развил эту идею в теории сравнительных преимуществ: фирма должна специализироваться на том виде деятельности, где ее альтернативные издержки ниже, чем у конкурентов.

Однако развитие цифровых технологий и платформенной экономики существенно изменило условия функционирования рынков. Когда рынок становится зрелым, темпы роста спроса снижаются, а конкуренция усиливается. Особенно ярко это проявилось в телекоммуникационной сфере, где большинство потребителей уже имеют доступ к мобильной связи и интернету. В таких условиях расширение деятельности и выход на новые рынки становится одним из способов поддержания роста бизнеса.

Причины перехода компаний к экосистемной модели

Помимо насыщения рынков существует несколько экономических факторов, которые делают экосистемную модель особенно привлекательной для крупных компаний.

Во-первых, компании стремятся увеличить пожизненную ценность каждого пользователя. В экосистеме компания может предлагать пользователю сразу несколько сервисов и получать доход из разных источников. Во-вторых, развитие экосистем позволяет более эффективно использовать уже существующую пользовательскую базу, что значительно снижает маркетинговые и рекламные расходы. В-третьих, цифровые сервисы позволяют расширять бизнес с относительно низкими дополнительными затратами. Наконец, важным фактором является использование данных пользователей для предложения персонализированных товаров и услуг [1].

Особенности функционирования экосистем

Ключевой особенностью экосистем является бесшовный пользовательский опыт: единый идентификатор (SberID, Яндекс ID, MTS ID) обеспечивает доступ ко всем сервисам платформы без повторной регистрации. История предпочтений пользователя в одном сервисе влияет на рекомендации в другом, что усиливает персонализацию [2].

Единая программа лояльности служит инструментом удержания клиента: баллы или кешбэк, накопленные в одном сервисе, можно использовать в другом. Подписочные модели (МТС Premium, СберПрайм) предоставляют комплекс скидок сразу на весь спектр услуг.

Существенную роль играет сбор и анализ больших данных. Экосистема аккумулирует информацию о потребительском поведении пользователя из множества точек взаимодействия, что позволяет делать сверхточные персональные предложения и снижать кредитные риски. Наконец, часть базовых сервисов (доставка, такси) может функционировать с минимальной маржой ради привлечения широкой аудитории, тогда как высокомаржинальные направления (финтех, облачные сервисы, реклама) обеспечивают основную прибыль.

Преимущества и риски экосистем

Для пользователей цифровые экосистемы предоставляют ряд преимуществ: удобство использования сервисов через единую среду, снижение транзакционных издержек, доступ к программам лояльности и персонализированным предложениям. Вместе с тем существуют и риски. Эффект «запирания» (lock-in) затрудняет переход к конкурентам по мере роста числа используемых сервисов. Концентрация персональных данных в рамках одной платформы порождает опасения относительно конфиденциальности.

Доминирование крупных экосистем способно ограничивать конкуренцию и сокращать число альтернативных сервисов на рынке.

Для бизнеса преимуществами являются диверсификация источников дохода, снижение затрат на привлечение клиентов, повышение устойчивости и возможность инвестирования в инновации. Среди рисков выделяют высокие инвестиционные требования, сложность управления разнородными направлениями бизнеса, репутационные риски и угрозу монополизации рынка.

Примеры российских цифровых экосистем

Экосистемная модель активно развивается в России в финансовом, технологическом и телекоммуникационном секторах.

Наиболее показательным примером является Сбер [3]. Изначально являясь традиционным финансовым институтом, компания последовательно расширяла деятельность в нефинансовые сегменты. Сегодня экосистема Сбера охватывает электронную коммерцию, сервисы доставки, онлайн-кинотеатр, медицинские и образовательные платформы.

Яндекс [4] прошел путь от поисковой системы до полноценной цифровой платформы, включающей транспортные сервисы (Яндекс Такси), доставку еды и товаров, картографические сервисы, облачные технологии и медиаплатформы.

МТС [5], изначально оператор мобильной связи, развивает медиасервисы, финансовые продукты, облачные технологии и цифровые платформы, трансформируясь из поставщика инфраструктуры связи в многофункциональную цифровую экосистему.

Данные примеры демонстрируют, что конкуренция все чаще происходит между экосистемами, а не между отдельными компаниями.

Заключение

Таким образом, развитие цифровых экосистем отражает глубокие изменения современной экономики. Компании постепенно отходят от модели узкой специализации и переходят к созданию комплексных цифровых платформ, объединяющих множество сервисов. Экосистемная модель позволяет увеличивать прибыль, удерживать пользователей и усиливать конкурентные преимущества. Одновременно возникают риски монополизации рынка и проблемы защиты пользовательских данных. В будущем роль цифровых экосистем в мировой и российской экономике будет продолжать возрастать.

Список используемых источников

1. Муратова М. А., Саитов Р. Е. Цифровые экосистемы как новая модель развития крупнейших компаний. М.: Финансовый университет при Правительстве Российской Федерации, 2023.

2. Головко С. М. Цифровые экосистемы как новая модель ведения бизнеса в условиях турбулентности в экономике // Вестник Евразийской науки. 2023. Т. 15. № s2. URL: https://esj.today/PDF/17FAVN223.pdf (дата обращения: 03.04.2026).

3. Официальный сайт Сбер [Электронный ресурс] // Сбер. URL: https://www.sber.ru (дата обращения: 03.04.2026).

4. Официальный сайт Яндекс [Электронный ресурс] // Яндекс. URL: https://yandex.ru (дата обращения: 03.04.2026).

5. Официальный сайт МТС [Электронный ресурс] // МТС. URL: https://mts.ru (дата обращения: 03.04.2026).

Статья представлена научным руководителем, доцентом кафедры экономики данных, кандидатом экономических наук А. В. Исаковым.

УДК 004.75

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ БЛОКЧЕЙН В ЛОГИСТИКЕ И КОНТРАКТАХ

О. В. Калимуллина (к.э.н., доцент кафедры ЭД СПбГУТ)
Е. В. Сидорова (студент группы МБИ-2511 СПбГУТ), sidorova.ev@sut.ru

Блокчейн выступает перспективным инструментом трансформации глобальных логистических цепочек благодаря децентрализованной архитектуре, обеспечивающей прозрачность, неизменность данных и автоматизацию через смарт-контракты. Практические внедрения (IBM Food Trust, TradeLens, Walmart) подтверждают сокращение времени верификации данных на порядки, однако сдерживающими факторами остаются высокие затраты, ограниченная масштабируемость и отсутствие единых стандартов. Перспективы связаны с интеграцией технологии с IoT, ИИ и Big Data для создания устойчивой инфраструктуры международных поставок.

блокчейн, логистика, смарт-контракты, прозрачность, данные, цепочка поставок, транзакция

В современном мире, где международная торговля развивается стремительными темпами, а экономические связи между странами становятся все более тесными, особую значимость приобретают вопросы совершенствования логистических процессов и укрепления контрактных отношений. Существующие подходы к управлению поставками и оформлению договоров уже не справляются с растущими требованиями к скорости, безопасности и прозрачности операций.

Революционным решением этих проблем может стать технология блокчейн, которая изначально создавалась для работы с криптовалютами, но теперь демонстрирует впечатляющий потенциал в других сферах [1]. Ее главные преимущества заключаются в отсутствии единого центра управления, невозможности изменения уже записанных данных и полной открытости для всех участников системы [2].

В современных логистических цепочках участвует множество различных организаций: производители, транспортные компании, таможенные службы, дистрибьюторы и розничные продавцы. При этом традиционные системы отслеживания грузов часто страдают от недостатка прозрачности, задержек в обмене информацией и риска подделки документов. Блокчейн позволяет создать единую систему, где каждый участник может видеть полную картину движения товара, а все операции надежно защищены от фальсификации.

Практическое применение технологии уже приносит впечатляющие результаты. Так, платформа IBM Food Trust позволяет проследить путь продукта питания от производителя до полки магазина. Совместный проект

Maersk и IBM под названием TradeLens объединил более ста организаций в сфере морских перевозок [3, 4]. Особенно показателен опыт компании Walmart, которая благодаря внедрению блокчейн-системы сократила время проверки поставок продуктов с недели до считанных секунд [5].

Особую роль в логистических процессах играют смарт-контракты – программные коды, автоматически выполняющие условия договора при наступлении определенных событий. Они помогают автоматизировать оплату при доставке груза, контролировать соответствие товара заявленным характеристикам и следить за соблюдением сроков поставки [6].

Несмотря на очевидные преимущества, внедрение блокчейн-технологий сталкивается с определенными трудностями: высокими затратами на старте, сложностями интеграции с существующими системами и отсутствием единых стандартов. Однако перспективы развития этой технологии выглядят многообещающе благодаря ее интеграции с другими инновационными решениями, такими как интернет вещей, искусственный интеллект и системы обработки больших данных [7].

Для наглядной демонстрации различий между традиционными логистическими системами и блокчейн-решениями в таблице 1 представлено сравнительное исследование по ключевым параметрам эффективности.

ТАБЛИЦА 1. Сравнение традиционных и блокчейн-систем в логистике

Параметр	Традиционная система	Блокчейн-система
Прозрачность	Ограниченная, зависит от участников	Высокая, доступна всем участникам сети
Скорость обработки данных	Зависит от ручного ввода и согласования	Высокая, автоматизация процессов
Безопасность данных	Риск взлома централизованных баз данных	Высокая, криптографическая защита
Издержки на посредников	Высокие (агенты, банки, нотариусы)	Низкие, автоматизация через смарт-контракты
Возможность отслеживания	Ограниченная, возможны пробелы в данных	Полная, история всех транзакций доступна
Масштабируемость	Легко масштабируется, но с потерей контроля	Ограниченная у некоторых платформ, требует оптимизации
Затраты на внедрение	Относительно низкие	Высокие на начальном этапе

Сравнительный анализ данных таблицы 1 наглядно демонстрирует существенное преимущество блокчейн-систем в логистике, где полная прозрачность операций, высокая скорость обработки данных и криптографическая защита информации значительно превосходят показатели традиционных систем, несмотря на более высокие начальные затраты на внедрение и определенные ограничения масштабируемости некоторых платформ.

По мере развития нормативной базы и появления новых успешных кейсов применения блокчейн в логистике можно ожидать дальнейшего расширения сферы его использования и совершенствования существующих решений. Компании, планирующие внедрение технологии, должны тщательно проанализировать свои бизнес-процессы, оценить экономическую эффективность и обеспечить подготовку персонала. Важным фактором успеха становится также сотрудничество с отраслевыми ассоциациями и регуляторами для формирования единых стандартов применения блокчейн-технологий [8].

Будущее технологии блокчейн в логистике связано с постоянным совершенствованием существующих решений, расширением международного сотрудничества и демонстрацией все более убедительных примеров экономической эффективности. По мере накопления практического опыта и развития технологической базы потенциал этой инновации будет раскрываться все полнее, трансформируя традиционные подходы к управлению цепочками поставок и контрактными отношениями [9].

Список используемых источников

1. Тапскотт Д., Тапскотт А. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World 2-е изд. Нью-Йорк: Penguin Random House, 2018. 432 с.

2. Суон М. Blockchain: Blueprint for a New Economy 1-е изд. Себастопол: O'Reilly Media, 2015. 152 с.

3. Йенсен Т., Хедман Дж., Хеннингссон С. How TradeLens Delivers Business Value With Blockchain Technology // MIS Quarterly Executive. 2019. № 18(4). С. 221–243.

4. Топ-5 блокчейн проектов в сфере логистики [Электронный ресурс]. 2018. URL: digiforest.io/blog/blockchain-in-logistics (дата обращения: 03.04.2026).

5. Шарма М., Кумар П. Adoption of Blockchain Technology: A Case Study of Walmart / Sharma M., Kumar P. // Blockchain Technology and Applications for Digital Marketing. Херши: IGI Global, 2021. С. 210–225.

6. Сурьялакшми С., Элаяраджа М. Blockchain in Logistics: Opportunities and Challenges // Pacific Business Review International. 2021. № 13. С. 147-151.

7. Накамото С. Bitcoin: A Peer to Peer Electronic Cash System [Электронный ресурс]. 2008. URL: bitcoin.org (дата обращения: 27.03.2026).

8. Всемирный экономический форум. Building Blocks: How Blockchain Could Transform Logistics and Supply Chains [Электронный ресурс]. Женева: Изд-во ВЭФ, 2019. 24 с. URL: weforum.org (дата обращения: 28.03.2026).

9. Дивинах А. Blockchain Technology in Supply Chain Management // Journal of Technology and Systems. 2024. № 6. С. 42-56.

УДК 327.82

ГАСТРОДИПЛОМАТИЯ КАК ВАЖНЫЙ ФАКТОР МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

А. Е. Капелюжная (студент группы ЗР-32 СПбГУТ),
kapeliuzhnaia.ae@sut.ru

Гастродипломатия приобретает все большее значение в системе международных отношений благодаря тому, что она выступает эффективным инструментом «мягкой силы», не требующим прямого политического давления. Распространение национальных кухонь, развитие гастрономических брендов и участие в международных культурных мероприятиях позволяют государствам формировать положительный имидж и выстраивать устойчивые связи с зарубежной аудиторией.

мягкая сила, гастродипломатия, полилатеризм, парадипломатия, национальный бренд

Гастродипломатия – это довольно древнее ответвление дипломатии, берущее свое начало в Древней Греции, однако в современную эпоху только в конце XX века оформилось как один из инструментов «soft power» («мягкой силы») [1-6]. Пол Рокоуэр, исполнительный директор Levantine Public Diplomacy, в своей работе «Recipes for Gastrodiplomacy» впервые описал термин гастродипломатии как «акт завоевания сердца и разума через желудок» [2]. Леонид Владимирович Гелибтерман, президент Международного этногастрономического центра, предложил другое определение. По его мнению, гастродипломатия – это комплексная программа, целью которой является изменение имиджа страны (региона), его позиционирование (перепозиционирование) с помощью национальной (региональной) кухни. «Как явление, гастродипломатия развивается по двум трендам: гастродипломатический полилатеризм и гастрономическая парадипломатия», – писал он в своей новой книге «Гастрономическая дипломатия» [4]. Сегодня гастродипломатия играет важную роль в отношениях между странами, которые выстраивают и укрепляют свой имидж через кулинарию. Гастрономическая дипломатия приобретает все более выраженный политический характер, и определение Гелибтермана корректно описывает настоящее время. В данной статье рассматриваются основные концепции гастродипломатии (soft power, гастродипломатический полилатеризм, гастрономическая парадипломатия) и их влияние на международные отношения.

Концепция «soft power» существует в своем нынешнем виде благодаря Джозефу Наю, американскому политологу, который в конце XX века сформулировал идею о том, что государства могут добиваться желаемого не через принуждение («hard power»), а через привлекательность культуры, ценностей и политики [1]. В настоящее время во всеми мире наблюдается активное распространение «soft power»: японское аниме, Голливуд, культурные обменные программы (FLEX, UGRAD). Гастродипломатия также выступает одним из инструментов «мягкой силы», поскольку национальная кухня является частью культурного кода страны. Через состав блюд, их вид, вкус, обстановку в кафе или ресторане в головах людей формируется определенный образ страны, блюда которой они пробуют. Подобный подход соотносится с позицией Гелибтермана, который рассматривает гастродипломатию как инструмент формирования имиджа государства.

Гастродипломатия нередко проявляется не только в популяризации кухни, но и в тонкой символической работе с меню. Показательным примером является ужин в Blue House в Сеуле в 2017 году, устроенный в честь Дональда Трампа. Меню было продумано как система символов: гостям подали говяжьи ребра, приготовленные с использованием соевого соуса, выдержанного более 360 лет – возраста, сопоставимого с эпохой Бенджамин Франклин, одного из отцов американской государственности. Одновременно в меню присутствовал и более тонкий политический сигнал – блюдо с креветками, ассоциируемыми с водами у спорных островов Докдо (Токто), что отсылало к территориальным притязаниям Южной Кореи. Таким образом, даже отдельные элементы меню могут выступать инструментами символической дипломатии и передачи политических смыслов.

В рамках гастродипломатии Гелибтермана выделяются два направления: гастродипломатический полилатеризм и парадипломатия. Гастродипломатический полилатеризм подразумевает взаимодействие государственных структур с негосударственными акторами для организации разных павильонов и стендов с национальными продуктами питания и напитками на международных мероприятиях. Например, в рамках всемирных выставок, таких как World Expo, государства используют национальную кухню как инструмент презентации своей культуры, формируя позитивный образ страны в глазах международной аудитории. Парадипломатия – это уже участие субнациональных органов власти в международных отношениях с целью повышения имиджа региона на международной арене. Например, 16-17 августа 2025 года в Санкт-Петербурге в пространстве Севкабель Порт был проведен фестиваль китайской еды и культуры «Нихао Шифу 2025», где более чем 30 кулинаров представили блюда разных регионов, а также были

проведены концерты с выступлениями музыкантов, танцоров, лекции и мастер-классы по искусству чайных церемоний и каллиграфии [6]. Эти примеры наглядно демонстрируют разницу между полилатеризмом и парадипломатией. Первый представляет из себя государственную инициативу продвижения национального бренда, тогда как второй выражен в деятельности отдельных регионов для собственного позиционирования на международной арене.

С учетом возрастающей роли гастродипломатии в международных отношениях вполне логичным является формирование гастрономических брендов и их продвижение за рубежом, открытие ресторанов с национальной кухней, а также адаптация под вкусы местных жителей, как это, например, делают китайские кафе и рестораны по всему миру.

Таким образом, гастродипломатия в современных международных отношениях выступает не только как инструмент культурного обмена, но и как важный элемент формирования внешнеполитического имиджа государства. Через механизмы «мягкой силы», а также такие направления, как гастродипломатический полилатеризм и гастрономическая парадипломатия, государства и регионы получают возможность выстраивать устойчивые связи с зарубежными аудиториями. Эффективное использование национальной кухни, развитие гастрономических брендов и адаптация к культурным особенностям других стран способны стать важным фактором успешной внешней политики и укрепления позиций государства на мировой арене.

Список используемых источников

1. Най Дж. Гибкая сила: как добиться успеха в мировой политике / пер. с англ. М.: Тренды, 2006.

2. Rockower P. S. Recipes for gastrodiplomacy // Place Branding and Public Diplomacy. 2012. Vol. 8. № 3. P. 235–246.

3. Thailand’s gastro-diplomacy // The Economist. 2002. URL: https://www.economist.com/asia/2002/02/21/thailands-gastro-diplomacy (дата обращения: 03.04.2026).

4. Гелибтерман Л. В. Гастрономическая дипломатия. М., 2025.

5. Asia – Food as ambassador – Thailand’s gastro-diplomacy // The Economist. 2002. Vol. 362. № 8261. P. 84. URL: https://www.econbiz.de/Record/-/10007481476 (дата обращения: 03.04.2026).

6. Фестиваль китайской еды и культуры «Нихао Шифу 2025». URL: https://justpiter.ru/event/festival-nihao-shifu-2025/ (дата обращения: 03.04.2026).

Статья представлена научным руководителем, кандидатом исторических наук, доцентом кафедры ИРВ СПбГУТ Т. В. Молчановой.

УДК 614.2

ПОЛИТИКА США ПО ПРОТИВОДЕЙСТВИЮ ЧЕТВЕРТОЙ ВОЛНЕ ОПИОИДНОГО КРИЗИСА: ФЕДЕРАЛЬНЫЙ, ШТАТНЫЙ И МЕСТНЫЙ УРОВНИ (2021–2025 гг.)

А. А. Кобильняк (магистрант гр. ЗР-41м СПбГУТ), kobilnyak.aa@sut.ru

В статье рассматриваются особенности государственного реагирования на современный этап опиоидного кризиса в Соединенных Штатах Америки в 2021–2025 годах. Анализируются приоритеты федеральной стратегии, изменения в нормативном регулировании лечения зависимости, механизмы законодательной поддержки и роль штатов и местных сообществ в профилактике передозировок, расширении доступа к помощи и снижении смертности.

опиоидный кризис, США, федеральная политика, штаты, местные сообщества, синтетические опиоиды, фентанил, передозировки

Опиоидный кризис в США сохраняет значение одной из наиболее острых медико-социальных и управленческих проблем современности. По данным Центров по контролю и профилактике заболеваний США, в 2023 г. в стране произошло около 105 тыс. смертей от передозировки наркотиками, причем почти 80 тыс. из них были связаны с опиоидами. При этом около 69 % всех смертей от передозировки были обусловлены синтетическими опиоидами, главным образом нелегально произведенным фентанилом и его аналогами. Одновременно усилился полисубстантный характер передозировок, что делает кризис более сложным для регулирования, чем на предыдущих этапах его развития [1].

Современная модель государственного реагирования на опиоидный кризис в Соединенных Штатах Америки особенно отчетливо проявилась в 2021–2025 гг., когда федеральная политика получила более целостное институциональное оформление. Существенное значение имело представление в октябре 2021 г. Стратегии предупреждения передозировок Министерства здравоохранения и социальных служб США. В последующие годы федеральные меры были дополнены обновлением правил лечения, расширением финансовой поддержки штатов и племенных сообществ, а также новыми законодательными решениями [2].

Ключевым федеральным рубежом рассматриваемого периода стала Стратегия предупреждения передозировок 2021 г. В ней был закреплен ком-

плексный подход к кризису, основанный на четырех приоритетах: первичной профилактике, снижении вреда, доказательном лечении и поддержке восстановления. Тем самым федеральная политика окончательно сместилась от узкого контроля оборота веществ к более широкой модели общественного здравоохранения, в которой предотвращение смертности рассматривается в связи с лечением, социальной поддержкой и межведомственной координацией [2].

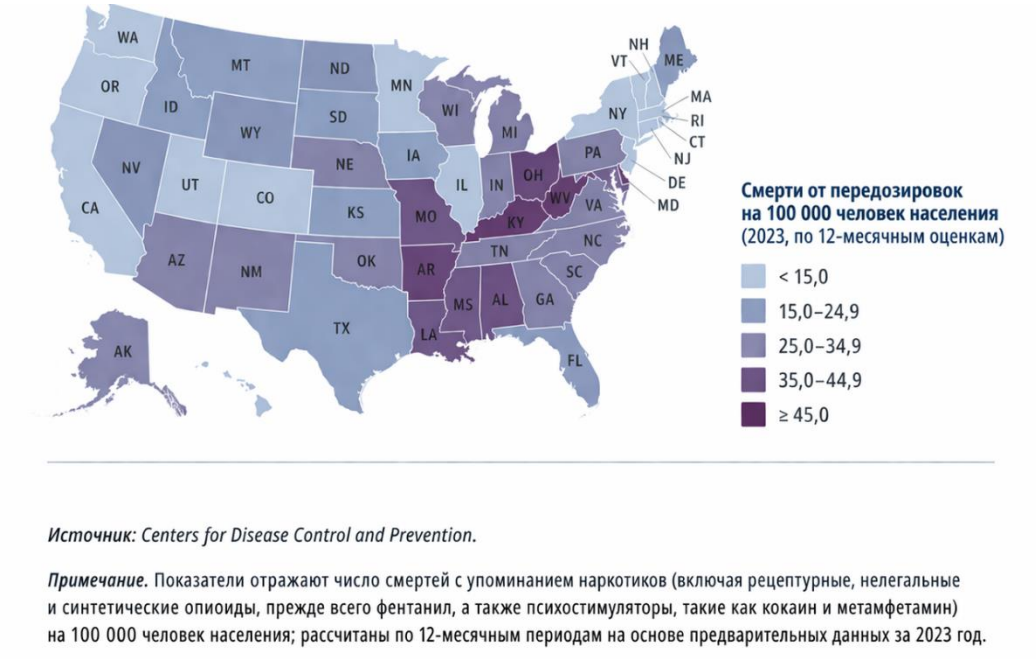
Следующим важным направлением стало обновление регуляторной базы лечения. В феврале 2024 г. Управление по вопросам психического здоровья и злоупотребления психоактивными веществами США выпустило итоговое правило «42 CFR Part 8», регулирующее деятельность программ лечения опиоидной зависимости. Новая редакция была направлена на расширение доступа к жизненно важным и научно обоснованным лекарственным средствам, снижение бюрократических барьеров, отказ от устаревших и стигматизирующих формулировок, а также усиление пациентоориентированного подхода. Правило вступило в силу 2 апреля 2024 г., а срок приведения практики в соответствие был установлен до 2 октября 2024 г. [3].

В 2025 г. федеральная политика получила дальнейшее развитие одновременно по двум направлениям. С одной стороны, были укреплены программы профилактики, лечения передозировок и поддержки психического здоровья через SUPPORT for Patients and Communities Reauthorization Act of 2025, то есть закон о продлении и укреплении программ помощи пациентам и сообществам. С другой стороны, был принят HALT Fentanyl Act, то есть закон о пресечении оборота смертельно опасных форм фентанила, окончательно закрепивший фентанилсвязанные вещества в перечне особо контролируемых веществ Списка I. Данные решения показывают, что федеральная политика 2025 г. сочетала две логики: медико-социальную и правоохранительную [4].

Однако эффективность федеральных решений во многом зависит от того, каким образом они реализуются на уровне штатов и местных сообществ. Это особенно хорошо видно на примере грантовых механизмов. В сентябре 2025 г. Министерство здравоохранения и социальных служб США через профильное агентство направило более 1,5 млрд долларов в рамках программ реагирования на опиоидный кризис для штатов и племенных сообществ. Эти средства предназначались для профилактики, обеспечения

препаратами для купирования передозировок, лечения, включая лекарственную терапию расстройства, связанного с употреблением опиоидов, и поддержки восстановления [5].

Территориальная дифференциация смертности от передозировок дополнительно подтверждает значимость штатного и местного уровней в реализации антикризисной политики США (рис. 1). Значительные различия показателей между штатами свидетельствуют о неоднородности факторов риска, включая доступность медицинской помощи, распространенность различных типов психоактивных веществ и социально-экономические условия. Это обусловливает необходимость гибкой адаптации федеральных мер на региональном и местном уровнях.



Источник: *Centers for Disease Control and Prevention.*

Примечание. Показатели отражают число смертей с упоминанием наркотиков (включая рецептурные, нелегальные и синтетические опиоиды, прежде всего фентанил, а также психостимуляторы, такие как кокаин и метамфетамин) на 100 000 человек населения; рассчитаны по 12-месячным периодам на основе предварительных данных за 2023 год.

Рис. 1. Смертность от передозировок наркотиками по штатам США, 2023 г.

Как видно из табл. 1, современная американская модель противодействия кризису имеет выраженный многоуровневый характер: федеральный центр формирует стратегию, правовые рамки и обеспечивает финансирование; уровень штатов осуществляет институциональную адаптацию принимаемых решений, распределение ресурсов и организацию системы оказания помощи; местные сообщества непосредственно реализуют профилактические, лечебные и восстановительные меры. Такая многоуровневая структура позволяет учитывать территориальные различия в масштабах и характере кризиса, а также повышает гибкость и адресность принимаемых мер. Взаимодействие указанных уровней власти и общественных институтов выступает ключевым условием эффективности антикризисной политики.

ТАБЛИЦА 1. Многоуровневая система противодействия опиоидному кризису в США в 2021–2025 гг.

Уровень политики	Основные инструменты	Практическая функция
Федеральный	Стратегия предупреждения передозировок 2021 г.; обновление правила 42 CFR Part 8 в 2024 г.; законодательные решения 2025 г.	Формирование общенациональных приоритетов, нормативных рамок и общих правил лечения и контроля
Уровень штатов	Реализация грантовых программ, адаптация инфраструктуры лечения, организация распределения препаратов для купирования передозировок	Перевод федеральных решений в региональные программы с учетом различий в потребностях и ресурсах

Практика реализации на субнациональном уровне показывает, что именно через штаты и местные сообщества федеральная стратегия приобретает прикладной характер. По данным Министерства здравоохранения и социальных служб США, с начала действия программы штатного реагирования почти 1,3 млн человек получили лечебные услуги, в том числе более 650 тыс. – лекарственную терапию расстройства, связанного с употреблением опиоидов; почти 1,5 млн человек получили услуги поддержки восстановления. Кроме того, получатели грантов распространили более 10 млн наборов препаратов для купирования передозировок, а такие препараты были использованы более чем в 550 тыс. случаев передозировки. Эти данные свидетельствуют о том, что основная нагрузка по непосредственному предотвращению смертности и сопровождению пациентов ложится именно на межуровневую сеть региональных и локальных исполнителей [5].

Вместе с тем анализ показывает, что современная модель противодействия кризису сохраняет внутренние противоречия. Ее сильной стороной является сочетание стратегического планирования, обновления правил лечения, финансовой поддержки регионов и законодательной активности. Однако сохраняются и ограничения: неравномерность административных возможностей штатов, различия в доступности лечения, а также тот факт, что кризис развивается уже не только как опиоидный, но и как полисубстантный.

Политика США по противодействию современной фазе опиоидного кризиса в 2021–2025 гг. приобрела более системный и многоуровневый характер. Федеральный центр задал стратегические ориентиры, пересмотрел регуляторные основы лечения, обеспечил финансовую поддержку штатам и племенным сообществам, а также продолжил законодательное оформление антикризисной повестки. В свою очередь, уровень штатов и местные сообщества стали пространством практической реализации этих решений. Это позволяет сделать вывод о том, что долгосрочная результативность американской модели зависит не только от содержания федеральных актов, но и от способности разных уровней власти и общественных институтов совместно снижать смертность, расширять доступ к лечению и обеспечивать устойчивое восстановление.

Список используемых источников

1. About Overdose Prevention. Overdose Prevention [Электронный ресурс] // Centers for Disease Control and Prevention. URL: https://www.cdc.gov/overdose-prevention/about/index.html (дата обращения: 26.03.2026).

2. U.S. Department of Health and Human Services Overdose Prevention Strategy [Электронный ресурс] // Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services. URL: https://aspe.hhs.gov/sites/default/files/ documents/101936da95b69acb8446a4bad9179cc0/overdose-prevention-strategy.pdf (дата обращения: 26.03.2026).

3. 42 CFR Part 8 Final Rule [Электронный ресурс] // Substance Abuse and Mental Health Services Administration. URL: https://www.samhsa.gov/substance-use/treatment/opioid-treatment-program/42-cfr-part-8 (дата обращения: 26.03.2026).

4. Fact Sheet: President Donald J. Trump Launches the Great American Recovery Initiative to Address the Addiction Crisis – The White House [Электронный ресурс] // The White House. URL: https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-launches-the-great-american-recovery-initiative-to-address-the-addiction-crisis/ (дата обращения: 26.03.2026).

5. HHS Provides More Than $1.5 Billion in State and Tribal Opioid Response Grants | HHS.gov [Электронный ресурс] // U.S. Department of Health and Human Services. URL: https://www.hhs.gov/press-room/hhs-state-tribal-opioid-response-grants-2025.html (дата обращения: 26.03.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры ИиРВ СПбГУТ А. В. Неровным.

УДК 005.8:663/664:681.5

В. В. Куликов (к.т.н., доцент, доцент кафедры СТЭД СПбГУТ)
Р. А. Сметанин (студент группы МБИ-2511з СПбГУТ), smetanin.ra@sut.ru

ОСНОВНЫЕ БИЗНЕС-ПРОЦЕССЫ ПРИ УПРАВЛЕНИИ ПРОЕКТАМИ В НПФ «ИМПУЛЬС»

В статье рассматриваются бизнес-процессы управления проектами в НПФ «Импульс» – компании-интеграторе, разрабатывающей АСУ ТП для молочных и пивных заводов. Предложен общий план управления проектом (ПУП), включающий пять этапов и Gate-модель с пятью контрольными точками, согласованные с группами процессов и областями знаний стандарта PMI PMBOK. Представленная схема утверждения проекта и разграничение ответственности между разработчиком и заказчиком позволяют минимизировать риски, связанные с частыми изменениями рецептур и удаленным тестированием. Внедрение разработанного подхода позволило снизить количество переделок на 30 % и сократить сроки приемочных испытаний.

PMI PMBOK, ANSI, управление проектами, Gate-модель, бизнес-процессы

Актуальность темы обусловлена цифровой трансформацией пищевой промышленности [1, 2], повышающей востребованность автоматизированных систем управления технологическими процессами (АСУ ТП). Однако проекты по разработке ПО для АСУ ТП сталкиваются со специфическими проблемами: частые изменения рецептур, необходимость удаленного тестирования, отсутствие у разработчика собственных монтажных мощностей и зависимость от сроков готовности оборудования заказчика. Возникает потребность в формализации управления проектами применительно к компаниям-системным интеграторам, к числу которых относится НПФ «Импульс». Отсутствие единого подхода приводит к задержкам, переделкам и финансовым потерям.

Объект исследования – деятельность НПФ «Импульс» по управлению проектами разработки АСУ ТП для молочных и пивных заводов. Предмет исследования – основные бизнес-процессы управления проектами, включая План управления проектом (ПУП), схему прохождения и утверждения проекта, а также их соответствие стандарту PMI PMBOK (ANSI) [3].

Цель работы – создание общего ПУП для НПФ «Импульс», включающего формализованное описание бизнес-процессов, схему утверждения и привязку к PMBOK. Для ее достижения решаются следующие задачи: описать структуру ПУП (этапы инициации, планирования, исполнения, мо-

ниторинга, завершения); представить Gate-модель с контрольными точками; сопоставить этапы ПУП с группами процессов PMBOK; выделить особенности тестирования (удаленный FAT, сухой тест, тесты на продукте).

Специфика деятельности НПФ «Импульс». Компания специализируется на проектировании АСУ ТП для молочных и пивных заводов в части разработки ПО, не выполняя монтаж оборудования (зона ответственности заказчика). Ключевые компетенции: закупка контроллеров Siemens (при необходимости), программирование PLC в TIA Portal, создание SCADA-конфигураций (PlantIT, SYFORA, WinCC), проведение удаленного Factory Acceptance Test (FAT), сухих тестов и тестов на продукте, анализ соответствия техническому заданию (ТЗ). Отсутствие монтажных мощностей накладывает особые требования к организации приемочных испытаний.

План управления проектом в НПФ «Импульс» включает пять последовательных этапов (рис. 1).



Рис. 1. План управления проектом

1. Инициация проекта: назначение менеджера проекта, аудит системы заказчика (типы контроллеров, версии ПО, требования к рецептурам и CIP-мойке).

2. Планирование работ: разработка пяти дочерних планов (план-график с WBS, коммуникации, качество, бюджет, риски). Формируется регистр типовых рисков (несовместимость ПО, задержка поставки контроллеров, изменение рецептур и др.).

3. Исполнение работ: разработка ТЗ на ПО, программирование PLC, создание SCADA-конфигураций, закупка оборудования, командообразование, контроль выполнения договора, графика и качества, работа по предупреждающим действиям.

4. Мониторинг: финальная сверка соответствия договору, графику и требованиям качества на завершающих стадиях.

5. Завершение: удаленный FAT, сухой тест на объекте, тесты на продукте, анализ соответствия ТЗ, устранение замечаний, подписание акта приемки, архивирование результатов.

Схема прохождения и утверждения проекта включает две взаимосвязанные схемы. Первая описывает внутренний цикл обработки заявки и формирования коммерческого предложения (КП) (рис. 2).

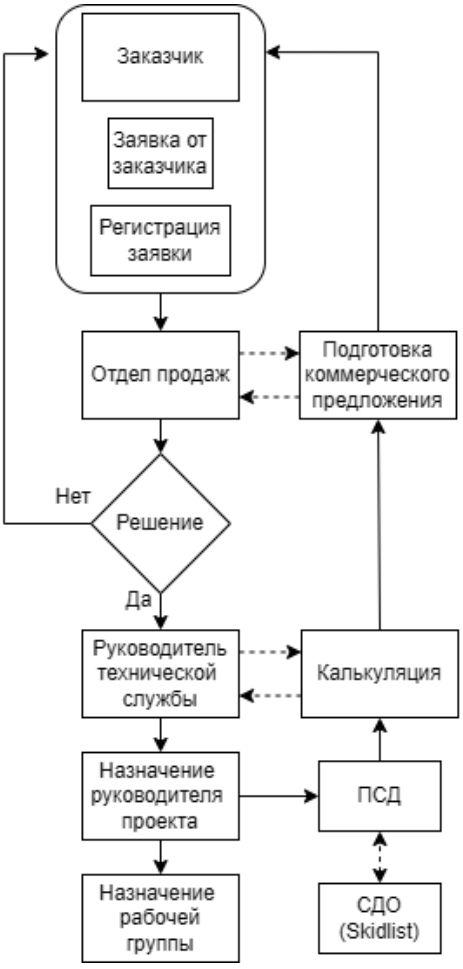


Рис. 2. Схема обработки заявки и формирования коммерческого предложения (КП)

Заказчик направляет заявку в отдел продаж, где принимается решение о целесообразности. При положительном решении руководитель техниче-

ской службы поручает руководителю проекта разработать проектно-сметную документацию (ПСД), после калькуляции затрат отдел продаж подготавливает финальное КП.

Вторая схема – Gate-модель с пятью контрольными точками (табл. 1), закрепленная в системе электронного документооборота.

ТАБЛИЦА 1. Контрольные точки утверждения проекта

Gate	Событие	Утверждающие	Выходной документ
1	Завершение инициации	Технический директор НПФ «Импульс»	Устав проекта
2	Утверждение планов (график, бюджет, ТЗ на ПО)	Руководитель проекта + главный технолог заказчика	Зафиксированное ТЗ
3	Успешное завершение FAT (удаленно)	Руководитель проекта + представители заказчика	Электронный протокол FAT
4	Успешное завершение сухого теста и тестов на продукте на объекте	Технический совет заказчика + менеджер проектов заказчика	Протокол сухого теста, протокол тестов на продукте
5	Анализ на соответствие ТЗ, закрытие проекта	Заказчик + Отдел продаж НПФ «Импульс»	Акт соответствия ТЗ, итоговый акт, архив

Соответствие PMI PMBOK (ANSI) [3,4]. Разработанный ПУП коррелирует с пятью группами процессов стандарта PMBOK. Анализ применения десяти областей знаний показал:

- управление интеграцией – связность этапов через единый план-график;
- управление содержанием – контроль изменений рецептур через утверждение ТЗ на Gate 2;
- управление сроками – учет критического пути (поставка контроллеров Siemens 16–20 недель);
- управление стоимостью – бюджетирование на основе смет и контроль освоенного объема (EVM);
- управление качеством – три уровня проверки (FAT, сухой тест, тесты на продукте);
- управление ресурсами – матрица ответственности RACI;
- управление коммуникациями – регламент статус-репортов и удаленных совещаний;

- управление рисками – регистр рисков с планами реагирования (резервные поставщики, альтернативные каналы связи);
- управление закупками – тендеры на поставку контроллеров, штрафные санкции;
- управление заинтересованными сторонами – карта влияния (главный технолог, начальник цеха, техсовет заказчика).

Практические результаты внедрения разработанного ПУП и Gate-модели в НПФ «Импульс»: снижение количества переделок ПО за счет раннего выявления несоответствий на удаленном FAT; сокращение продолжительности приемочных испытаний на объекте; уменьшение командировочных расходов.

Заключение. В НПФ «Импульс» выстроены формализованные бизнес-процессы управления проектами, соответствующие пяти группам процессов и десяти областям знаний PMI PMBOK. ПУП включает этапы инициации, планирования, исполнения, мониторинга и завершения. Gate-модель с пятью контрольными точками обеспечивает прозрачность утверждения. Особенностью компании является проведение удаленного FAT, сухих тестов и тестов на продукте при отсутствии собственного монтажа. Внедрение модели позволило снизить переделки на 30 % и сократить время приемочных испытаний на две недели. Представленный опыт может быть полезен руководителям проектов и техническим директорам организаций в сфере промышленной автоматизации пищевых производств.

Список используемых источников

1. Потехина Е., Золкин А., Кузьмин А. Проектирование адаптивных систем цифрового управления технологическими процессами в региональных секторах пищевой промышленности: учебное пособие для вузов. СПб.: Лань, 2025. 240 с.

2. Филатов В. В., Безпалов В. В., Женжебир В. Н. [и др.]. Проектирование информационных систем управления бизнес-процессами предприятий пищевой и перерабатывающей промышленности: учебник. М.: Университетская книга, 2021. 693 с.

3. Руководство к Своду знаний по управлению проектами (Руководство PMBOK®). 7-е изд. [Б. м.]: Project Management Institute, 2021. 368 с.

4. Павлов А. Н. Управление проектами на основе стандарта PMI PMBOK®. Изложение методологии и опыт применения: учебное пособие. 7-е изд. М.: Лаборатория знаний, 2025. 272 с.

УДК 004.8

ИЗМЕНЕНИЕ РОЛИ МЕНЕДЖЕРА В УСЛОВИЯХ ВНЕДРЕНИЯ НЕЙРОСЕТЕЙ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Б. Н. Лапков (студент группы МБИ-2511 СПбГУТ), lapkov.bn@sut.ru

В наше время активно рассматривается трансформация роли менеджера в условиях внедрения нейросетей и технологий искусственного интеллекта в бизнес-процессы. Анализируются изменения в управленческих функциях, требования к компетенциям руководителей и влияние цифровых технологий на процесс принятия решений. Отмечается, что внедрение нейросетей способствует автоматизации рутинных задач, повышению точности анализа данных и смещению роли менеджера в сторону стратегического управления и интерпретации информации. Рассматриваются также основные риски и ограничения, связанные с использованием искусственного интеллекта в управлении.

нейросети, искусственный интеллект, менеджмент, цифровая трансформация, управленческие решения, автоматизация

В условиях стремительного развития цифровых технологий и усиления конкуренции на глобальных рынках особую актуальность приобретает вопрос трансформации управленческой деятельности. Внедрение нейросетей и систем искусственного интеллекта (ИИ) оказывает существенное влияние на структуру бизнес-процессов и функции управления, что приводит к изменению роли менеджера в организации.

Традиционно менеджер выполнял функции планирования, организации, мотивации и контроля, сформулированные в рамках классической теории управления. Однако современные технологии позволяют автоматизировать значительную часть этих задач (табл. 1), особенно связанных с обработкой информации и контролем процессов [1].

Нейросети представляют собой один из ключевых инструментов искусственного интеллекта, способный анализировать большие объемы данных, выявлять скрытые закономерности и формировать прогнозы с высокой степенью точности [2]. Их применение в бизнесе охватывает такие области, как маркетинг, финансы, управление персоналом и логистика.

Внедрение нейросетей приводит к существенным изменениям в управленческих функциях. Во-первых, происходит снижение роли рутинного контроля, поскольку системы ИИ способны автоматически отслеживать показатели деятельности и выявлять отклонения. Во-вторых, возрастает значение аналитической функции, так как менеджер должен интерпретировать результаты, полученные с помощью алгоритмов [3].

ТАБЛИЦА 1. Сравнение роли менеджера до/после внедрения нейросетей

Параметр	Традиционный менеджмент	Менеджмент с использованием нейросетей
Принятие решений	Основано на опыте и интуиции	Основано на анализе данных и прогнозах
Обработка информации	Ручная, ограниченные объемы	Автоматизированная, большие данные
Контроль процессов	Постоянный ручной контроль	Автоматический мониторинг через ИИ
Скорость принятия решений	Низкая/средняя	Высокая
Роль менеджера	Контролер и администратор	Аналитик и стратег
Ошибки	Человеческий фактор	Ошибки алгоритмов и данных

Кроме того, меняется сам процесс принятия решений. Если ранее решения принимались на основе ограниченного объема данных и опыта руководителя, то сегодня они все чаще основываются на аналитике, сформированной нейросетями. Это повышает обоснованность решений, но одновременно создает зависимость от технологий [4].

В связи с этим формируются новые требования к компетенциям менеджеров. Ключевыми становятся цифровая грамотность, способность работать с данными, критическое мышление и умение взаимодействовать с интеллектуальными системами (табл. 2). Менеджер превращается в координатора взаимодействия между человеком и технологией, а также в стратегического лидера [5].

ТАБЛИЦА 2. Ключевые компетенции менеджера в условиях ИИ

Компетенция	Содержание	Значение
Цифровая грамотность	Понимание принципов работы ИИ и нейросетей	Позволяет эффективно использовать технологии
Data-driven мышление	Принятие решений на основе данных	Повышает точность управления
Критическое мышление	Оценка результатов работы алгоритмов	Снижает риски ошибок
Гибкость и адаптивность	Быстрая реакция на изменения	Важно в цифровой среде
Управление изменениями	Внедрение новых технологий в коллектив	Снижает сопротивление персонала
Этическое мышление	Понимание ответственности за решения ИИ	Обеспечивает устойчивое развитие

Несмотря на очевидные преимущества, внедрение нейросетей связано с рядом рисков. К ним относятся возможность ошибок алгоритмов, проблемы интерпретации результатов, а также этические вопросы, связанные с ответственностью за принимаемые решения. Кроме того, сотрудники могут оказывать сопротивление изменениям, что требует эффективного управления организационными преобразованиями [6].

Таким образом, внедрение нейросетей и искусственного интеллекта не приводит к исчезновению роли менеджера, а трансформирует ее. Основной акцент смещается с выполнения операционных функций на стратегическое управление, анализ данных и принятие комплексных решений в условиях высокой неопределенности.

Список используемых источников

1. Davenport T., Ronanki R. Artificial Intelligence for the Real World // Harvard Business Review. 2018. № 1. С. 108–116. [Электронный ресурс]. URL: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world (дата обращения: 05.04.2026).

2. Goodfellow I., Bengio Y., Courville A. Deep Learning. Кембридж: MIT Press, 2016. 775 с. [Электронный ресурс]. URL: https://www.deeplearningbook.org (дата обращения: 05.04.2026).

3. Brynjolfsson E., McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. Нью-Йорк: W. W. Norton & Company, 2014. 306 с. [Электронный ресурс]. URL: https://secondmachineage.com (дата обращения: 05.04.2026).

4. Jarrahi M. H. Artificial Intelligence and the Future of Work: Human-AI Symbiosis in Organizational Decision Making // Business Horizons. 2018. Т. 61. № 4. С. 577–586. [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/pii/S0007681318300556 (дата обращения: 05.04.2026).

5. World Economic Forum. The Future of Jobs Report 2023. Женева: World Economic Forum, 2023. 163 с. [Электронный ресурс]. URL: https://www.weforum.org/reports/the-future-of-jobs-report-2023 (дата обращения: 05.04.2026).

6. Raisch S., Krakowski S. Artificial Intelligence and Management: The Automation–Augmentation Paradox // Academy of Management Review. 2021. Т. 46. № 1. С. 192–210. [Электронный ресурс]. URL: https://journals.aom.org/doi/10.5465/amr.2018.0072 (дата обращения: 05.04.2026).

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом экономических наук, доцентом О. В. Калимуллиной.

УДК 659.113.25:316.77:004.738.5

ИСПОЛЬЗОВАНИЕ ДАННЫХ СОЦИАЛЬНЫХ СЕТЕЙ ДЛЯ ПРОГНОЗИРОВАНИЯ ПОТРЕБИТЕЛЬСКИХ ТРЕНДОВ

В. И. Масляк (студент группы РСО-2523 СПбГУТ), masliak.vi@sut.ru

Социальные сети в последние годы стали одним из наиболее значимых источников информации о поведении потребителей и их интересах. Пользователи регулярно публикуют отзывы, рекомендации и обсуждения различных товаров, формируя большие объемы пользовательского контента. Анализ подобных данных позволяет выявлять изменения потребительских предпочтений и определять формирование новых рыночных тенденций. Сравнительный анализ обсуждений различных категорий продукции позволяет выявить особенности пользовательской активности в социальных сетях.

социальные сети, анализ данных, потребительские тренды, маркетинг, пользовательская активность

В эпоху цифрового переустройства экономических систем социальные платформы перестают быть просто местами для общения. Сегодня они превращаются в стратегически ценные резервуары поведенческих данных. Каждый день миллионы пользователей генерируют колоссальные объемы контента: от текстовых отзывов и лайков до фотоотчетов о покупках и развернутых рекомендаций – и все это становится сырьем для анализа потребительских паттернов.

Подобные сведения фиксируют подлинные запросы целевой аудитории и дают возможность отслеживать колебания покупательского интереса во времени. Как показывают замеры ВЦИОМ, «социальные сети и мессенджеры уверенно вошли в топ-5 ежедневных источников информации россиян наравне с телевидением и новостными сайтами» [1]. Более того, сегодня покупатели все чаще сверяют свои решения с суждениями, полученными внутри онлайн-сообществ.

Социальные сети открывают уникальный канал для мониторинга покупательского поведения в режиме «здесь и сейчас». В противоположность классическим подходам, пользовательский контент рождается непроизвольно и поэтому точно передает живые реакции аудитории, минуя искажения, свойственные опросам.

Академические работы фиксируют, что «цифровая среда способствует формированию горизонтальных коммуникаций, при которых потребители становятся не только объектами, но и активными участниками маркетинговых процессов» [2]. В этом контексте контент, создаваемый пользователями, превращается в измеритель потребительских настроений и может выступать инструментом прогнозирования спроса.

С целью установить особенности расшифровки данных из социальных сетей был предпринят анализ пользовательского контента на примере двух продуктовых категорий: декоративной косметики и ноутбуков. Выбор сделан в пользу именно этих категорий, поскольку они расходятся по своей природе и по тому, как устроена логика принятия покупательских решений в каждой из них.

В категории декоративной косметики типичное наполнение социальных сетей строится вокруг двух доминант. Доминанта номер один – преобладание зрительных образов. Доминанта номер два – сильно выраженное эмоциональное участие со стороны тех, кто пишет посты. Человек берет камеру, снимает себя до и после использования продукта, делится субъективными впечатлениями и выкладывает ролик в профиль. Здесь ключевой вес имеют визуал и сторонние рекомендации. Именно это сочетание превращает циркуляцию информации не в плавный обмен, а в лавинообразное распространение. И на этой подвижной почве постепенно выкристаллизовывается то, что в перспективе превратится в устойчивый потребительский тренд.

Зеркально иная ситуация наблюдается, когда речь заходит о ноутбуках. Здесь царит не эмоция, а холодный расчет. Пользователи сосредоточены на сухих цифрах: сравнивают одну модель с другой, скрупулезно изучают объем оперативной памяти, тип процессора, разрешение экрана и время автономной работы. Данная схема иллюстрирует рациональный тип покупательского поведения, когда выбор делается на базе объективных сведений и взвешивания доступных альтернатив.

Результаты анализа структурированы в виде сравнительной характеристики пользовательского контента, представленной в таблице 1.

Приведенные в таблице 1 данные свидетельствуют о прямой зависимости: формат пользовательского контента определяется типом товара и сопряженной с ним моделью поведения покупателя.

ТАБЛИЦА 1. Различия пользовательского контента по типу товара

Критерий	Косметика	Ноутбуки
Тип восприятия	Эмоциональный	Рациональный
Контент	Визуальный	Аналитический
Основа доверия	Отзывы	Факты
Принятие решения	Импульсивное	Обоснованное
Роль соцсетей	Тренды	Информация

Суть полярности проста. Первый тип контента – царство эмоций и суждений. Второй тип – владения логики, цифр и проверяемых фактов. Выявленная глубокая разница – не академический курьез. Это рабочий инструмент для прогноза рыночных трендов. Постоянно фиксируя то, как именно трансформируется поведение сетевой аудитории, можно распознать самые ранние, еще не окрепшие сигналы – те самые предвестники, которые сулят скорые изменения в структуре того, что и в каких объемах будут покупать потребители.

Повышение плотности упоминаний товара – как правило, индикатор нарастающего интереса к нему. Повышение уровня вовлеченности указывает на расширение охвата и усиление интереса к категории. При этом эффективность прогнозирования напрямую зависит от учета специфики анализируемого сегмента.

Подход к анализу диктуется типом продукта. Там, где заправляют эмоции, главные источники инсайтов – визуальные образы и пользовательские советы. Там, где товар технически сложен, решающее значение переходит к содержанию дискуссий: техническим спецификациям и сравнительным рейтингам разных моделей.

Подводя итог, можно сказать следующее. В эпоху цифровой экономики тот, кто научился работать с массивами данных из социальных сетей, получает в руки надежный рабочий механизм. Устройство, которое не просто снимает показатели с рынка «здесь и сейчас», а позволяет забежать вперед и высмотреть, какой путь выберут покупательские настроения уже в самом ближайшем будущем.

Проведенный анализ подтверждает: то, что люди выкладывают в сеть, это не просто срез их сегодняшних вкусов. Это еще и ранний индикатор грядущих колебаний спроса, позволяющий увидеть их в зародыше. В основе

системной организации лежит прямая зависимость: природа продукта задает формат контента о нем. А из этого соотношения, в свою очередь, вытекают принципиально разные логики потребительского выбора – в разрезе различных товарных сегментов.

Если системно принимать во внимание описанные выше расхождения между сегментами, открываются две возможности. Во-первых, повышается точность аналитических моделей – они перестают работать по принципу «усредненной таблетки». Во-вторых, маркетинговые инструменты становятся точечными: они начинают адресно подгоняться под особенности каждого отдельно взятого рыночного сегмента. Практический выход от учета описанных расхождений сводится к двум позициям. Первая – аналитические модели выходят на более высокий уровень точности. Вторая – маркетинговые стратегии обретают возможность адресной подстройки под специфику каждого рыночного сегмента.

Технологическая траектория дальнейшего развития методов работы с социальными данными пролегает через внедрение машинного обучения и систем обработки естественного языка. Результатом станут автоматическое отслеживание зарождающихся трендов и кратный рост надежности прогнозов.

Представленное исследование позволяет утверждать, что при условии системного учета товарной специфики данные из социальных сетей превращаются в полноценный, высокоэффективный инструмент для исследования и предвидения потребительских трендов в условиях цифровой экономики.

Список используемых источников

1. Всероссийский центр изучения общественного мнения (ВЦИОМ). ВЦИОМ подвел основные итоги уходящего года в сфере медиа [Электронный ресурс] // ВЦИОМ. Новости. 2024. 18 дек. URL: https://wciom.ru/sobytie/vciom-podvel-osnovnye-itogi-ukhodjashchego-goda-v-sfere-media (дата обращения: 29.04.2026).

2. Чернышев А. Н. Цифровой маркетинг: теория и практика. М.: Юрайт, 2023. 256 с.

Статья представлена научным руководителем, деканом факультета СТЭД СПбГУТ, кандидатом политических наук, доцентом Д. В. Шутманом.

УДК 659.4

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА СОЗДАНИЕ РЕКЛАМНЫХ МАТЕРИАЛОВ

Д. А. Михеев (студенты группы РСО-46 СПбГУТ)
М. Ю. Слотин (студент группы РСО-46 СПбГУТ), slotin.mju@sut.ru

В статье рассматривается, как генеративные нейросети меняют процессы производства, персонализации и медиапланирования, снижая порог входа и одновременно повышая спрос на архитекторов смысла. Анализируются экономические эффекты, этические риски (авторское право, deepfake) и новая роль специалиста – от технического исполнителя к редактору и стратегу. Автор приходит к выводу, что будущее рекламы – за синергией человеческого интеллекта и вычислительной мощности алгоритмов.

искусственный интеллект (ИИ), рекламные материалы, креатив, генеративные нейросети, промпт-инжиниринг

Реклама всегда была сферой, где искусство тесно связано с технологиями. Если раньше разрыв между креативной концепцией и ее реализацией измерялся неделями, а бюджет на производство одного ролика мог исчисляться миллионами, то сегодня искусственный интеллект сокращает и бюджет, и дни работы. С точки зрения рекламного сообщества, происходящее просто очередной технологический сдвиг, как это было с переходом от печати к телевидению. В этой статье мы рассмотрим, как ИИ влияет на создание рекламных материалов, разберем новые роли на рынке, этические дилеммы и ответим на главный вопрос: искусственный интеллект – это замена специалиста или его инструмент?

Еще пять лет назад использование ИИ в рекламе ограничивалось программной покупкой – автоматической покупкой медийной рекламы на основе данных о поведении пользователя. Искусственный интеллект отвечал за доставку сообщения, но не за его содержание. Сегодня ситуация кардинально изменилась. Генеративные нейросети: Midjourney, DALL-E, Sora, ChatGPT и их локальные аналоги, стали полноценными инструментами креативного производства.

С точки зрения рекламного производства, выделяются три этапа, где ИИ уже стал мейнстримом:

Генерация идей. Нейросеть не просто быстро думает, она способна обрабатывать терабайты данных о рынке, конкурентах и культурном контексте за секунды. Креативные агентства используют LLM (большие языковые модели) для брейнштorма, где машина предлагает неожиданные комбинации смыслов, отсекая заведомо провальные гипотезы на основе исторических данных.

Визуализация и продакшн. Это самый заметный этап. Раньше, чтобы сделать качественный фото- или видеоряд, требовалась команда из продюсеров, операторов, режиссеров. Сегодня арт-директор с навыками промпт-инжиниринга способен создать сотню вариантов креативов еще до того, как будет подписан договор с продакшн-студией [1].

Адаптация и локализация. Глобальные бренды столкнулись с проблемой масштабируемости креатива. Сделать 100 уникальных видеороликов для разных регионов с разными культурными кодами ранее было экономически нецелесообразно. ИИ-инструменты например: синтез речи и генерация фонов, позволяют автоматически адаптировать один ролик на десятки языков, меняя внешность актеров, тексты на вывесках и фоновую атрибутику под конкретный рынок [2].

С точки зрения рекламодателя или клиента, главное влияние ИИ – это демократизация доступа к качеству. Раньше порог входа в телевизионную или наружную рекламу был высоким. Теперь малый бизнес может создавать видеоролики с дорогой картинкой при помощи нейросетей, не имея бюджета уровня больших компаний.

Однако у этого феномена есть и обратная сторона. Мы наблюдаем девальвацию рутинного труда. Ретушеры, фотографы предметной съемки, линейные продюсеры и даже некоторые копирайтеры теряют рынок. Простые задачи, которые раньше кормили целые отделы, теперь решает один специалист, владеющий связкой ChatGPT + Midjourney + Photoshop. Но падение спроса на технических специалистов сопровождается ростом спроса на архитекторов смыслов. Рекламный рынок сегодня платит не за умение работать кистью или мышкой, а за умение формулировать запрос (промпт), управлять контекстом и выстраивать стратегию [3].

Классическая реклама всегда была монологом. Бренд создавал одно сообщение для миллионов. ИИ меняет эту концепцию на диалог и даже индивидуальную настройку.

Технологии динамического креатива на базе ИИ позволяют собирать рекламный баннер или видеоролик в реальном времени из «кубиков»: текста, фона, изображения товара, призыва к действию. Система анализирует:

- погоду за окном пользователя (холодно – показываем горячий кофе, жарко – холодный латте);
- историю просмотров (пользователь искал красные кроссовки – в креативе будут красные кроссовки, а не синие);
- геолокацию (на билборде в центре Москвы – один визуальный ряд, на остановке в регионе – другой, учитывающий локальный контекст).

Это ведет к тому, что понятие рекламный материал размывается. Теперь это не статичный файл, а живой организм, который подстраивается под зрителя в миллисекунду. С точки зрения эффективности, CTR (кликабельность) таких кампаний часто в 2–3 раза выше, чем у статичных аналогов.

Наиболее ожесточенные споры в профессиональном сообществе вызывает вопрос: «Разрушит ли ИИ креативность?».

Авторы считают, что ИИ не убивает креативность, он убивает посредственность. Раньше агентства могли «продавать» клиентам средние идеи, обосновывая их сложностью производства. Теперь клиент может сам сгенерировать и получить 50 вариантов за минуту.

Новая роль специалиста по рекламе – главный редактор. Если раньше ценность заключалась в том, чтобы создать идею из ничего, то теперь ценность заключается в том, чтобы отобрать лучшую идею из тысячи сгенерированных, доработать ее, проверить на соответствие юридическим нормам, бренд-безопасности и этике.

Авторы видят зарождение новой специализации – Промт арт директор. Это человек, который:

- понимает психологию восприятия;
- знает архитектуру нейросетей (какая сеть лучше рисует текстуры, а какая – людей);
- владеет методами пост-обработки, чтобы убрать типичные ошибки ИИ (неестественные руки, странные глаза, искаженные логотипы).

Такое явление, как нейросети, вносят коррективу в рекламное сообщество, и несмотря на плюс, также привносит множество новых проблем. Но мы поговорим только об основных.

Проблема 1: Авторское право и уникальность.

Нейросети обучаются на миллиардах изображений, часто взятых без согласия авторов. Сейчас по всему миру идут судебные процессы, которые

определят будущее индустрии. Рекламные агентства уже сейчас вынуждены прописывать в договорах с клиентами гарантии использования генеративных моделей, чтобы не получить иск за использование стиля известного художника в коммерческом креативе.

Проблема 2: Глубокая фальсификация.

Возможность подделать голос и внешность человека с помощью ИИ. Уже были случаи, когда создавались рекламные интеграции с участием звезд, которые этого не одобряли, или использовался синтез голоса диктора без лицензии. Для индустрии это оборачивается ростом затрат на юридическую верификацию и разработку цифровых водяных знаков.

Проблема 3: Серая зона правды.

ИИ может генерировать несуществующие события, места и свойства товаров. Если раньше реклама должна была соответствовать закону «О рекламе» (в РФ – ФЗ № 38), где запрещена недостоверная информация, то сейчас возникает риск создания слишком идеального продукта. Потребитель получает рекламу, где шоколад течет неестественно красиво, а кожа лица сияет невозможным светом – и это уже формирует искаженные ожидания и недоверие.

Подводя итог с точки зрения перспектив развития рекламного рынка, можно выделить три сценария, которые будут доминировать в ближайшие 3–5 лет.

Рост агентств, где работает всего один специалист. ИИ снижает барьеры для предпринимательства в рекламе. Один специалист, владеющий ИИ-инструментарием, сможет предоставлять полный цикл услуг (стратегия + креатив + медиаплан + аналитика), который раньше был доступен только штату из 10–15 человек. Это приведет к фрагментации рынка: крупные холдинги будут конкурировать с армией фрилансеров.

Конвергенция креатива и аналитики. Раньше специалисты говорили на разных языках. ИИ становится переводчиком. Будущие рекламные платформы будут позволять создавать креатив прямо в интерфейсе медийного кабинета, тут же тестируя его на фокус-группах из цифровых аватаров до того, как потрачен реальный бюджет.

Эмоциональный интеллект как последний бастион. Человеческий фактор останется там, где требуется глубокое понимание культурного контекста, табу и эмпатии. ИИ может сгенерировать, но он не знает, как это отразится на репутации бренда в конкретной политической или социальной

среде. Креативные директора, которые смогут сочетать скорость ИИ с человеческой мудростью и чувством этики, станут главной ценностью рынка.

Влияние искусственного интеллекта на создание рекламных материалов сложно переоценить. С точки зрения рекламы, это не просто очередной инструмент вроде фотошопа, это изменение всей индустрии. Мы движемся от экономии ресурсов к экономии времени и, наконец, к экономии внимания. Рекламный материал перестает быть конечным продуктом и превращается в гибкий поток данных, адаптирующийся под контекст.

Победит в новой реальности не тот, кто запретит ИИ или будет игнорировать его, а тот, кто перестроит процессы. Рекламодателям придется пересмотреть бюджеты, перераспределив средства с линейного производства на технологическую инфраструктуру и компетенции промпт-инжиниринга. Искусственный интеллект не отменил главного принципа рекламы: «Нужно продавать то, что нужно людям, в том месте и в то время, когда они готовы купить». Но он дал нам возможность делать это настолько точно и красиво, как не могли себе представить даже футурологи десятилетие назад.

Список используемых источников

1. Рынок видеопродакшена: как ИИ меняет правила игры в рекламе // ФедералПресс. 2025. 28 ноября. URL: https://fedpress.ru/news/77/society/3414130 (дата обращения: 26.03.2026)

2. Короткевич Д. Тренды в SMM – 2026: что будет работать в соцсетях / Д. Короткевич // Markway. 2025. 27 ноября. URL: https://markway.ru/blog/trendy-v-smm-2026-chto-budet-rabotat-v-soczsetyah/ (дата обращения: 26.03.2026)

3. Генерация продвижения: как применение ИИ меняет рекламный рынок / А. Мирidонов // Коммерсантъ. 2026. 23 января. URL: https://www.kommersant.ru/doc/8361860 (дата обращения: 26.03.2026).

Статья представлена научный руководителем, кандидатом политических наук, доцентом Д. В Шутманом.

УДК 334.7

СОТРУДНИЧЕСТВО ГОСУДАРСТВА И БИЗНЕСА В СФЕРЕ КРЕАТИВНОЙ ЭКОНОМИКИ КИТАЯ

Т. В. Молчанова (к.и.н., доцент каф. ИиР СПбГУТ)
И. Ю. Чернокозов (студент группы ЗР-32 СПбГУТ),
chernokozov.iiu@sut.ru

Развитие креативной экономики в Китае приобретает все более важное значение в условиях цифровой трансформации и перехода к инновационной модели хозяйствования. Повышенное внимание к данной сфере обусловлено тем, что креативные индустрии формируют значительную добавленную стоимость, стимулируют технологическое развитие и способствуют укреплению национальной конкурентоспособности. Активное участие государства в поддержке данного сектора создает благоприятные условия для взаимодействия бизнеса и публичных институтов.

креативная экономика, государственно-частное сотрудничество, креативные индустрии, государственные инвестиции, субсидии, анимация, видеоигры, цифровая экономика

Креативная экономика Китая занимает важное место в системе национального хозяйства, выступая одним из наиболее быстрорастущих направлений, оказывающих существенное влияние на экономическое развитие, технологический прогресс и укрепление культурных позиций страны в мире [1]. В условиях цифровой трансформации и перехода к инновационной модели роста развитие креативных индустрий стало рассматриваться в Китае не только как источник прибыли, но и как важный инструмент модернизации экономики, расширения внутреннего спроса и усиления культурного влияния государства за рубежом [1]. Особенность китайской модели заключается в активном участии государства в формировании институциональной среды, финансировании отрасли и регулировании ее ключевых направлений, при этом значительная часть практической реализации сосредоточена в руках частного бизнеса [1].

Креативная экономика в Китае охватывает широкий круг отраслей, включающих цифровые медиа, кино, дизайн, рекламу, анимацию, игровую индустрию, издательское дело, культурный туризм и производство цифрового контента [1]. В отличие от западных моделей, где развитие креативных индустрий в большей степени определяется частной инициативой и рыночной конкуренцией, в Китае ключевую роль играет государство, задающее стратегические ориентиры и формирующее условия для роста [1]. Такой

подход связан с особенностями китайской экономической системы, в которой рыночные механизмы сочетаются с долгосрочным государственным планированием [2]. Именно поэтому развитие креативной экономики в КНР осуществляется в логике управляемой модернизации, при которой частный сектор сохраняет коммерческую инициативу, но действует в рамках государственных приоритетов [1].

Одним из наиболее значимых инструментов государственной поддержки стало создание специализированных механизмов финансирования креативного сектора. Важнейшее место среди них занимает China Cultural Industry Investment Fund – государственный инвестиционный фонд, ориентированный на поддержку культурных и креативных проектов [3]. Его деятельность направлена на финансирование перспективных компаний в сфере цифрового контента, киноиндустрии, анимации, новых медиа и культурных технологий [3]. В отличие от традиционного бюджетного субсидирования, данный фонд функционирует как инвестиционный инструмент, сочетающий государственное участие с рыночными механизмами отбора и сопровождения проектов [3]. Это позволяет не только поддерживать отрасль финансово, но и повышать ее инвестиционную дисциплину, ориентируя компании на коммерческую устойчивость и рыночную эффективность [3].

Значительная роль в развитии креативной экономики Китая принадлежит системе адресных субсидий, предоставляемых государством отдельным сегментам отрасли. Наиболее активно меры поддержки применяются в анимационной и игровой индустрии, которые рассматриваются как стратегически значимые направления цифровой экономики [4]. Государственная поддержка в этой сфере включает налоговые льготы, гранты, компенсации части производственных затрат, субсидии на экспорт цифровой продукции, а также региональные программы стимулирования студий, работающих в области анимации и видеоигр [4]. Подобный подход позволил Китаю в сравнительно короткие сроки сформировать крупный и конкурентоспособный рынок цифрового развлекательного контента, ориентированный как на внутреннего потребителя, так и на внешние рынки [5].

Особое место в данной системе занимает игровая индустрия, ставшая одним из наиболее прибыльных сегментов китайской креативной экономики [6]. Ее развитие во многом обеспечивалось взаимодействием государства и крупных частных корпораций, прежде всего Tencent и NetEase, которые сумели выстроить устойчивую модель коммерциализации цифрового

контента в условиях жесткого государственного регулирования [6; 7]. Частный бизнес в данном случае выступает не только как производитель и инвестор, но и как основной технологический драйвер отрасли, обеспечивающий разработку платформ, цифровую инфраструктуру, продвижение контента и его интеграцию в международные рынки [6]. Государство, в свою очередь, сохраняет контроль над нормативной средой, лицензированием, цензурной политикой и стратегическим распределением ресурсов [4]. Такая модель позволяет сочетать высокую рыночную динамику с институциональной управляемостью [1].

Сходный механизм действует и в анимационной индустрии, развитие которой в Китае рассматривается не только как экономическая, но и как культурно-политическая задача [4]. Поддержка анимационных студий осуществляется через систему субсидий, льготного налогообложения, государственных заказов и программ продвижения национального контента [4]. Это связано с тем, что анимация в китайской модели рассматривается как важный инструмент формирования культурной идентичности, продвижения национальных ценностей и укрепления «мягкой силы» государства [1]. В результате государственная поддержка в данном сегменте направлена не только на стимулирование производства, но и на повышение качества культурного продукта, его экспортной привлекательности и идеологической управляемости [4].

Вместе с тем китайская модель взаимодействия государства и бизнеса в сфере креативной экономики имеет не только преимущества, но и ограничения. Ее сильной стороной является высокая концентрация ресурсов, способность быстро масштабировать перспективные направления и формировать крупные национальные компании, конкурентоспособные на мировом рынке [1]. Однако значительная зависимость отрасли от государственной регуляторной политики делает ее чувствительной к административным ограничениям, цензурным барьерам и изменениям политических приоритетов [1]. Кроме того, высокая степень контроля над содержанием креативного продукта ограничивает свободу творческого производства и сужает пространство для независимых инициатив [2].

Таким образом, сотрудничество государства и бизнеса в сфере креативной экономики Китая представляет собой устойчивую модель управляемого партнерства, основанную на сочетании государственного стратегического планирования и рыночной активности частного сектора [1].

Государство формирует институциональные условия, финансирует приоритетные направления и задает рамки развития, тогда как бизнес обеспечивает технологическую динамику, коммерциализацию и масштабирование креативного продукта [3]. Подобная модель позволила Китаю превратить креативные индустрии в один из значимых элементов национального экономического роста и инструмент укрепления своих позиций в глобальном культурном и цифровом пространстве [8].

Список используемых источников

1. Логунцова И. В. Особенности креативной экономики Китая // Государственное управление. Электронный вестник. 2023. № 98. С. 21–30.

2. Гумерова Г. И. Цифровые платформы креативных индустрий: опыт России и Китая // Проблемы экономики и юридической практики. 2024. Т. 20. № 2. С. 97–104.

3. China Cultural Industry Investment Fund [Электронный ресурс]. URL: http://www.ccif.com.cn (дата обращения: 27.04.2026).

4. Министерство культуры и туризма Китайской Народной Республики [Электронный ресурс]. URL: https://www.mct.gov.cn (дата обращения: 27.04.2026).

5. Государственное статистическое управление Китайской Народной Республики [Электронный ресурс]. URL: https://www.stats.gov.cn (дата обращения: 27.04.2026).

6. Tencent Holdings Limited. Annual Report 2023 [Электронный ресурс]. URL: https://www.tencent.com/en-us/investors.html (дата обращения: 27.04.2026).

7. NetEase, Inc. Annual Report 2023 [Электронный ресурс]. URL: https://ir.netease.com (дата обращения: 27.04.2026).

8. UNCTAD. Creative Economy Outlook 2022 [Электронный ресурс]. URL: https://unctad.org/publication/creative-economy-outlook-2022 (дата обращения: 27.04.2026).

УДК 328.184

ЛОББИСТСКАЯ ДЕЯТЕЛЬНОСТЬ: ПОНЯТИЕ И ЦЕЛИ РЕГУЛИРОВАНИЯ

М. М. Набиев (студент группы РСО-2524 СПбГУТ), nabiev.mm@sut.ru
Д. В. Шутман (к.п.н., доцент, декан факультета СТЭД СПбГУТ)

История института лоббизма – постепенный процесс, который обусловлен комплектом различных факторов, нацеленных на урегулирование отношений тех, кто стремится извлечь пользу от государства, хотя развитие этого института охватывает период от Средневековья до наших времен.

Слово «лоббизм» происходит от английского слова lobby – «коридор». Изначально это понятие описывало неформальные встречи политиков в коридорах для обсуждения актуальных вопросов, что по сути являлось «коридорной политика».

По мнению авторов, Э. Войтенко и А. Парфенчикова сформулировали одно из самых понятных и лаконичных определений лоббизма [1, 2]:

«Лоббизм – это один из элементов политической системы государства, который отвечает за поддержание ее общего развития и стабильности» [2].

Более глубокое и подробное определение сформулировал А. С. Чертков: «Лоббизм – институт представительства, подчиненный нормам общественного взаимодействия; набор специальных технологий, которые в совокупности составляют лоббистскую деятельность, направленную на продвижение интересов отдельных групп в органах государственной или муниципальной власти с целью влияния на принятие политических и иных других решений, влияющих на деятельность субъектов экономической или политической деятельности» [1].

Авторы продемонстрируют «лоббизм» в системе понятий современного интернет-пользователя, чтобы показать, на сколько обширна сфера влияния института лоббизма (рис. 1).

Существуют два подхода к сфере лоббистского влияния:

1. Сфера лоббистского влияния ограничивается только органами законодательной власти.
2. Сфера лоббистского влияния распространяется и на законодательную, и на исполнительную власть, как в Америке.



Рис. 1. «Лоббизм» в системе понятий современного интернет-пользователя [1]

Традиции лоббизма начинаются с западноевропейских стран и США. Это сфера скрытого воздействия на формирование политических решений, оказывания давления как на законотворческую деятельность, так и на общественность.

Самые важные законы, принятие которых оказали существенное влияние на развитие института лоббизма:

1946 год – в США был принят первый закон о лоббизме «Закон о федеральном регулировании лоббистской деятельности». Закон закрепил требования об обязательной регистрации лоббистов [1].

1995 год – был принят закон, регламентирующий лоббизм в США «Закон о раскрытии лоббистской деятельности». Если закон 1946 года узаконил деятельность лоббистов только в законодательной сфере, то через почти 50 лет зону ответственности лоббистов перенесли и на исполнительную власть [1].

Лоббистский инструментарий – совокупность методов, средств и приемов, которые для представления и отстаивания интересов конкретных групп в органах государственной власти (рис. 2). Как правило, при осуществлении лоббистской деятельности, инструментарий применяется в сочетании [1].

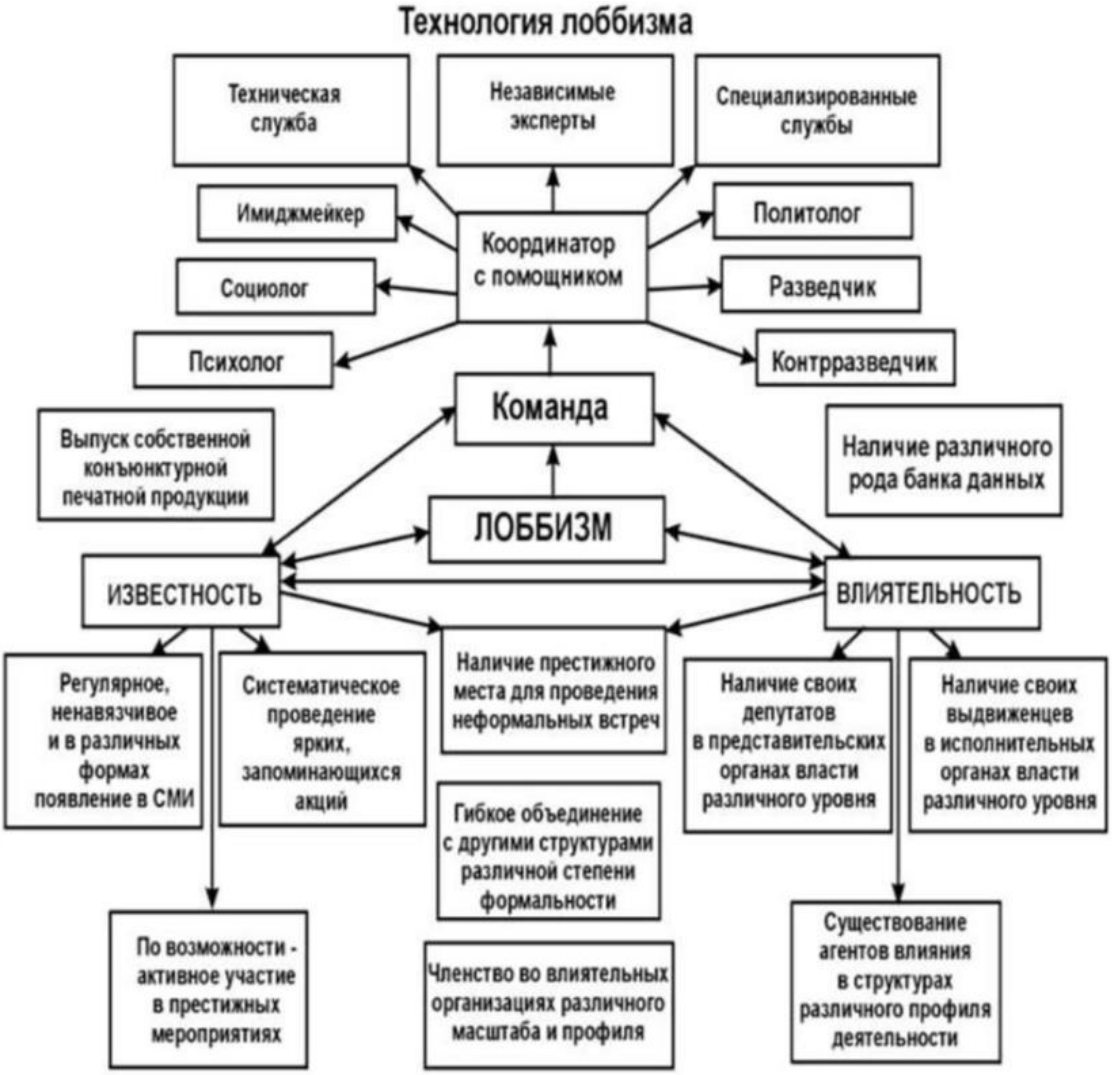


Рис. 2. Технология лоббизма [1]

Лоббиста часто путают со специалистом Government Relations (GR, «отношения с органами государственной власти»). Лоббист – специалист-консультант, эксперт, как правило нанятый компанией для реализации проектов, GR-специалист – сотрудник компании, занимающийся взаимодействием с органами государственной власти. Часто оба этих специалиста работают совместно, что делает их взаимодействие наиболее эффективно.

Задача регулирования лоббистской деятельности состоит из двух ключевых аспектов: с одной стороны, это обеспечение прозрачности внешнего воздействия на политические решения, а с другой стороны – создание механизмов общественного надзора за деятельностью государственных структур. В связи с этим можно выделить следующие цели регулирования лоббизма:

- развитие профессии лоббиста, повышение уровня общественного доверия как к институту лоббизма, так и к работе государственных органов;

- создание мер против коррупции;
- предоставление возможностей заинтересованным сторонам участвовать в принятии государственных решений, которые влияют на права и обязанности сторон;
- минимизация неформального взаимодействия отдельных групп интересов и должностных лиц;
- предоставление гарантий открытости и легитимности принятия государственных решений [2].

Сегодня институт лоббизма должен рассматриваться исключительно как демократический правовой механизм, с помощью которого субъекты лоббизма добиваются согласований различных интересов общества, гарантий защиты права граждан на участие в управлении государством. Для достижения прозрачности воздействия на подготовку и принятие государственных решений требуется официальные законы лоббистских отношений, которые будут их регулировать [2].

Список используемых источников

1. Чертков А. С. Институт лоббизма: история, функции и регулирование. М.: МУИВ, 2024. 113 с. ISBN: 978-5-9580-0766-0.

2. Войтенко Э., Парфенчикова А. Регулирование GR и лоббизма в России: Статус-кво или поиск новых решений. М.: Альпина ПРО, 2026. 248 с. ISBN: 978-5-206-00381-9.

Статья представлена научным руководителем, деканом СТЭД СПбГУТ, кандидатом политических наук, доцентом Д. В. Шутманом.

УДК 004.9:658

СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ РОССИЙСКОГО ИТ-ИНТЕГРАТОРА В СОВРЕМЕННЫХ УСЛОВИЯХ

А. А. Русакова (студент группы БИ-23 СПбГУТ), rusakova.an@sut.ru

В докладе представлены результаты анализа архитектуры предприятия ИТ-интегратора. Дана характеристика предметной области, построена бизнес-модель по шаблону А. Остервальдера, разработана цепочка создания ценности. Описана организационная структура и дана краткая характеристика предприятия. В итоге были разработаны рекомендации по совершенствованию бизнес-архитектуры на основе анализа построенных моделей.

бизнес-модель, архитектура предприятия, цепочка создания ценности, системный интегратор

Современные российские ИТ-компании, особенно работающие в сегменте системной интеграции и производства вычислительной техники, сталкиваются с необходимостью изменения операционных моделей. Это связано с санкционными ограничениями, курсом на импортозамещение и изменением структуры спроса. В этих условиях важным инструментом становится архитектура предприятия, позволяющая согласовать бизнес-стратегию, процессы и инфраструктуру [1].

Объектом исследования выбрано АО «РАМЭК-ВС» – системный интегратор полного цикла, имеющий собственное производство в Санкт-Петербурге, работающий преимущественно с государственными заказчиками (включая Министерство обороны). Цель работы – выявить недостатки текущей архитектуры и предложить целевые изменения с использованием стандартных артефактов: бизнес-модели по Остервальдеру, цепочки создания ценности, стратегической карты, моделей AS-IS и TO-BE.

На первом этапе была построена бизнес-модель «как есть» (табл. 1) [2]. Ключевая особенность – сильная зависимость от государственных контрактов, узкие каналы сбыта (тендеры и прямые продажи), слабое присутствие в коммерческом сегменте и отсутствие цифровых каналов маркетинга.

Анализ цепочки создания ценности по М. Портеру на рис. 1 показал, что основные процессы (закупка, сборка, контроль качества, отгрузка) выполняются преимущественно вручную или с низким уровнем автоматизации. Входящая логистика основана на бумажном документообороте, контроль качества – выборочный визуальный, клиентский сервис ограничен телефоном и электронной почтой [3].

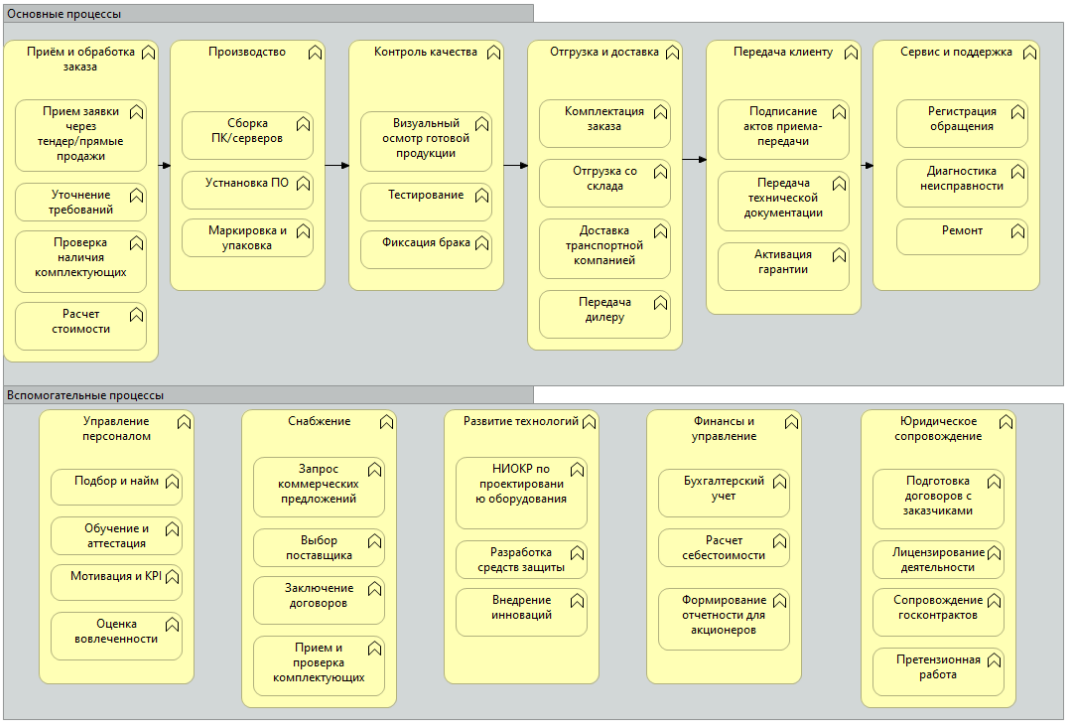


Рис. 1. Цепочка создания ценности «как есть»

Организационная структура – линейно-функциональная, не выделены подразделения по работе с малым и средним бизнесом и цифровым маркетингом.

ТАБЛИЦА 1. Бизнес-модель "как есть" по шаблону А. Остервальдера

<table>
<tr>
<td rowspan="2">Ключевые партнеры
Ведущие мировые производители ИТ-оборудования (Intel, AMD), Merlion, компания «Сафиб», поставщики комплектующих для производства</td>
<td>Ключевые виды деятельности
Производство компьютерной техники, системная интеграция, разработка средств защиты информации, сервисное и техническое обслуживание, поставка оборудования</td>
<td rowspan="2">Ценностные предложения
Российская компьютерная техника из реестра Минпромторга, полный цикл услуг от консалтинга до сервисного сопровождения, решения для защиты с гостайной, технологическая независимость и импортозамещение, контроль качества на всех этапах производства</td>
<td>Взаимоотношение с клиентами
Индивидуальные проекты, долгосрочные гос. Контракты, сервисная поддержка и обслуживание после продажи, личные консультации</td>
<td rowspan="2">Потребительские сегменты
Гос. Структуры, силовые ведомства, крупные промышленные предприятия, образовательные и мед. Учреждения, корпоративные заказчики из разных отраслей</td>
</tr>
<tr>
<td>Ключевые ресурсы
Собственный производственный комплекс в СПб, персонал (435 чел.),</td>
<td>Каналы сбыта
Прямые продажи через отдел продаж, сайт,</td>
</tr>
</table>

	лицензии ФСТЭК, собственные разработки, офисы в СПб и МСК		дистрибьюторская сеть, гос. Тендеры и закупки	
Структура издержек Затраты на производство и закупку комплектующих, расходы на содержание производственного комплекса, оплата труда сотрудников, затраты на НИОКР и разработку, расходы на лицензирование и сертификацию, маркетинговые расходы			**Потоки поступления доходов** Продажа компьютерной техники собственного производства, доходы от системной интеграции (проекты «под ключ»), поступления от сервисного обслуживания, доходы от поставки оборудования (дистрибуция), средства от государственных контрактов	

Целевая бизнес-модель (табл. 2) предполагает расширение клиентских сегментов за счет малого и среднего бизнеса, развитие подписных облачных сервисов. В цепочке создания ценности на рис. 2 добавлены новые процессы: портал самообслуживания, чат-бот на основе ИИ, ITSM-система, а также EDI для автоматизации закупок и WMS для складского учета [3].

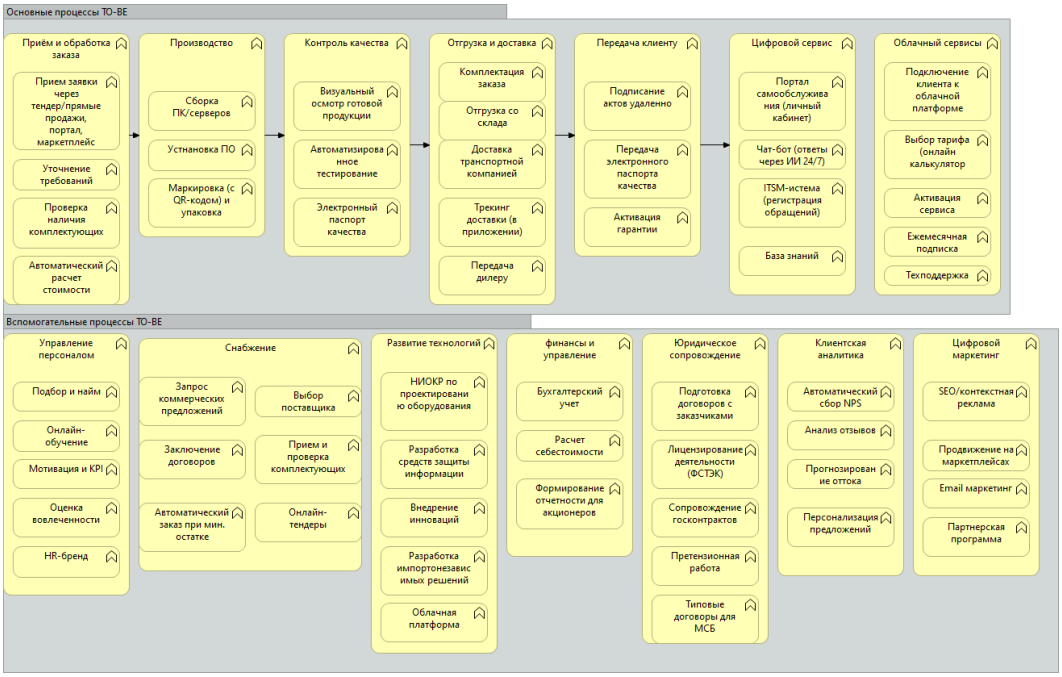


Рис. 2. Цепочка создания ценности "как будет"

Стратегическая карта на рис. 3 включает четыре перспективы – финансы, клиенты, внутренние процессы, обучение и развитие [4]. Финансовая перспектива ориентирована на рост прибыли с 2,6 до 3 млрд руб. к 2026 году, а также снижение затрат на привлечение клиентов (с 74 до 60 тыс.

руб.). В клиентской перспективе целевыми показателями являются доля брака в закупках (снижение с 4,55 % до 4,71 %), количество повторных обращений (рост с 5 до 8) и увеличение производительности труда. Перспектива внутренних процессов отражает необходимость автоматизации поддержки (целевой уровень 85 %) и сохранения ключевых сотрудников (83,33 %). В перспективе обучения и развития запланировано увеличение количества программ повышения квалификации (с 1 до 3) и рост затрат на обучения до 134 тыс. руб. [5].

ТАБЛИЦА *1*. Бизнес-модель по шаблону А. Остервальдера «как будет»

<table>
<tr>
<td rowspan="2">Ключевые партнеры
Добавляются российские производители комплектующих (уход от импортозависимости), интеграторы в новых отраслях (финтех, ритейл), образовательные учреждения для подготовки кадров (для рабочих)</td>
<td>Ключевые виды деятельности
Разработка полностью российских ПК, активный маркетинг в коммерческом секторе, развитие направления облачных решений</td>
<td rowspan="2">Ценностное предложение
Полностью импортонезависимые решения (дополнительно), быстрая обработка заявок и прозрачность проектов, гибкие условия для малого и среднего бизнеса, лизинг и рассрочка для коммерческих клиентов</td>
<td>Взаимоотношение с клиентами
Портал самообслуживания для отслеживания статуса обращений, база знаний коммерческих ИТ-продуктов, регулярные вебинары и консультации для малого бизнеса</td>
<td rowspan="2">Потребительские сегменты
Малый и средний бизнес (новый целевой сегмент), ритейл и финансовый сектор, стартапы и технологические компании, сохраняются государственные структуры</td>
</tr>
<tr>
<td>Ключевые ресурсы
Партнерская сеть в регионах, цифровая платформа для взаимодействия с клиентами, отдел по работе с коммерческими заказчиками</td>
<td>Каналы сбыта
Партнерская программа для региональных интеграторов, активное присутствие в социальных сетях и профильных сообществах</td>
</tr>
<tr>
<td colspan="3">Структура издержек
Затраты на разработку импортонезависимых решений, расходы на цифровой маркетинг, инвестиции в развитие партнерской сети</td>
<td colspan="2">Потоки поступления доходов
Доходы от подписных сервисов (облачные решения), комиссионные от партнерских продаж, доходы от типовых решений для МСБ (коробочные продукты)</td>
</tr>
</table>

Проведенное исследование показало, что архитектура АО «РАМЭК-ВС» требует системной трансформации по нескольким направлениям: автоматизация цепочки поставок (*EDI*), внедрение *WMS* и *ITSM* [5], организация портала самообслуживания, развитие облачных сервисов с подписной моделью. Предложенные изменения позволяют снизить долю ручного труда,

повысить прозрачность процессов для клиентов и создать новые источники регулярного дохода.

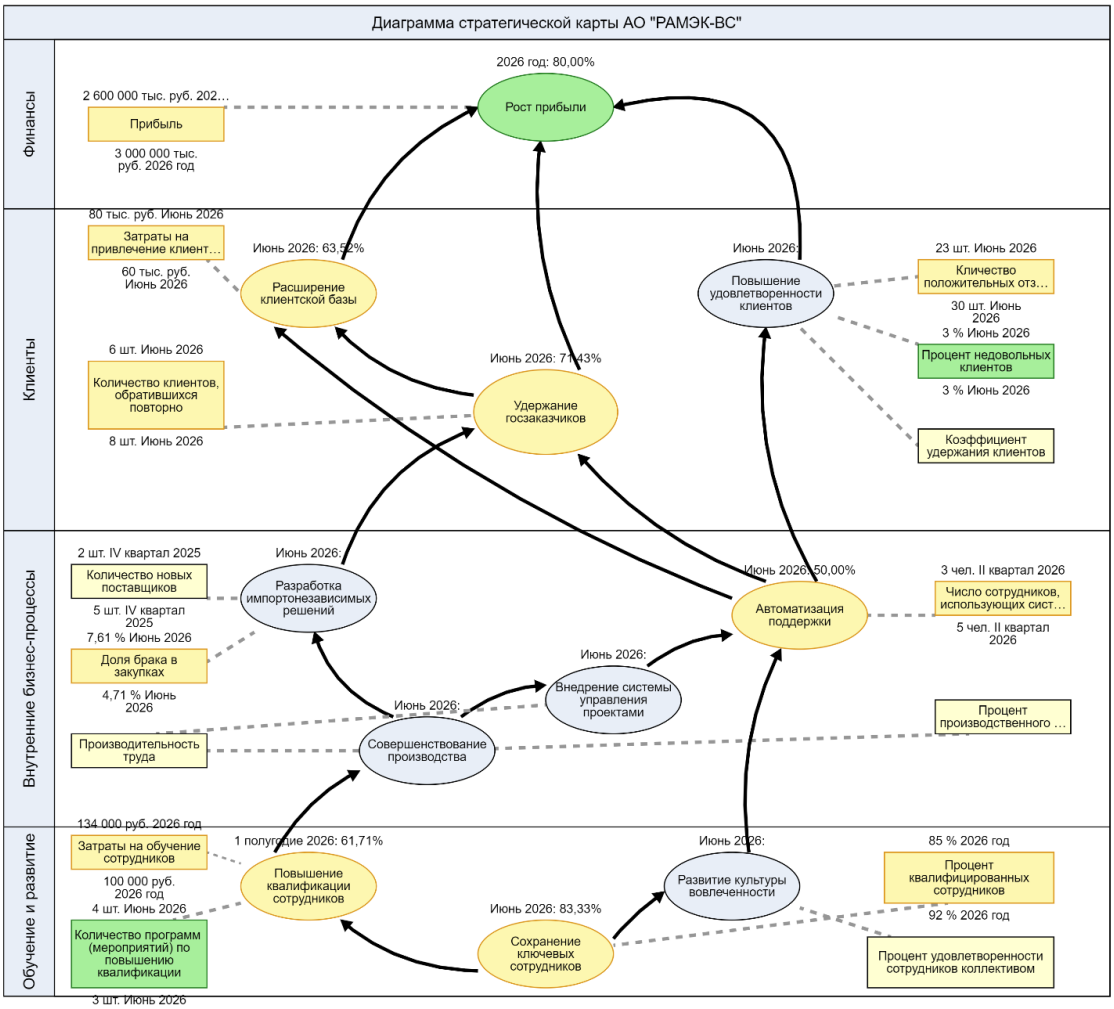


Рис. 3. Стратегическая карта

Разработанные модели могут быть использованы при планировании дорожной карты изменений.

Список используемых источников

1. Папушин, Д. Что делает интегратора сильным партнером для цифровой трансформации / Д. Папушин // РБК Компании. 2026. 3 февраля.

2. Остервальдер, А. Построение бизнес-моделей: настольная книга стратега и инноватора / А. Остервальдер, И. Пинье; пер. с англ. Москва: Альпина Паблишер, 2011. 288 с.

3. Шиболденков, В. А. Обзор моделей конфигурации создания ценности в наукоемких организациях (на примере ракетно-космической промышленности) / В. А. Шиболденков, С. С. Гаврилов // Вестник университета. 2023. № 8. С. 80–90.

4. Каплан, Р. С. Стратегические карты. Трансформация нематериальных активов в материальные результаты / Р. С. Каплан, Д. П. Нортон; пер. с англ. Москва: Олимп-Бизнес, 2007. 512 с.

5. Чугунова, О. А. Создание стратегических карт менеджеров / О. А. Чугунова, Н. А. Тимофеева // Молодой ученый. 2014. № 8 (67). С. 632–635.

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом педагогических наук, доцентом А. М. Атаян.

УДК 65.011.56:004.9

ЭВОЛЮЦИЯ И РОЛЬ ERP-СИСТЕМ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕДПРИЯТИЯ

В. С. Смирнова (студент группы МБИ-2511з СПбГУТ),
smirnova.vs@sut.ru

В статье рассматриваются современные ERP-системы как ключевой инструмент управления ресурсами предприятия, анализируется их эволюция и тенденции развития. Раскрывается роль ERP в цифровой трансформации бизнеса. Описаны методологии внедрения и предложен подход к оценке эффективности на основе сбалансированной системы показателей.

ERP-система, цифровая трансформация, управление ресурсами, методологии внедрения, импортозамещение, эффективность, сбалансированная система показателей

В условиях цифровизации бизнеса скорость принятия решений и операционная эффективность становятся ключевыми факторами конкурентоспособности. Центральное место среди инструментов управления занимают ERP-системы (Enterprise Resource Planning) – программные решения, объединяющие финансы, производство, цепочки поставок, продажи и управление персоналом в единой базе данных. Они выступают «центральной нервной системой» бизнеса, обеспечивая согласованную работу отделов на основе достоверного источника информации [1].

Для малых и средних производственных предприятий внедрение ERP особенно актуально: оно позволяет преодолеть разрозненность данных, автоматизировать ручной учет, ускорить обработку информации и создать единую аналитическую платформу для мониторинга KPI. Однако специфика таких предприятий (ограниченные бюджеты, отсутствие крупного ИТ-персонала, потребность в быстрой отдаче) требует адаптированных методологий и решений.

Современное понимание ERP выходит далеко за рамки простого учета. Механизм работы системы строится на глубокой интеграции, при которой все функциональные модули оперируют единой базой данных. Это автоматизирует сквозные процессы: от резервирования товара и формирования логистических задач до создания финансовых документов и обновления отчетности в реальном времени. Устраняется проблема изолированных

информационных «островков», минимизируются ошибки, формируется единая картина деятельности компании [1].

Эволюция ERP охватывает более 60 лет [2]. В 1960-х годах появились системы MRP (Material Requirements Planning) для расчета потребности в сырье при массовом производстве. В 1980-х годах концепция MRP II (Manufacturing Resource Planning) расширила фокус на оборудование, трудовые и финансовые ресурсы, создав «замкнутый цикл» планирования. В 1990-х годах аналитическая фирма Gartner ввела термин ERP: вместо изолированных систем для разных отделов предлагалась единая интегрированная среда с общей базой данных. На рубеже 2000-х годов началась эпоха ERP II – расширенных систем, интегрирующихся с CRM (управление взаимоотношениями с клиентами) и SCM (управление цепочками поставок), а также появились облачные решения по модели SaaS. С 2010-х годов развитие определяется цифровизацией и интеллектуализацией: в ERP встраиваются искусственный интеллект (ИИ), машинное обучение для предиктивной аналитики, интернет вещей (IoT), роботизация процессов (RPA) [2]. К 2026 году ИИ стал ключевым элементом архитектуры, а концепция агентного ИИ позволяет системам не только предлагать решения, но и выполнять действия в заданных рамках [3].

Согласно данным Market.us, мировой рынок ERP в 2023 году оценивался в 65,2 млрд долл. США, а к 2033 году достигнет 200,7 млрд (среднегодовой темп роста 11,9 %). По способу развертывания лидирует сегмент On-Premise (64,8 %) за счет требований контроля и безопасности. По бизнес-функциям доминируют финансы (29,1 %). Крупные предприятия занимают 67,3 % рынка, а обрабатывающая промышленность – 24,5 % отраслевого использования. Более 95 % организаций отмечают улучшение процессов после внедрения ERP, среднее сокращение складских запасов составляет 11–22 % [4].

В России с 2022 года наблюдаются кардинальные изменения из-за ухода западных вендоров (SAP, Oracle). К концу 2025 года доля отечественных ERP-решений достигла 75 % рынка [5]. Абсолютный лидер – экосистема «1С» (70–80 % рынка), также представлены «Галактика», «Турбо ERP», Global ERP [5]. Эпоха вынужденного импортозамещения сменяется этапом осознанного выбора: российские разработчики системно дорабатывают решения под требования крупного корпоративного сегмента [6]. Однако исследование «КОРУС Консалтинг» (февраль 2026 г.) показало, что только 10,3 % компаний воспринимают ERP как «ядро» управленческого

контура, а у более 43 % организаций система внедрена не полностью или требует оптимизации [7]. При этом 24,1 % компаний по-прежнему используют устаревшую 1С: УПП, поддержка которой прекращается в 2027 году [7].

Цифровая трансформация – это не просто добавление новых функций, а глубокое преобразование бизнес-процессов, позволяющее выходить на новые рынки. Более половины крупнейших мировых компаний активно формируют стратегию цифровой трансформации. В этом контексте ERP-системы выступают фундаментальным инструментом, обеспечивающим сбор, хранение, обработку и анализ данных как стратегического актива [1].

Современные ERP-решения основаны на облачных технологиях, используют ИИ и машинное обучение [3]. Они обеспечивают интеллектуальную автоматизацию рутинных задач, повышение операционной эффективности и предоставление руководству актуальной аналитики в реальном времени. Архитектурно ERP построены по модульному принципу (финансы, закупки, производство, персонал и др.) с единым централизованным хранилищем данных. Интеграция с CRM, платформами электронной коммерции и отраслевыми решениями через API, ESB или iPaaS формирует единое цифровое пространство [1].

Внедрение ERP приносит стратегические преимущества: рост производительности за счет автоматизации и освобождения сотрудников от рутины; устранение разрозненности информации и создание единого источника достоверных данных; повышение прозрачности управления и ускорение принятия решений; снижение операционных и регуляторных рисков благодаря усилению контроля и прогнозной аналитике; а также консолидация ИТ-инфраструктуры, упрощение обслуживания и повышение гибкости компании [1].

Отраслевая ценность ERP подтверждается практикой: коммунальные предприятия оптимизируют управление основными фондами, производственные компании контролируют качество и использование активов, ритейлеры интегрируют онлайн- и офлайн-каналы, сервисные организации управляют проектами и ресурсами. Таким образом, ERP становятся не просто преимуществом, а обязательным условием конкурентоспособности [1].

Успех внедрения ERP во многом зависит от выбора и адаптации методологии. В научной литературе выделяют модели жизненного цикла: модель Бэнкрофта (пять фаз от планирования до запуска), модель Росса (включая стабилизацию и непрерывное совершенствование), модель Эстевеса

(полный цикл от принятия решения до вывода из эксплуатации), трехфазную модель Парра и др. [2].

В последние годы классические каскадные методологии (Waterfall) уступают место гибким (Agile) и гибридным подходам. Гибридное управление сочетает структурированность Waterfall на этапе планирования архитектуры и интеграции с гибкостью Agile (итеративность, вовлечение пользователя) на этапах конфигурирования и разработки. Это позволяет быстрее получать обратную связь, корректировать приоритеты и демонстрировать работающие прототипы, снижая риски проекта [3].

Типовые этапы внедрения ERP:

1. Предварительное планирование – анализ показателей, разработка бизнес-кейса, планов управления изменениями и рисками.

2. Планирование – официальный старт, формирование проектной группы, выбор методологии, составление графика.

3. Настройка и реинжиниринг – короткая диагностика «болей» пользователей, картирование бизнес-процессов, обучение команды, устранение неэффективных процессов.

4. Проектирование системы – утверждение высокоуровневого проекта, создание интерактивного прототипа.

5. Конфигурирование и тестирование – настройка прототипа, загрузка реальных данных, приемочное тестирование пользователями (UAT).

6. Установка и запуск – создание производственной среды, обучение, ввод в эксплуатацию, параллельная работа со старой системой для снижения рисков, фаза стабилизации [3].

Критические факторы успеха внедрения включают поддержку высшего руководства; обязательный реинжиниринг бизнес-процессов (BPR), поскольку автоматизация хаоса ведет к провалу; управление изменениями и культурой, так как сопротивление сотрудников является причиной неудач в значительной доле проектов; качество данных и миграцию – очистку нормативно-справочной информации до старта; а также компетенции и привлечение внешних консультантов, поскольку независимые эксперты снижают риски [1, 3].

Оценка эффективности внедрения ERP требует комплексного подхода, выходящего за рамки традиционного финансового анализа. Наиболее адекватной является сбалансированная система показателей (BSC), которая декомпозирует стратегические цели по четырем проекциям [8]:

● финансы – ROI (целевой уровень не менее 30 % годовых), сокращение цикла конвертации денежных средств, ускорение оборачиваемости запасов;

● клиенты – качество сервиса, доля идеальных заказов (95 % и выше), коэффициент удержания клиентов;

● бизнес-процессы – сокращение операционного цикла заказа, повышение производительности труда, снижение ручных операций, прозрачность цепочки создания ценности;

● обучение и развитие – уровень принятия системы пользователями (цель – вовлеченность не менее 70 % активных пользователей), прозрачность зон ответственности, скорость адаптации новых сотрудников.

Только при таком сбалансированном подходе внедрение ERP становится не заменой программного обеспечения, а драйвером устойчивого роста компании [8].

ERP-системы прошли долгий путь от узкоспециализированных MRP до интеллектуальных платформ с ИИ и облачной архитектурой [2]. Они играют центральную роль в цифровой трансформации, обеспечивая интеграцию данных, операционную эффективность и стратегическую аналитику [1]. Российский рынок ERP после ухода западных вендоров перешел к активному импортозамещению, где лидирует экосистема «1С», однако остаются проблемы неполной реализации потенциала систем [5-7].

Успех внедрения ERP определяется не столько выбором программного продукта, сколько грамотной методологией (гибридные подходы), реинжинирингом процессов, управлением изменениями и качеством данных [3]. Оценка эффективности должна быть комплексной, используя сбалансированную систему показателей, охватывающую финансы, клиентов, процессы и персонал [8]. Для малых и средних производственных предприятий адаптированные ERP-решения становятся ключевым инструментом повышения конкурентоспособности в условиях цифровой экономики.

Список использованных источников

1. What is ERP: Definition, benefits, and common challenges // Right People Group. Режим доступа: URL: https://rightpeoplegroup.com/blog/erp-definition-benefits-challenges (дата обращения: 03.04.2026).

2. История ERP-систем // ERPOnline. Режим доступа: URL: https://www.erp-online.ru/erp/hist/ (дата обращения: 03.04.2026).

3. Как ERP превращаются в экосистему цифровых решений // CNews. Режим доступа: URL: https://www.cnews.ru/articles/2025-07-27_kak_erp_prevrashchayutsya_v_ekosistemu (дата обращения: 03.04.2026).

4. ERP Software Market // Market.us. Режим доступа: URL: https://market.us/report/erp-software-market/ (дата обращения: 03.04.2026).

5. Необдуманное суетливое импортозамещение ERP закончилось. Итоги года и перспективы рынка // TAdviser. Режим доступа: URL: https://clck.ru/3Sqxtz (дата обращения: 03.04.2026).

6. Новый этап цифровой трансформации: ERP: время стратегических решений // РБК Компании. Режим доступа: URL: https://companies.rbc.ru/news/6b6vq2u2Tg/novyij-etap-tsifrovoj-transformatsii-erp-vremya-strategicheskih-reshenij/ (дата обращения: 03.04.2026).

7. Исследование «КОРУС Консалтинг»: у 43 % компаний ERP внедрена не полностью или требует оптимизации // КОРУС Консалтинг. Режим доступа: URL: https://korusconsulting.ru/press-centr/issledovanie-korus-konsalting-u-43-kompaniy-erp-vnedrena-ne-polnostyu-ili-trebuet-optimizatsii/ (дата обращения: 03.04.2026).

8. Автоматизация сбалансированной системы показателей (BSC) в 1С:ERP // Первый Бит. Режим доступа: URL: https://nfp2b.ru/2019/02/26/avtomatizatsiya-sbalansirovannoj-sistemy-pokazatelej-bsc-v-1s-erp (дата обращения: 03.04.2026).

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом экономических наук, доцентом М. Б. Вольфсоном.

УДК 338

ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА В ЛОГИСТИКЕ КАК ИНСТРУМЕНТ ФОРМИРОВАНИЯ ПРОЗРАЧНОГО РЫНКА ПЕРЕВОЗОК (НА ПРИМЕРЕ «ГОСЛОГ»)

П. С. Столетова (студент группы ЭМ-21в СПбГУТ), stoletova.ps@sut.ru

В статье проводится анализ единой цифровой платформы «ГосЛог» как инструмента цифровизации логистической отрасли России. В работе будут рассмотрены принципы работы системы, предпосылки ее возникновения, процесс документооборота, преимущества для участников рынка: экспедиторов, заказчиков и подрядчиков, а также возможные риски нововведения. Обосновывается значимость платформы как инструмента формирования открытой и эффективной транспортной экосистемы.

логистика, цифровизация, ЭДО, цифровая трансформация экономики

Актуальность данной статьи обусловлена цифровизацией бизнес-процессов организаций и государства вне зависимости от отрасли. Помимо этого, Российская Федерация держит курс на цифровизацию экономики, внедряя цифровые решения в различные сферы деятельности общества. Одним из последних решений в данной области стал ФЗ «О внесении изменений в ФЗ «О транспортно-экспедиционной деятельности» и отдельные законодательные акты РФ», принятый Государственной Думой 27 мая 2025 года, по которому все коммерческие логистические организации будут обязаны вести документооборот, связанный с движением грузов, в электронной форме, предоставляя информацию на специальную платформу «ГосЛог» с 1 сентября 2026 года [1]. Данное нововведение затрагивает логистику на уровне государства, всем компаниям предстоит перестроится на новый формат работы, изучить и внедрить технологию электронного документооборота. Закон может привести к множеству последствий, которые будут описаны в данной статье.

Рассмотрим основные транспортно-экспедиторские документы, которыми обмениваются игроки рынка:

- заявки на перевозку или поручение экспедитору (служит основанием для оказания транспортных услуг перевозчика заказчику);
- экспедиторские расписки (подтверждает, что экспедитор принял груз от клиента или грузоотправителя и готов к перевозке);

● путевые листы (фиксируют состояние автомобиля, расход топлива, километраж, маршрут, водителя).

До внедрения электронного документооборота в логистику процесс обмена документами выглядел следующим образом:

1. Создание заявки на перевозку экспедитору клиентом.

2. Создание экспедиторской расписки при получении груза для перевозки.

3. При необходимости, создание товарно-транспортной накладной.

4. Создание транспортной накладной (должна быть подписана в 4х экземплярах: для заказчика, получателя, экспедитора, как приложение к счету на оплату).

5. Все подрядчики и водители, участвующие в процессе перевозки, подписывают ТН.

6. Документ о взвешивании груза также подписывается (груз не всегда взвешивается).

7. Подписание акта приема и акта передачи на каждом обрабатывающем терминале.

8. Подписание экспедиторской расписки при получении груза клиентом.

9. После совершения перевозки экспедитор выставляет счет и предоставляет акт выполненных работ, который также необходимо подписать клиенту [2].

Процесс обмена документами в логистике многоуровневый, трудоемкий, ресурсозатратный и имеет большое количество участников, каждый из которых подписывает документы на определенном этапе.

Изучим исторические детали, чтобы понять, откуда происходит идея о внедрении цифровой платформы «ГосЛог». В 2020 году министерство транспорта провело эксперимент по переводу транспортных документов в цифровой формат, а также по использованию ЭДО для обмена. ГИБДД и Ространснадзор контролировали процесс через тестовую информационную систему. Эксперимент закончился в 2025 году и выполнил поставленные цели. С 2022 года добровольное использование ЭТрН (электронных транспортных накладных) закрепили в законодательстве, а с 2024 года ведется разработка сервиса ГосЛог [3, 4].

ГосЛог – это национальная цифровая транспортно-логистическая платформа. В ней появятся реестры перевозчиков и экспедиторов, цифровые паспорта перевозок, мониторинг грузов и дорожной обстановки. Платформа

будет интегрирована с данными ГИБДД, ГИС ЭПД (государственной информационной системой электронных перевозочных документов), с МВД, Ространснадзором, ФНС, провайдерами электронных подписей и ЭДО.

Для участия в транспортном электронном документообороте необходимо выпустить сертификат квалифицированной электронной подписи для уполномоченных лиц, выбрать и подключиться к оператору информационной системы электронных перевозочных документов (полный список предоставлен Министерством Транспорта России [5]), приобрести и настроить технические средства для всех участников ЭДО (в том числе для водителей и иных сотрудников) [3].

Будет рассмотрен потенциальный эффект от внедрения единой транспортно-логистической платформы, а также информационной системы электронных перевозочных документов в отрасль для различных участников процесса на основе таблицы 1.

ТАБЛИЦА 1. Потенциальный эффект от внедрения ЭДО в логистику («ГосЛог»).

Участники	Положительный эффект	Отрицательный эффект (риски)
Участники отрасли (экспедиторы, подрядчики, заказчики)	-ускорение процесса подписания документов и снижение времени на доставку документов -сокращение расходов на доставку документов и ведение архива -сокращение расходов на оргтехнику и бумагу -полный контроль над логистическими операциями -снижение потерь документов -расчет возможных вариантов перевозки -мониторинг инцидентов на путях сообщения -снижение числа ненадежных компаний	-закрытие компаний, которые работали по «серой» схеме -доминирование наиболее крупных компаний на рынке, из-за закрытия малого бизнеса -усложнение выхода новых участников на рынок -пристальный контроль со стороны государства -рост числа штрафов -необходимость расходов на обучение сотрудников и внедрение ЭДО
Государство	-прозрачность логистики -доступ к документам для МВД, РосТрансНадзор, ФНС -создание «белого» бизнеса -моделирование транспортных потоков -отслеживание нарушений -комплексная аналитика	-снижение количества компаний на рынке, все их сотрудники остаются без работы

Участники	Положительный эффект	Отрицательный эффект (риски)
Для всех участников в целом (бизнес, конкуренты и государство)	-снижение затрат на транспортировку грузов на 16,5 % -увеличение пропускной способности маршрутов на 15 % -цифровой профиль участника перевозки -прослеживаемость грузов в реальном времени -цифровой паспорт перевозки	
Общество в целом	-мониторинг приоритетной доставки социально значимых грузов	

Участники грузоперевозок (экспедиторы, подрядчики и заказчики) благодаря внедрению государственной информационной системы электронных перевозочных документов получат следующие преимущества: ускорение процесса подписания документов (снижение времени на доставку документов, поскольку в ЭДО она происходит мгновенно), сокращение расходов на доставку и хранение документов, сокращение расходов на бумагу и оргтехнику до 170 млрд рублей [6], руководители и менеджеры получат полный контроль над логистическими процессами (отслеживание перевозок в реальном времени), снижение времени на обработку документов, минимизация ошибок в документах и потерь документов.

Помимо очевидных преимуществ, организации смогут использовать специализированные сервисы и возможности платформы, что позволит: снизить число недобросовестных компаний, а соответственно – снизить риски при выборе контрагентов; производить мониторинг инцидентов благодаря данным из ГИБДД и других служб, которые фиксируют ДТП и заторы, прогнозируют дорожно-транспортную обстановку. Это позволит в том числе просчитывать вероятность задержки грузов на маршруте [4]. Появится возможность расчета вариантов перевозки, благодаря интеграции с сервисами и наличию информации о всех участниках на платформе. Будут учитываться: скорость, цена, вид груза, удобство перевозки, ситуация на дорогах [4].

Риски, которые могут наступить для участников грузоперевозок при введении данной системы: закроются компании, которые работали по «серой» схеме, соответственно снизится число участников рынка. Это также может привести к возникновению олигополии и доминированию неболь-

шого числа компаний на рынке, усложнится выход для новых игроков. Будет происходить пристальный контроль со стороны государства. Такие службы как ФНС, МВД, Ространснадзор смогут мгновенно получать все данные о компаниях и их перевозках. Это может привести к росту штрафов для компаний. Помимо этого, организациям будет необходимо подготовится к внедрению ЭДО и подключению к платформе, приобрести технические средства и обучить сотрудников, что подразумевает дополнительные расходы.

Государство при внедрении данной системы получит следующий положительный эффект: повышение прозрачности логистики, доступ к информации о компаниях для всех ключевых государственных служб в режиме «онлайн», создание «белого» бизнеса за счет его прозрачности, моделирование транспортных потоков (анализ содержания грузов, маршрутов и частоты перевозок, что позволит планировать инфраструктуру и управлять экономикой) [4], оперативное отслеживание нарушений компаниями – повышение бюджета за счет штрафов. Также благодаря платформе сформируется единая база данных о складах, терминалах, портах, дорогах и автопарках, сервисы платформы смогут использовать ее для аналитики и прогнозов.

К рискам государства можно отнести то, что могут закрыться малые участники бизнеса. Люди, работавшие в таких компаниях, останутся без работы и будут вынуждены искать новую или брать государственные пособия по безработице.

Преимущества для всех участников, то есть и для участников перевозок, и для государства, будут следующие: снижение затрат на транспортировку грузов на 16,5 % [6], увеличение пропускной способности маршрутов на 15 % [6], наличие цифрового профиля участника перевозки со всех необходимой информацией о нем [4], возможность прослеживаемости грузов **(**благодаря интеграции с другими платформами и «цифровому паспорту перевозки»; на основе этой информации можно увидеть, где сейчас находится груз) [4].

Для общества эта система будет важна, благодаря наличию сервиса приоритетной доставки грузов, значимых для общества. Сервис будет оценивать загруженность магистралей и следить, чтобы, при наличии срочной потребности, лекарства, продукты и гуманитарная помощь получали приоритет при доставке. Иными словами, сервис будет координировать действия ведомств и участников логистической цепочки [4].

Подводя итоги, можно сказать, что внедрение единой цифровой платформы «ГосЛог» представляет собой системную трансформацию логистической отрасли, направленную на создание прозрачного и эффективного рынка грузоперевозок. Платформа обеспечивает комплексную цифровизацию документооборота, интеграцию с государственными системами и предоставление участникам рынка инструментов для оптимизации логистических процессов. Ожидаемые эффекты включают снижение затрат на транспортировку на 16,5 %, увеличение пропускной способности маршрутов на 15 % и формирование «белого» бизнеса за счет прозрачности операций. Однако цифровизация сопровождается определенными рисками: закрытием компаний, работавших по «серым» схемам, усилением государственного контроля и необходимостью инвестиций в техническое оснащение и обучение персонала. Таким образом, успешное внедрение «ГосЛог» требует сбалансированного подхода, учитывающего как экономические преимущества цифровизации, так и социальные последствия для участников рынка.

Список используемых источников

1. РОССИЙСКАЯ ФЕДЕРАЦИЯ. «ФЕДЕРАЛЬНЫЙ ЗАКОН. О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ФЕДЕРАЛЬНЫЙ ЗАКОН "О ТРАНСПОРТНО-ЭКСПЕДИЦИОННОЙ ДЕЯТЕЛЬНОСТИ" И ОТДЕЛЬНЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ». URL: https://normativ.kontur.ru/document? moduleId=1&documentId=500386&p=1210&utm_source=yandex&utm_medium=organic&utm_startpage=kontur.ru %2Flogistika %2Fspravka %2F22576-elektronnye _transportnye_nakladnye&utm_orderpage=kontur.ru %2Flogistika %2Fspravka %2F22576-elektronnye_transportnye _nakladnye (дата обращения 01.04.2026).

2. Схема логистического документооборота. URL: https://cyberleninka.ru/article/n/shema-logisticheskogo-dokumentooborota-i-problemy-vnedreniya-elektronnogo-dokumentooborota-v-logisticheskih-organizatsiyah/viewer (дата обращения 10.03.2026).

3. Переход на электронные транспортные накладные в 2026 году: кто обязан применять и когда. URL: https://kontur.ru/logistika/spravka/22576-elektronnye_transportnye _nakladnye (дата обращения 23.03.2026).

4. ГосЛог в 2026: полное руководство для экспедиторов и перевозчиков. URL: https://kontur.ru/logistika/spravka/83369-rukovodstvo_dlya_ekspeditorov_i_perevozchikov (дата обращения 10.03.2026).

5. Реестр операторов ИС ЭПД. URL: https://mintrans.gov.ru/activities/214/376/377/380?ysclid=mj11wqb1mj779004036 (дата обращения 10.03.2026).

6. Дан старт мультимодальным перевозкам в рамках создания Национальной цифровой транспортно-логистической платформы («ГосЛог»)». URL: https://mintrans.gov.ru/press-center/news/11463 (дата обращения 04.04.2026).

Статья представлена научным руководителем, преподавателем кафедры ЭД СПбГУТ О. А. Посоховой.

УДК 33.012.434

ЭКОСИСТЕМА КАК СКРЫТАЯ ФОРМА МОНОПОЛИЗАЦИИ РЫНКА НА ПРИМЕРЕ РОССИЙСКИХ КОМПАНИЙ

Д. Сулейманов (студент группы БИ-2513 СПбГУТ), suleimanov.d@sut.ru

Стремительный рост таких платформ, как Яндекс, Сбер и ВК, привел к стиранию классических конкурентных границ и появлению скрытых механизмов доминирования, что создало новые вызовы для ФАС. На примере российских компаний в работе выявляются ключевые факторы экосистемы и скрытой монополизации, проблемы в антимонопольном законодательстве РФ. Проводится критический анализ обозначенных положений, и оцениваются риски для государства, экономики и бизнеса.

экосистема, монополизация, российский рынок, антимонопольное законодательство, Яндекс, Сбер, ВК

Цифровая экосистема – явление, которое имеет относительно недолгую историю. Начиная с 2000-х годов, экосистемы постепенно меняли структуру рынков. Цель данной работы – проанализировать потенциальное влияние экосистемы на экономику и бизнес, а также выявить конкретные факторы, способные оказать такое воздействие.

Что такое экосистема? В антимонопольном законодательстве РФ нет официального трактования. Можно сформулировать следующее определение. Экосистема – это множество разных приложений из различных сфер или подсфер одной компании, соединенных в единую систему или в единую инфраструктуру. Экосистемы, в свою очередь, делятся на множество групп, но выделим лишь некоторые, а именно: по распространению и по структуре. В первом случае экосистема делится на глобальную и национальную. Чтобы определить, к какой группе относится та или иная экосистема какой-либо компании, надо посмотреть на индекс транснационализации: если он выше 25 %, то такая экосистема считается глобальной, а ниже 25 % – национальной. В качестве примера можно взять Google (≈44 %) и Яндекс (≈18 %). Во втором случае экосистема делится на открытую, гибридную и закрытую. Отличия заключаются в степени открытости платформы для других компаний.

Яндекс – крупнейшая IT-компания в России, которая имеет масштабную экосистему, и, как было сказано выше, ее экосистема национального рода, как и у Сбера и ВК. В распоряжении Яндекса находится множество платформ из разных сфер. К примеру: мобильность (Яндекс Такси, Яндекс

Драйв); покупки и доставка (Яндекс Доставка, Яндекс Маркет); финансы (Яндекс Пэй); информация и навигация (Яндекс Браузер, Яндекс Навигатор, Яндекс Карты); фудтех и e-grocery (Яндекс Лавка, Яндекс Еда). Также компания имеет центральное приложение (Яндекс GO), единую базу для всех платформ и единую систему регистрации (ID), что позволяет соединить все свои платформы в единую экосистему, интегрируя их друг с другом, тем самым сократив свои расходы на серверы и рекламу и получив новое конкурентное преимущество. А чтобы удержать пользователей, была введена система подписок (Яндекс Плюс) и виртуальный помощник (Алиса). Стратегия Яндекса заключается в том, чтобы заходить на те рынки, на которых: 1) у компании уже будет преимущество; 2) приложение легко интегрировать в экосистему; 3) приложение будет дополнять экосистему и интегрироваться с другими приложениями компании.

При выходе на новый рынок компания действует агрессивно, путем вытеснения ключевых игроков, уходя в фиксированный убыток, устанавливая цены ниже конкурентных, давая большие кэшбеки и преимущества, интегрируя новое приложение в свою экосистему и систему подписок, чтобы захватить существенную часть данного рынка. Такую стратегию компания может себе позволить за счет экосистемы и повышения цен в других приложениях компании. По структуре экосистема Яндекса гибридная, т. к. имеет множество закрытых (Яндекс Пэй) и открытых (Яндекс Еда) платформ. Доли рынка Яндекса в разных сферах: поиск ≈ 67 %; такси ≈ 99 % (по данным 2024 г.); онлайн-кино ≈ 29,3 %; фудтех и e-grocery ≈ 31,1 % [1].

Сбер – это пример цифровой экосистемы, которая объединяет финансовые и повседневные сервисы в единое пространство. Ее цель – помогать клиентам решать задачи в разных сферах жизни. Сбербанк сменил название на «Сбер» в 2020 году в рамках масштабного ребрендинга, который был связан с трансформацией компании из традиционного банка в многофункциональную экосистему. Это изменение отражает новую стратегию развития, ориентированную на предоставление широкого спектра услуг, выходящих за рамки классических банковских операций. Сбер включает в себя такие сферы, как: финансы (Сбербанк); покупки и доставка (Мегамаркет, Купер); медиа и развлечение (Okko); здоровье (СберЗдоровье); фудтех и e-grocery (Самокат). Центральное приложение компании – это Сбер, которое также имеет систему подписок, единую систему регистрации (Сбер ID), виртуального помощника «Гига чат» и денежный суррогат, такой как «Сбер-

Спасибо», которое можно обменять на реальные деньги по курсу 1 СберСпасибо = 0,5 рубля. В совокупности это дает мощный сдерживающий эффект, препятствующий переходу пользователей в другие банки, который еще и усиливается подпиской СберПрайм. В отличие от Яндекса, Сберу трудно собрать типичный паттерн пользователя из-за банковской тайны. По структуре экосистема Сбера была ранее закрытой, но, чтобы не быть «жестко закрытой», с 2021 года предоставляет открытый API, приглашая партнеров и независимых разработчиков создавать приложения. Их платформа SmartMarket позволяет сторонним разработчикам получать доступ к технологическим инструментам «Сбера», так что можно сказать, что в настоящее время экосистема Сбера является гибридной. Стратегия компании – это сбор разных приложений вокруг банка (т. е. основного ядра компании), чтобы те деньги, которые поступают пользователю, хранились и оседали в других приложениях компании [2]. По доле рынка Сбера в разных сферах: медиа и развлечение ≈ 18,7 %; финансы (депозиты физ. лицам ≈ 50 %; кредиты физ. лицам ≈ 46 %; депозиты юр. лицам ≈ 22 %; кредиты юр. лицам ≈ 37 %; активы ≈ 30 %); фудтех и e-grocery ≈ 16,4 %; здоровье ≈ 20 %.

ВК – технологическая компания, которая до 12 октября 2021 года называлась Mail.ru Group. Цель – соединять людей, сервисы и компании, создавая простые и удобные инструменты коммуникации. ВК включает в себя такие приложения, как: медиа и развлечение (Дзен, Mail.ru, ВК игры, ВК клипы, ВК видео и т.д.); коммуникация (ВК, Одноклассники, Макс); образование (Skillfactory, Учи.ru, Сферум, Skillbox, VK Education); товары и услуги (Aliexpress, Юла); магазин приложений (RuStore). Не имеет центрального приложения, системы подписок, но содержит единую систему регистрации (ID). По структуре экосистема ВК полностью открыта и строится вокруг сотрудничества с разными компаниями. Стратегия компании – это полное закрепление за собой сферы коммуникации, образования и развлечения. Общая доля рынка в данных сферах составляет 95 % рунета [3]. Основываясь на проведенном анализе компаний, составим факторы экосистем и скрытой монополии.

Факторы экосистемы: 1) центральное приложение; 2) единая база клиентов; 3) единая система регистрации; 4) единая платежная система; 5) система подписок; 6) взаимоинтеграция.

Ключевые факторы скрытой монополизации: 1) система подписок; 2) система единой учетной записи; 3) множество приложений из разных сфер и подсфер; 4) виртуальный помощник.

Рассмотрим, в чем же преимущества и недостатки открытой, закрытой и гибридной экосистем.

Преимущества открытой экосистемы: 1) позволяет достаточно быстро создать экосистему за счет привлечения сторонних разработчиков и партнеров; 2) законодательство часто поддерживает открытые экосистемы, что упрощает взаимодействие с регуляторами. Недостатки: 1) придется контролировать качество сервисов; 2) безопасность.

Преимущество закрытой экосистемы состоит в полном контроле за качеством сервисов на платформе. Недостатки: 1) медленный рост и ограниченное число предложений; 2) регуляторы против закрытых платформ (например, Центробанк выступает за ограничение закрытых экосистем, которые предлагают пользователю готовые пакеты услуг).

Преимущества гибридной экосистемы: 1) контроль качества в направлениях, критичных для экосистемы; 2) мониторинг безопасности в чувствительных направлениях (платежи, персональные данные). Недостатки: 1) ограниченный рост; 2) регуляторы могут посчитать недостаточно открытыми такие экосистемы.

Как видим, экосистемы дают необычные конкурентные преимущества, а также позволяют более агрессивно заходить на новые сферы, вытесняя или даже монополизируя данный рынок (как на примере с Яндексом). ФАС не регулирует такие действия, потому что экосистема была новым явлением для российского рынка. С выходом пятого пакета антимонопольного законодательства ситуация улучшилась, но остаются некоторые проблемы, такие как: отсутствие понятия «экосистема» в законе, ценообразование и кросс-субсидирование, отсутствие в законодательстве возможности учитывать расходы на развитие экосистемы при анализе цен и отсутствие единого подхода к установлению доминирования для разных типов цифровых платформ. Если не решать данные проблемы, то появляются такие риски, как: снижение конкретной среды (трудности для малого и среднего бизнеса); технологический регресс или стагнация из-за отсутствия естественных конкурентов; появление внутренних учетных единиц (денежных суррогатов) [4].

Проведенный анализ позволил выявить взаимосвязь между экосистемой и монополизацией рынка, определить ключевые факторы влияния, обозначив данные положения на примере российских компаний. Полученные результаты могут быть использованы в дальнейших исследованиях для разработки критериев по оценке монополии с экосистемным подходом.

Список использованных источников

1. Яндекс объявляет финансовые результаты за IV квартал 2025 года и 2025 год [Электронный ресурс]. URL: https://yandex.ru/company/news/17-02-2026 (дата обращения: 27.03.2026)..

2. Какую платформу создать для экосистемы: открытую или закрытую [Электронный ресурс]. URL: https://handh.ru/post/ecosystem-platform (дата обращения: 20.03.2026)

3. Официальный сайт ВК [Электронный ресурс] // О компании. URL: https://vk.company/ru/company/about/ (дата обращения: 19.03.2026).

4. Сопина, Н.В. Проблемы монополизации деятельности цифровых платформ и экосистем // Известия Санкт-Петербургского государственного экономического университета. СПб.: Изд-во СПбГЭУ, 2025. № 2 (152). С. 7-12.

Статья представлена научным руководителем, старшим преподавателем кафедры ЭД СПбГУТ, кандидатом экономических наук Т. И. Ююкиной.

УДК 339.9

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ SAUDI ARAMCO: БИЗНЕС-МОДЕЛЬ И ЭКОНОМИКА ПРОМЫШЛЕННЫХ ДАННЫХ

Ю. С. Третьякова (студент группы БИ-2513 СПбГУТ),
tretiakova.ius@sut.ru

В статье рассматриваются бизнес-модель и производственные данные государственной нефтяной компании Saudi Aramco как фактор создания стоимости. Выявлены направления цифровой трансформации: от ресурсной базы и стратегии к количественным показателям, затем – к месту в отрасли и экономике. Особое значение уделено анализу новых феноменов – экономики данных и цифровых сервисов.

Saudi Aramco, транснациональная корпорация, вертикальная интеграция, ОПЕК+, монетизация данных

Saudi Aramco – национальная нефтяная компания, которая превратилась в интегрированного энергетического гиганта. Ее деятельность охватывает полный цикл: от геологоразведки и добычи углеводородов до глубокой переработки и нефтехимии.

Основной продукцией являются: сырая нефть (компания является крупнейшим в мире экспортером), природный газ (активно наращивает добычу для внутреннего потребления и экспорта СПГ), а также нефтехимическая продукция – пластмассы, синтетический каучук, ароматические углеводороды.

В отличие от европейских компаний (например, Shell), у которых активы рассредоточены по всему миру, Saudi Aramco использует стратегию «сбытовых альянсов». Компания не просто продает нефть, а создает совместные предприятия в странах-потребителях, чтобы гарантировать долгосрочный спрос. Ключевым приоритетом является Азия: Китай (совместные предприятия с Sinopec и Huajin), Индия (проект Mega Refinery в Махараштре), Малайзия, Южная Корея (S-Oil). В США компании принадлежит крупнейший в Америке нефтеперерабатывающий комплекс Port Arthur в Техасе. В Европе Aramco имеет долю в нефтепереработке в Нидерландах и других странах [1]. Таким образом, уже на этом этапе видна главная особенность Aramco: при глобальном масштабе сбыта основные производственные мощности (добыча) остаются в стране базирования.

Saudi Aramco является вертикально интегрированной корпорацией. Это означает, что она контролирует всю производственную цепочку: от скважины до заправочной станции и пластиковой гранулы. В структуру

компании входят: разведка и добыча (основа бизнеса, генерирующая основную прибыль благодаря низкой себестоимости), а также переработка, логистика, нефтехимия и сбыт. По состоянию на 2017-2018 годы отношение мощностей переработки к добыче у Aramco было заметно ниже, чем у супермейджеров (Exxon, Shell). К 2026 году этот разрыв значительно сократился за счет активных покупок активов (например, консолидация SABIC) [1, 2].

Именно вертикальная интеграция позволяет компании реализовывать глобальную стратегию, которая базируется на трех столпах, логически дополняющие друг друга.

1. Доминирование в добыче: компания стремится сохранить статус крупнейшего производителя нефти в мире с самой низкой себестоимостью (ниже 20 долл. за баррель). Это позволяет ей выживать в периоды обвала цен и «выдавливать» с рынка высокозатратных конкурентов (например, производителей сланцевой нефти США). Важным элементом выступает сохранение свободных мощностей (около 2-3 млн барр./сут.), которые служат «подушкой безопасности» для мирового рынка, позволяя Aramco мгновенно увеличивать добычу в случае дефицита.

2. Расширение переработки и химии – эта стратегия направлена на снижение рисков: когда цены на сырую нефть падают, прибыль от переработки и нефтехимии позволяет компенсировать потери.

3. Диверсификация и новые технологии – компания инвестирует в водород, возобновляемую энергетику (солнечные панели) и цифровизацию (AI, блокчейн для отслеживания поставок).

Доля компании в мировой добыче нефти составляет около 10-12 %. Весь ОПЕК+ контролирует около 40–50 % рынка [3], но Aramco является лишь частью этого альянса. Для сравнения: доля США в мировой добыче составляет около 15-18 %, которая разделена между сотнями компаний (Exxon, Chevron, ConocoPhillips и множеством независимых сланцевых производителей). Таким образом, Aramco является крупнейшим единоличным производителем, но не производит половину всей нефти планеты.

Saudi Aramco стабильно входит в ТОП-5 крупнейших компаний мира по версиям Fortune Global 500 и Forbes Global 2000. В рейтинге Forbes Global 2000 (2025) она занимает места в первой тройке, конкурируя за лидерство с Apple, Microsoft и JPMorgan Chase. По прибыльности Aramco занимает 1-2 места в мире среди всех корпораций [4, 5].

Говоря о других ТНК страны базирования, следует упомянуть SABIC (Saudi Basic Industries Corporation). Ранее это был независимый гигант химической промышленности (4-й в мире), однако в 2020 году Saudi Aramco

выкупила 70 % акций, и сейчас SABIC является ее дочерней структурой [1]. Таким образом, произошло усиление вертикальной интеграции: Aramco предоставляет сырье, а SABIC производит из него пластик.

Основными конкурентами Aramco на рынке нефти остаются ExxonMobil (США), Shell (Великобритания, Нидерланды), CNPC (Китай). Благодаря государственной поддержке и низкой себестоимости, Aramco находится в более выигрышной позиции, чем американские и европейские конкуренты [6].

Существует системный механизм координации. Saudi Aramco выступает главным инструментом политики Саудовской Аравии в рамках соглашения ОПЕК+ (10 стран-союзников, включая Россию). В отличие от свободного рынка США, где компании конкурируют, Aramco координирует объемы добычи с другими государствами. Цель – управление ценами. Когда цены падают (ниже 70-80 долл. за баррель, Brent), страны ОПЕК+ коллективно сокращают квоты добычи, чтобы создать искусственный дефицит и поднять цены [3]. Роль Aramco в этом механизме уникальна: как обладатель самых больших свободных мощностей, она является «регулятором» рынка. Компания несет на себе основную нагрузку по сокращению добычи во время падения спроса, что позволяет поддерживать рентабельность высокозатратных производителей (например, США). Тем самым низкая себестоимость добычи и свободные мощности превращаются не только в конкурентное преимущество, но и в инструмент глобального ценового регулирования.

Saudi Aramco представляет собой уникальный эмпирический пример, где промышленные данные становятся самостоятельным фактором создания стоимости. Ежесуточный сбор компании составляет порядка 10 млрд телеметрических записей (временные ряды давления, температуры, вибрации). Накопленные данные охватывают 90-летний период эксплуатации месторождений, что создает репрезентативную выборку для обучения моделей машинного обучения на длинных исторических горизонтах.

Важное методологическое замечание – данная модель монетизации является воспроизводимой только при соблюдении трех условий: длительная история накопления данных (не менее 10-15 лет непрерывного сбора); суверенная инфраструктура обработки на краю сети (Edge AI) без передачи сырых данных третьим лицам; гибридная модель (физические уравнения и машинное обучение), обеспечивающая интерпретируемость прогнозов для инженерного персонала.

Ключевыми направлениями цифровой трансформации Saudi Aramco являются: цифровые двойники месторождений и оборудования; предиктивная аналитика (прогнозирование отказов); автоматизация бурения и управления скважинами; единая платформа сбора и обработки промышленных данных [1].

Монетизация данных у Saudi Aramco осуществляется по трем основным каналам:

- предоставление данных как услуги (Data-as-a-Service) для подрядчиков и партнеров;
- коммерческая продажа прогнозных моделей, например, моделей прогнозирования износа оборудования;
- лицензирование цифровых двойников месторождений и производственных объектов.

Saudi Aramco начинает продавать предиктивную аналитику и прогнозные модели партнерам уже в формате сервиса. В результате данные перестают быть исключительно внутренним инструментом оптимизации и превращаются в самостоятельный источник выручки. Именно в этом и проявляется экономика данных в действии как завершающий элемент стратегии компании, где традиционные ресурсные преимущества органично дополняются цифровыми сервисами.

Список используемых источников

1. Saudi Aramco. Annual Report 2025. Dhahran, 2026 [Электронный ресурс]. URL: https://www.aramco.com/en/investors (дата обращения: 26.04.2026).

2. Saudi Aramco. Sustainability Report 2024. Dhahran, 2025 [Электронный ресурс]. URL: https://www.aramco.com/en/investors (дата обращения: 26.04.2026).

3. OPEC. Monthly Oil Market Report 2025. Vienna, 2025 [Электронный ресурс]. URL: https://www.opec.org/ (дата обращения: 26.04.2026).

4. Fortune Media IP Limited. Fortune Global 500 2025 [Электронный ресурс]. URL: https://fortune.com/ranking/global500/ (дата обращения: 26.04.2026).

5. Forbes Global 2000 (2025) [Электронный ресурс]. URL: https://www.forbes.com/lists/global2000 (дата обращения: 16.03.2026)

6. Королевство Саудовская Аравия. Vision 2030: Стратегия диверсификации экономики. Riyadh, 2016 [Электронный ресурс]. URL: https://www.vision2030.gov.sa/en (дата обращения: 26.04.2026).

Статья представлена научным руководителем, старшим преподавателем кафедры ЭД СПбГУТ, кандидатом экономических наук Т. И. Ююкиной.

УДК 005.5+004.8

ОСОБЕННОСТИ И ПРОБЛЕМЫ ОРГАНИЗАЦИИ РАБОТЫ САЛОНА КРАСОТЫ И БЬЮТИ-КОВОРКИНГА

Д. Д. Шерстнева (студент группы БИ-23 СПбГУТ), sherstneva.dd@sut.ru

В условиях трансформации бьюти-индустрии наблюдается переход от традиционной модели салонов красоты к формату бьюти-коворкингов. В статье рассмотрены особенности функционирования данных форматов, выявлены ключевые различия, а также проанализированы основные проблемы, связанные с организацией записи клиентов и загрузкой рабочих мест. Особое внимание уделено вопросам автоматизации процессов с использованием современных цифровых решений.

салон красоты, бьюти-коворкинг, запись клиентов, автоматизация, управление услугами, цифровые сервисы

Современная бьюти-индустрия претерпевает значительные изменения, связанные с развитием новых форм организации труда [1-5]. Наряду с традиционными салонами красоты активно распространяется формат бьюти-коворкингов, представляющий собой пространство для аренды рабочих мест мастерами на гибких условиях.

Актуальность исследования обусловлена ростом популярности коворкинг-модели, а также необходимостью совершенствования процессов управления записью клиентов и использования рабочих ресурсов. Целью работы является анализ особенностей функционирования салонов красоты и бьюти-коворкингов, а также выявление проблем, связанных с организацией записи клиентов и загрузкой рабочих мест.

Основные модели организации работы

Традиционный салон красоты представляет собой иерархическую структуру, в которой мастер является наемным сотрудником, а ключевые функции (поиск клиентов, запись, маркетинг) выполняются администрацией.

Бьюти-коворкинг, напротив, предполагает самостоятельную деятельность мастеров, которые арендуют рабочие места и самостоятельно управляют своей клиентской базой.

В таблице 1 представлены основные различия между двумя моделями.

ТАБЛИЦА 1. Различие моделей

Параметр	Традиционный салон	Бьюти-коворкинг
Статус мастера	Наемный сотрудник	Самозанятый/ИП
Оплата места	Фиксированная аренда или процент (40–50 % с чека)	Почасовая аренда (обычно 150–250 руб/час)
Кто ведет запись	Администратор	Сам мастер
Кто ищет клиентов	Салон	Мастер
График работы	Фиксированный	Гибкий
Входной порог	Высокий (стажировка, испытательный срок)	Низкий (оплатил час – работаешь)

Анализ деятельности предприятий бьюти-сферы показывает наличие ряда системных проблем. Одной из ключевых является снижение рентабельности. В ряде регионов наблюдается превышение числа закрытий салонов над открытиями, что свидетельствует о высокой конкуренции и росте издержек.

Существенные трудности связаны с организацией записи клиентов. Во многих салонах до сих пор используются устаревшие методы – телефонные звонки и бумажные журналы, что приводит к следующим последствиям:

- потеря клиентов из-за перегруженности линии;
- ошибки в расписании;
- невозможность оперативной обработки заявок.

Дополнительной проблемой является высокая нагрузка на администраторов, которые выполняют большое количество рутинных операций:

- прием звонков;
- ведение расписания;
- подтверждение записей

Это увеличивает операционные расходы и снижает качество обслуживания.

Переход мастеров к коворкинг-формату обусловлен рядом факторов.

Во-первых, это экономическая выгода. В традиционных салонах мастер получает лишь часть стоимости услуги, тогда как в коворкинге он сохраняет большую долю дохода.

Во-вторых, важную роль играет организационная свобода:

- самостоятельное формирование графика;
- выбор ценовой политики;
- отсутствие жесткого контроля со стороны администрации.

Кроме того, коворкинг способствует профессиональному развитию за счет взаимодействия с другими специалистами и обмена опытом.

Одним из ключевых направлений решения выявленных проблем является внедрение цифровых систем управления.

Современные платформы позволяют:

- организовать онлайн-запись клиентов 24/7;
- автоматизировать напоминания;
- управлять загрузкой рабочих мест;
- снизить количество неявок.

Использование таких решений дает преимущества для всех участников процесса:

Для клиентов:

- удобство записи;
- доступность сервиса в любое время;
- возможность выбора мастера.

Для мастеров:

- прозрачное расписание;
- снижение административной нагрузки;
- повышение эффективности работы.

Для владельцев:

- оптимизация загрузки ресурсов;
- снижение затрат;
- повышение качества сервиса.

Бьюти-коворкинг является современной и гибкой альтернативой традиционной модели салона красоты. Его развитие обусловлено стремлением мастеров к самостоятельности и снижению издержек.

Внедрение цифровых решений позволит существенно повысить эффективность работы, улучшить качество обслуживания и обеспечить более рациональное использование ресурсов.

Список используемых источников

1. Щемелева И. И. Коворкинг как инструмент организации трудовой деятельности // Теория и практика общественного развития. 2025. № 6. URL: https://cyberleninka.ru/article/n/kovorking-kak-instrument-organizatsii-trudovoy-deyatelnosti (дата обращения: 22.04.2026).

2. Бабич С., Пархименко В. Коворкинг: концепция и перспективы // Наука и инновации. 2014. № 136. URL: https://cyberleninka.ru/article/n/kovorking-kontseptsiya-i-perspektivy (дата обращения: 22.04.2026).

3. Прокопенко К. А., Тихоненко Д. В. Автоматизация работы салона красоты // Актуальные проблемы авиации и космонавтики. 2021. № URL: https://cyberleninka.ru/article/n/avtomatizatsiya-raboty-salona-krasoty (дата обращения: 22.04.2026).

4. Хрипков Р. Н. Инновационные решения для рабочих мест и найма в секторе бьюти-сферы // Евразийский научный журнал. 2023. № 11. URL: https://cyberleninka.ru/article/n/innovatsionnye-resheniya-dlya-rabochih-mest-i-nayma-v-sektore-byuti-sfery (дата обращения: 22.04.2026).

5. Шремед Д. М. Особенности применения классических маркетинговых приемов с целью повышения посещаемости предприятия (на примере салона красоты) // Практический маркетинг. 2018. № 2 (252). URL: https://cyberleninka.ru/article/n/osobennosti-primeneniya-klassicheskih-marketingovyh-priemov-s-tselyu-povysheniya-poseschaemosti-predpriyatiya-na-primere-salona (дата обращения: 22.04.2026).

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом педагогических наук, доцентом А. М. Атаян.

СРЕДСТВА СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

УДК 621.391

ЭНЕРГЕТИЧЕСКИЙ РАСЧЕТ РАДИОЛИНИИ СПУТНИКОВОЙ СВЯЗИ С УЧЕТОМ ПОТЕРЬ СИГНАЛА В ГИДРОМЕТЕОРАХ

О. В. Билиба (студент группы ИКТВ-11 СПбГУТ) , biliba.ov@sut.ru

При проведении энергетических расчетов в радиолиниях спутниковой связи на ослабление сигналов оказывает влияние много факторов, одним из которых является наличие гидрометеоров в космическом пространстве. Наличие такого показателя при проведении расчетов позволит точнее оценивать параметры радиолинии спутниковой связи.

радиолинии спутниковой связи, земная станция, ретранслятор связи, гидрометеоры

В линии спутниковой связи с прямой ретрансляцией сигналов происходит непосредственное усиление и ретрансляция информационного сигнала и шумов ретранслятора. В силу независимости шумов на участках связи можно считать, что суммарное отношение мощности шумов к мощности сигнала на линии определяется выражением:

$$\left(\frac{P_{\text{ш}}}{P_{\text{с}}}\right)_{\Sigma} = \left(\frac{P_{\text{ш}}}{P_{\text{с}}}\right)_{\text{вх РС}} + \left(\frac{P_{\text{ш}}}{P_{\text{с}}}\right)_{\text{вх ЗС}}, \quad (1)$$

где $\left(\frac{P_{\text{ш}}}{P_{\text{с}}}\right)_{\text{вх РС}}$ и $\left(\frac{P_{\text{ш}}}{P_{\text{с}}}\right)_{\text{вх ЗС}}$ – отношение мощности шума и сигнала соответственно на первом и втором участках линий связи в полосе частот демодулятора ЗС.

Выражение (1) можно представить в виде:

$$\frac{1}{h_0^{2*}} = \frac{1}{h_1^{2*}} + \frac{1}{h_2^{2*}}, \quad (2)$$

где $h_0^{2*} = h_{\Sigma}^{2*}$ – требуемое соотношение сигнал/шум на линии спутниковой связи или входе демодулятора приемника ЗС, определяющее заданное

качество передачи информации, т.е. $p^*_{\text{ош}}$; h_1^{2*}, h_2^{2*} – требуемое отношение сигнал/шум на участках ЗС–РС и РС–ЗС соответственно

При предъявлении требований к h_1^{2*} и h_2^{2*} следует учесть, что специфической особенностью радиолинии спутниковой связи в данном случае является неравнозначность интервалов ЗС–РС и РС–ЗС в энергетическом соотношении. Это обусловлено тем, что эффективно излучаемая мощность передатчиков ЗС и реальная чувствительность их приемников, как правило, значительно превышает мощности передатчика и чувствительность приемника РС [1].

Очевидно и то, что для выполнения заданных требований по h_0^{2*} на линии спутниковой связи, на ее участках h_1^{2*} и h_2^{2*} должны быть больше h_0^{2*} на некоторую величину a и b соответственно, т.е.

$$h_1^{2*} = ah_0^{2*}, h_2^{2*} = bh_0^{2*}. \quad (3)$$

Тогда, подставив выражения (3) в (2), получим

$$a = \frac{b}{b-1}. \quad (4)$$

График зависимости коэффициентов нормирования качества связи на участках линии спутниковой связи при превышении сигналов представлен на рисунке 1.

Выражение (3) позволяет распределить заданное отношение h_0^{2*} по двум участкам линии связи [2].

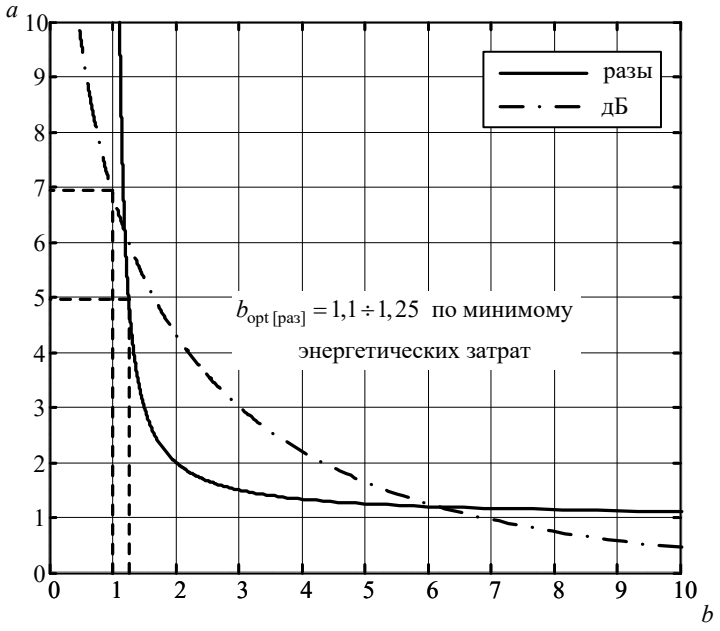


Рис. 1. Коэффициенты нормирования качества на участках линии спутниковой связи

Например, задавшись превышением отношения сигнал/шум h_2^{2*} на участке РС–ЗС, равным $b = 1$ дБ ($b_{[\text{разы}]} = 1{,}26$), видим, что необходимое превышение отношения сигнал/шум h_1^{2*} на участке ЗС–РС должно составлять порядка $a = 7$ дБ ($a_{[\text{разы}]} \approx 5$).

Анализ функциональной зависимости коэффициентов нормирования позволяет сделать следующие выводы:

- значения коэффициентов a и b всегда больше 1;
- равенство коэффициентов нормирования соответствует случаю равенства энергетических затрат на обоих участках линии;
- область выбора коэффициентов в зоне $1 < b < 2$ соответствует варианту, когда энергетика РС жестко ограничена, а ЗС – нет;
- область выбора коэффициентов $1 < a < 2$ соответствует обратной ситуации.

При проектировании военных полевых линий спутниковой связи приходится учитывать ограничения на энергетику не только на РС, но и на ЗС. Поэтому значения коэффициентов рекомендуется выбирать в пределах $a_{[\text{раз}]} = 5 \div 10$, $b_{[\text{раз}]} = 1{,}26 \div 1{,}11$.

Список используемых источников

1. Антенно-фидерные устройства и распространение радиоволн: Учебник для вузов/ Г. А. Ерохин, О. В. Чернышев, Н. Д. Козырев, В. Г. Кочержевский; Под ред. Г. А. Ерохина. 2-е изд., испр. М.: Горячая линия – Телеком, 2004. 491 с.: ил.

2. Марков Г. Т., Петров Б. М., Грудинская Г. П. Электродинамика и распространение радиоволн. Учебн. пособие для вузов. М.: Сов. Радио, 1960. 376 с., ил.

Статья представлена научным руководителем, доцентом кафедры РРТСС ВУЦ СПбГУТ, кандидатом технических наук А. К. Сагдеевым.

УДК 621.396.94

ПОДХОДЫ К ПОСТРОЕНИЮ И МОДЕЛИРОВАНИЮ СПУТНИКОВОГО СЕГМЕНТА В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А. Н. Григорчук (преподаватель СПбГУТ, подполковник (запаса), доцент)
И. А. Евдокимов (студент группы Р-31 СПбГУТ), evdokimov.ia@sut.com

В статье проводится обзор архитектуры и требований к сетям связи специального назначения. Особое внимание уделяется спутниковому сегменту как ключевому элементу обеспечения глобального покрытия и устойчивости каналов управления. Рассматриваются основные физические ограничения, влияющие на качество связи в мобильных системах, включая временные задержки и допплеровские сдвиги частоты. Для оценки влияния орбитальных параметров на характеристики канала предложен метод численного моделирования с использованием пакета MATLAB Satellite Communications Toolbox. Приведен пример программной реализации алгоритма расчета ключевых параметров для низкоорбитальных группировок, что позволяет обосновать выбор технических решений при проектировании сетей специального назначения.

сети связи специального назначения, ВС РФ, спутниковая связь, задержка распространения, доплеровский сдвиг, MATLAB, моделирование каналов связи, низкоорбитальные спутники

В современных условиях ведения боевых действий и обеспечения национальной безопасности критически важную роль играют системы командования и управления. Эффективность напрямую зависит от надежности и пропускной способности сетей связи специального назначения. Одним из приоритетных направлений развития телекоммуникационной инфраструктуры является интеграция космических аппаратов в единую сеть обмена данными. Это обусловлено необходимостью обеспечения связью рассредоточенных группировок войск, мобильных командных пунктов и автономных платформ в любых географических регионах.

Спутниковый сегмент СССН должен удовлетворять жестким требованиям по скрытности, устойчивости к радиоэлектронному подавлению и времени доставки информации. Однако физические законы распространения радиоволн накладывают объективные ограничения на работу каналов связи. В частности, при использовании низкоорбитальных спутниковых систем, обладающих преимуществами в виде меньшей задержки сигнала и требований к мощности передатчика, возникают значительные допплеровские сдвиги частоты и переменные временные задержки [1].

Целью данной работы является обзор ключевых аспектов построения спутникового сегмента сетей специального назначения, а также демонстрация методики оценки физических параметров канала связи.

Обзор архитектуры и требований к сетям специального назначения

Сети связи специального назначения представляют собой комплекс технических средств, обеспечивающих обмен информацией между органами управления и подчиненными элементами в интересах обороны и безопасности. Архитектура таких сетей обычно строится по иерархическому принципу и включает следующие уровни:

1. Магистральный уровень: обеспечивает связь между центральными узлами управления. Здесь часто применяются геостационарные спутники для обеспечения постоянного покрытия.

2. Тактический уровень: требует высокой мобильности и оперативного развертывания. Низкоорбитальные спутники предпочтительнее из-за меньшего времени задержки сигнала (latency), что критично для систем реального времени [2].

3. Уровень оконечных устройств: Мобильные терминалы, носимые комплексы связи, беспилотные системы.

Основные требования к СССН в контексте спутниковой связи включают:

- глобальность покрытия: возможность установления сеанса связи в любой точке земного шара;
- устойчивость: способность сети функционировать в условиях частичного вывода спутников из строя или воздействия помех;
- качество обслуживания: гарантированная полоса пропускания и предсказуемые задержки.

Проблемы физического уровня в мобильных спутниковых каналах

При проектировании СССН инженеры сталкиваются с рядом физических эффектов, которые необходимо компенсировать на этапе планирования сети.

1. Временная задержка распространения. Задержка сигнала определяется расстоянием между передатчиком и приемником. Для спутниковых каналов она складывается из времени прохождения сигнала до космического аппарата и обратно. В системах реального времени (например, видеоконференцсвязь командных пунктов или телеметрия БПЛА) большие задержки могут снижать эффективность управления. Для низкоорбитальных спутников задержка варьируется в зависимости от угла места спутника над горизонтом.

2. Доплеровский сдвиг частоты. Высокая орбитальная скорость спутников ЛЕО (порядка 7 км/с) приводит к значительному изменению частоты принимаемого сигнала вследствие эффекта Доплера. Это требует применения алгоритмов частотной компенсации в приемной аппаратуре специальных терминалов. Величина сдвига зависит от радиальной составляющей скорости спутника относительно наземной станции.

3. Зоны видимости и сеансы связи. В отличие от геостационарных спутников, аппараты на низкой орбите находятся в зоне видимости наземной станции ограниченное время. Для обеспечения непрерывности связи в СССН необходимо использовать группировки спутников и алгоритмы handover.

Для решения задач анализа вышеуказанных параметров применяется современное программное обеспечение, позволяющее моделировать орбитальную динамику и параметры канала. В настоящее время эффективным инструментом является пакет расширений MATLAB Satellite Communications Toolbox, представляющий инструменты для динамического моделирования указанных эффектов [2].

Методика моделирования параметров канала связи

Для количественной оценки влияния орбитальных параметров на характеристики канала в интересах проектирования СССН был разработан алгоритм расчета ключевых параметров. Процесс исследования включает следующие этапы, реализованные в среде MATLAB с использованием обновленных имен переменных для улучшения читаемости кода.

1. Инициализация сценария моделирования.

Задаются временные параметры моделирования, соответствующие потенциальному сеансу связи или суткам мониторинга обстановки. На основе этих параметров формируется объект спутникового сценария simObj.

```
tStart = datetime(2023, 5, 15, 10, 0, 0);
tStop = tStart + hours(24);
dt = 60;
 % Формирование объекта сценария
simObj = satelliteScenario(tStart, tStop, dt);
```

2. Добавление узлов сети (спутник и наземная станция).

Спутник добавляется в сценарий с использованием данных о его орбите из TLE-файла (двухстрочные элементы орбиты), что позволяет моделировать реальное положение группировки. Наземная станция (например,

подвижный командный пункт) задается своими географическими координатами с помощью функции gs.

```
tleName = "orbit_data.txt";
sat = satellite(simObj, tleName);
gsName = "Москва";
lat = 55.75; % Широта
lon = 37.61; % Долгота
gs = groundStation(simObj, "Name", gsName,...
 "Latitude", lat, "Longitude", lon);
```

3. Анализ видимости.

Функция acc определяет интервалы времени, когда спутник находится в зоне видимости наземной станции. Это позволяет производить расчеты только для тех моментов, когда канал связи существует, что критично для планирования сеансов передачи данных в СССН [2].

```
acc = access(sat, gs);
vis = accessStatus(acc);
```

4. Итерационный расчет параметров канала.

В цикле по каждому временному шагу, где есть видимость, выполняются расчеты геометрических и кинематических параметров:

- Азимут, угол места и наклонная дальность с помощью функции aer.
- Временная задержка сигнала рассчитывается как отношение дальности к скорости света.
- Вектор скорости спутника получается с помощью функции states.
- Выделяется радиальная составляющая скорости, определяющая допплеровский эффект.

```
for i = 1:numSteps
 t = timeVector(i);
 if vis(i)
 [az(i), el(i), rng(i)] = aer(sat, gs, t);
 tau(i) = rng(i) / c; % Расчет задержки
 [~, vSat] = states(sat, t,...
 "CoordinateFrame", "geographic");
 % Расчет радиальной скорости и доплера
 end
end
```

5. Расчет доплеровского сдвига.

На основе радиальной скорости и несущей частоты сигнала вычисляется абсолютный доплеровский сдвиг частоты [3, 4].

```
fc = 12e9; % Несущая частота 12 ГГц
fr = (c./ (c – radialVelocity)) * fc;
```

```
fd = fr - fc;
```

6. Визуализация и сохранение результатов.

Строятся графики зависимости параметров от времени, вычисляются производные характеристики (рис. 1). Результаты сохраняются для последующего анализа и внесения корректив в параметры модемов специальной аппаратуры.

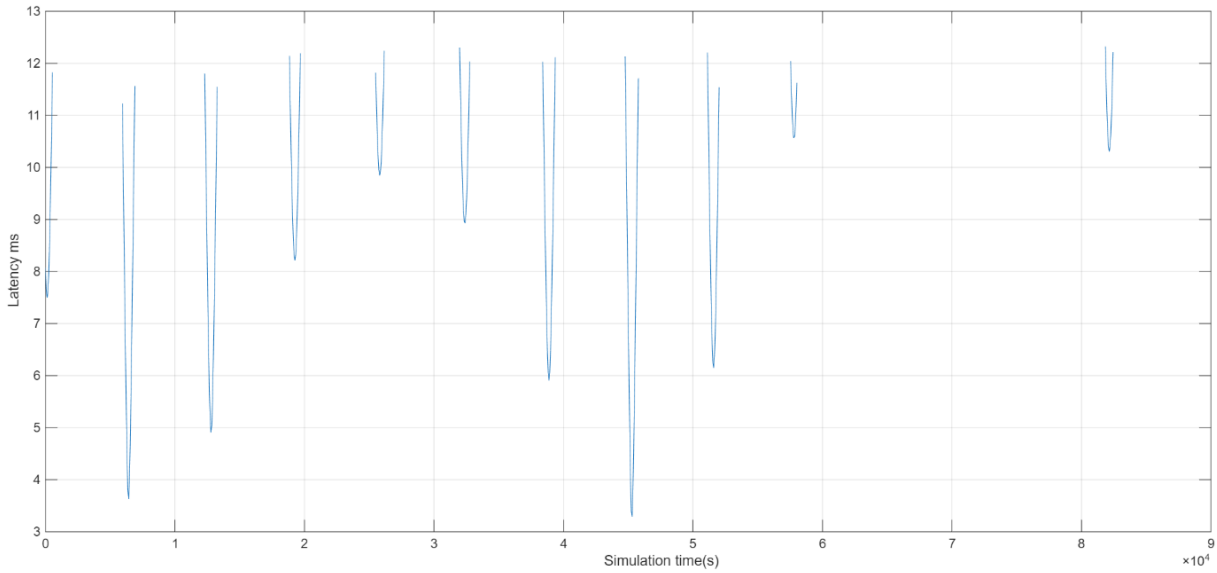


Рис. 1. График зависимости задержки распространения сигнала от времени

Выполнение разработанного скрипта позволяет получить набор графических зависимостей, демонстрирующих характер изменения задержки и доплеровского сдвига в течение сеанса связи (рис. 2).

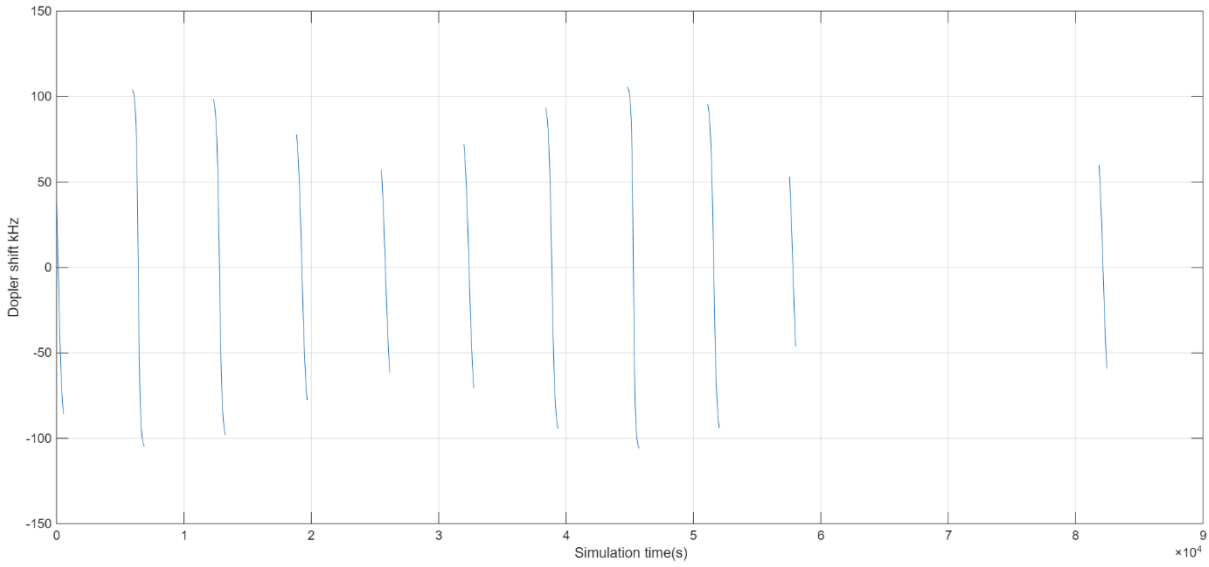


Рис. 2. График зависимости доплеровского сдвига частоты от времени

Анализ результатов показывает, что для низкоорбитальных спутников диапазон изменения доплеровского сдвига может достигать десятков килогерц, что требует соответствующей полосы захвата следящих систем приемников.

Проведенное исследование демонстрирует эффективное применение MATLAB Communications Toolbox для анализа параметров спутниковых каналов связи. Предложенная методика обеспечивает точную оценку временных и частотных характеристик для различных конфигураций спутниковых систем.

Разработанный алгоритм обладает модульной структурой, что позволяет адаптировать его для анализа спутников с различными орбитальными параметрами и конфигурациями наземных станций. Это делает методику преактивным инструментом для проектирования перспективных спутниковых систем.

Список используемых источников

1. Чечин Г. В. Спутниковая связь: Учебное пособие. 2004. 538 с.

2. Сомов А. М. Распространение радиоволн и антенны спутниковых систем связи. Учебное пособие для вузов. М.: Горячая линия – Телеком. 2015. 456 с.

3. Сомов А. М. Спутниковые системы связи: Учебное пособие для вузов. Под ред. А. М. Сомова, 2011. 244 с.

4. Документация Satellite Communications Toolbox. Экспонента. URL: https://docs.exponenta.ru/satcom/ug/calculate-latency-and-doppler-in-a-satellite-scenario.html (дата обращения: 05.03.2026).

Статья представлена доцентом кафедры РРТСС, кандидатом технических наук А. К. Сагдеевым.

УДК 621.391

ПРИМЕНЕНИЕ MIMO-АРХИТЕКТУРЫ ДЛЯ ПОВЫШЕНИЯ ДАЛЬНОСТИ И УСТОЙЧИВОСТИ УКВ-РАДИОСВЯЗИ

А. Н. Обухов (студент группы ИКТВ-11 СПбГУТ), obukhov.an@sut.ru

В статье рассматриваются возможности применения MIMO-архитектуры для повышения дальности и устойчивости УКВ-радиосвязи. Показано, что использование нескольких передающих и приемных антенн позволяет эффективнее использовать многолучевое распространение радиоволн, повышать отношение сигнал/шум и улучшать энергетические характеристики радиолинии. Особое внимание уделено работе системы в условиях отсутствия прямой видимости, городской застройки и лесистой местности. Приводятся основные преимущества технологии MIMO, практические результаты ее применения, а также ограничения, связанные с энергопотреблением, синхронизацией и сложностью аппаратной реализации.

MIMO, УКВ-радиосвязь, радиолиния, пространственное разнесение, многолучевое распространение, повышение дальности связи

MIMO (Multiple Input Multiple Output) представляет собой технологию беспроводной связи, основанную на использовании нескольких антенн на передающей и принимающей сторонах радиолинии [1, 2]. Основная идея данной технологии заключается в одновременной передаче нескольких сигналов в одном частотном диапазоне, что позволяет повысить устойчивость связи, увеличить пропускную способность канала и улучшить энергетические характеристики радиолинии [1, 3].

В традиционных системах радиосвязи используется одна передающая и одна приемная антенна, то есть архитектура SISO (Single Input Single Output). При такой организации радиосигнал распространяется по одному основному каналу, что делает систему более чувствительной к затуханию, многолучевому распространению и другим факторам, ухудшающим качество связи. Технология MIMO позволяет повысить надежность радиоканала за счет использования нескольких независимых путей распространения сигнала и пространственной обработки на стороне приема [1, 2].

К основным преимуществам применения MIMO-архитектуры в системах УКВ-радиосвязи относятся пространственное разнесение, увеличение отношения сигнал/шум и повышение пропускной способности канала. Пространственное разнесение позволяет передавать и принимать сигнал по нескольким независимым каналам, снижая влияние замираний и многолучевости. Это особенно важно в сложной радиосреде, например в городской застройке, лесных массивах и на пересеченной местности, где отраженные сигналы могут быть использованы для повышения устойчивости приема [1, 2, 3].

Другим важным преимуществом является увеличение отношения сигнал/шум. За счет совместной обработки сигналов, поступающих с нескольких приемных антенн, становится возможным более эффективное восстановление передаваемой информации. Это повышает энергетический выигрыш радиолинии и способствует увеличению дальности устойчивой связи. Кроме того, использование нескольких пространственных потоков позволяет передавать данные параллельно в пределах одного частотного канала, увеличивая скорость передачи без расширения занимаемой полосы частот [1, 3, 4].

Принцип функционирования системы MIMO заключается в одновременной передаче нескольких сигналов через разные антенны передатчика. На приемной стороне несколько антенн принимают сигналы, распространяющиеся по различным траекториям. Специальные алгоритмы обработки позволяют разделять пространственные потоки и комбинировать их для восстановления исходной информации [2, 5, 6].

Принцип работы системы MIMO представлен на рис. 1. В рассматриваемой конфигурации используются две передающие и две приемные антенны, что позволяет формировать два пространственных канала передачи данных. При этом сигнал распространяется по нескольким траекториям, отражаясь от различных объектов окружающей среды. В традиционных системах такие отражения нередко приводят к интерференции и ухудшению качества связи. Однако в системах MIMO отраженные сигналы могут использоваться как дополнительные источники информации, повышающие устойчивость приема [1, 2].

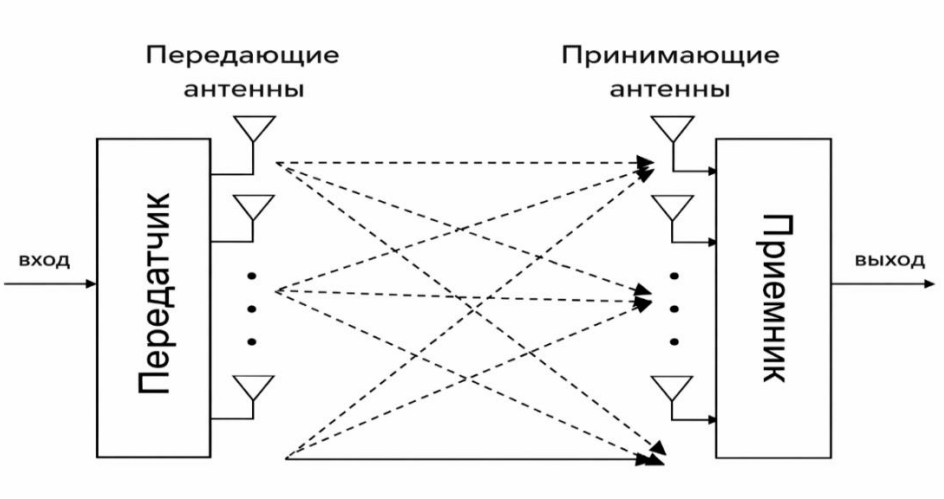


Рис. 1. Принцип работы системы MIMO

Согласно результатам теоретических и экспериментальных исследований, применение MIMO-архитектуры позволяет повысить энергетические характеристики радиоканала, улучшить устойчивость связи и эффективнее использовать многолучевое распространение сигнала [1, 2, 3]. В городской среде радиосигналы отражаются от зданий, сооружений и других объектов инфраструктуры, формируя множество альтернативных путей распространения. Принимающая сторона MIMO-системы способна анализировать сигналы, поступающие с различных направлений, и объединять их для повышения качества приема. Таким образом, многолучевое распространение, традиционно рассматриваемое как источник помех, в MIMO-системах может использоваться как дополнительный ресурс для повышения надежности радиосвязи [1, 2].

Практические исследования и результаты моделирования подтверждают эффективность применения технологии MIMO в радиосистемах различного назначения, в том числе в условиях сложной радиосреды [2, 3, 5, 6]. Использование нескольких антенн обеспечивает повышение устойчивости приема, улучшение качества передачи и рост пропускной способности канала. Это особенно важно для УКВ-радиосвязи, где условия распространения сигнала могут существенно изменяться в зависимости от местности, препятствий и наличия прямой радиовидимости.

Одним из наиболее важных преимуществ технологии MIMO является ее эффективность в условиях отсутствия прямой видимости между абонентами. В городской среде отражения от зданий формируют дополнительные каналы передачи, а в лесистой местности пространственное разнесение позволяет уменьшить влияние затухания радиоволн при прохождении через растительность. Благодаря этому достигается повышение надежности связи и увеличение рабочей дальности радиолинии по сравнению с традиционными одноантенными системами [1, 2, 3].

Зависимость дальности радиосвязи от количества используемых антенн представлена на рис. 2. Анализ показывает, что увеличение числа антенных элементов в системе MIMO позволяет значительно повысить эффективность радиоканала. Однако одновременно возрастает сложность аппаратной реализации, требования к обработке сигналов и энергопотребление оборудования.

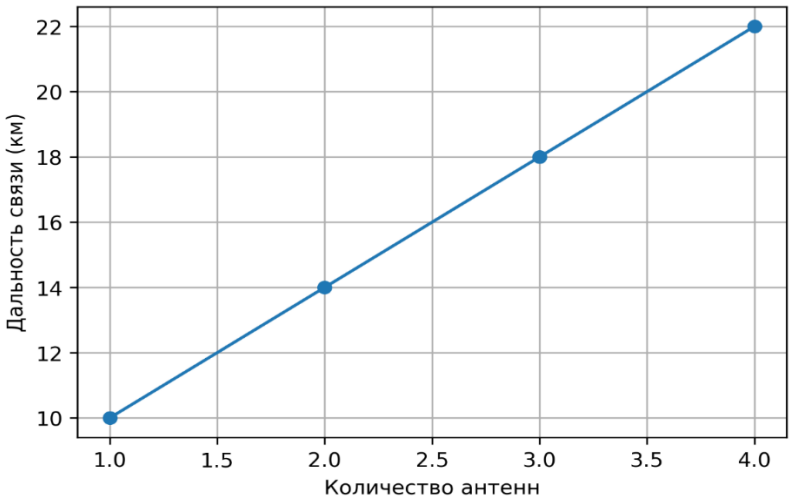


Рис. 2. Рост дальности связи при увеличении числа антенн

Сводная оценка основных характеристик технологии MIMO приведена в таблице 1.

ТАБЛИЦА 1. Сводная оценка технологии MIMO

Параметр	Характеристика
Основная цель	Повышение устойчивости связи, SNR и пропускной способности канала
Ключевой механизм	Использование нескольких антенн и пространственных каналов передачи
Эффект в сложной среде	Снижение влияния многолучевости и замираний сигнала
Практический результат	Рост дальности связи в открытой, городской и лесистой местности
Основные ограничения	Энергопотребление, синхронизация, стоимость и конструктивная сложность

Несмотря на значительные преимущества, применение технологии MIMO связано с рядом технических ограничений. Одним из основных факторов является повышенное энергопотребление, поскольку использование нескольких передающих и приемных трактов требует дополнительных энергетических ресурсов. Еще одной проблемой является сложность синхронизации антенных элементов. Для корректной работы системы необходимо обеспечить точную временную и фазовую синхронизацию сигналов, поступающих с различных антенн. Кроме того, увеличение числа антенных элементов приводит к усложнению конструкции радиостанции и увеличению ее стоимости [2, 3, 5].

Таким образом, применение MIMO-архитектуры в системах УКВ-радиосвязи является эффективным способом повышения устойчивости, дальности и пропускной способности радиоканала. Наибольшая эффективность технологии проявляется в условиях сложной радиосреды и отсутствия прямой видимости, где многолучевое распространение может использоваться не как источник помех, а как дополнительный ресурс повышения качества связи. Вместе с тем практическое внедрение MIMO требует учета ограничений, связанных с энергопотреблением, синхронизацией и усложнением аппаратной реализации [1, 2, 3].

Список используемых источников

1. Бакулин М. Г., Крейнделин В. Б., Панкратов Д. Ю. Применение технологии MIMO в современных системах беспроводной связи разных поколений // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 4. С. 4–12.

2. Панкратов Д. Ю., Степанова А. Г. Компьютерное моделирование технологии MIMO для систем радиосвязи // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 12. С. 33–37.

3. Ермолаев В. Т., Флаксман А. Г., Лысяков Д. Н. Увеличение пропускной способности MIMO-системы радиосвязи с параллельной передачей данных по собственным подканалам // Вестник Нижегородского университета им. Н. И. Лобачевского. 2010. № 3(1). С. 79–86.

4. Панкратов Д. Ю., Степанова А. Г. Алгоритм демодуляции на основе метода Чебышева для систем MIMO // Фундаментальные проблемы радиоэлектронного приборостроения. 2018. Т. 18. № 4. С. 1057–1061.

5. Панкратов Д. Ю., Степанова А. Г. Моделирование систем MIMO // Фундаментальные проблемы радиоэлектронного приборостроения. 2017. Т. 17. № 4. С. 1052–1056.

6. Панкратов Д. Ю., Степанова А. Г. Вычислительная сложность алгоритмов демодуляции систем MIMO с большим числом антенн // DSPA: Вопросы применения цифровой обработки сигналов. 2021. Т. 11. № 1. С. 11–20.

Статья представлена научным руководителем, доцентом кафедры РРТСС ВУЦ СПбГУТ, кандидатом технических наук А. К. Сагдеевым.

УДК 623.61

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ НА ОСНОВЕ АНАЛИЗА ОПЫТА СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

А. А. Скаредин (студент группы ИКТВ-11 ВУЦ СПбГУТ),
skaredin.aa@sut.ru

Специальная военная операция (СВО) выявила существенные недостатки классической системы связи тактического звена управления, базирующейся на средствах пятого поколения и иерархическом принципе построения. В условиях массированного применения противником средств радиоэлектронной борьбы и высокоточного оружия традиционные подходы к организации связи демонстрируют низкую устойчивость, недостаточную пропускную способность и ограниченную живучесть. В работе проведен анализ организационно-штатной структуры батальона, состава средств связи и классических способов организации связи. На основе выявленных недостатков сформулированы предложения по повышению эффективности системы связи, включающие техническое переоснащение, внедрение распределенных пунктов управления, интеграцию всех родов связи в единую информационно-телекоммуникационную сеть и совершенствование системы подготовки кадров. Предлагаемые решения позволяют повысить устойчивость, скрытность и непрерывность управления в условиях современных вооруженных конфликтов.

тактическое звено управления, система связи, специальная военная операция, радиоэлектронная борьба, помехозащищенность, живучесть, единая информационная сеть

Современные вооруженные конфликты характеризуются высокой динамикой боевых действий, массированным применением высокоточного оружия, средств радиоэлектронной борьбы (РЭБ) и беспилотных летательных аппаратов. В данных условиях существенно возрастают требования к системам управления войсками, технической основой которых является связь. Наиболее критическое значение это приобретает в тактическом звене управления – на уровнях от батальона до отделения, где боевые задачи реализуются в непосредственном соприкосновении с противником, а любой сбой в передаче информации может привести к невыполнению поставленной задачи и неоправданным потерям личного состава [1].

Специальная военная операция (СВО), проводимая с февраля 2022 года, стала первым для Вооруженных Сил Российской Федерации опытом масштабного вооруженного противоборства с противником, обладающим

сопоставимым военно-техническим потенциалом и современными средствами РЭБ. Опыт данной операции позволил выявить существенные недостатки классической системы связи тактического звена, сложившейся в конце XX века и закрепленной действующими наставлениями [2].

Классическая система связи мотострелкового (танкового) батальона строится по иерархическому принципу с комплексным применением радиосвязи, радиорелейной и проводной связи. Основу системы составляют командно-штабные машины (КШМ) командира батальона и начальника штаба, оснащенные радиостанциями средней мощности (Р-123М, Р-173, Р-168-5УН). Ротационное звено управляется портативными радиостанциями, взводное и отделенческое – носимыми радиостанциями малой мощности (Р-168-0,5У, Р-168-0,1У). Связь строится по принципу радиосетей: сеть командира батальона, сети рот, сети обеспечения. Радиорелейная связь применяется для организации многоканальных линий с вышестоящим штабом, проводная – преимущественно в обороне.

Анализ реального применения данной системы в ходе СВО выявил ряд системных недостатков, делающих ее уязвимой перед лицом современных средств РЭБ и высокоточного оружия [3].

Низкая помехозащищенность. Классическая система создавалась для условий эпизодического применения средств РЭБ и не учитывает возможность тотального подавления радиоэфира. Скорость псевдослучайной перестройки рабочей частоты (ППРЧ) штатных радиостанций пятого поколения Р-168 «Акведук» (до 100 скачков/с) оказалась недостаточной для противодействия современным комплексам РЭБ, способным ставить прицельные помехи «в след». Работа на фиксированных частотах, часто становившаяся вынужденной мерой из-за сложностей синхронизации, делала радиосети легкой добычей для перехвата и подавления. Радиорелейные линии, несмотря на большую помехозащищенность, также уязвимы для прицельных помех.

Ограниченная дальность и устойчивость в низовом звене. Нормативные показатели дальности носимых радиостанций (2 км для Р-168-0,5У, 1 км для Р-168-0,1У) в условиях городской застройки, пересеченной местности и при наличии помех часто недостижимы. Экранирующее действие зданий, холмов, металлоконструкций приводит к потере управления взводами и отделениями, особенно при действии штурмовых групп в глубине обороны. Это вынуждает командиров использовать сигнальные средства, что демаскирует их и ведет к повышенным потерям.

Недостаточная пропускная способность. Система ориентирована преимущественно на голосовой обмен. Передача целеуказаний, координат, видеоинформации с беспилотных летательных аппаратов затруднена и требует развертывания дополнительных каналов (например, СВЧ-радиосетей), что не всегда возможно. Отсутствие у командиров тактического звена доступа к единой информационной сети снижает ситуационную осведомленность и замедляет принятие решений.

Низкая живучесть. Требования по выносу мощных радиостанций на удаление от КНП и размещению КШМ в укрытиях с дистанционным управлением часто нарушаются. В результате вскрытие КНП средствами разведки противника ведет к его огневому поражению, выводя из строя должностных лиц и средства связи. Система, лишенная ядра, теряет устойчивость и непрерывность управления.

Несоответствие структуры радиосетей новым формам боя. Основной тактической единицей стали штурмовые группы (отделение-взвод). Классическая структура (батальон – рота – взвод) оказалась громоздкой. Радиосети командиров рот перегружены, не обеспечивают управление в звене «взвод – отделение – солдат». Отсутствие отдельных взводных сетей (из-за нехватки радиостанций) вынуждает использовать голос и сигналы, что в городском бою невозможно [4].

Зависимость от коммерческих спутниковых систем. Широкое использование терминалов Starlink создало критическую зависимость. Отключение доступа в критические моменты приводило к потере важнейших каналов связи. Отечественные военные спутниковые системы показали низкую надежность в полевых условиях, сложность настройки и громоздкость оборудования.

Недостаточный уровень подготовки личного состава. Поступление новых радиостанций шестого поколения (Р-187 «Азарт») с высокой скоростью ППРЧ (до 20 000 скачков/с) и возможностью IP-ретрансляции вызвало трудности. Личный состав пытался использовать их в старых режимах, не реализуя защитный потенциал. Потребовалось целенаправленное обучение для преодоления негативного отношения к новой технике.

Выявленные недостатки свидетельствуют о том, что классическая система связи батальона не соответствует требованиям, предъявляемым современными вооруженными конфликтами. Опыт СВО требует безотлагательного принятия мер по ее модернизации. В связи с этим сформулированы следующие направления повышения эффективности.

Техническое переоснащение. Форсированное насыщение войск радиостанциями шестого поколения Р-187 «Азарт» с высокой скоростью ППРЧ, что делает их практически неуязвимыми для существующих средств постановки помех «в след». Разработка и внедрение новых алгоритмов помехоустойчивого кодирования, автоматического выбора частот. Создание и оснащение каждого военнослужащего малогабаритными средствами связи с режимом ретрансляции, способными обеспечить связь в городской застройке. Продолжение работ по интеграции современных средств связи в объекты бронетанкового вооружения и техники.

Повышение живучести. Внедрение принципа распределенных пунктов управления, при котором средства связи рассредоточиваются на местности, а должностные лица управляют ими дистанционно по проводным или волоконно-оптическим линиям. Применение мощных радиоизлучающих средств по принципу «выстрелил – ушел» – работа короткими сеансами с последующей сменой позиции. Совершенствование систем дистанционного управления и создание мобильных защищенных укрытий для должностных лиц [5].

Интеграция и унификация. Создание единой информационно-телекоммуникационной сети тактического звена на основе программно-конфигурируемых и самоорганизующихся mesh-сетей, объединяющей все роды связи (радио, радиорелейную, спутниковую, проводную) и автоматически маршрутизирующей трафик по доступным каналам в зависимости от помеховой обстановки и загруженности. Обеспечение сопряжения со средствами других силовых ведомств через унифицированные интерфейсы и шлюзы. Интеграция в сеть средств разведки (БПЛА) для создания замкнутого контура разведки и огневого поражения.

Развитие системы подготовки кадров. Пересмотр программ боевой подготовки с учетом опыта СВО. Обучение работе на современных комплексах связи должно стать обязательным для всех категорий командиров – от командира отделения до командира батальона. Создание современных тренажеров для отработки навыков в условиях, приближенных к боевым (с имитацией помех, огневого воздействия, быстрой смены обстановки). Подготовка специалистов, способных настраивать и восстанавливать сложную технику в полевых условиях.

Предлагаемые решения базируются на реальном боевом опыте, подтвердившем эффективность радиостанций шестого поколения, усилителей

мощности, наземных и воздушных ретрансляторов. Применение радиостанций Р-187-П1 совместно с усилителями мощности УМ-20 и УМ-40 позволило значительно увеличить дальность связи в тактическом звене. Интеграция этих средств в бронеобъекты обеспечила прирост управляемости и возможность работы в помехозащищенном режиме на дальности до 24 км. Положительно зарекомендовали себя режимы IP-ретрансляции и многопролетной ретрансляции, а также использование самоорганизующихся mesh-сетей [6].

Реализация предложенных направлений позволит существенно повысить эффективность системы связи тактического звена управления по ключевым показателям: устойчивости (помехозащищенности, живучести, надежности), непрерывности, достоверности, своевременности, скрытности, пропускной способности, доступности и управляемости. Это обеспечит командирам возможность оперативно и гарантированно управлять подразделениями в любых условиях обстановки, что является одним из ключевых факторов достижения победы в современном бою.

Список используемых источников

1. Организация связи в мотострелковом (танковом) батальоне общевойскового соединения: учеб. пособие / Е. В. Зяблицев, А. А. Карпенко, В. М. Козырев [и др.]; под ред. Г. М. Машкова. СПб.: СПбГУТ, 2014. 52 с.

2. Опыт применения средств связи в ходе специальной военной операции: аналитический обзор / под общ. ред. В. В. Герасимова. М.: Изд-во ГШ ВС РФ, 2023. 87 с.

3. Иванов А. А., Петров Б. В. Повышение помехоустойчивости радиосвязи в тактическом звене управления // Вестник связи. 2024. № 2. С. 34–41.

4. Скаредин А. А. Научно-исследовательская работа: отчет о НИР / Скаредин А. А. СПб.: СПбГУТ, 2026. 6 с.

5. Шевченко А. В. Метод построения самоорганизующихся сетей радиосвязи в тактическом звене // Актуальные проблемы инфотелекоммуникаций: материалы XIII Междунар. науч.-техн. конф., Санкт-Петербург, 21–22 нояб. 2024 г. СПб.: СПбГУТ, 2024. С. 156–160.

6. Груздев Д. А., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Инфотелекоммуникационная система специального назначения и система радиоподавления как объект конфликта // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах. Санкт-Петербург, 2024. С. 696-699.

Статья представлена научным руководителем начальником цикла – старшим преподавателем военного учебного центра Д. С. Самаркиным.

СПбГУТ)))