

**2025**

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

# **СТУДЕНЧЕСКАЯ ВЕСНА**

## **СБОРНИК НАУЧНЫХ СТАТЕЙ**



**VESNA.SUT.RU**

**СПбГУТ)))**



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

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

**СТУДЕНЧЕСКАЯ ВЕСНА**

13-15 мая 2025

**Сборник научных статей**

**СПб ГУТ)))**

Санкт-Петербург

2025

УДК 001:061.3(082)  
ББК 72  
С 88

**79-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна-2025»:** сб. науч. ст. / Под ред. А. В. Рабина; сост. А. А. Дзюбаненко, И. М. Татарникова. СПб.: СПбГУТ, 2025. 569 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, и. о. начальника 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

### Заместитель председателя

**Окунева Д. В.** – кандидат технических наук, проректор по проектной деятельности СПбГУТ

### Члены организационного комитета

**Бобровский В. И.** – доктор технических наук, доцент, и.о. директора НИИ «Технологии связи» СПбГУТ

**Дружков К. В.** – кандидат экономических наук, директор департамента экономики и финансов СПбГУТ

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

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

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

**Гребелина Н. В.** – начальник управления информатизации СПбГУТ

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.

## 8 ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

- 8 **Баскова А. Ю.** Моделирование звуковых эффектов с применением кепстрального анализа
- 12 **Белов М. С.** Измерение профиля пучка лазера на выходе 6-сердцевинных микроструктурированных оптических волокон с разной закруткой
- 16 **Блан Ф. С.** Архитектура и применение сетей, определяемых знаниями
- 22 **Бразовский Г. Р.** WDM мультиплексор для полимерных оптических волокон
- 27 **Бразовский Г. Р., Яцкова А. Е.** Экспериментальное исследование учебной пассивной оптической сети в лаборатории кафедры ОКСС
- 32 **Брюшинин А. Ю., Пивоваров Д. С.,** Анализ требований функционала программных средств для систем искусственного интеллекта
- 37 **Гольдштейн А. Б., Елисеев С. М.** Новые возможности и новые задачи включения виртуальных операторов MVNO в сети поколений 5G 6G
- 43 **Елагин В. С., Поляков С. А.** Применение моделей прогнозирования в задачах управления жизненным циклом АПК
- 51 **Елагин В. С., Серикова М. П.,** Применение графовых нейронных сетей для классификации криптовалютного трафика
- 56 **Жиляков В. П.** Акустические особенности концертных и спортивных площадок и их влияние на проектирование систем звукоусиления
- 62 **Зимин А. В., Кондратьев А. М.** Использование сетей Петри для тестирования сетевых протоколов
- 67 **Катыкин Д. А., Туманова Е. И.** Исследование методов по улучшению распознавания объектов в условиях затрудненной видимости
- 71 **Колпаков С. В.** Математическое моделирование работы оптического Фурье-процессора
- 75 **Кравец Е. В., Подсветова В. П.** Методы обеспечения качества обслуживания (QoS)
- 81 **Кравец Е. В., Подсветова В. П.** Управление городским освещением
- 87 **Кропанина А. А.** Особенности передачи информационных сообщений через канал акустического трансформатора
- 91 **Мочалов А. А.** Методы обучения нейросети DTLN в задаче шумоподавления
- 95 **Орехова В. О.** Влияние параметров конфигурации сети 5G NR на спектральные характеристики сигналов
- 100 **Татаренков Д. А., Трапезникова Е. А.** Применение генеративных нейросетей для формирования виртуальных ракурсов
- 104 **Татаренков Д. А., Фомин П. В.** Роль ротоскопии в обеспечении реалистичности комбинированных съемок с 3D-объектами
- 110 **Терентьева С. А.** Разработка психоакустической модели Perceptual Evaluation of Audio Quality
- 116 **Хафизов Р. Т.** Пространственный звук в виртуальной и дополненной реальности
- 120 **РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА**
- 120 **Алексеев А. Э.** Планирование и оптимизация транспортной сети оператора для улучшения показателей GTP Loss
- 125 **Гмырин В. В.** Оценки точности параметров радионавигационного сигнала
- 130 **Деткова В. М., Надаршин М. Б., Слюсаренко М. В.** Применение ферромагнитного резонанса в ферритовых фильтрах



- 135 **Коробейников А. Н., Носенко Е. И., Седышев Э. Ю.** Механический коммутатор для передающих линий СВЧ диапазона
- 140 **Мельникова М. А.** Сравнительный анализ методов обеспечения внутрисистемной ЭМС в низкоорбитальных спутниковых системах связи
- 144 **Пирогов Н. С.** Исследование особенностей распространения СВЧ сигналов над водной поверхностью
- 150 **Попугаев Д. Г. Шабанов А. П.** Анализ правовых аспектов технологий блокчейн в управлении предприятием
- 153 **Процкий П. А.** Разработка метода выявления дефектов на металлических поверхностях в реальном времени
- 160 **Сидоров А. Д.** Цифровизация лабораторной работы «Исследование апериодического разряда конденсатора. Определение емкости конденсатора»
- 163 **Смирнов Д. П.** Обзор методов внесения предсказания
- 168 **Чернышов А. С.** Исследование и разработка RAG-системы для извлечения и анализа пространственной информации из текстовых данных
- 172 **ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ**
- 172 **Алиев А. Э.** Анализ трансформации рынка информационных технологий в условиях санкционного давления
- 178 **Байзигитов М. М., Панчин А. В.** Применение методов объяснимого ИИ для медицинской диагностики на основе лабораторных данных
- 183 **Баранов С. Н., Краева Е. В., Тарасова Д. В.** Автоматизация медицинских процессов в стоматологии: функциональный подход к проектированию программного обеспечения
- 189 **Бариев Д. Р.** Проектирование информационной системы для автоматического подбора музыкальных композиций на основе анализа визуальных характеристик изображения
- 194 **Большаков Г. В., Козлов П. И.** Формирование модели информационной системы для поддержки студенческих стартапов
- 200 **Бура А. П., Жуков М. А., Колганов И. М., Кураш Д. И., Орлова К. А.** Теория графов в продолжении рода с прогнозом
- 204 **Вайтович Д. В.** Проектирование гибкой обучающей платформы для работы с API
- 209 **Васильков А. А., Даненко Д. А., Харлова А. А.** Исследование зависимости между корректностью программ и стилем программирования
- 215 **Верещагин Р. А.** Разработка информационной системы для управления учебным взаимодействием между преподавателями и студентами
- 221 **Верещагин Р. А., Жаранова А. О.** Разработка алгоритма сравнения документов на основе лемматизации и нормализованного редакционного сходства
- 224 **Вивчарь Р. М., Гончаров В. А.** Методика поиска корневых причин нарушений нормального функционирования гибридной сети
- 229 **Винокурова Д. В.** Программный подход к выбору начальных приближений для решения нелинейных уравнений численными методами
- 235 **Волков М. А.** Автоматизация учета ресурсов телекоммуникационного оборудования с использованием протокола SNMP
- 243 **Восьмаков Д. И.** Разработка информационной системы для студентов и преподавателей университета
- 249 **Герасимова М. В., Калинина С. С.** Интеграция системного анализа и веб-дизайна в процессе разработки современных информационных систем

- 254 **Голактионов Д. А., Раковский О. В.** Трансформерные архитектуры и FEW-Shot Learning новая парадигма в машинном обучении для современных информационных систем
- 260 **Голощанов А. С., Мерзляков М. В., Филиппова Е. В.** Проектирование информационной системы для мониторинга Северного сияния и других астрономических явлений
- 264 **Громов В. В., Пашенкова В. В.** Применение частных блокчейн-сетей для фиксации торговых операций на зерновых биржах в целях повышения прозрачности ценообразования
- 270 **Дмитриев М. С., Зверева С. А.** История и тенденция развития нейросетей
- 275 **Довыденков А. С.** Проектирование хеш-функции для хеш-таблицы
- 280 **Жаранов Д. О.** Проектирование интеллектуальной системы прогнозирования личностных характеристик на основе анализа музыкальных предпочтений
- 285 **Журов Е. А., Крутицкий А. Н., Романцов И. А.** Методы анализа больших данных: от традиционных к современным
- 291 **Кечко В. В.** Прогнозирование деградации качества FPLV-связи с применением методов машинного обучения: сравнительный анализ подходов
- 296 **Кинкульская К. В., Коровкина Е. В.** Искусственный интеллект в медицинской диагностике
- 299 **Ковалев В. С., Коровкина Е. В.** Анализ технологии MCR и ее преимуществ
- 303 **Коломиец А. Р., Морозов М. Е.** Разработка многопоточных приложений для построения и прохождения неидеальных лабиринтов
- 309 **Котелин П. В., Скалецкая И. Е.** Программное решение для расчета факторов сходимости и воспроизводимости, влияющих на процесс измерений
- 314 **Лопаткина Е. А.** Технические аспекты проявления людо-нарративного диссонанса в игровых системах
- 319 **Луценко Д. А., Тумин М. А., Хайдаршин К. Р.** Сравнительный анализ современных алгоритмов трекинга объектов на основе нейронных сетей
- 325 **Платонов А. О., Кларк А. Е.** Построение трехмерной модели местности на основе облака точек в среде Unity
- 329 **Позняк М. О.** Проектирование системы мониторинга безопасности детей с возможностью частного и централизованного контроля
- 335 **Пугачевский А. О.** Использование интеллектуальных ассистентов и чат-ботов для поддержки учителей и учеников в школе
- 339 **Раковский О. В., Турлыков И. И.** Исследование цифровых инструментов построения и споровождения индивидуальных образовательных траекторий
- 342 **Сидоров Д. В.** Оценка малых языковых моделей при взаимодействии с Model Context Protocol в локальных системах
- 349 **Филиппов К. А.** Смарт-контракты: применение и вызовы в реальных сценариях
- 353 **Фирсов В. Н.** Гибридный метод разметки данных с микрообратной связью и отложенной верификацией на примере неисправностей асинхронных электродвигателей
- 358 **Чухарев И. А.** Анализ основных методов предобработки образовательных данных
- 362 **Якубова О. А.** Разработка программного комплекса моделирования группового поведения персонала в процессе деятельности организации

**367 КИБЕРБЕЗОПАСНОСТЬ**

- 367 Алексеева К. Е., Дюсметова А. А., Пестов И. Е.** Анализ поверхности атаки в среде виртуализации zVirt
- 373 Алехин Р. В., Камалова А. О., Пестов И. Е., Платонова Т. А., Смирнов Д. Н.** Исследование зависимости времени передачи данных в различных типах облачных инфраструктур от выбранного алгоритма шифрования
- 378 Бирих Э. В., Гаврилов П. Р.** Методика комплексной оценки уровня зрелости системы информационной безопасности организации
- 382 Борисов А. А., Зозуля Г. С.** Методы обеспечения безопасности в сетях на основе туманных вычислений
- 387 Васильев Н. А., Лещинский Б. С., Ситдииков Д. С.,** Кибербезопасность в беспроводных сетях
- 391 Вахтель В. Ю.** Анализ стойкости протоколов квантового распределения ключей к атаке типа перехват-отправка на основе квантового канала в свободном пространстве
- 395 Ильин Я. А., Махмутова Н. Ф.** Разработка защищенного решения для настройки устройств с использованием технологии NFC
- 400 Казакова А. В.** Анализ существующих методов верификации моделей искусственного интеллекта для обеспечения их целостности при передаче
- 406 Карышев А. И.** OSINT в социальных сетях: разработка инструмента автоматизированного анализа цифровой безопасности аккаунтов
- 411 Ковцур М. М., Киструга А. Ю., Филимонов В. Е.** Сравнительный анализ Javascript-библиотек для визуализации графов в системе мониторинга беспроводных сетей
- 417 Красов А. В., Пимашин Е. Н., Раковский С. А.** Хеширование исходного кода с использованием TREE-SITTER: CALL HASH, IMP HASH, SEM HASH
- 422 Лебедева Д. А., Лагутина С. В.** Анализ эффективности методов защиты от фишинга
- 427 Манохина Г. А., Пестов И. Е.** Механизмы обеспечения информационной безопасности программного комплекса средств виртуализации «Брест»
- 432 Мокринский Н. И.** Методика вложения цифровых водяных знаков в байт-код Java посредством модификации опкодов, анализ и реализация
- 438 Паунежев М. Х.** Система детектирования скрытой съемки экрана
- 442 Пестов И. Е., Федотовская А. Д.** Анализ временных задержек платформ больших данных для выявления аномалий и злоумышленников от теории к практике
- 448 Пешкина В. В.** Модифицированный алгоритм Евклида деления в кольце классов вычетов
- 553 Потемкина Ю. Ф.** Автоматизированное моделирование процессов аутентификации для анализа безопасности системы
- 457 Сидельников А. С.** Сравнительный анализ open-source сканеров уязвимостей
- 461 Соколов И. В.** Адаптация квазибиологических принципов под задачи защиты информации
- 466 Третьякова А. С.** Анализ эффективности систем защищенного электронного документооборота
- 471 Хаддад М. Н.** Исследование механизмов информационной безопасности беспроводных сетей
- 477 Шагисултанов Т. А.** Анализ производительности EBPF и IPTABLES в задачах сетевой фильтрации контейнерных приложений
- 484 Шарифов Р. Г.** Исследование свойств WAZUH при построении защищенного компонента JBC

**490 СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ И ЭКОНОМИКА ДАННЫХ**

- 490 Багери Н. А.** Иран во Второй мировой войне: от нейтралитета до Тегеранской конференции
- 497 Баранова П. В.** Государственная регуляция китайского жестового языка в контексте авторитарного политического режима
- 501 Бармин Е. Ф.** Конкурентные преимущества банка в условиях цифровой трансформации на примере ВТБ
- 506 Волчик О. В., Федорова С. А.** Разработка алгоритма создания процессной модели исполнительного органа государственной власти
- 512 Кривенко А. С.** Особенности продвижения историко-просветительских проектов (на примере «История российского предпринимательства»)
- 517 Лапшина Е. Н., Мустафаев М. Р.** Эффективный корпоративный контент: стратегии, креатив и аналитика
- 523 Макаров В. В., Фокичев А. А.** Влияние технологии 5G на развитие услуг для бизнеса в телекоммуникациях
- 529 Макарова С. Б.** Теоретико-методологические подходы и рекомендации по продвижению событийных мероприятий
- 534 Михайлюк В. С.** Позиция государства по отношению к церкви в современной Финляндии
- 539 Постникова Д. Н.** Особенности организации местной власти в Китае на примере СУАР
- 543 Скрынченко К. А.** Связи с общественностью в театральной сфере: успешные практики работы с молодежной аудиторией
- 547 Соколов П. В.** Роль социальных сетей в формировании имиджа бренда и его влиянии на потребителей
- 551 Соловьев Н. С.** Исследование возможностей искусственного интеллекта в диагностике сурдологических заболеваний

**557 СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

- 557 Вилкова Ю. Д., Цыгоняева А. Ю.** Особенности продвижения госорганизаций посредством социальных сетей
- 563 Власов И. А., Скрыков И. А.** Расчет и компенсация реактивной составляющей проволочных антенн диапазона 200 метров

## ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 681.84.087

А. Ю. Баскова (студент группы Р-41м, СПбГУТ), [baskova.au@sut.ru](mailto:baskova.au@sut.ru)

### МОДЕЛИРОВАНИЕ ЗВУКОВЫХ ЭФФЕКТОВ С ПРИМЕНЕНИЕМ КЕПСТРАЛЬНОГО АНАЛИЗА

*В данной работе рассматривается применение кепстрального анализа для моделирования звуковых эффектов, что представляет собой важный аспект в области обработки аудиосигналов. Кепстральный анализ, основанный на преобразовании Фурье, позволяет выделять характеристики звука, которые не всегда очевидны во временной или частотной области. Особое внимание уделяется алгоритмам синтеза звука, использующим кепстральные представления для изменения тембра, реверберации и других акустических параметров.*

*синтез звука, звуковые эффекты, кепстральный анализ, нелинейная обработка сигналов*

Звуковые эффекты играют важную роль в музыке, кино и видеоиграх, создавая атмосферу и усиливая эмоциональное восприятие. В последние годы методы цифровой обработки сигналов стали основным инструментом для создания и манипуляции звуковыми эффектами. Одним из таких методов является кепстральный анализ, который позволяет выявлять и анализировать различные характеристики звуковых сигналов, которые не всегда очевидны во временной или частотной области. В данной статье рассматривается применение кепстрального анализа для моделирования звуковых эффектов.

Кепстральный анализ – это метод нелинейной обработки сигналов, основанный на преобразовании Фурье. Преобразование сигнала в его кепстр является гомоморфным преобразованием, которое отображает свертку в сложение.

Он включает в себя следующие этапы:

1. Преобразование Фурье: Сигнал преобразуется в частотную область с использованием дискретного преобразования Фурье.

2. Взятие логарифм спектра.

3. Обратное преобразование Фурье.

Таким образом формула для расчета кепстра имеет следующий вид [1]:

$$C[n] = \sum_{n=0}^{N-1} \log \left( \left| \sum_{n=0}^{N-1} x_n e^{-j\frac{2\pi}{N}kn} \right| \right) e^{j\frac{2\pi}{N}kn},$$

где  $C[n]$  – кепстральные коэффициенты,  $x_n$  – значения дискретного сигнала.

Кепстральный анализ позволяет создавать алгоритмы, реализующие получение тембральных характеристики звука, которые можно использовать для синтеза новых звуковых эффектов, например, таких как реверберация. Реверберация – это эффект, который имитирует отражение звука от поверхностей в помещении. Кепстральный анализ может быть использован для создания алгоритмов, которые моделируют характеристики реверберации, анализируя кепстральные коэффициенты исходного звукового сигнала и применяя их к синтезированному сигналу.

На рис. 1 верхний график иллюстрирует исходный сигнал и его задержанную во времени копию (эхо-сигнал), меньшую по уровню. Нижний график демонстрирует сумму вышеуказанных сигналов:

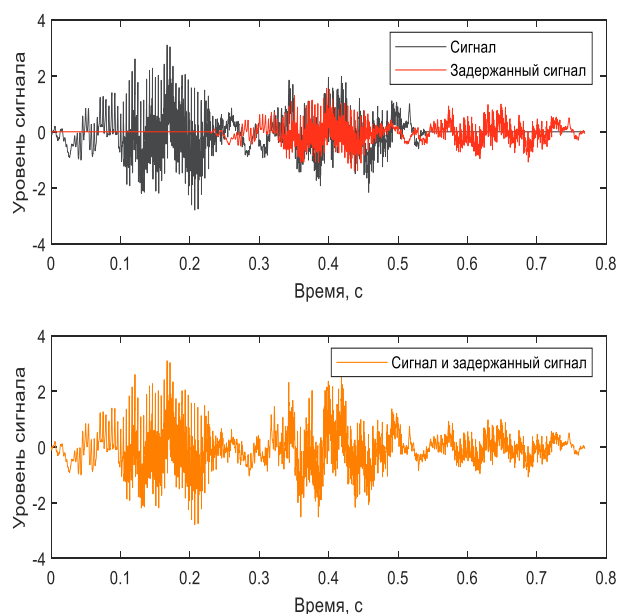


Рис. 1. График исходного сигнала и сигнала задержанного во времени

Применение кепстрального анализа позволяет детектировать сигнал, задержанный во времени, и его длительность задержки. Результат работы кепстрального анализа представлен на рис. 2:

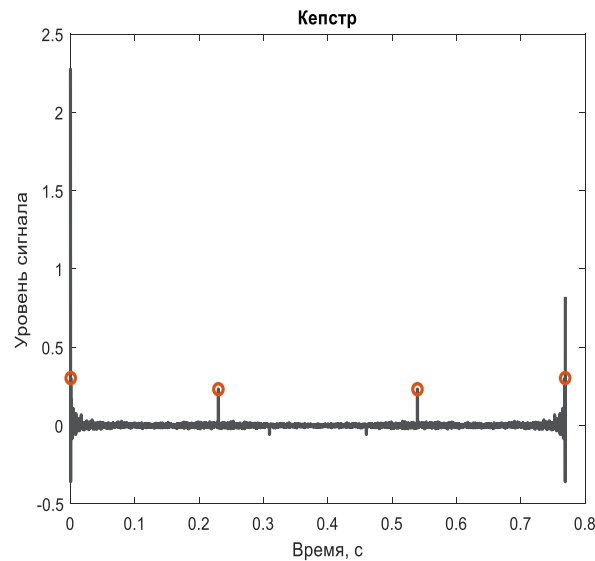


Рис. 2. Кепстр суммы исходного и задержанного во времени сигналов

На графике отображается время прихода основного сигнала (0 сек.) и время прихода отраженного сигнала (0.22 сек). Уровень сигнала обозначен красными пиками. Таким образом кепстральный анализ, применяя фильтрацию, дает возможность отфильтровать эхо-сигнал, позволяя получить исходный сигнал без влияния эффекта реверберации (рис. 3).

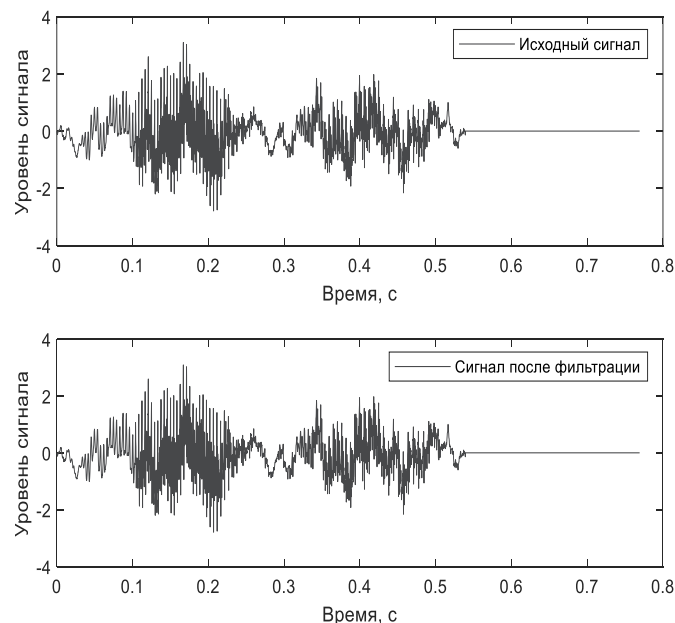


Рис. 3. Осциллограммы исходного сигнала (верхний график) и сигнала после фильтрации (нижний график)

Амплитуда разностного сигнала пренебрежимо мала. Поэтому артефакты сигнала после фильтрации так же малы и не заметны на слух.

Коэффициенты эхо-сигнала в кепстральной области позволяют манипулировать данным сигналом, регулируя его уровень и время прихода, что способствует гибкости в использовании звукового эффекта реверберации [2].

Кепстральный анализ является мощным инструментом для моделирования звуковых эффектов. Его применение в создании реверберации, синтезе звуковых тембров и моделировании искажений открывает новые горизонты для композиторов и музыкантов. В дальнейшем развитие алгоритмов и методов, основанных на кепстральном анализе, может привести к созданию еще более сложных и интересных звуковых эффектов.

#### **Список используемых источников**

1. Rabiner L. R., Juang B.-H. Fundamentals of Speech Recognition. Prentice Hall. 1993.
2. Ellis D. P. W. Prediction of Speech Intelligibility Using Mel-Frequency Cepstral Coefficients // IEEE Transactions on Audio, Speech, and Language Processing. 2025.

*Статья представлена научным руководителем, старшим преподавателем кафедры цифрового телевидения и метрологии Свиной О. А.*



УДК 681.7.068

## ИЗМЕРЕНИЕ ПРОФИЛЯ ПУЧКА ЛАЗЕРА НА ВЫХОДЕ 6-СЕРДЦЕВИННЫХ МИКРОСТРУКТУРИРОВАННЫХ ОПТИЧЕСКИХ ВОЛОКОН С РАЗНОЙ ЗАКРУТКОЙ

М. С. Белов (студент группы 2215А-24, СПбГУТ), [belov.ms@sut.ru](mailto:belov.ms@sut.ru)

*В данной работе сопоставлены результаты измерений профиля пучка оптического излучения источника белого света в дальнем поле на выходе опытных образцов микроструктурированных кварцевых волокон длиной 2 м, отличающихся степенью закрутки. Волокна, разработанные и успешно изготовленные с наведенной в процессе вытяжки закруткой 100 и 600 оборотов на метр, имеют наружный диаметр 125 мкм, содержат шесть  $\text{GeO}_2$ -легированных сердцевин диаметром 8,7 мкм с квазиступенчатым профилем показателя преломления высотой 0,0300.*

*многосердцевинные микроструктурированные оптические волокна, киральные микроструктурированные оптические волокна, профиль пучка оптического излучения, условия равномерной радиальной засветки*

В последние десятилетия многосердцевинные микроструктурированные оптические волокна (МСОВ) с различной геометрией и составом материалов вызывают устойчивый научный интерес благодаря их уникальным волноводным свойствам и потенциалу применения в сенсорике, высокомогущей фотонике и телекоммуникационных системах на базе пространственного мультиплексирования [1, 2]. Особенно перспективными представляются МСОВ с легированными сердцевинами и наведенной закруткой, которые позволяют эффективно управлять модовой структурой передаваемого излучения и его пространственным распределением [3].

Данная работа посвящена экспериментальному исследованию профиля пучка белого света в дальней зоне после прохождения через отрезки длиной 2 метра опытных микроструктурированных оптических волокон с шестью  $\text{GeO}_2$ -легированными сердцевинами, изготовленных с разными степенями закрутки: 100 и 600 оборотов на метр (об/м). Исследуемые МСОВ были возбуждены в условиях радиальной равномерной засветки (ROFL conditions) через одномодовое волокно стандарта ITU-T G.652 [4, 5]. Центрирование торца ОВ и исследуемого МСОВ обеспечивалось прецизионным воздушным зазором в диапазоне 150...200 мкм. Данная конфигурация позволила обеспечить одновременное возбуждение всех шести сердцевин.

Исследуемые МСОВ включали шесть  $\text{GeO}_2$ -легированных сердцевин с диаметром 8.7 мкм, равноудаленных от центра ОВ на расстоянии двойного шага гексагональной решетки микроструктуры (14.4 мкм) и 121 капилляр (воздушное отверстие) диаметром 4.6 мкм (рис. 1). Заготовки германосиликатных сердцевин со ступенчатым профилем показателя преломления изготавливались из опорных труб из кварцевого стекла, содержащих более 1000 ppm гидроксильных групп (аналог Heraeus Suprasil Standard, Saint-Gobain Spectrosil A/B, Corning HPFS 7980, JGS1, Dynasil 1100 / Dynasil 4100, КУ-1 по ГОСТ 15130-86). Полученные сердцевинны реализованы методом MCVD и характеризовались квази-ступенчатым профилем с максимальной разностью значений показателя преломления 0.0300, содержащим  $\text{GeO}_2$  в кварцевом стекле 20.5 мол. %. Профиль показателя преломления обозначен квази-ступенчатым из-за технологического дефекта: характерного провала в центре стержня и сглаженных переходов между сердцевинной и оболочкой. Внешний диаметр всех волокон соответствовал стандартному телекоммуникационному значению – 125 мкм.

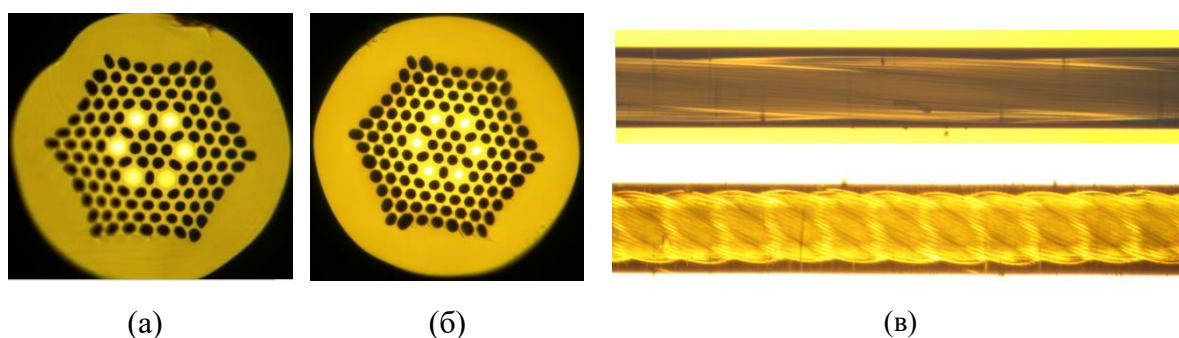


Рис. 1. Фотографии опытных образцов кварцевых киральных 6- $\text{GeO}_2$ -сердцевинных МСОВ: (а) закрутка 100 об/м; (б) закрутка 600 об/м; (в) продольное сечение

Закрутка волокон в 100 и 600 об/м наводилась непосредственно в процессе вытяжки волокна путем модификации вытяжной башни и использования вращающегося, при помощи коллекторного двигателя, блока подачи. Полученные образцы успешно демонстрировали устойчивое наличие спиральной геометрии при высокой повторяемости структуры.

Экспериментальная установка показана на рисунке 2. Для анализа распределения выходного излучения использовалась ИК-камера с экспозицией 50.0 мс. Полученные профили нормализовались, выравнивались по центру и представлены с одинаковым масштабом 1000x1000 отн. ед.

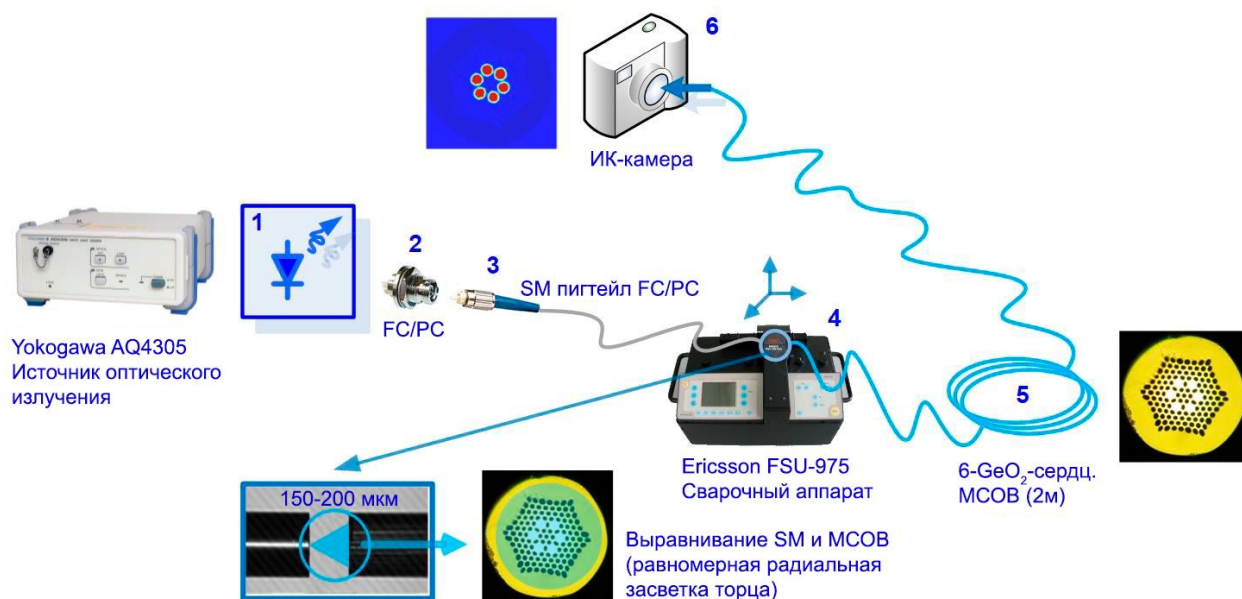


Рис. 2. Установка для измерения профиля пучка белого света в дальнем поле

Наиболее наглядно различия между волокнами с разной степенью закрутки проявились в распределении интенсивности света вдоль центра оси "у", где при закрутке 600 об/м наблюдалось значительное «стягивание» модового поля в центры германосиликатных сердцевин из периферийной (относительно ее положения в структуре ОВ) «кварцевой» части поперечного сечения МСОВ по сравнению с 100 об/м. Так, для волокна с наведенной закруткой 100 об/м ширина пиков по полувысоте (FWHM) оказалась в среднем в 1.7 раза больше, чем для волокна с 600 об/м. Результаты измерения профиля пучка и результаты постобработки (вычитания) полученных паттернов приведены на рисунке 3.

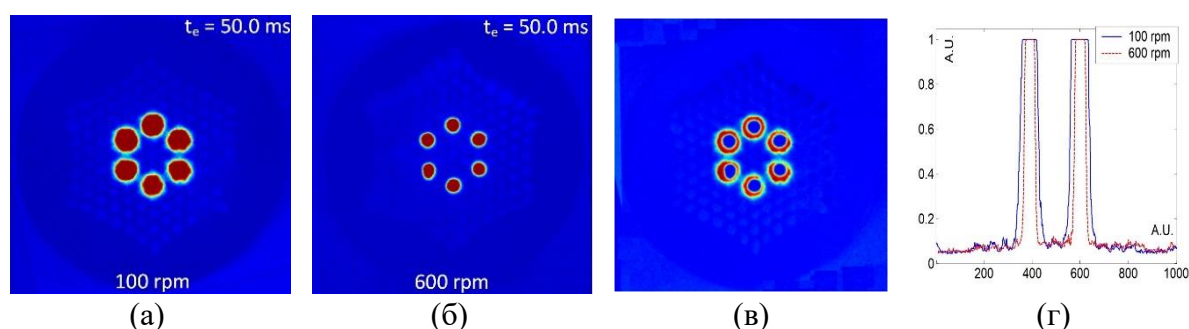


Рис. 3. Профили пучка излучения белого источника в дальнем поле на выходе 6-GeO<sub>2</sub>-сердцевинных МСОВ: (а) 100 об/м; (б) 600 об/м; (в) и (г) результаты вычитания

Таким образом, проведенные измерения профиля пучка белого света в дальней зоне при прохождении через закрученные 6-сердцевинные МСОВ наглядно продемонстрировали эффект «стягивания» поля суперпозиции

мод при разной степени закрутки. Данный эффект перераспределения энергии в область сердцевин в зависимости от степени закрутки открывает перспективы для оптимизации проектирования МСОВ в задачах создания компактных сенсоров, мультиплексоров, а также новых фотонных компонентов для систем с пространственным мультиплексированием.

#### Список используемых источников

1. Buczynski R. Photonic crystal fibers // Acta Physica Polonica. 2004. Vol. 106. № 2. PP. 141–143. DOI:10.12693/APhysPolA.106.141.
2. Liu Zh., Tam H. Y. Selected Topics on Optical Fiber Technologies and Applications. Chapter 1. Fabrication and Sensing Applications of Special Microstructured Optical Fibers. Intechopen, 2018.
3. Ma X., Zhu C., Hu I.-N., Kaplan A., Galvanauskas A. Single-mode chirally-coupled-core fibers with larger than 50µm diameter cores // Optics Express. 2014. Vol. 22. DOI:10.1364/OE.22.009206.
4. Cunningham D., Nowell M. EMB, WCMB and ROFL testing // IEEE 802.3z Task Force. Presentation materials. July 1997. URL: [https://grouper.ieee.org/groups/802/3/z/public/presentations/july1997/DC\\_modbw.pdf](https://grouper.ieee.org/groups/802/3/z/public/presentations/july1997/DC_modbw.pdf) (дата обращения 07.05.2025).
5. Optical Fibres, Cables and Systems. ITU-T Manual. Geneva, 2009.

*Статья представлена научным руководителем, профессором кафедры ОКСС СПбГУТ, доктором технических наук, профессором Бурдиным А. В.*

УДК 004.72

Ф. С. Блан (аспирант группы 2215А-24, СПбГУТ), [blan.fs@sut.ru](mailto:blan.fs@sut.ru)

## АРХИТЕКТУРА И ПРИМЕНЕНИЕ СЕТЕЙ, ОПРЕДЕЛЯЕМЫХ ЗНАНИЯМИ

*Сети, определяемые знаниями (Knowledge-Defined Networking, KDN) – инновационная парадигма управления сетями, интегрирующей искусственный интеллект для обеспечения интеллектуального сетевого поведения. В данной статье представлена пятиплоскостная архитектура KDN с центральной плоскостью знаний для автоматизации принятия решений, а так же рассмотрены ключевые сценарии применения в управлении трафиком, обеспечении безопасности и виртуализации сетей.*

*сети, определяемые знаниями, архитектура сети, машинное обучение, интеллектуальное управление, автоматизация сетей*

Современное развитие сетевых технологий характеризуется переходом от статических, жестко конфигурируемых архитектур к более гибким и программируемым решениям. Эволюция от традиционных сетей к программно-определяемым сетям (Software-Defined Networking, SDN) продемонстрировала значительные преимущества централизованного управления, программируемости и динамической конфигурации сетевых устройств [1]. Однако современные вызовы телекоммуникационной отрасли, включающие экспоненциальный рост трафика, требования к низким задержкам, необходимость поддержки разнообразных приложений и услуг, а также растущую сложность сетевых инфраструктур, требуют более интеллектуальных и адаптивных решений управления.

Концепция сетей, определяемых знаниями (Knowledge-Defined Networking, KDN), представляет следующий эволюционный этап в развитии сетевых архитектур, где знания, полученные с помощью методов искусственного интеллекта и машинного обучения, становятся основой для автоматизированного и интеллектуального управления сетевой инфраструктурой [2]. В отличие от традиционного подхода SDN, основанного на централизованном контроле потоков данных, KDN интегрирует плоскость знаний, которая использует передовые алгоритмы машинного обучения для анализа сетевых данных, выявления паттернов поведения и генерации интеллектуальных стратегий управления.

Архитектурная основа KDN, продемонстрированная на рисунке 1, представляет собой расширенную версию традиционной структуры SDN и

включает пять взаимосвязанных логических плоскостей: плоскость передачи данных, плоскость управления, плоскость мониторинга, плоскость знаний и плоскость приложений. Каждая из этих плоскостей выполняет специализированные функции, обеспечивая комплексное интеллектуальное управление сетевой инфраструктурой. Центральным элементом архитектуры выступает плоскость знаний, которая собирает, обрабатывает и анализирует данные из всех остальных плоскостей, генерируя на их основе знания для оптимизации работы сети.

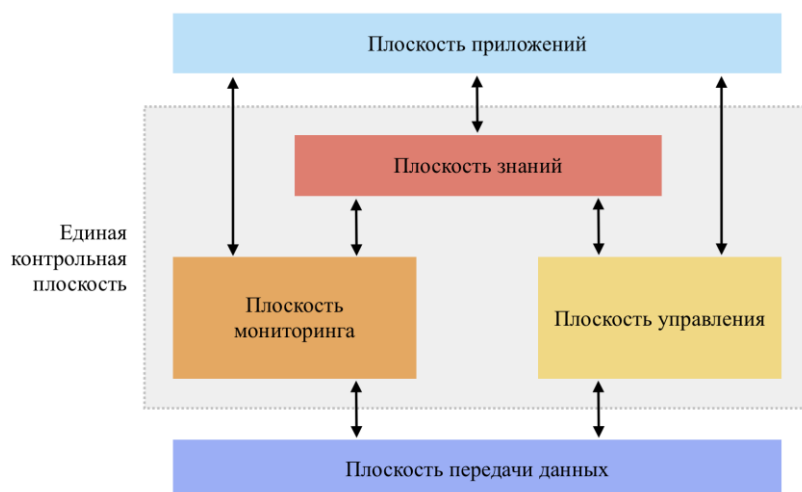


Рис. 1. Схематическая блок-диаграмма архитектуры сетей, определяемых знаниями

Плоскость передачи данных в архитектуре KDN сохраняет свою основную функцию обработки и передачи пакетов данных в соответствии с правилами и политиками, получаемыми от плоскости управления. Однако в контексте KDN эта плоскость требует существенно большей вычислительной мощности и пропускной способности по сравнению с традиционными SDN-решениями, поскольку объем управляющей информации и телеметрических данных, передаваемых между плоскостями, значительно возрастает. Устройства плоскости данных должны поддерживать расширенные возможности сбора статистики, мониторинга и адаптивной настройки параметров в реальном времени.

Плоскость управления в KDN выполняет координацию маршрутизации, распределения ресурсов и управления потоками данных, активно интегрируя знания, полученные от плоскости знаний, для принятия более интеллектуальных и обоснованных решений. В зависимости от требований к масштабируемости, отказоустойчивости и производительности, плоскость управления может быть реализована в различных архитектурных конфигу-



рациях: централизованной, где один контроллер управляет всей сетью; распределенной, где управление распределено между несколькими контроллерами; или гибридной, сочетающей преимущества обоих подходов.

Плоскость мониторинга отвечает за непрерывный сбор телеметрических данных, контроль состояния сетевых устройств, отслеживание параметров производительности и настройку показателей качества обслуживания (Quality of Service, QoS). Важной особенностью KDN является четкое разделение функций мониторинга и управления, что существенно упрощает процессы диагностики, поиска и устранения неисправностей. Плоскость мониторинга использует специализированные протоколы для сбора данных и предоставляет унифицированный интерфейс для взаимодействия с другими компонентами системы.

Центральным и наиболее инновационным компонентом архитектуры KDN выступает плоскость знаний, которая состоит из трех специализированных подуровней, каждый из которых выполняет определенные функции в процессе генерации, обработки и распространения знаний [3]. Подуровень генерации знаний использует разнообразные методы машинного обучения, включая обучение с учителем для прогнозирования на основе размеченных данных, обучение без учителя для выявления скрытых паттернов в неразмеченных данных, и глубокое обучение для решения сложных нелинейных задач анализа и классификации. Этот подуровень извлекает описательные знания из потоков сырых данных, поступающих от других плоскостей, и преобразует их в структурированную форму, пригодную для дальнейшего анализа и принятия решений.

Подуровень композиции знаний выполняет функции объединения и синтеза различных типов знаний, используя редакторы онтологий для создания семантических связей между разнородными данными и генераторы правил для формирования политик управления на основе накопленных знаний и пользовательских намерений. Этот подуровень также реализует механизмы обучения с подкреплением, позволяющие системе адаптироваться к изменяющимся условиям и оптимизировать свое поведение на основе получаемой обратной связи от сетевой среды.

Подуровень управления и распределения знаний обеспечивает централизованное хранение всех типов знаний, включая сгенерированные знания, сформированные правила и политики, а также исходные данные и управляющие сообщения. Этот подуровень отвечает за стандартизацию форматов представления знаний, обеспечение их совместимости между различными

компонентами системы, и эффективное распределение знаний между плоскостями в соответствии с установленными приоритетами и политиками доступа [4].

Плоскость приложений предоставляет высокоуровневый программный интерфейс для определения бизнес-политик, пользовательских намерений и требований к качеству обслуживания, которые автоматически транслируются в конкретные конфигурации и правила управления через механизмы плоскости знаний. Эта плоскость включает два основных подуровня: подуровень определения намерений и политик, позволяющий администраторам задавать высокоуровневые цели и ограничения, и подуровень обновления намерений и политик, который динамически адаптирует эти цели на основе текущего состояния сети и накопленных знаний.

Применение технологии KDN охватывает широкий спектр сценариев использования в современных телекоммуникационных системах. В области управления трафиком KDN обеспечивает интеллектуальную маршрутизацию с учетом текущего состояния сети, прогнозирование загрузки каналов связи на основе исторических данных и паттернов поведения пользователей, динамическое перераспределение полосы пропускания в соответствии с приоритетами приложений, и автоматическую балансировку нагрузки для оптимизации использования сетевых ресурсов. Алгоритмы машинного обучения анализируют многомерные паттерны трафика, выявляют аномалии в поведении сети и предсказывают потенциальные проблемы до их возникновения.

В сфере обеспечения информационной безопасности KDN реализует проактивный подход, основанный на интеграции методов обнаружения аномалий, предиктивной аналитики и автоматического реагирования на угрозы [5]. Система способна в реальном времени анализировать сетевой трафик, выявлять подозрительную активность, классифицировать типы атак и автоматически применять соответствующие защитные меры. Централизованная плоскость знаний обеспечивает согласованность политик безопасности во всей сетевой инфраструктуре и позволяет быстро распространять информацию о новых угрозах между всеми компонентами системы.

Виртуализация сетей и технология разделения сетевых ресурсов представляют еще одну важную область применения KDN. Система поддерживает создание множественных изолированных виртуальных сетевых сегментов на единой физической инфраструктуре, каждый из которых может



иметь индивидуальные политики управления, требования к производительности и уровни качества обслуживания. Интеллектуальное управление ресурсами обеспечивает оптимальное распределение вычислительных мощностей, пропускной способности и других сетевых ресурсов между виртуальными сегментами с учетом их текущих потребностей и приоритетов.

В контексте управления большими данными и облачных вычислений KDN оптимизирует процессы передачи, хранения и обработки больших объемов информации в центрах обработки данных. Система минимизирует задержки при передаче данных, обеспечивает эффективное использование вычислительных ресурсов через интеллектуальную балансировку нагрузки, и автоматически адаптирует конфигурацию сети к изменяющимся требованиям приложений и услуг.

Перспективным направлением развития KDN является создание полностью автономных сетевых систем, способных к самоконфигурации, самооптимизации, самовосстановлению и самозащите без значительного участия человека-оператора. Такие системы используют принципы роевого интеллекта, распределенного принятия решений и непрерывного обучения для поддержания оптимальной производительности в динамично изменяющихся условиях эксплуатации.

Архитектура KDN с интегрированной плоскостью знаний представляет качественно новый подход к проектированию и управлению сетевыми инфраструктурами, обеспечивая беспрецедентный уровень автоматизации, адаптивности и интеллектуальности. Пятиплоскостная структура создает основу для эффективного взаимодействия между различными компонентами системы и позволяет реализовать сложные сценарии управления, которые были недоступны в традиционных сетевых архитектурах. Внедрение технологии KDN открывает новые возможности для создания сетей следующего поколения, способных автономно адаптироваться к изменяющимся требованиям и обеспечивать высокое качество обслуживания в условиях растущей сложности телекоммуникационных систем.

#### **Список используемых источников**

1. Hakiri A., Gokhale A., Berthou P., Schmidt D.C., Gayraud T. Software-defined Networking: Challenges and Research Opportunities for Future Internet // *Computer Networks*. 2014. Vol. 75. Part A. PP. 453–471. DOI:10.1016/j.comnet.2014.10.015.
2. Mestres A., Rodriguez-Natal A., Carner J., Barlet-Ros P., Alarcón E., Solé-Simó M., et al. Knowledge-Defined Networking // *ACM SIGCOMM Computer Communication Review*. 2017. Vol. 47. Iss. 3. PP. 2–10. DOI:10.1145/3138808.3138810.

3. Zhang C., Patras P., Haddadi H. Deep Learning in Mobile and Wireless Networking: A Survey // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 3. PP. 2224–2287. DOI:10.1109/COMST.2019.2904897.

4. Jarrahi M.H., Askay D., Eshraghi A., Smith P. Artificial intelligence and knowledge management: A partnership between human and AI // Business Horizons. 2023. Vol. 66. Iss. 1. PP. 87–99. DOI:10.1016/j.bushor.2022.03.002.

5. Ashtari S., Zhou I., Abolhasan M., Shariati N., Lipman J., Ni W. Knowledge-defined networking: Applications, challenges and future work // Array. 2022. Vol. 14. Article 100136. DOI:10.1016/j.array.2022.100136.

*Статья представлена научным руководителем, и. о. декана факультета ИКСС, доцентом кафедры ИКС СПбГУТ, кандидатом технических наук Елагиным В. С.*

УДК 535.92

Г. Р. Бразовский (ассистент кафедры ОКСС, СПбГУТ), [brazovskii.gr@sut.ru](mailto:brazovskii.gr@sut.ru)

## WDM МУЛЬТИПЛЕКСОР ДЛЯ ПОЛИМЕРНЫХ ОПТИЧЕСКИХ ВОЛОКОН

*Повышение требований к широкополосности линий связи в межблочных системах привело к внедрению полимерных оптических волокон (ПОВ) вместо медножильных кабелей. Однако быстрый рост скорости и объемов передаваемых данных заставляет инженеров искать способы увеличения пропускной способности ПОВ. Одним из решений, успешно применяющимся в линиях на основе кварцевых оптических волокон, является спектральное уплотнение WDM, позволяющее организовать в одном ПОВ несколько каналов, разделенных по длине волны. В работе предлагается перспективная конструкция мультиплексора для систем связи на основе ПОВ.*

*спектральное уплотнение каналов, WDM, полимерное оптическое волокно, мультиплексор, демультиплексор*

В настоящее время наблюдается стремительный рост необходимой скорости передачи данных, в т.ч. и в коротких межблочных соединениях. Из-за невозможности преодоления ограничений широкополосности медножильных кабельных линий необходимо изменение среды передачи. Одним из решений являются полимерные оптические волокна (ПОВ) [1], которые уже применяются в автомобилестроении (шина MOST) и высоковольтной области. Сейчас рассматриваются возможности использования спектрального уплотнения каналов (Wavelength Division Multiplexing, WDM) в ПОВ для будущих применений [2, 3].

Основным компонентом волоконно-оптической системы связи (ВОСС) с WDM являются мультиплексоры, позволяющие объединять и разделять спектральные каналы.

Для ВОСС на основе кварцевых волокон мультиплексоры – серийно выпускаемые устройства, но для ПОВ готовых решений не существует. В большинстве публикаций, посвященных WDM в ПОВ, предлагается использовать мультиплексор на основе сплиттера и пропускающих полосовых фильтров [3], однако из-за отсутствия заводских сплиттеров такое решение не просто реализовать.

В данной работе предлагается альтернативная конструкция двухканального мультиплексора для ПОВ (рисунок 1). Предлагаемый мультиплексор состоит из трех линз (1) и дихроичного зеркала (2). Рассмотрим его работу в режиме демультиплексирования.

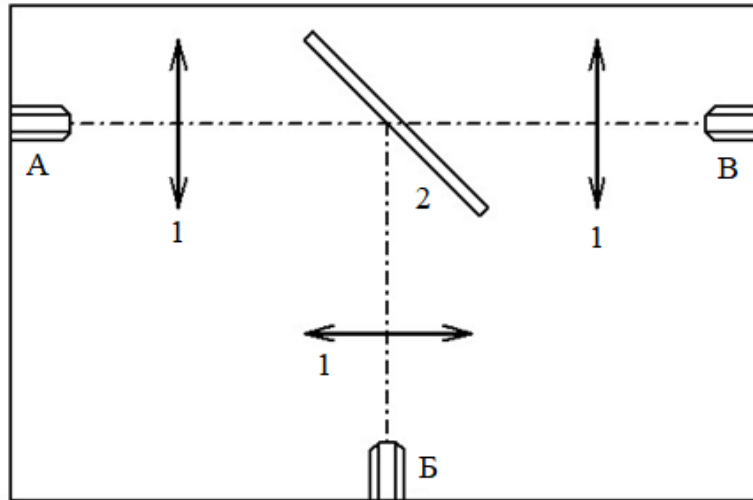


Рис. 1. Схема предлагаемого мультиплексора

Свет, содержащий две длины волны, выходит из торца оптического волокна А расходящимся пучком. При помощи линзы, расположенной на фокусном расстоянии от торца волокна, расходящийся пучок света преобразуется в параллельный. Далее свет попадает на дихроичное зеркало, которое, являясь тонкопленочным фильтром, пропускает свет, соответствующий по длине волны одному выделяемому каналу, и отражает свет второго канала. Далее излучение каналов при помощи линз, собирается в выходные волокна Б и В.

Для экспериментального подтверждения работоспособности схемы был изготовлен опытный образец, изображенный на рисунке 2.

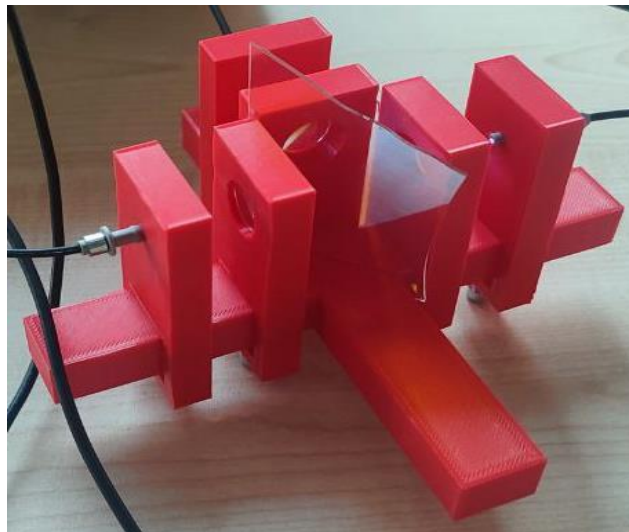


Рис. 2. Фотография экспериментального образца мультиплексора предложенной конструкции

Для определения матриц потерь экспериментального образца мультиплексора использовалась схема, изображенная на рисунке 3. Она включает RGB-светоизлучающий диода (RGB-СИД), соединительное волокно (ОВ1), испытуемый мультиплексор (M1) и измеритель оптической мощности OPTOKON OFT-820-POF (ИОМ). RGB-СИД представляет собой объединенные в едином корпусе три светодиода с разными центральными длинами волн, которые можно включать поочередно. У экземпляра, использованного при проведении измерений, центральные длины волн составляют  $\lambda_1 = 430$ ,  $\lambda_2 = 525$  и  $\lambda_3 = 650$  нм.

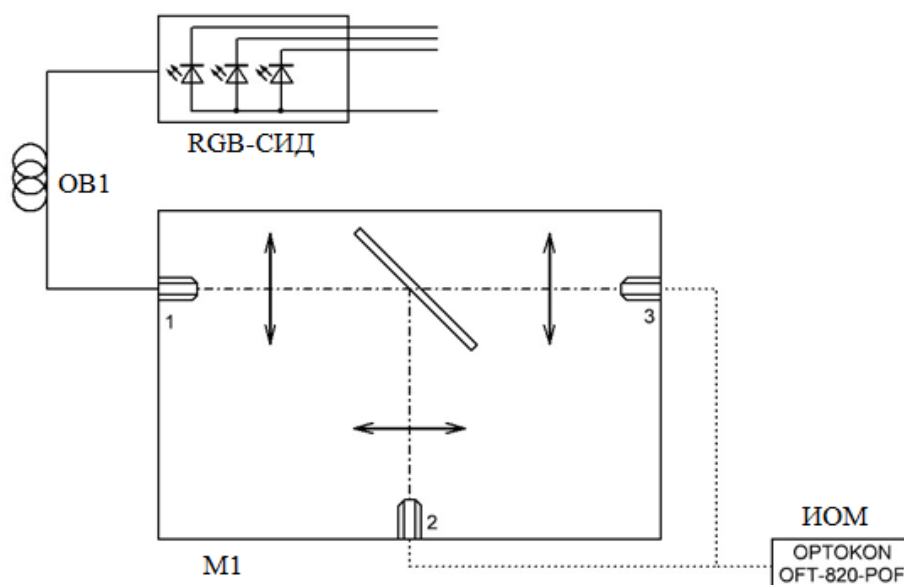


Рис. 3. Схема измерения характеристик мультиплексора

Предварительно была определена мощность  $P_{in\ i}$  излучения RGB-СИД на длинах волн  $\lambda_i$  ( $i = 1, 2, 3$ ). Для проведения измерений RGB-СИД подключался коротким отрезком оптического волокна к ИОМ. Затем излучение от RGB подавалось по очереди на каждый из трех портов мультиплексора, с помощью ИОМ измерялись мощности излучения на всех остальных портах и рассчитывались коэффициенты матрицы потерь по выражению:

$$a_{i,j} = 10\lg \left( \frac{P_{ini}}{P_{outj}} \right) \quad (1)$$

где  $a_{i,j}$  – коэффициент матрицы столбца  $i$  строки  $j$ ,  $P_{ini}$  – оптическая мощность, поступающая на вход  $i$  мультиплексора,  $P_{outj}$  – оптическая мощность на выходе  $j$  мультиплексора.

Измерения были проведены отдельно для каждой из трех длин волн. Результаты измерений матриц потерь мультиплексора приведены в таблицах 1–3.

ТАБЛИЦА 1. Матрица потерь сигнала в мультиплексоре на длине волны 430 нм

| Потери,<br>дБ | вход/выход | 1     | 2     | 3     |
|---------------|------------|-------|-------|-------|
|               | 1          | –     | 20,86 | 6,26  |
|               | 2          | 20,76 | –     | 34,86 |
|               | 3          | 6,16  | 34,86 | –     |

ТАБЛИЦА 2. Матрица потерь сигнала в мультиплексоре на длине волны 650 нм

| Потери,<br>дБ | вход/выход | 1    | 2    | 3    |
|---------------|------------|------|------|------|
|               | 1          | –    | 8,6  | 27,2 |
|               | 2          | 9,2  | –    | 33,9 |
|               | 3          | 28,2 | 33,9 | –    |

ТАБЛИЦА 3. Матрица потерь сигнала в мультиплексоре на длине волны 525 нм

| Потери,<br>дБ | вход/выход | 1    | 2    | 3    |
|---------------|------------|------|------|------|
|               | 1          | –    | 11,1 | 9,7  |
|               | 2          | 11,4 | -    | 32,4 |
|               | 3          | 9,6  | 32,4 | –    |

Из таблиц 1 и 2 видно, что экспериментальный образец может использоваться для объединения/разделения длин волн 430 (порт 3) и 650 (порт 2) нм. Полученная изоляция каналов составляет не менее 20,76 дБ.

Из таблицы 3 видно, что для излучения с длиной волны 525 нм мультиплексор работает как неселективный разветвитель: потери примерно одинаковы для обоих выходных портов, что обусловлено спектральными характеристиками использованного дихроичного зеркала.

Измерения характеристик экспериментального образца показали перспективность предлагаемой конструкции. Для улучшения спектральных характеристик следует заменить дихроичное зеркало. Замена линз позволит сделать мультиплексор предложенной конструкции более миниатюрным.

Благодаря своей наглядности экспериментальный образец вошел в состав разрабатываемой в настоящее время лабораторной установки по изучению перспективных технологий на основе многомодовых оптических волокон, которая будет внедрена в учебный процесс.

#### **Список используемых источников**

1. POF Handbook: Optical Short Range Transmission Systems / Olaf Ziemann, Jürgen Krauser, Peter E. Zamzow, Werner Daum; Springer Berlin – Heidelberg: Springer Berlin, 2008. 884 p. ISBN:978-3-540-76628-5.
2. Wavelength Division Multiplexing Network over Polymer Optical Fiber Using Fabricated Couplers for Informatics Communications / M. Sulaiman, H. Ramza, M. Harun // *Procedia Technology*. 2013. PP. 1211-1217. DOI:10.1016/j.protcy.2013.12.315.
3. WDM over POF: the inexpensive way to break through the limitation of bandwidth of standard POF communication / M. Haupt, U. H. P. Fischer. // *Photonics Packaging, Integration, and Interconnects VII*. 2007. 10 p.

*Статья представлена научным руководителем, зав. кафедрой ОКСС СПбГУТ, кандидатом технических наук Былиной М. С.*

**УДК 654.739**

**Г. Р. Бразовский** (ассистент кафедры ОКСС, СПбГУТ)

**А. Е. Яцкова** (студент группы ИКТО - 38, СПбГУТ), [Iatskova.ae@sut.ru](mailto:Iatskova.ae@sut.ru)

## **ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ УЧЕБНОЙ ПАССИВНОЙ ОПТИЧЕСКОЙ СЕТИ В ЛАБОРАТОРИИ КАФЕДРЫ ОКСС**

*На кафедре ОКСС в ауд. 619 смонтирована учебная пассивная оптическая сеть. В работе проведено рефлектометрическое исследование данной сети. Рефлектометр подключался со стороны магистрального и со стороны абонентского участка. По рефлектограммам определены длины и коэффициенты затухания участков, а также потери в сплиттере 1х32. Полученные результаты будут использованы для новой лабораторной работы по рефлектометрическим измерениям сетей PON.*

*пассивные оптические сети, оптический рефлектометр, рефлектограммы, вносимые потери, оптический разветвитель (сплиттер)*

В Санкт-Петербургском государственном университете телекоммуникаций имени профессора М. А. Бонч-Бруевича в лаборатории кафедры ОКСС создана учебная пассивная оптическая сеть. Для плановой проверки и определения возможностей развития сети было проведено ее рефлектометрическое исследование. В ходе диагностики проверена целостность всех оптических волокон (ОВ) магистрального и абонентского участков сети, измерены их затухания и рассчитаны коэффициенты затухания, определены потери в оптическом сплиттере.

На рисунке 1 представлена схема измерения. Сеть состоит из катушки ОВ1 с волокном, имитирующим магистральный участок сети, оптического разветвителя (сплиттера) 1х32 и волокна ОВ2, соединяющего сплиттер и абонентскую розетку. В связи с малой длиной ОВ2 (не более 2-3 метров) для проведения измерений вносимого затухания сплиттера была добавлена дополнительная катушка ОВ3 (длина около 2 км). Буквой А обозначена точка подключения оптического рефлектометра (ОР) для измерения со стороны линейного терминала, буквой В – со стороны абонентского терминала.



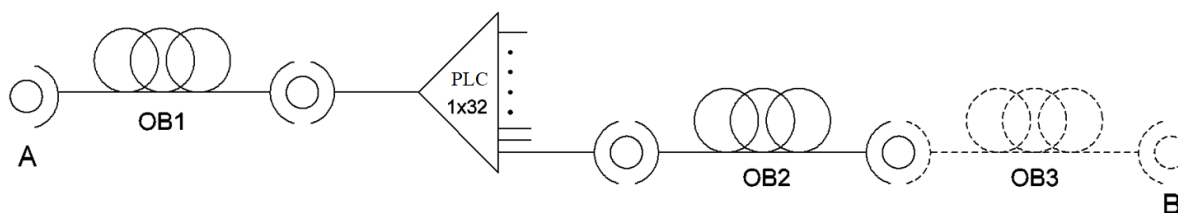


Рис. 1. Схема исследуемой сети

Принцип работы ОР заключается в том, что в исследуемую линию связи подается мощный зондирующий импульс, после чего измеряется мощность и время запаздывания вернувшихся в ОР импульсов. Возвращение импульсов происходит в результате отражения на неоднородностях показателя преломления (ПП), размер которых существенно превышает длину волны излучения, и релеевского рассеивания на релеевских центрах – неоднородностях, сравнимых по размеру с длиной волны (рис. 2) [1].

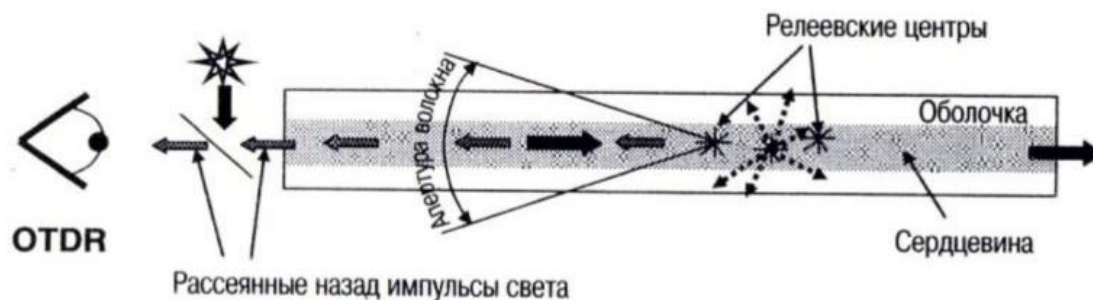


Рис. 2. Формирование сигнала обратного рассеяния

Вернувшееся на вход ОР излучение называют сигналом обратного рассеяния (СОР). Зависимость уровня мощности СОР от времени (расстояния) называют рефлектограммой. Пересчет измеренного времени  $T$  в расстояние  $L$  внутри ОР осуществляется по формуле:

$$L = \frac{cT}{2n} \quad (1)$$

где  $n$  – групповой ПП света в волокне,  $c$  – скорость света в вакууме.

Релеевские центры распределены равномерно вдоль ОВ, поэтому, анализируя СОР, можно определять параметры линии: ее длину, вносимые потери, коэффициенты затухания на отдельных участках, потери в соединениях ОВ и т. д.

Доля обратно рассеянного излучения обычно мала, поэтому в ОР используют импульсы большой мощности и длительности, а также высокочувствительные фотоприемники. Кроме того, для улучшения соотношения сигнал/шум используется многократное усреднение результатов измерения.

При каждом удвоении времени измерений шумы уменьшаются примерно на 0.75 дБ [1].

Каждый тип неоднородности имеет свой характерный вид на рефлектограмме: отражающая неоднородность (трещина, торец ОВ, разъёмное соединение) проявляется отраженным импульсом, за которым следует перепад СОР, а неотражающая или малоотражающая (сварное соединение, изгиб) – перепадом СОР. ОВ между неоднородностями имеет вид прямой с отрицательным коэффициентом наклона, прямо пропорциональным величине коэффициента затухания [1-3].

На рисунке 3 и 4 представлены рефлектограммы исследуемой сети. По рефлектограммам определены длины и коэффициенты затухания ОВ1 и ОВ3, а также вносимые потери сплиттера, которые определялись по изменению уровня СОР до и после сплиттера (таблица 1). Для уменьшения методической погрешности измерений вносимые потери сплиттера определялись как среднее арифметическое от результатов измерения в двух направлениях.

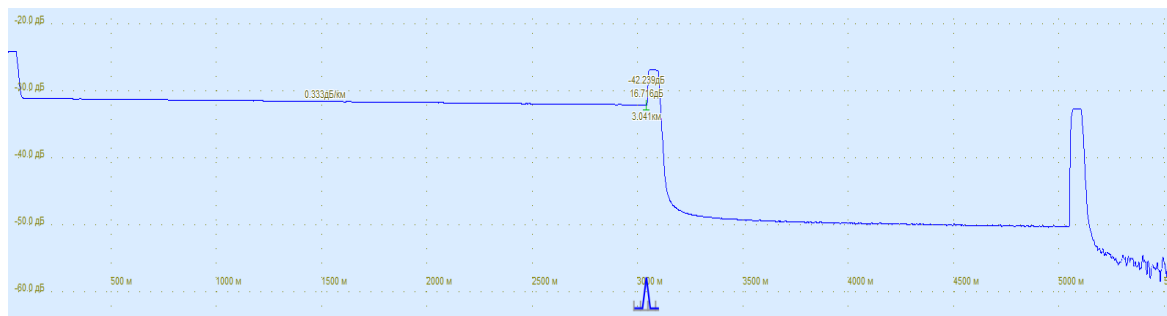
ТАБЛИЦА 1. Результаты рефлектометрического исследования на длине волны 1310 нм

| Длина волны, нм | ОВ1       |                        | ОВ3       |                        | Сплиттер            |                           |
|-----------------|-----------|------------------------|-----------|------------------------|---------------------|---------------------------|
|                 | Длина, км | Коэф. затухания, дБ/км | Длина, км | Коэф. затухания, дБ/км | Вносимые потери, дБ | Собственное затухание, дБ |
| 1310            | 3,041     | 0,333                  | 1,996     | 0,343                  | 17,787              | 2,73                      |
| 1550            | 3,047     | 0,190                  | 1,995     | 0,193                  | 17,401              | 2,35                      |

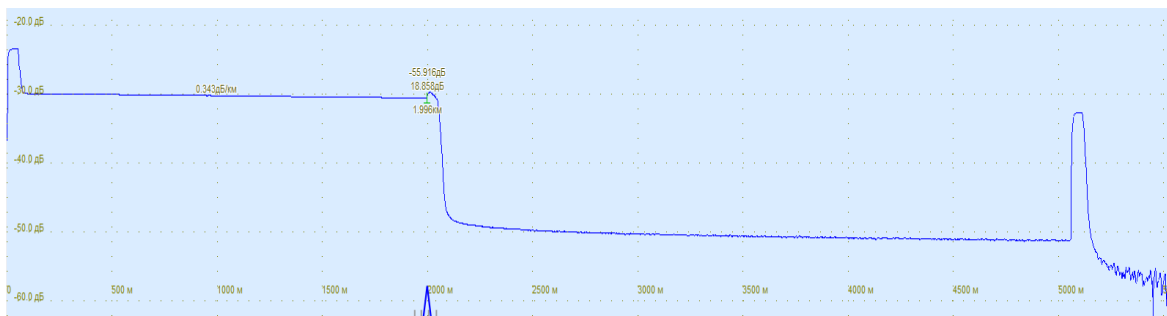
Собственные потери сплиттера определялись как разность между измененным значением потерь и потерями разветвления  $a_{\min}$ , которые для сплиттера с равномерным делением мощности определяются по формуле:

$$a_{\min} = 10 \log \left( \frac{P_{\text{ВХ}}}{P_{\text{ВЫХ}}} \right) = 10 \log(N) \quad (2)$$

где  $P_{\text{ВХ}}$  и  $P_{\text{ВЫХ}}$  – мощность излучения на входе и на одном из выходов сплиттера,  $N$  – число выходов [2].

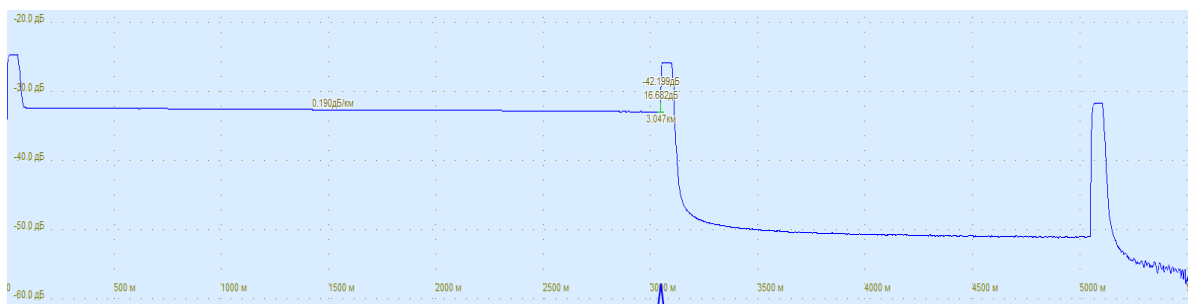


а)

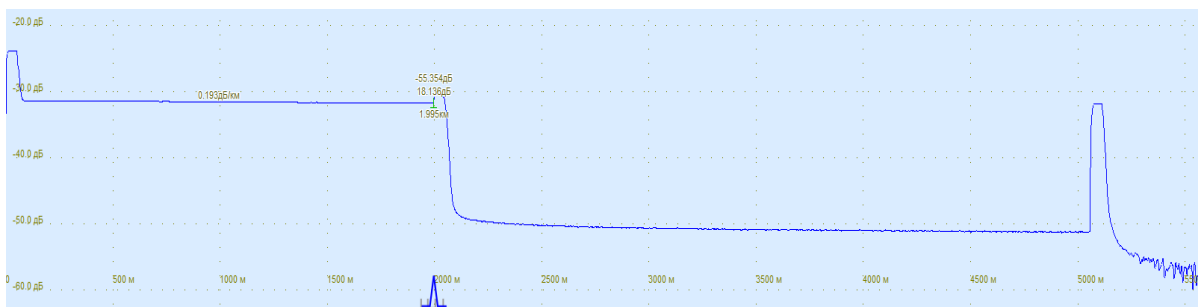


б)

Рис. 3. Рефлектограмма на длине волны 1310 нм, зарегистрированная при подключении рефлектометра со стороны: а – линейного терминала, б – абонентского терминала



а)



б)

Рис. 4. Рефлектограмма на длине волны 1550 нм, зарегистрированная при подключении рефлектометра со стороны: а – линейного терминала, б – абонентского терминала

Полученные в результате проведенного исследования результаты будут использованы для создания новой лабораторной работы по дисциплине «Высокоскоростные оптические системы связи для транспортных сетей и сетей доступа».

#### **Список используемых источников**

1. Листвин А.В., Листвин В.Н. Рефлектометрия оптических волокон // Москва: ЛЕ-САРарт, 2005. 208 с. ISBN 5-902367-03-4.
2. Соллер Б. Дж., Гиффорд Д. К., Вольф М. С., Фроггатт М. Э. Оптическая рефлектометрия высокого разрешения // Фотоника. 2019. Том 13. № 5. С. 452-460. DOI: 10.22184/FRos.2019.13.5.452.460.
3. Русакова, Е. А. Волоконно-оптические системы передачи: практикум / Е. А. Русакова, М. С. Мухамедзянов. Екатеринбург: УрГУПС, 2016. 56 с

*Статья представлена научным руководителем, ассистентом кафедры ОКСС СПбГУТ Бразовским Г. Р.*

УДК 004.8

**А. Ю. Брюшинин** (студент группы ИКТИ-45м, СПбГУТ),  
[briushinin.aiu@sut.ru](mailto:briushinin.aiu@sut.ru)

**Д. С. Пивоваров** (студент группы ИКТИ-45м, СПбГУТ),  
[pivovarov.ds@sut.ru](mailto:pivovarov.ds@sut.ru)

## **АНАЛИЗ ТРЕБОВАНИЙ ФУНКЦИОНАЛА ПРОГРАММНЫХ СРЕДСТВ ДЛЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

*В данной статье исследуются ключевые требования к программным средствам для систем искусственного интеллекта в сетях и системах связи, необходимые для их эффективного функционирования. Особое внимание уделяется производительности, достигаемой оптимизацией алгоритмов и использованием аппаратных ресурсов для обработки больших объемов данных в реальном времени. Анализируются аспекты надежности, включая тестирование, обнаружение и исправление ошибок, а также обработку неполных и некорректных данных. Рассматривается масштабируемость, достигаемая за счет распределенных вычислений и облачных ресурсов. Обсуждаются вопросы безопасности, связанные с защитой данных и предотвращением несанкционированного доступа. Подчеркивается важность гибкости, обеспечивающей адаптацию к изменяющимся условиям, и удобства использования, включающего интуитивный интерфейс и понятную документацию. Цель статьи – выявить ключевые направления для разработки программных средств, обеспечивающих высокую эффективность и надежность ИИ в сетях и системах связи, что позволит внедрять и эффективно использовать системы ИИ.*

*искусственный интеллект, сети связи, программные средства, машинное обучение, глубокое обучение*

### **Анализ требований**

Программные средства для систем искусственного интеллекта (ИИ) в сетях и системах связи должны обладать высокой производительностью, надежностью, масштабируемостью, адаптивностью, безопасностью и гибкостью. Удовлетворение этих требований позволит обеспечить эффективную работу систем ИИ и достичь поставленных целей. На рисунке 1 проиллюстрированы требования к системам ИИ [1, 2].

## Требования к системам ИИ в сетях связи



Рис. 1. Требования к системам ИИ

### Определение требований к надежности и безопасности программных средств

Требования к программным средствам для систем искусственного интеллекта (ИИ) в сетях и системах связи включают надежность и безопасность. Надежность подразумевает высокую степень устойчивости к сбоям, что достигается через механизмы резервирования и восстановления данных. Важным аспектом является работа с большими массивами данных, где необходимо выявление и восстановление пропущенных или некорректных значений. Существуют различные методы для этого, включая удаление объектов, математические методы и использование метрик. Поиск выбросов, то есть аномальных значений, также критичен для надежности моделей ИИ. Методы их обнаружения включают логическое выявление, анализ отдельных и нескольких признаков, а также метрические, геометрические и кластеризационные подходы [3, 4, 6].

Обеспечение безопасности программного обеспечения, работающего на основе искусственного интеллекта, предполагает защиту данных от несанкционированного доступа и различных угроз. Для этого применяются такие методы, как фильтрация входящих данных, использование антивирусного программного обеспечения, шифрование и регулярный аудит безопасности. Важно ограничивать доступ к информации и обеспечивать ее защиту как при передаче, так и при хранении [5].

## Определение требований к производительности и масштабируемости программных средств

Для достижения высокой эффективности при работе с большими объемами данных и сложными алгоритмами необходимым условием является высокая скорость обработки информации, что достигается оптимизацией алгоритмов и использованием мощных аппаратных ресурсов. Оптимизация включает в себя подходы по минимизации функции потерь, что повышает точность прогнозов модели ИИ. Градиентный спуск – один из алгоритмов, используемых для этой задачи, обновляющий параметры модели в направлении, противоположном градиенту функции потерь. Также важна настройка гиперпараметров, которые определяют структуру и процесс обучения модели. Для обеспечения высокой производительности искусственного интеллекта в сетях и системах связи требуется мощная аппаратная часть, включая CPU, GPU и TPU, которые позволяют эффективно обрабатывать большие объемы данных [7, 8].

Рассмотрим, то как применяются аппаратные средства на разных этапах обучения модели искусственного интеллекта. Для простоты разделим многогранный процесс обучения модели на 3 фазы: Сбор данных, обучения, обработка и вывод. На рисунке 2 проиллюстрирован процесс обучения модели ИИ.

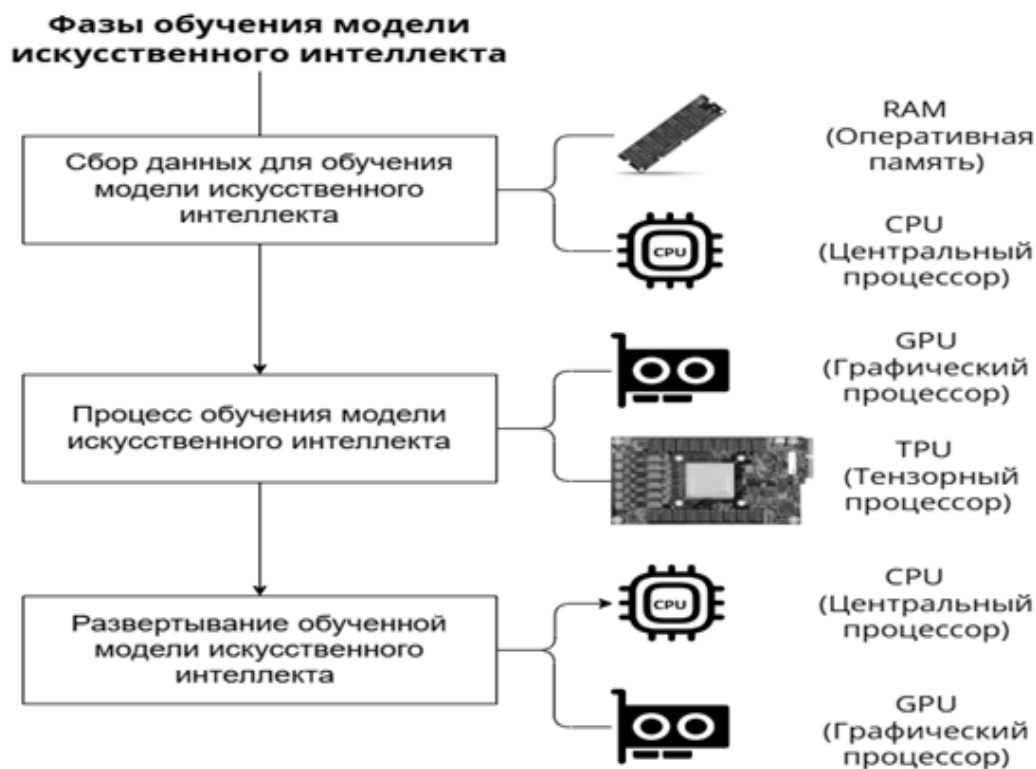


Рис. 2. Процесс обучения модели искусственного интеллекта

Процесс обучения модели искусственного интеллекта можно разделить на три этапа. Первый этап включает сбор информации (полезных данных), где важно собрать качественные данные и провести предварительную обработку для выявления ошибок, недостоверной или отсутствующей информации. После первого этапа начинается следующий, на котором модель искусственного интеллекта выбирается и обучается на предварительно обработанных данных, что, в свою очередь, требует значительных вычислительных (аппаратных) ресурсов, которыми могут выступать такие устройства, как CPU, GPU и TPU. По завершении второго этапа начинается последний этап, на котором обученная модель ИИ разворачивается на пограничном компьютере, что требует меньше ресурсов и позволяет быстро делать выводы на основе новых данных. Также стоит упомянуть, что при настройке модели ИИ для работы с большими данными часто требуется оптимизация и использование систем с общей и распределенной памятью для параллельных вычислений. [9].

На рисунке 3 проиллюстрированы модели общей и распределенной памяти.

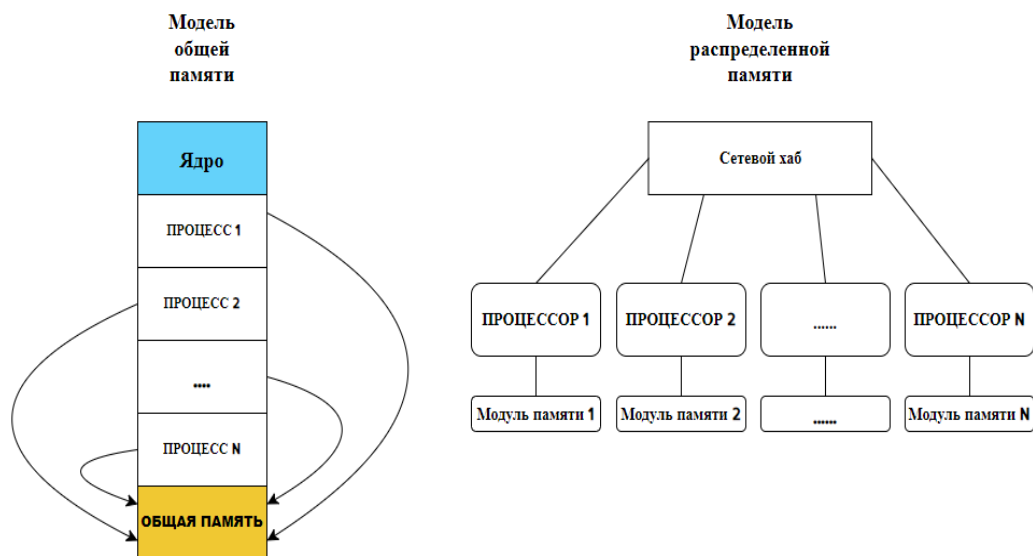


Рис. 3. Модель общей и распределенной памяти

Анализ показал, что программное обеспечение для систем искусственного интеллекта должно отвечать ряду требований, включая высокую производительность, масштабируемость, надежность, гибкость, безопасность и простоту использования. Учет этих требований создаст необходимую основу для достижения высокой эффективности при внедрении систем искусственного интеллекта в область сетей и систем связи.



**Список используемых источников**

1. Намиот Д. Е. Об устойчивости и безопасности систем искусственного интеллекта / Д. Е. Намиот, Е. А. Ильюшин // International Journal of Open Information Technologies. 2022. № 9. URL: <https://cyberleninka.ru/article/n/ob-ustoychivosti-i-bezopasnosti-sistem-iskusstvennogo-intellekta> (дата обращения 24.04.2025).
2. Shi, Y. Adversarial Machine Learning in Wireless Communications: Opportunities and Challenges / Y. Shi [и др.] // IEEE Wireless Communications Letters. 2019. Vol. 8, № 5. PP. 1476-1479. DOI: <https://doi.org/10.1109/LWC.2019.2920427>. URL: <https://ieeexplore.ieee.org/document/8738053> (дата обращения 24.04.2025).
3. Липатов А. Г. Возможности использования искусственного интеллекта для управления большими информационными массивами данных BIG DATA / А. Г. Липатов // Инновации и инвестиции. 2023. № 5. URL: <https://cyberleninka.ru/article/n/vozmozhnosti-ispolzovaniya-iskusstvennogo-intellekta-dlya-upravleniya-bolshimi-informatsionnymi-massivami-dannyh-big-data> (дата обращения 24.04.2025).
4. Быков К. В. Особенности предобработки данных для применения машинного обучения / К. В. Быков // Молодой ученый. 2021. № 53 (395). С. 1-4. URL: <https://moluch.ru/archive/395/87491/> (дата обращения 24.04.2025).
5. Щербаков А. Е. Исследование применения искусственного интеллекта и машинного обучения в области кибербезопасности: техники обнаружения аномалий и предотвращения угроз / А. Е. Щербаков // Вестник науки. 2023. № 7 (64), т. 1. С. 151-156. ISSN 2712-8849. URL: [vestnik-nauki.com/article/9436](https://vestnik-nauki.com/article/9436) (дата обращения 24.04.2025).
6. Дулесов А. С. Обзор основанных на техниках машинного обучения методов обнаружения выбросов в данных / А. С. Дулесов, А. В. Байшев // ИВД. 2023. № 6 (102). URL: <https://cyberleninka.ru/article/n/obzor-osnovannyh-na-tehnikah-mashinnogo-obucheniya-metodov-obnaruzheniya-vybrosov-v-dannyh> (дата обращения 24.04.2025).
7. Донской В. И. Интеллектуальная оптимизация на основе машинного обучения: современное состояние и перспективы (обзор) / В. И. Донской // ТВИМ. 2020. № 1 (46). URL: <https://cyberleninka.ru/article/n/intellektualnaya-optimizatsiya-na-osnove-mashinnogo-obucheniya-sovremennoe-sostoyanie-i-perspektivy-obzor> (дата обращения 24.04.2025).
8. Анафиев А. С. Обзор подходов к решению задачи оптимизации гиперпараметров для алгоритмов машинного обучения / А. С. Анафиев, А. С. Карюк // ТВИМ. 2022. № 2 (55). URL: <https://cyberleninka.ru/article/n/obzor-podhodov-k-resheniyu-zadachi-optimizatsii-giperparametrov-dlya-algoritmov-mashinnogo-obucheniya> (дата обращения 24.04.2025).
9. Аппаратные средства для ИИ: обзор рынка // СТА.RU. 2023. 29 июня. URL: <https://www.cta.ru/articles/cta/obzory/apparatnye-sredstva/165899/> (дата обращения 24.04.2025).

*Статья представлена научным руководителем, доцентом кафедры СС и ПД СПбГУТ, кандидатом технических наук Аль-Свейти Малик А. М.*

УДК 004.722

А. Б. Гольдштейн (д.т.н., профессор кафедры ИКС, СПбГУТ)

С. М. Елисеев (аспирант группы 1113А-20, СПбГУТ), [eliseev.sm@sut.ru](mailto:eliseev.sm@sut.ru)

## НОВЫЕ ВОЗМОЖНОСТИ И НОВЫЕ ЗАДАЧИ ВКЛЮЧЕНИЯ ВИРТУАЛЬНЫХ ОПЕРАТОРОВ MVNO В СЕТИ ПОКОЛЕНИЙ 5G/6G

*Исследуется сдвиг парадигмы виртуальных операторов MVNO (Mobile Virtual Network Operators) при включении в сети поколений 5G/6G, связанный с радикальными изменениями сетевых технологий виртуализацией сетевых функций, шарингом и слайсингом, облачными и туманными вычислениями и т.д. Предложены новые подходы к проектированию MVNO для работы с PMNO (Physical Mobile Network Operators) поколений 5G/6G, описываются основные критерии для анализа вероятностно-временных характеристик включения MVNO в PMNO.*

*5G, MVNO, Network Slicing, QoS, вероятностно-временные характеристики*

Технологические решения сетей 5/6G кратно расширили спектр сервисов, которые могут предоставлять базовые опорные операторы мобильной связи PMNO. Вместе с этим, соответственно расширяются сферы деятельности и виртуальных мобильных операторов MVNO, арендующих ресурсы PMNO и реализующих услуги под собственным брендом [1].

Новые области, в которых могут быть представлены операторы MVNO:

- комплексные решения и платформы для приложений Интернета Вещей IoT;
- целевые предложения для систем виртуальной и дополненной реальности VR/AR№
- выделенные сети и тарифы для облачных игровых сервисов;
- изолированные сети для платформ тактильного интернета и беспилотного транспорта.

Сети 5/6G открывают ряд ключевых задач для полноценного и взаимовыгодного сотрудничества опорных PMNO и виртуальных MVNO:

- проработка технологических подходов к интеграции MVNO и PMNO с учетом новых заложенных функциональных решений 5/6G, которых ранее не было в сетях предыдущих поколений;
- описание и оптимизация новых моделей MVNO. Проработка и выбор эффективных стратегий функционирования MVNO;
- систематизация сценариев взаимодействия MVNO / PMNO и описание новых договоров SLA (Service Level Agreement);

- моделирование и анализ вероятностно-временных характеристик сетей PMNO и MVNO для различных архитектур интеграций и типов предоставляемых сервисов MVNO.

Базовыми подходами к интеграции PMNO и MVNO являются технологии MOCN (Multi-Operator Core Network) и GWCN (Gateway Core Network). Данные подходы подробно изучены и активно применяются в сетях действующих мобильных операторов 2/3/4G. В сетях 5/6G такие решения также применимы. При технологии MOCN интеграция производится на уровне базовых станций RAN PMNO (рис. 1) [2].

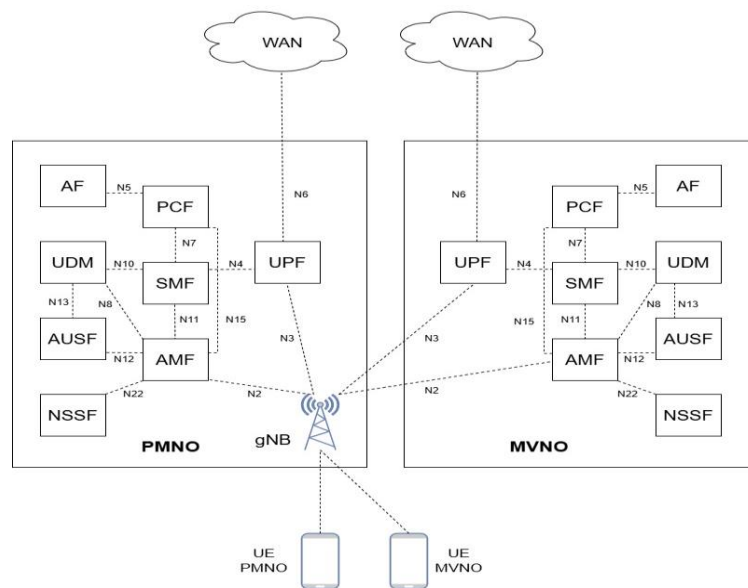


Рис. 1. Архитектура MOCN в сетях 5G

В GWCN точки стыка находятся в опорных сетях (рис. 2) [3].

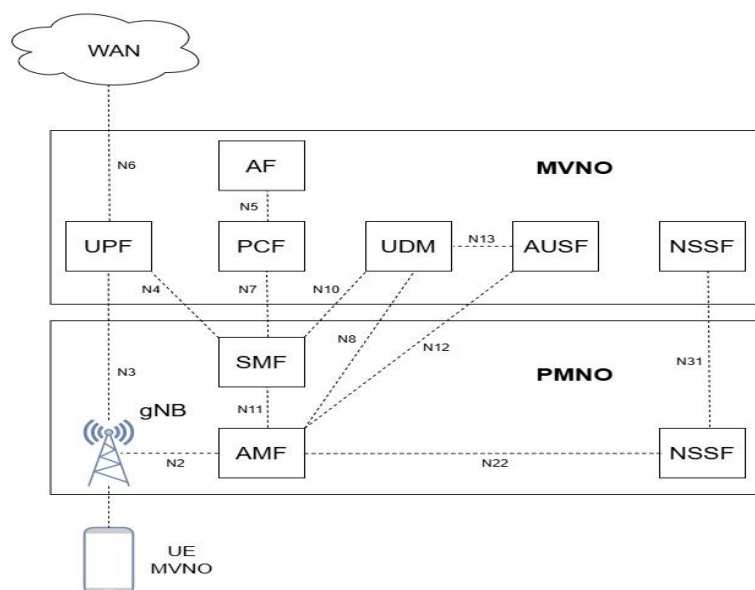


Рис. 2. Архитектура GWCN в сетях 5G

Принципиально новые решения к интеграции PMNO и MVNO в сетях 5G/6G определяются подходами, основанными на технологиях Network Slicing и виртуализации сетевых технологий NFV (Network Function Virtualization) [4]. Разделение сети PMNO на логические сетевые сегменты (слайсы) позволяет не только предоставлять сервисы с различными параметрами качества обслуживания, но и предоставлять их в аренду виртуальным операторам MVNO. Данный подход выведен в отдельную парадигму NsaaS (Network Slice as a Service) – «Сегмент сети как услуга» (рис. 3) [5].

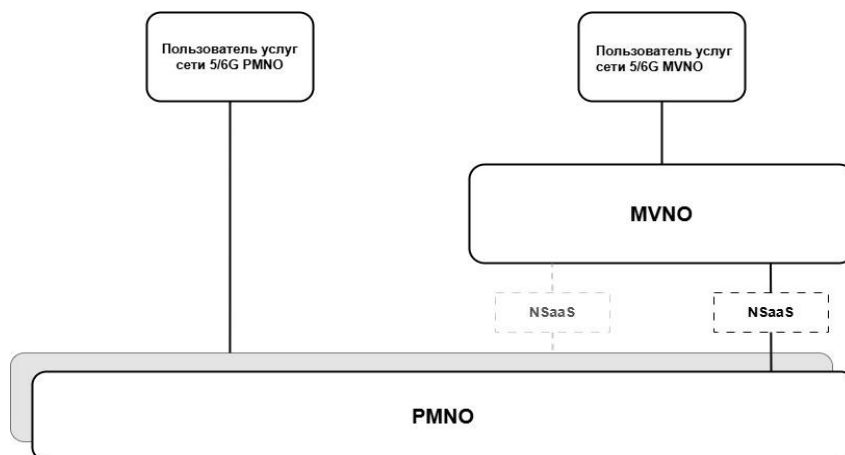


Рис. 3. Парадигма NsaaS для MVNO

Сценарии взаимодействия, заложенные в NsaaS, включают в себя возможности мониторинга, контроля и управления сетевым сегментом силами MVNO через стандартные целевые интерфейсы сети 5G/6G. Как в опорной сети, так и в подсистеме RAN. В частности, в сетях 5G процедуры управления обеспечиваются стеком SMF (stack management function), который состоит из функций CSMF, NSMF, NSSMF [6].

Парадигма NsaaS предоставляет ряд преимуществ для MVNO:

- высокие скорости запуска и внедрения MVNO с широким функциональным доступом. Данные метрики, а также целый ряд других, используются в математических моделях, описывающих каждую архитектуру интеграции MVNO к PMNO;
- минимальные затраты и ограниченность технических компетенций MVNO;
- доступ к механизмам управления и контроля подсистемой радиодоступа со стороны MVNO;
- возможность подключения MVNO к нескольким MNO в рамках парадигмы NsaaS.

Ключевыми задачами для организации MVNO на основе NsaaS являются обеспечение изоляции сетевых сегментов и реализация автономного и децентрализованного управления сегментами.

Модели построения MVNO NsaaS представлены на рисунке 4:

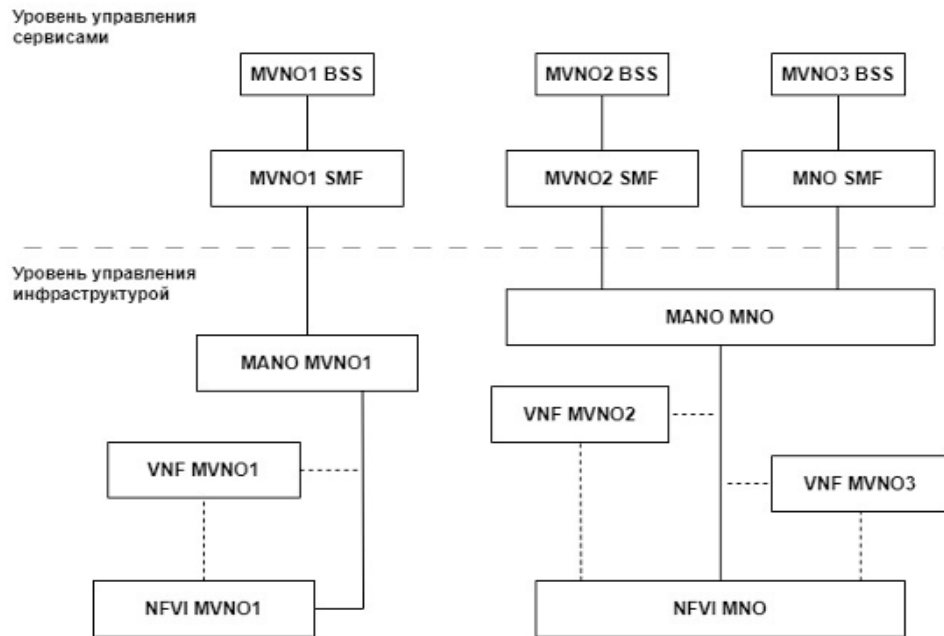


Рис. 4. Модели MVNO NsaaS

- MVNO с индивидуально выделенным стеком управления SMF, подсистемой MANO NFV, инфраструктурой NFVI;
- MVNO с индивидуально выделенным стеком управления SMF, который взаимодействует NFV MANO и NFVI опорного оператора PMNO;
- MVNO, управляющий выделенным сетевым сегментом через SMF PMNO.

Наиболее значимые критерии при выборе подхода и модели построения MVNO определяются вероятностно-временными характеристиками при взаимодействии с PMNO. Базовые численные параметры ВВХ для виртуального оператора:

- время установления соединения, которое состоит из задержки сигнального обмена, процессов авторизации и аутентификации и времени выделения ресурсов:

$$T_{\text{connect}} = T_{\text{signal}} + T_{\text{auth}} + T_{\text{alloc}}$$

- вероятность успешного подключения:

$$P_{\text{success}} = 1 - P_{\text{failure}}$$

где  $P_{\text{failure}}$  – вероятность отказа, вызванная сбоями в работе узлов, сетевыми перерывами, ошибками различных процедур и т.д.

• среднее время обслуживания, в том числе время ожидания в очереди.  
Для модели M/M/1:

$$M[T_{\text{connect}}] = \frac{1}{\mu - \lambda}$$

где  $\mu$  – интенсивность обслуживания,  $\lambda$  – интенсивность входящих запросов.  
– Вероятность перегрузки, когда интенсивность запросов MVNO превышает возможности PMNO:

$$P_{\text{overload}} = \frac{\frac{\rho^N}{N!}}{\sum \frac{\rho^k}{k!}}$$

где  $\rho = \frac{\lambda}{\mu}$ .

Данные метрики, а также целый ряд других, используются в математических моделях, описывающих каждую архитектуру интеграции MVNO к PMNO.

Сети 5/6G и заложенные в них технологии открывают для MVNO следующую главу в развитии с широкими перспективами. Описанные в данной работе задачи требуют детального анализа, систематизации и математического моделирования. Предложенные подходы к построению MVNO на основе Network Slicing и NFV позволяют пересмотреть всю концепцию виртуальных операторов. Можно предположить, что в сетях 5/6G большая часть операторов будет виртуальными.

#### Список используемых источников

1. Гольдштейн Б. С. Инфокоммуникационные сети и системы. СПб.: БХВПетербург, 2019. 208 с.
2. 3GPP TS 23.501 V15.3.0 (2018-09) System Architecture for the 5G System.
3. Тихвинский В. О., Терентьев С. В., Коваль В. А., Девяткин Е. Е. Развитие сетей мобильной связи от 5G Advanced к 6G: проекты, технологии, архитектура. М.: Техносфера, 2023. 321 с.

4. Елисеев С., Гринева А. Подходы к виртуализации сетей мобильных операторов связи поколения 4/5G // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021, стр. 426-429.

5. 5G; Management and Orchestration; Concepts, Use Cases and Requirements, document TS 128 530 V15.0.0 TS 28.530 Version 15.0.0 Release 15), ETSI, 2018.

6. 3GPP TS 28.533 V15.0.0 (2018-10) Management and orchestration; Architecture framework.

*Статья представлена научным руководителем, доктором технических наук, профессором кафедры ИКС Гольдштейном А. Б.*

**УДК 004**

**В. С. Елагин** (к.т.н., и. о. декана факультета ИКСС СПбГУТ),  
[v.elagin@sut.ru](mailto:v.elagin@sut.ru)

**С. А. Поляков** (магистрант группы ИКТМ-22м СПбГУТ),  
[polyakov.sa@sut.ru](mailto:polyakov.sa@sut.ru)

## **ПРИМЕНЕНИЕ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ В ЗАДАЧАХ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ АПК**

*В статье рассматриваются подходы к применению моделей прогнозирования в задачах управления жизненным циклом аппаратно-программных комплексов (АПК). Особое внимание уделено этапам эксплуатации, обслуживания и проектирования, где прогнозные алгоритмы позволяют обеспечить проактивное управление состоянием систем, повысить их надежность и сократить издержки. Описана интеграция таких моделей с системами конфигурационного учета (CMDB), ITSM-платформами, средствами мониторинга и автоматизации. Подчеркивается значение предиктивной аналитики как инструмента цифровой трансформации управления ИТ-инфраструктурой.*

*прогнозирование, аппаратно-программный комплекс, жизненный цикл, мониторинг, управление состоянием*

### **Введение**

Прогнозирование состояния аппаратно-программных комплексов (АПК) позволяет существенно повысить эффективность управления их жизненным циклом – от ввода в эксплуатацию до списания. В условиях эксплуатации сложных сетевых устройств, таких как видеоконференц-серверы, своевременное предсказание отклонений и потенциальных сбоев способствует переходу от реактивного к проактивному управлению инфраструктурой.

### **Жизненный цикл АПК и его этапы**

Жизненный цикл аппаратно-программного комплекса (АПК) представляет собой совокупность фаз, проходящих от момента идеи и проектирования до окончательного вывода системы из эксплуатации [1]. Понимание этого цикла крайне важно как для архитекторов и инженеров, так и для специалистов по эксплуатации и техническому обслуживанию. Каждый этап формирует определенные требования к надежности, мониторингу и прогнозированию состояния, а также влияет на общую устойчивость и срок службы системы.





Рис. 1. Жизненный цикл АПК

Первым этапом является проектирование и выбор компонентов. На данной стадии разрабатывается архитектура системы, принимаются решения о выборе аппаратных платформ, программного обеспечения, интерфейсов взаимодействия и механизмов сбора данных. Следующий этап – развертывание и настройка, где осуществляется физическая установка оборудования, его подключение и программная конфигурация. Основным и наиболее продолжительным является этап эксплуатации. В течение этого времени осуществляется постоянная работа комплекса в рабочей среде. В рамках эксплуатации также неотъемлемым является этап обслуживания и обновления. Финальным этапом является вывод из эксплуатации.

Таким образом, жизненный цикл АПК представляет собой непрерывный процесс, в рамках которого интеграция средств мониторинга и прогнозирования состояния становится не просто полезной, а необходимой. Эти средства позволяют не только повысить эффективность эксплуатации, но и существенно продлить срок службы системы, минимизировать потери и повысить устойчивость всей информационной инфраструктуры.

### Роль прогнозных моделей на разных этапах

Прогнозные модели играют критически важную роль на всех этапах жизненного цикла аппаратно-программных комплексов. Их интеграция позволяет не только повысить надежность и отказоустойчивость систем, но и существенно улучшить эффективность технического обслуживания, а также

сократить эксплуатационные издержки. Подход к использованию прогнозных алгоритмов становится все более системным и комплексным – от этапа проектирования до окончательного вывода системы из эксплуатации.

На этапе эксплуатации, который является самым длительным и насыщенным в жизненном цикле АПК, прогнозные модели служат основой для непрерывного контроля и анализа состояния. Их главная функция – это выявление скрытых закономерностей и трендов, которые невозможно определить при поверхностном мониторинге. Модели позволяют анализировать тонкие отклонения от нормального поведения, фиксировать динамику параметров, а также выявлять аномалии задолго до наступления критических сбоев [2]. Например, постепенное увеличение температуры, рост числа перезапусков сервисов или нестабильное поведение сетевых интерфейсов могут быть ранними признаками деградации компонентов. В этом контексте прогнозные модели становятся не просто вспомогательным инструментом, а интеллектуальным уровнем автоматизированной диагностики.

Во фазе обслуживания и обновления значимость прогнозирования возрастает еще больше. Здесь модели обеспечивают переход от реактивного обслуживания, при котором вмешательства происходят уже после отказа, к предиктивному техническому обслуживанию (*predictive maintenance*) – концепции, основанной на упреждающем подходе. Это позволяет не просто реагировать на инциденты, а планировать замену или ремонт до возникновения сбоев, избегая аварийных ситуаций и незапланированных простоев [3]. Такой подход приводит к снижению затрат на обслуживание за счет оптимизации графиков ТО, минимизации количества экстренных выездов и уменьшения потребности в резервных мощностях.

Интересно отметить, что на стадии проектирования, хотя прогнозные модели напрямую еще не применяются, их влияние осуществляется ретроспективно – через анализ данных, накопленных за время эксплуатации предыдущих версий системы. Эти данные становятся источником ценной информации для архитекторов и инженеров, которые проектируют новое поколение устройств. Например, если по итогам эксплуатации выясняется, что определенные компоненты регулярно выходят из строя после определенного срока или при определенных нагрузках, это становится основанием для пересмотра их использования в будущих моделях.

Итак, прогнозные модели становятся неотъемлемым элементом на всех стадиях жизненного цикла АПК: в эксплуатации они позволяют поддерживать устойчивое функционирование, в обслуживании – рационализируют

ресурсы и повышают эффективность, а на этапе проектирования – формируют базу знаний для будущих инженерных решений. Такой подход открывает путь к созданию интеллектуальных, самодиагностируемых и самоуправляемых систем нового поколения.

### **Интеграция с системами управления**

Эффективность применения моделей прогнозирования состояния аппаратно-программных комплексов (АПК) напрямую зависит от их способности взаимодействовать с другими компонентами экосистемы управления ИТ-инфраструктурой. Изолированное использование даже самой точной модели теряет практическую ценность, если ее выводы не могут быть оперативно интерпретированы, визуализированы и применены для принятия решений. Именно поэтому критически важно обеспечить тесную интеграцию алгоритмов прогнозирования с существующими платформами, отвечающими за конфигурационный учет, обслуживание, мониторинг и автоматизацию.

Одним из ключевых компонентов является CMDB (Configuration Management Database) – база данных конфигурационного управления, которая содержит актуальную информацию обо всех элементах инфраструктуры [4]. Интеграция прогнозных моделей с CMDB позволяет не только привязывать предсказания и оценки риска к конкретным экземплярам устройств, но и учитывать контекст их использования, архитектурные зависимости и историю изменений.

Другой важной точкой интеграции являются ITSM-платформы (например, ServiceNow, OTRS, BMC Remedy), которые отвечают за управление инцидентами, заявками и проблемами [5]. Внедрение прогнозной аналитики в такие системы позволяет существенно повысить автоматизацию процессов обслуживания. При превышении порогов риска или при обнаружении трендов, указывающих на надвигающийся сбой, система может автоматически создавать инциденты или задачи на техническое обслуживание. Это позволяет заранее уведомить инженеров, выделить ресурсы и подготовить необходимые действия до возникновения отказа. Кроме того, предсказания могут учитываться в SLA и отчетах, влияя на планирование и оценки эффективности работы ИТ-службы.

Для анализа и визуализации прогностических данных широко применяются системы мониторинга, такие как Zabbix, Prometheus и Grafana. Именно через эти инструменты осуществляется наглядное отображение

ключевых метрик и прогнозов в виде графиков, тепловых карт, дашбордов и временных рядов [6]. Такая визуализация позволяет операторам и инженерам не только видеть текущее состояние инфраструктуры, но и понимать ожидаемые тренды и потенциальные точки отказов. В частности, в Grafana можно на одном дашборде совместить фактические данные и предсказанные значения, что позволяет сравнивать, анализировать расхождения и оперативно корректировать действия [7].

В результате интеграция моделей прогнозирования с CMDB, ITSM-платформами, системами мониторинга и автоматизации превращает аналитику в практический инструмент повышения надежности, снижения затрат и увеличения жизненного цикла АПК. Такой подход соответствует современным требованиям к цифровой трансформации инфраструктур и обеспечивает устойчивость в условиях растущей сложности и масштабов систем.

### **Примеры применения в промышленности и телекоммуникациях**

Телекоммуникационная отрасль представляет собой один из наиболее чувствительных к сбоям и задержкам сегментов цифровой инфраструктуры, поскольку надежность передачи данных напрямую влияет на качество предоставляемых услуг и удовлетворенность клиентов. Именно поэтому внедрение предиктивных моделей в данной сфере стало неотъемлемой частью современных подходов к управлению аппаратно-программными комплексами. Прогнозирование здесь приобретает особую значимость, поскольку позволяет не только обеспечивать непрерывность сервисов, но и оптимизировать эксплуатационные расходы и техническую поддержку.

Одним из распространенных направлений применения прогнозных алгоритмов в телеком-инфраструктуре является оценка износа портов и плат в маршрутизаторах и коммутаторах. Эти компоненты подвержены постепенному физическому старению из-за циклических нагрузок, температурных колебаний и загрязнения. Предиктивные модели, обученные на исторических данных эксплуатации, позволяют выявлять признаки деградации – например, учащающиеся ошибки CRC, флуктуации в уровне сигнала или частые переподключения линков. Таким образом, можно заранее идентифицировать порты, находящиеся в предаварийном состоянии, и своевременно их заменить без ущерба для сети.

Особое значение предиктивная аналитика имеет в управлении серверами мультимедийной обработки, включая видеоконференц-серверы, SIP-шлюзы и медиа-платформы. Эти системы подвержены неравномерной

нагрузке, зависящей от времени суток, количества активных пользователей и сценариев использования. Модели прогнозирования здесь позволяют заранее оценить вероятность наступления перегрузки – например, по росту потребления CPU, задержкам обработки аудио/видео или увеличению очередей на ввод-вывод. В результате можно заранее масштабировать ресурсы или перераспределить трафик, избегая отказов в пиковые периоды.

В телеком-среде также весьма перспективным направлением становится анализ влияния внешних факторов окружающей среды на отказоустойчивость оборудования. Используя данные IoT-датчиков (температура, влажность, вибрации) и сопоставляя их с журналами инцидентов, модели машинного обучения могут выявлять скрытые корреляции [8]. Например, может быть обнаружено, что перегрев оборудования в контейнерных базовых станциях коррелирует с определенными погодными условиями, или что повышенная влажность ведет к сбоям в передающих блоках. Эти знания позволяют перейти к более точной и адаптивной эксплуатации, в том числе с учетом климатических рисков.

Таким образом, в телекоммуникационной отрасли предиктивные модели находят применение в различных аспектах – от оценки физического износа компонентов до анализа сетевой нагрузки и влияния внешней среды. Это позволяет операторам поддерживать высокий уровень надежности сервисов, снижать издержки на обслуживание и минимизировать непредвиденные простои. В условиях постоянного роста требований к качеству связи и объему передаваемых данных такие решения становятся не просто полезными, а критически необходимыми для устойчивой работы телеком-инфраструктуры.

### **Экономические и эксплуатационные эффекты**

Внедрение прогнозных моделей в управление состоянием аппаратно-программных комплексов (АПК) приносит ощутимые практические результаты, выражающиеся как в экономических показателях, так и в повышении общей надежности инфраструктуры [9]. Один из ключевых эффектов – значительное сокращение затрат на внеплановые ремонты и восстановительные работы. За счет своевременного выявления признаков деградации и приближающихся отказов системы переходят от реактивного к проактивному обслуживанию. Это позволяет сократить число критических инцидентов и аварийных выездов, что по данным ряда исследований может снижать затраты на внеплановое обслуживание на 40–60 %.

Немаловажным результатом становится и повышение доступности АПК: за счет предотвращения сбоев и более эффективного планирования технических работ уменьшается общее время простоя. Это особенно актуально для критически важных систем, где каждая минута недоступности может приводить к прямым финансовым потерям или снижению качества обслуживания пользователей. Прогнозные алгоритмы позволяют заранее моделировать вероятность выхода из строя, что делает планирование ремонта или замены компонентов более управляемым процессом.

Таким образом, предиктивные модели становятся не только инструментом технической диагностики, но и фактором стратегического управления, влияющим на экономику, эффективность и репутацию организации.

## **Заключение**

В современном технологическом ландшафте, где отказоустойчивость, предсказуемость и эффективность эксплуатации аппаратно-программных комплексов (АПК) приобретают критическую значимость, интеграция прогнозных моделей в управление жизненным циклом становится неотъемлемым элементом цифровой трансформации инфраструктурных систем. Модели прогнозирования позволяют не только своевременно выявлять потенциальные отклонения и риски, но и трансформировать саму философию обслуживания – от реактивной к проактивной, а в перспективе и к полностью автономной.

Таким образом, прогнозирование состояний становится не только инструментом повышения эффективности эксплуатации, но и фактором стратегического управления жизненным циклом АПК, обеспечивающим технологическую устойчивость и экономическую целесообразность эксплуатации в условиях постоянно усложняющейся ИТ-среды.

## **Список используемых источников**

1. Грицкевич С. А., Шабуров А. А. Жизненный цикл технических систем: учебное пособие. Новосибирск: СГУГиТ, 2020. 120 с. URL: [https://lib.sgugit.ru/irbisfulltext/2020/14.02.20/Грицкевич\\_Шабуров/Грицкевич\\_Шабуров\\_макет2.pdf](https://lib.sgugit.ru/irbisfulltext/2020/14.02.20/Грицкевич_Шабуров/Грицкевич_Шабуров_макет2.pdf) (дата обращения 01.05.2025).
2. Lee, J. J., & Yang, B. H. (2020). Big Data Analytics for Predictive Maintenance and Reliability in Manufacturing. Springer. URL: <https://doi.org/10.1007/978-3-030-42734-7> (дата обращения 25.04.2025).
3. Manogaran, G., Raj, M. A., & P., S. (2020). Internet of Things (IoT) for Predictive Maintenance Springer. URL: <https://doi.org/10.1007/978-3-030-20495-9> (дата обращения 25.04.2025).

4. BMC Software. (2019). CMDB Best Practices: Integrating Predictive Maintenance Models. URL: <https://www.bmc.com> (дата обращения 25.04.2025).
5. ServiceNow. (2020). Predictive Maintenance and AI Integration in IT Service Management // ServiceNow White Paper. URL: <https://www.servicenow.com> (дата обращения 25.04.2025).
6. Zabbix. (2021). Integrating Predictive Models with Monitoring Tools for IT Systems // Zabbix Documentation. URL: <https://www.zabbix.com> (дата обращения 26.04.2025).
7. Grafana Labs. (2021). Monitoring Predictive Maintenance Data with Prometheus and Grafana // Grafana Labs. URL: <https://grafana.com> (дата обращения 25.04.2025).
8. Khan, M. B. S. M., & L, H. J. (2018). Predictive Analytics for IT Infrastructure: Ensuring Continuous Monitoring and Risk Management // International Journal of Computer Applications, 181(10), 32-38. DOI:<https://doi.org/10.5120/ijca2018916820> (дата обращения 26.04.2025).
9. Yeung, A. W. K., & Liu, F. X. C. (2019). The Role of Predictive Analytics in IT Operations Management // Journal of Cloud Computing: Advances, Systems and Applications, 8(1), 4. DOI:<https://doi.org/10.1186/s13677-019-0170-2> (дата обращения 26.04.2025).

УДК 004.8:004.7

**В. С. Елагин** (к.т.н., и. о. декана факультета ИКСС СПбГУТ),  
[v.elagin@sut.ru](mailto:v.elagin@sut.ru)

**М. П. Серикова** (студент группы ИКТМ-42м, СПбГУТ,  
[serikova.mp@sut.ru](mailto:serikova.mp@sut.ru))

## ПРИМЕНЕНИЕ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ КЛАССИФИКАЦИИ КРИПТОВАЛЮТНОГО ТРАФИКА

*Классификация криптовалютного трафика представляет собой сложную задачу из-за высокого уровня шифрования и гетерогенности данных. В статье исследуется применение графовых нейронных сетей (GNN) для решения этой проблемы. Рассматриваются их способность моделировать сетевые структуры, последние достижения в области анализа блокчейн-трафика и вызовы, такие как нехватка данных и вычислительная сложность. Исследования показывают, что GNN достигают точности до 95 %, превосходя традиционные методы. Предлагаются решения, включая синтетические данные и оптимизацию архитектур, что подчеркивает потенциал GNN для сетевой безопасности.*

*графовые нейронные сети, криптовалютный трафик, классификация трафика, машинное обучение, блокчейн*

Классификация сетевого трафика играет ключевую роль в обеспечении безопасности и оптимизации ресурсов в современных сетях. Криптовалютный трафик, связанный с блокчейн-технологиями, представляет особую сложность из-за высокого уровня шифрования, такого как SSL/TLS, и динамичных паттернов транзакций. Традиционные методы, такие как анализ портов и глубокий анализ пакетов (DPI), демонстрируют низкую эффективность, достигая точности от 30 до 70 % [1]. Анализ портов постепенно теряет значение, так как все чаще используются динамические порты, а DPI не способен анализировать содержимое зашифрованных пакетов. Поэтому возникают новые требования к методам, которые могут учитывать сложные связи внутри сетевых данных. Одним из таких подходов являются графовые нейронные сети (GNN): они описывают трафик в виде графа, где узлы соответствуют аккаунтам или устройствам, а ребра – потокам данных или транзакциям. Используя информацию от соседних узлов и пространственно-временные зависимости, GNN особенно хорошо подходят для анализа сетей на основе блокчейна.

Криптовалютный трафик отличается не только высоким уровнем шифрования, но и разнообразием используемых протоколов и приложений.



Блокчейн-технологии формируют сложные сетевые структуры, в которых транзакции связывают между собой аккаунты и устройства, образуя графовые зависимости. Традиционные методы машинного обучения, такие как Random Forest или сверточные нейронные сети (CNN), достигают точности до 90 % в задачах классификации обычного трафика, но их производительность снижается для зашифрованного трафика из-за отсутствия доступа к содержимому пакетов [2]. GNN, напротив, превосходят эти методы, так как способны анализировать топологию сети и извлекать контекст из связей между узлами. Например, в исследовании [3] представлена модель BT2, которая использует GNN для отслеживания транзакций Bitcoin. Модель интегрирует улучшенный алгоритм агрегации выборок, основанный на Dice Similarity, и достигает точности 86 % на наборе данных Elliptic, содержащем 203,769 узлов и 234,355 ребер. Это демонстрирует способность GNN эффективно обрабатывать большие графы и выявлять скрытые взаимосвязи.

Недавние исследования подтверждают потенциал GNN в классификации криптовалютного трафика. В работе [4] изучено применение различных архитектур GNN, включая Graph Convolutional Networks (GCN), Graph Attention Networks (GAT), Chebyshev spatial convolutional networks и GraphSAGE, для классификации транзакций Bitcoin. Авторы показывают, что комбинация GNN с линейным слоем и пропусками соединений улучшает результаты, достигая точности до 95 %. GCN агрегируют признаки соседних узлов с помощью свертки, тогда как GAT используют механизм внимания для присвоения весов наиболее значимым связям, что особенно полезно для гетерогенных данных [5]. Другое исследование [6] предлагает модель DIAM, которая формулирует задачу классификации как задачу над направленными мультиграфами с атрибутами ребер. Модель включает модуль Edge2Seq, автоматически обучающий представления узлов, сохраняющие паттерны параллельных транзакций, что улучшает выявление незаконных аккаунтов. Аналогично, в [7] используется подграфовое контрастивное обучение для обнаружения групп, занимающихся отмыванием денег, с помощью алгоритма Bit-CHetG, который строит однородные подграфы из гетерогенного графа адресов и транзакций.

Для классификации криптовалютного трафика сеть моделируется как ориентированный граф  $G = (V, E)$ , где  $V$  – множество узлов (аккаунты или устройства), а  $E$  – множество ребер (транзакции или потоки данных). Признаки узлов включают метаданные, такие как IP-адреса или балансы, а при-

знаки ребер – размеры пакетов, временные интервалы и протоколы. Архитектуры GNN, такие как GCN и GAT, позволяют агрегировать информацию от соседних узлов. Например, в GCN обновление признаков узла описывается уравнением, которое отображено в формуле 1:

$$h_v^{(l+1)} = \sigma \left( W^{(l)} \sum_{u \in N(v)} \frac{h_u^{(l)}}{|N(v)|} + B^{(l)} h_v^{(l)} \right), \quad (1)$$

где  $h_v^{(l)}$  – вектор признаков узла  $v$  на слое  $l$ ,  $N(v)$  – соседи узла,  $\sigma$  – функция активации. GAT, в свою очередь, использует коэффициенты внимания, что отражено в формуле 2.

$$\alpha_{vu} = \frac{\exp(\text{LeakyReLU}(\alpha^T [Wh_v || Wh_u]))}{\sum_{k \in N(v)} \exp(\text{LeakyReLU}(\alpha^T [Wh_v || Wh_k]))} \quad (2)$$

Что позволяет модели фокусироваться на наиболее релевантных связях [5]. Эти подходы эффективны для зашифрованного трафика, так как не требуют доступа к содержимому пакетов.

На рисунке 1 изображен пример графа криптовалютного трафика, где узлы – аккаунты, а ребра – транзакции.

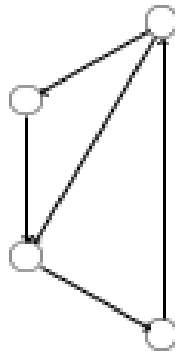


Рис 1. Пример графа криптовалютного трафика

Результаты исследований показывают, что GNN достигают высоких метрик производительности. Например, в [4] сообщается о точности 95 % и F1- score 0.93 для обнаружения мошеннических транзакций. Это превосходит традиционные методы, такие как DPI (50–80 %) и Random Forest (85–90 %), благодаря способности GNN анализировать графовые структуры [2]. В таблице 1 ниже представлено сравнение методов классификации.

ТАБЛИЦА 1. Сравнение методов классификации трафика

| Метод         | Точность ( %) | F1-score  | Подходит для зашифрованного трафика |
|---------------|---------------|-----------|-------------------------------------|
| Анализ портов | 30–70         | 0.40–0.60 | Нет                                 |
| DPI           | 50–80         | 0.50–0.70 | Нет                                 |
| Random Forest | 85–90         | 0.80–0.85 | Да                                  |
| CNN/RNN       | 88–92         | 0.85–0.90 | Да                                  |
| GNN           | 92–95         | 0.90–0.93 | Да                                  |

Несмотря на успехи, применение GNN сталкивается с вызовами. Нехватка качественных данных остается ключевой проблемой, так как большинство наборов данных, таких как Elliptic, ограничены по объему или доступности [3]. Высокая вычислительная сложность также ограничивает использование GNN в реальном времени, особенно для больших графов. Разнообразие протоколов и устройств делает трафик неоднородным, из-за чего трудно создать универсальные модели. Чтобы преодолеть эти ограничения, исследователи предлагают использовать синтетические данные, создаваемые с помощью графовых генеративных моделей, например GraphVAE [8].

Оптимизация архитектур GNN, включая методы субграфового сэмплирования и разреженные вычисления, помогает снизить вычислительные затраты [9]. Совмещение графовых нейронных сетей с существующими подходами машинного обучения открывает возможности для повышения точности и масштабируемости анализа трафика. Представление трафика в виде графа делает классификацию криптовалютных операций более устойчивой к шифрованию, что делает GNN перспективным инструментом для задач безопасности и выявления мошенничества. Благодаря способности анализировать сложные сетевые структуры, такие модели уже стали важной частью современных решений в области сетевой защиты. В дальнейшем внимание исследователей стоит уделить созданию открытых наборов данных, адаптации GNN к работе в реальном времени и интеграции с другими методами машинного обучения. Развитие этих направлений может значительно повысить эффективность классификации и способствовать более безопасному использованию блокчейн-технологий.

**Список используемых источников**

1. Pham T. Anomaly Detection in Bitcoin Network Using Graph Neural Networks // IEEE Access. 2023. URL: <https://arxiv.org/pdf/1611.03941> (дата обращения 10.05.2025).
2. Li Z., He E. Graph Neural Network-Based Bitcoin Transaction Tracking Model // IEEE Access, 2024. URL: [https://www.researchgate.net/publication/371739046\\_Graph\\_Neural\\_Network-Based\\_Bitcoin\\_Transaction\\_Tracking\\_Model](https://www.researchgate.net/publication/371739046_Graph_Neural_Network-Based_Bitcoin_Transaction_Tracking_Model) (дата обращения 10.05.2025).
3. Kim Y., et al. Security Mechanism for Detecting Malicious Events in Blockchain Network Traffic // Journal of Information Security and Applications, 2022. URL: [https://www.researchgate.net/publication/352717409\\_Anomaly\\_Detection\\_based\\_on\\_Traffic\\_Monitoring\\_for\\_Secure\\_Blockchain\\_Networking](https://www.researchgate.net/publication/352717409_Anomaly_Detection_based_on_Traffic_Monitoring_for_Secure_Blockchain_Networking) (дата обращения 10.05.2025).
4. Enhancing Anti-Money Laundering Frameworks: An Application of Graph Neural Networks in Cryptocurrency Transaction Classification // IEEE Journals, 2024.
5. Murzin, M. V., Kulikov, I. A., Zhukova, N. A. Methods for Constructing Graph Neural Networks // LETI Transactions on Electrical Engineering & Computer Science, 2024.
6. Chen, L.; Wang, P.; Wang, Y. Effective Multi-Graph Neural Networks for Illicit Account Detection on Cryptocurrency Transaction Networks. Entropy 2024, Vol. 26, № 211.
7. Bitcoin Money Laundering Detection via Subgraph Contrastive Learning. ResearchGate, 2024. Vol. 26 (3), № 211. DOI:10.3390/e26030211
8. Review of blockchain application with Graph Neural Networks, Graph Convolutional Networks and Convolutional Neural Networks // URL: <https://arxiv.org/abs/2410.00875> (дата обращения 10.05.2025).
9. Adloori H. Graph Network Models To Detect Illicit Transactions in BlockChain // URL: <https://arxiv.org/abs/2410.07150> (дата обращения 10.05.2025).

УДК 534.843.1

В. П. Жиряков (студент группы Р-41м, СПбГУТ), [zhiryakov.vp@sut.ru](mailto:zhiryakov.vp@sut.ru)

## АКУСТИЧЕСКИЕ ОСОБЕННОСТИ КОНЦЕРТНЫХ И СПОРТИВНЫХ ПЛОЩАДОК И ИХ ВЛИЯНИЕ НА ПРОЕКТИРОВАНИЕ СИСТЕМ ЗВУКОУСИЛЕНИЯ

*Системы звукоусиления на стадионах и в концертных залах требуют особого подхода из-за сложной архитектуры и больших объемов помещений. Применение распределенных конфигураций, временной синхронизации и направленных сабвуферов позволяет повысить разборчивость речи и обеспечить равномерное звуковое покрытие. В работе рассматриваются ключевые принципы проектирования с учетом акустических характеристик пространства.*

*акустика, звукоусиление, стадионы, концертные площадки, моделирование*

Качество звукового сопровождения массовых мероприятий напрямую зависит от акустических свойств площадки и корректного проектирования системы звукоусиления. Концертные залы, стадионы, ледовые арены – каждый тип помещения имеет характерные проблемы: длительное время реверберации, высокий уровень фонового шума и низкая разборчивость речи. В больших закрытых помещениях и на открытых аренах значительный объем пространства способствует увеличению времени реверберации и появлению эха. Сложная архитектура – наличие трибун, перекрытий, куполов – вызывает неравномерное распределение звукового давления и появление мнимых источников звука [1]. В результате, без применения специальных инженерных решений, в зале могут возникать участки с недостаточным уровнем звукового давления либо с недостаточной разборчивостью речи.

Геометрия современных арен – это вогнутые стены, купольные перекрытия, трибуны и металлические конструкции. Все эти материалы приводят к появлению множества сильных отражений, формирующих длительное реверберационное поле [1]. При неравномерном распределении звукового давления в зале возникают области с провалами и пиками громкости. Концертные залы, напротив, представляют собой закрытые помещения относительно небольшого объема (несколько сотен или тысяч мест). Их архитектура и отделка спроектированы для обеспечения благоприятной акустики.

В правильно спроектированном концертном зале сильные поздние отражения контролируются с помощью звукопоглощающих и рассеивающих элементов.

Во время проведения массовых мероприятий, особенно спортивных, уровень фонового шума в зале может достигать 80–85 дБ и выше. Источниками шума являются разговоры, аплодисменты, выкрики, а также акустические артефакты самой архитектуры помещения. Наличие устойчивого шумового фона существенно снижает динамический диапазон системы звукоусиления и требует увеличения мощности сигналов, особенно при передаче речевой информации. Для сравнения, в концертном зале уровень фонового шума достигает 35–40 дБ. В таблице 1 приведены примеры уровней шума от различных источников [2].

ТАБЛИЦА 1. Значения уровня шума для различных источников

| Источник шума               | Уровень, дБ |
|-----------------------------|-------------|
| Тихий парк                  | 20          |
| Тихая улица                 | 30          |
| Средний уличный шум         | 50-60       |
| Стадион                     | 75-85       |
| Зал театра (концертный зал) | 35-45       |
| Аудитория, зал заседаний    | 55          |

Как видно из таблицы, исходные шумовые условия на больших спортивных аренах заведомо хуже, чем в тихих залах, и система звукоусиления должна компенсировать это. Плотная заполненная людьми арена звучит иначе, чем пустая: сами зрители поглощают звук (особенно высокие частоты) и одновременно создают шум. Одним из важнейших параметров звукового восприятия является критическая дистанция – расстояние, на котором уровни прямого и отраженного звука становятся равными [2]. За пределами этой зоны основную долю в звуковой картине начинают формировать отражения, а не исходный сигнал. В спортивных сооружениях, где слушатели зачастую располагаются на значительном удалении от источника звука, критическая дистанция может быть превышена уже на первых рядах трибун.

Для решения акустических проблем на концертных и спортивных площадках применяются комплексные распределенные системы звукоусиления. Их основная задача – обеспечить равномерный охват всех зрительских зон разборчивым звуком.

Основная конфигурация звукоусилительной системы обычно включает несколько специализированных подсистем, каждая из которых обслуживает определенную зону площадки. Примеры типовых конфигураций представлены на рис. 1.

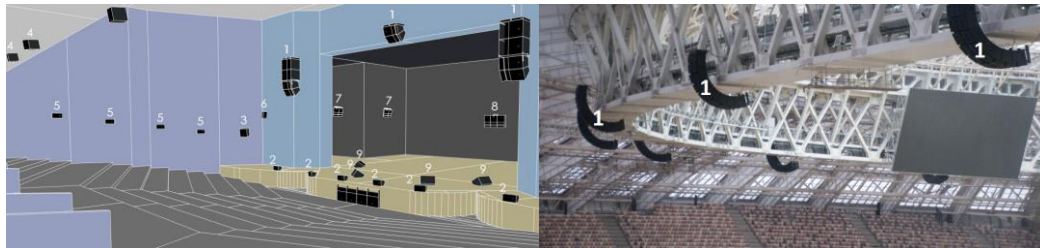


Рис. 1. Примеры размещения звукоусилительных систем на площадках разного типа. Типовая конфигурация звуковой системы концертного зала с выделением различных зон озвучивания (слева), система основных линейных массивов на спортивном стадионе (справа): 1 – main system; 2 – frontfill; 3 – downfill; 4 – delay; 5 – sidefill.

Main system обеспечивает общий звуковой фронт и покрывает большую часть зрительного пространства. Как правило, это подвесные линейные массивы устанавливаемые в верхней части сцены. Frontfill и downfill служат для озвучивания ближней зоны перед сценой, компенсируя недостаток звукового давления в участках, не охваченных основным массивом. Delay предназначены для компенсации акустических задержек при значительном удалении зрителей от основных источников звука. Sidefill используются для обеспечения равномерного звукового покрытия боковых и задних секторов зала или стадиона. Это особенно актуально для площадок сложной формы, где значительная часть зрителей находится вне эффективного покрытия центральной системой [3].

Эффективность распределенных систем звукоусиления на концертных и спортивных площадках во многом зависит от точности временной и фазовой настройки отдельных компонентов. Главная задача этих настроек – обеспечить одновременный приход звука от различных источников, устранив эхо и повысив разборчивость речи.

Временная синхронизация достигается при помощи цифровых задержек (DSP-процессоров), которые компенсируют разницу во времени распространения звука от основной системы до дополнительных массивов

(например, Delay и Frontfill). Например, Delay-линии получают сигнал с задержкой, равной времени прохождения звука от основной системы до точки расположения этих линий. Это гарантирует, что прямой звук от удаленных громкоговорителей придет к слушателю синхронно с основным.

Фазовая настройка необходима для согласования сигналов от нескольких громкоговорителей в перекрывающихся зонах звучания. Без такой коррекции могут возникать интерференционные провалы и резонансы, особенно в области низких частот.

Отдельное внимание при проектировании систем звукоусиления уделяется низкочастотному звену. Сабвуферные системы на концертных и спортивных площадках требуют особого подхода в связи с большой длиной волны и сложностью управления их направленностью. Главной проблемой низкочастотного излучения является его всенаправленность, что приводит к возникновению интерференционных зон и нежелательному распространению звука за пределы основной зоны прослушивания. Для управления направленностью сабвуферов применяются специальные массивы и схемы расстановки [3].

Наиболее распространены следующие конфигурации:

- кардиоидная конфигурация – это пара сабвуферов, один из которых развернут в противоположную сторону и получает сигнал с задержкой и инверсией фазы. Такая схема направляет излучение вперед и эффективно подавляет уровень звука в тыловой зоне;

- End-fire массив – линейная цепочка сабвуферов, на которые подается один и тот же сигнал с равномерным увеличением задержки от переднего к заднему. Такая схема усиливает излучение вперед и ослабляет его в обратном направлении, обеспечивая направленное распространение низких частот;

- Stacking-схема («инвертированный стек») – вертикальная группа из трех сабвуферов, где центральный развернут назад и получает сигнал с задержкой и инверсией фазы. Конфигурация формирует кардиоидное излучение вперед с выраженным ослаблением звука в тыловой зоне.

На рис. 2 представлены расчетные схемы направленности описанных конфигураций, где цвета обозначают уровни звукового давления: красный соответствует примерно 120 дБ, желтый – около 100 дБ, зеленый – около 90 дБ. Расчеты и моделирование схем направленности сабвуферных массивов были выполнены в программе EASE Focus с использованием сабвуферов ProTone T28.



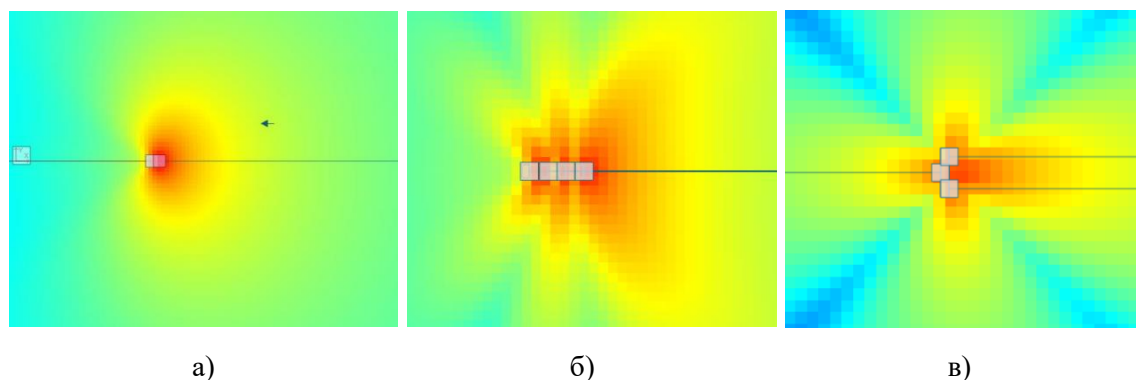


Рис. 2. Типовые схемы направленности сабвуферных массивов: а – кардиовидная конфигурация; б – End-fire массив; в – stacking-схема; частота 100 Гц.

Акустические особенности концертных и спортивных площадок предъявляют повышенные требования к проектированию систем звукоусиления. Большой объем помещений, длительное время реверберации, высокий уровень фонового шума и сложная архитектура затрудняют передачу речевых и музыкальных сигналов с требуемой разборчивостью и равномерностью. Эффективное решение этих задач возможно только при использовании распределенных конфигураций звукоусиления, включающих основную систему, фронтальные и боковые зоны заполнения, линии задержки и прочие группы.

Для обеспечения согласованной работы всех компонентов необходима точная временная и фазовая настройка [4, 5]. Особую роль играет правильная организация низкочастотного звена: использование направленных сабвуферных массивов позволяет управлять распространением басов и снижать уровень нежелательных отражений. Моделирование акустического поля и предварительная техническая оценка системы в специализированных программных средах позволяют учитывать акустические параметры площадки еще на стадии проектирования. Такой подход обеспечивает достижение высокой разборчивости речи, равномерного звукового покрытия и надежной работы звукоусиления в условиях различной сложности.

#### Список используемых источников

1. Катунин, Г. П. Акустика помещений: учебное пособие / Г. П. Катунин. – Москва: Ай Пи Ар Медиа, 2024. 192 с. ISBN:978-5-4497-3529-4.
2. Ковалгин Ю. А., Свинына О. А., Фадеев А. А. Расчет аппаратно-студийных комплексов телерадиовещания и аудиотехники. Часть 2. Расчет систем озвучения и звукоусиления. 2016.
3. Ковалгин Ю. А., Вологдин Э. И. Аудиотехника. Учебник для вузов. М.: Горячая линия – Телеком, 2013. 742 с. ISBN 978-5-9912-0241-1.

4. Исаков Ю. И. Цифровая обработка звуковых сигналов в музыкальной акустике. Электроакустическая система активного управления звуковым полем // Вестник музыкальной науки: науч. журн. 2016. № 2(12). С 60–71.

5. Чернов К. А. Исследование акустических характеристик студии звукозаписи // Радиоэлектроника молодежь в XXI веке: материалы 23 Международного молодежного форума. 2019. Т. 3. С. 94–95.

*Статья представлена научным руководителем, старшим преподавателем кафедры ЦТМ СПбГУТ Свинойной О. А.*

УДК 004.415

А. В. Зимин (ст. преподаватель кафедры ИКС, СПбГУТ), [zimin@sut.ru](mailto:zimin@sut.ru)А. М. Кондратьев (студент группы ИКТМ-42м, СПбГУТ), [kondratev.am@sut.ru](mailto:kondratev.am@sut.ru)

## ИСПОЛЬЗОВАНИЕ СЕТЕЙ ПЕТРИ ДЛЯ ТЕСТИРОВАНИЯ СЕТЕВЫХ ПРОТОКОЛОВ

*В данной работе рассматривается возможность применения сетей Петри для моделирования и тестирования сетевых протоколов, что особенно актуально в условиях усложнения архитектур сетей пятого поколения и роста затрат на тестирование их работы. На примере транзакции INVITE протокола SIP демонстрируется построение и анализ модели. Делается вывод о корректности работы модели и ее применимости для тестирования.*

*Сети Петри, сетевые протоколы, тестирование, SIP*

Важность тестирования протоколов, особенно с переходом к более сложным и многогранным сетям 5 поколения, только возрастает. При этом становится практически невозможно проводить тестирование на реальном оборудовании для каждой возможной реализации архитектуры сети ввиду больших расходов на создание тестовых площадок. Вместо этого имеет смысл использования моделирования работы необходимой реализации. Одним из способов создания модели, позволяющей оценить работоспособность реализации решения, являются сети Петри.

Сети Петри были разработаны и представлены Карлом Петри в 1962 году как графический и математический инструмент для построения модели и описания работы процессов некой системы.

С точки зрения математики сеть Петри – это набор множеств:

$$N = (P, T, F), P \cap T = \emptyset, \quad (1)$$

где  $P = \{p_1, p_2, \dots, p_n\}$  – множество вершин позиций;

$T = \{t_1, t_2, \dots, t_n\}$  – множество вершин переходов;

$F \subseteq (P \times T) \cup (T \times P)$  – множество направленных дуг, при этом можно разделить  $F$  на два подмножества;

$I = (P \times T)$  – набор входящих в переход дуг;

$O = (T \times P)$  – набор выходящих из перехода дуг;

Однако сеть Петри не может «работать» в таком виде. Для ее работы необходимо еще одно множество – множество меток  $M$ .

$$M = \{\mu: \forall p \in P; \mu(p) \rightarrow N\}, \quad (2)$$

Функция  $\mu$  выставляет каждой позиции неотрицательное целое число. Сама функция называется функцией маркировки (или разметки) сети, а  $M$  – маркировкой сети. Таким образом, набор  $S = (P, T, F, M)$  является маркированной сетью Петри.  $M$  на графе обозначается в виде точек, находящихся в позициях, или чисел, обозначающих количество маркеров в позиции.

Работой сети Петри является срабатывание переходов. При срабатывании перехода удаляются маркеры из позиций, дуги которых ведут в переход ( $I = (P \times T)$ ), и добавляются маркеры в позиции, дуги у которых приходят из сработавшего перехода ( $O = (T \times P)$ ) (рис. 1).

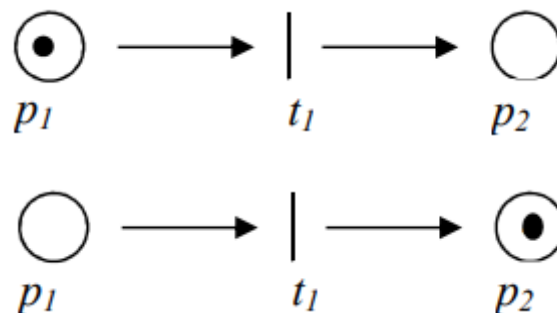


Рис. 1. Срабатывание перехода  $t_1$

С помощью данных переходов можно описать различные процессы работы протокола, что позволит разработать модели, которые могут использоваться как для функционального, так и для нагрузочного тестирования.

## Тестирование с использованием сетей Петри

Общая высокоуровневая схема тестирования протокола представлена на рисунке 2 [1].

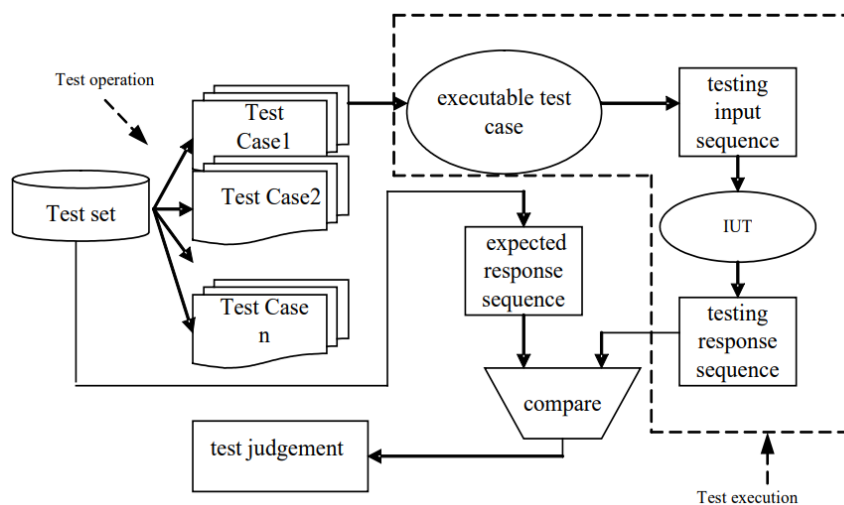


Рис. 2. Архитектура теста

Разработка тестовой модели начинается с анализа стандартов, описывающих необходимый протокол. На основе требований стандартов и планируемой схемы сети составляется перечень тестов. В случае использования сетей Петри тесты представляют собой непосредственно набор различных сетей, используемых для разных сценариев работы протокола. Для каждого теста также определяется ожидаемый результат, в данном случае, искомая финальная маркировка сети Петри.

В рамках проведения теста задается необходимый сценарий работы системы. После запуска симуляции работы реализации полученный результат сравнивается с ожидаемым результатом, который был задан ранее. Если итоговая маркировка сети совпадет с требуемым результатом, то считается, что функциональный тест для этого сценария пройден.

### Тестирование протокола SIP с помощью сетей Петри

Разберем принцип работы тестирования протоколов с помощью сетей Петри на примере протокола SIP. Работа протокола SIP основывается на транзакциях. Предлагаемая сеть Петри описывает INVITE транзакцию со стороны клиента и сервера (рис. 3) [2, 3].

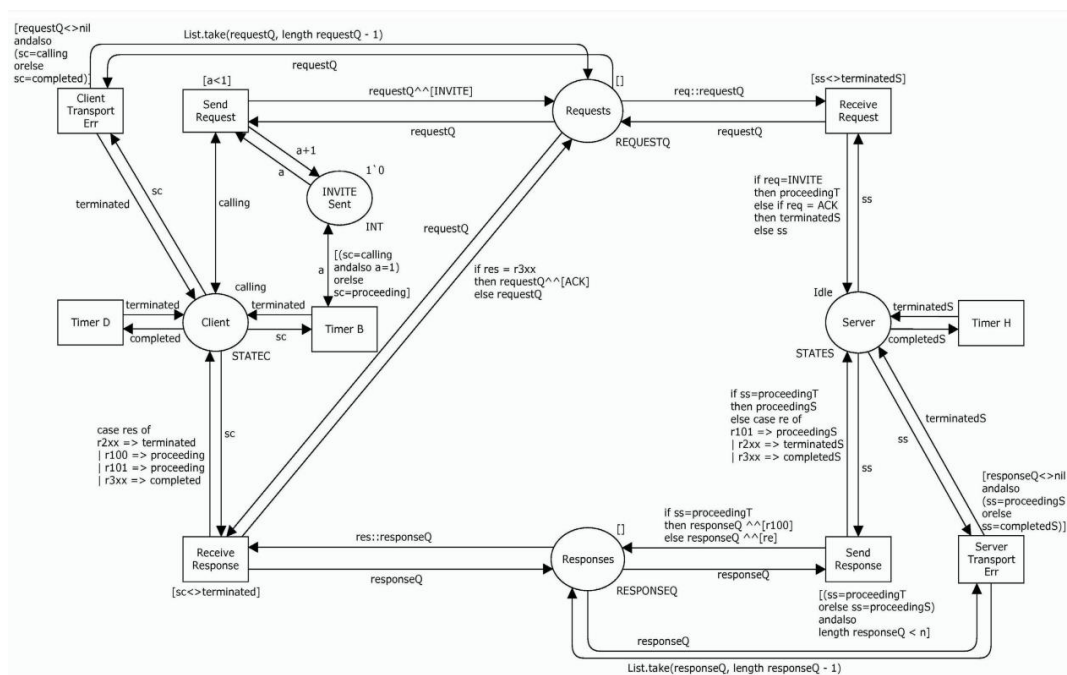


Рис. 3. Сеть Петри для INVITE транзакции

Для того, чтобы убедиться в правильной работе протокола, необходимо проанализировать данную сеть Петри на достижимость определенных финальных маркировок и наличие или отсутствие таких циклов, при которых

сеть все еще работает, но никогда не сможет достичь какой-либо финальной маркировки (livelock), а также отсутствие маркировок, при которых сеть больше не работает, но и не была достигнута одна из финальных маркировок (deadlock). Наилучшей финальной маркировкой является отсутствие меток (сообщений) в сети при условии, что Client и Server находятся в terminated состоянии (успешное завершение транзакции).

В результате моделирования сети при размере очереди Responses  $n=3$  и начальной маркировке, определяющей клиентское устройство в состоянии отправки INVITE (Client – Calling) получают следующие финальные маркировки (таблица 1):

ТАБЛИЦА 1. Финальные маркировки сети Петри для INVITE транзакции

| Маркировка | Client     | Requests | Server      | Responses          | INVITE Sent |
|------------|------------|----------|-------------|--------------------|-------------|
| 5          | Terminated | []       | Idle        | []                 | 1           |
| 19         | terminated | []       | terminatedS | [r100, r2xx]       | 1           |
| 26         | terminated | []       | terminatedS | []                 | 1           |
| 31         | terminated | []       | terminatedS | [r100, r3xx]       | 1           |
| 32         | terminated | []       | terminatedS | [r100]             | 1           |
| 33         | terminated | []       | terminatedS | [r2xx]             | 1           |
| 39         | terminated | []       | terminatedS | [r100, r1xx, r2xx] | 1           |
| 47         | terminated | []       | terminatedS | [r3xx]             | 1           |
| 51         | terminated | []       | terminatedS | [r100, r1xx, r3xx] | 1           |
| 52         | terminated | []       | terminatedS | [r100, r1xx]       | 1           |
| 53         | terminated | []       | terminatedS | [r100, r2xx]       | 1           |
| 58         | terminated | [ACK]    | terminatedS | []                 | 1           |
| 59         | terminated | []       | terminatedS | [r1xx, r3xx]       | 1           |
| 60         | terminated | []       | terminatedS | [r1xx]             | 1           |
| 64         | terminated | []       | terminatedS | [r1xx, r1xx, r2xx] | 1           |
| 66         | terminated | []       | terminatedS | [r1xx, r1xx, r3xx] | 1           |
| 67         | terminated | []       | terminatedS | [r1xx, r1xx, r2xx] | 1           |

В итоге получается 17 возможных финальных маркировок. При этом ни одна из них не является deadlock-ом, так как в каждом случае клиент и сервер находятся в состоянии terminated, что указывает на завершение транзакции, независимо от того, успешное оно или нет. Несмотря на то, что в данной сети присутствуют циклы (маркировки 11-23-40-56), в сети нет live-lock-циклов. Из каждой из этих маркировок есть возможность добраться до одной из финальных маркировок. Анализ работы модели показал, что в данной конфигурации SIP INVITE транзакция будет успешно заканчиваться, не оказываясь в циклах, из которых нет возможности выбраться.

Таким образом видно, что сети Петри позволяют смоделировать различные ситуации, которые могут произойти при работе протокола. При этом проверка сети Петри на достижимость определенной маркировки или живость сети позволяют проверить, что предлагаемая реализация архитектуры сети позволит успешно предоставлять необходимый функционал.

#### **Список используемых источников**

1. Liang Zhang, Hao Fang, De Qin Shu. Research on Protocol Conformance Testing Method Based on Petri net. // Proceedings of the 2015 4th National Conference on Electrical, Electronics and Computer Engineering. DOI:10.2991/nceee-15.2016.168.
2. Liu J., Liu, L. A Coloured Petri Net Approach to the Functional and Performance Analysis of SIP Non-INVITE Transaction. // Transactions on Petri Nets and Other Models of Concurrency IX. LNCS. Vol. 8910. DOI:10.1007/978-3-662-45730-6\_8.
3. Ding L. G., Liu L. Modelling and analysis of the INVITE transaction of the session initiation protocol using coloured Petri nets. // PETRI NETS 2008. LNCS. Vol. 5062. PP. 132–151. DOI:10.1007/978-3-540-68746-7\_12.

*Статья представлена научным руководителем, профессором кафедры ИКС СПбГУТ, доктором технических наук, профессором Гольдштейном А. Б.*

УДК 004.93'1

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

## ИССЛЕДОВАНИЕ МЕТОДОВ ПО УЛУЧШЕНИЮ РАСПОЗНАВАНИЯ ОБЪЕКТОВ В УСЛОВИЯХ ЗАТРУДНЕННОЙ ВИДИМОСТИ

*В данной статье представлен обзор существующих методов для улучшения распознавания объектов в условиях затрудненной видимости, таких как: ночь, снег, дождь и т.д. Проведен сравнительный анализ по критериям стоимости, дистанции работы, потреблению ресурсов, а также дана оценка одиночной и групповой эффективности.*

*видео, компьютерное зрение, затрудненная видимость, искусственный интеллект*

Современные технологии позволяют системам компьютерного зрения видеть в различных условиях, включая условия затрудненной видимости [1]. Существует технологии, позволяющий с помощью различных методов получить верное представление о сложно различимом объекте. В основе этого подхода лежит отдельное или комбинированное использование методов: цветокоррекция, перехода в другой спектр видимости и использовании системы LiDAR [2].

Перед переходом к описанию методов необходимо определить понятие среды с затрудненной видимостью. Такая среда представляет собой пространство между объектами и системой наблюдения, которая характеризуется рядом неблагоприятных факторов, влияющих на качество изображения:

- низкий контраст сцены – при слабом освещении или в тумане объекты сливаются с фоном, теряя четкость границ;
- рассеивание света – частицы воды, снега или пыли рассеивают свет, снижая видимость и размывая детали изображения;
- потеря текстурных признаков – при недостаточной видимости теряются мелкие детали поверхности объектов, важные для их различения;
- блики и засветы – яркие источники света (например, фары ночью) создают блики, которые маскируют объекты;
- искажения и артефакты – капли на объективе, запотевание или отражения ухудшают качество визуальной информации [1].



Определив суть проблемы, опишем методы, позволяющие минимизировать сложность определения объектов в данных средах.

Самым простым методом является обработка цвета, контрастности и насыщенности кадра видео или фотографии. Подобный метод может быть уже внедрен в видеоаппаратуру или добавлен путем отдельного блока обработки по ключевым паттернам изображения. Обработка может быть, как статической (применение одного и того же алгоритма действий) или адаптивной с применением алгоритмов, что определяют степень яркости, насыщенности и контрастности, и меняют исходя из этих данных [3]. На примере изображений на рис. 1 и 2 можно убедиться, что даже простая обработка кадра видео или изображения уже значительно повышает распознаваемость объектов.

Переход в другой спектр открывает уже большие возможности. Применяя камеры ночного зрения или тепловизионные, больше нет необходимости зависеть от уровня освещенности. Блики и низкий контраст среды тоже не создадут помех, что можно увидеть на рис. 3 и 4. Заметно насколько больше открылось наблюдателю информации об объектах и субъектах при переходе в другой спектр видимости [4].



Рис. 1. Изображение до обработки



Рис. 2. Изображение после обработки

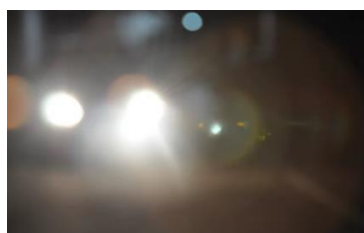


Рис. 3. Изображение с обычной камеры



Рис. 4. Изображение с тепловизионной камеры

Технология LiDAR, которая использует направленный лазер для измерения расстояний, позволит создать отказоустойчивую модель совместно с видеосистемами в случаях, когда даже не помог переход в другой спектр, как например в случаях снегопада. А также, что не менее важно, максимальная дальность определения объектов с падением доли определения всего на

10 % в туманной среде, увеличивается практически в 10 раз, что видно в таблице 2.

После определения основных технологий, становится возможным их сравнение по индивидуальным характеристикам. В таблице 1 представлены обобщенные показатели эффективности рассматриваемых методов. Следует отметить, что критерий «Сложность внедрения» был оценен относительно технологии коррекции изображения, принятой за базовый уровень. Это позволило сопоставить трудозатраты и технические требования других подходов в сравнении с наиболее простым и доступным методом.

Кроме того, все остальные критерии, представленные в таблице, выражены в виде диапазонов значений, что обусловлено значительным разбросом параметров моделей.

ТАБЛИЦА 1. Сравнение технологий по общим критериям

| Критерий                     | Коррекция изображений      | Переход в другой спектр видимости | LiDAR                       |
|------------------------------|----------------------------|-----------------------------------|-----------------------------|
| Необходимый ур. освещенности | 100 - 10.000 лк            | 0 - 1 лк                          | Не зависит от освещения     |
| Сложность внедрения          | Низкая                     | Средняя                           | Высокая                     |
| Стоимость реализации         | 0 - 1000 Р                 | 50.000 - 500.000 Р                | 100.000 - 5.000.000 Р       |
| Потребление ресурсов         | 1 - 5 Вт<br>0.5 - 2 GFLOPS | 5 - 30 Вт<br>2 - 10 GFLOPS        | 15 - 60 Вт<br>5 - 30 GFLOPS |
| Задержка обработки           | 1 – 100 мс                 | 8 – 200 мс                        | 10 – 200 мс                 |
| Рабочая дистанция            | 0 - 30 м                   | 1 - 200 м                         | 2 - 500 м                   |

Для объективного сравнения эффективности различных технологий возможно использование количественных метрик, таких как точность и средняя точность, усредненная по всем классам объектов mAP. Точность (%) характеризует долю корректно распознанных объектов относительно общего числа сделанных системой предсказаний. mAP (%), в свою очередь, представляет собой обобщенную метрику, учитывающую как точность, так и полноту распознавания по всем классам объектов.

Как и в таблице 1, представленные значения данных метрик приведены в виде диапазонов, что связано с различиями в используемых наборах данных, условиях тестирования и настройках моделей в отдельных исследованиях.

ТАБЛИЦА 2. Сравнение технологий в кол-ве распознаваний в разных средах [5, 6]

| Условие (среда) | Коррекция изображений, % | Переход в другой спектр (ИК), mAP % | LiDAR, %                           |
|-----------------|--------------------------|-------------------------------------|------------------------------------|
| Туман           | 30 - 50                  | 90 +<br>(при видимости ~ 13 м)      | 60 – 80<br>(при видимости ~ 100 м) |
| Снегопад        | 25 - 40                  | 70 – 85                             | 65 – 75                            |
| Дождь           | 30 - 50                  | 90 – 95                             | 70 – 85                            |
| Ночь            | 20 - 40                  | 90 - 95                             | 85 - 95                            |

Подводя итог по вышеизложенному, можно сделать следующие выводы. В различных условиях преобладание тех или иных методов разнится, что подтверждается данными с таблиц. В условиях, где преобладает вода (туман, дождь, снег) LiDAR показывает себя хуже, чем переход в другой спектр, так как капли воды рассеивают измерительный лазерный луч, что мешает работе, однако дальность определения с использованием LiDAR в разы возрастает. Технология коррекции изображений показывает себя хуже конкурентов, однако ее дешевизна и простота не позволяют полностью отойти от данной технологии. Связи с этим стоит рассматривать гибридные системы, в которых методы будут страховать друг друга, что позволит заполучить все преимущества, оставив лишь один недостаток – стоимость реализации.

#### Список используемых источников

1. Горячкин Б. С., Китов М. А. Компьютерное зрение E-scio. 2020. №. 9 (48). С. 317-345. URL: <https://cyberleninka.ru/article/n/kompyuternoe-zrenie-1> (дата обращения 20.04.2025).
2. Акинин М. В., Акинина Н. В., Солдатенко И. С. Устройство синтезированного видения. 2017 // URL: <https://elibrary.ru/item.asp?id=38292933> (дата обращения 22.04.2025).
3. Потапов А. С. Системы компьютерного зрения. Учебное пособие. СПб: Университет ИТМО, 2016. 161 с.
4. Власов С. Ю., Кипов М. Х.: Машинное зрение в условиях плохой видимости, 2023.
5. IEEE P2020 Automotive Imaging White Paper.
6. Himanshu Gupta, Oleksandr Kotlyar, Robust Object, Henrik Andreasson Detection in Challenging Weather Conditions // IEEE Explore. 2024 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) 2024. 10 p.

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

УДК 004-932:535

Колпаков С. В. (магистрант группы ИКТФ-46м, СПбГУТ),  
[new.account.73@mail.ru](mailto:new.account.73@mail.ru)

## МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РАБОТЫ ОПТИЧЕСКОГО ФУРЬЕ-ПРОЦЕССОРА

*В работе рассмотрена возможность математического моделирования работы когерентного оптического Фурье-процессора с жидкокристаллическим пространственным модулятором на входе с использованием быстрого преобразования Фурье из программы Matlab. Получены выходные сигналы Фурье-процессора при обработке как двумерных сигналов (изображений), так и одномерных входных сигналов.*

*математическое моделирование, оптический фурье-процессор, быстрое преобразование Фурье, Matlab*

Оптический Фурье-процессор позволяет с помощью одной линзы выполнять преобразование Фурье одномерных и двумерных сигналов, подаваемых на его вход пространственным модулятором света в виде распределения комплексной амплитуды света, рис. 1. Выходные сигналы процессора формируются в виде пространственного распределения амплитуды света в задней фокальной плоскости линзы и регистрируются там, как правило, матричным фотоприемником.

Представляет интерес исследование возможности применения такой системы при оптической обработке разного типа сигналов. Если отвлечься от ряда факторов, мало влияющих на работу процессора, это исследование проще проводить не экспериментально, а с помощью математического моделирования.

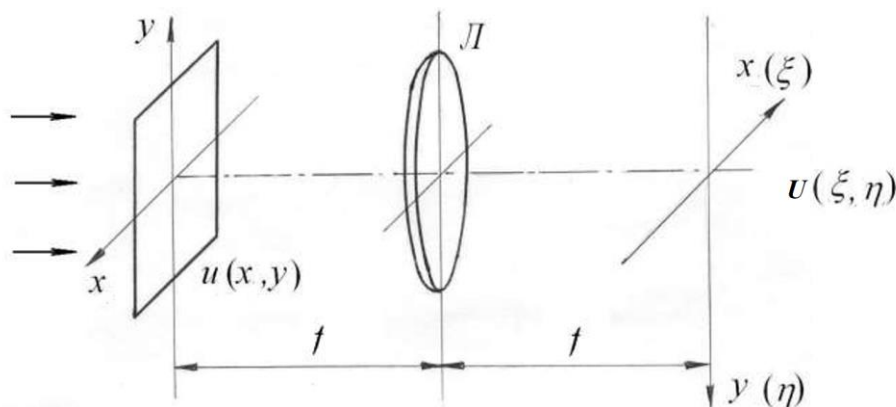


Рис. 1. Схема оптического фурье-процессора

При моделировании приходится решать две задачи: сформировать входной оптический сигнал с учетом особенностей работы пространственного модулятора света и настроить математическую программу преобразования Фурье и вывод выходных сигналов на монитор. В качестве устройства ввода входных сигналов в моделируемой оптической системе использовался жидкокристаллический модулятор света (ЖК ПМС), оптический сигнал на выходе которого совпадал с подаваемым на его вход двумерным входным сигналом в виде png файла с размерностью по числу пикселей ЖК матрицы (1024x768). Для вычисления преобразования Фурье была выбрана программа БПФ из Matlab.

Интерфейс программы Matlab представлен на рис.2. Можно задавать следующие параметры преобразования Фурье: прямое или обратное преобразование Фурье, частоту дискретизации исходного сигнала, интервал дискретизации. Рабочая часть Matlab поделена на три области: первая область – это область с изображениями, с которыми мы работаем, вторая с рабочим пространством, состоящее из множества переменных, созданных во время сеанса работы системы Matlab, также можно добавлять новые переменные в рабочее пространство загрузкой запомненных ранее рабочих пространств, или же путем непосредственного ввода переменных. Также есть третья часть, командное окно, это основное место для ввода и выполнения команд. В нем можно напрямую вводить команды, функции, выражения и получать результаты их выполнения в реальном времени. Четвертая область – это всплывающее окно, выводящее результаты моделирования.

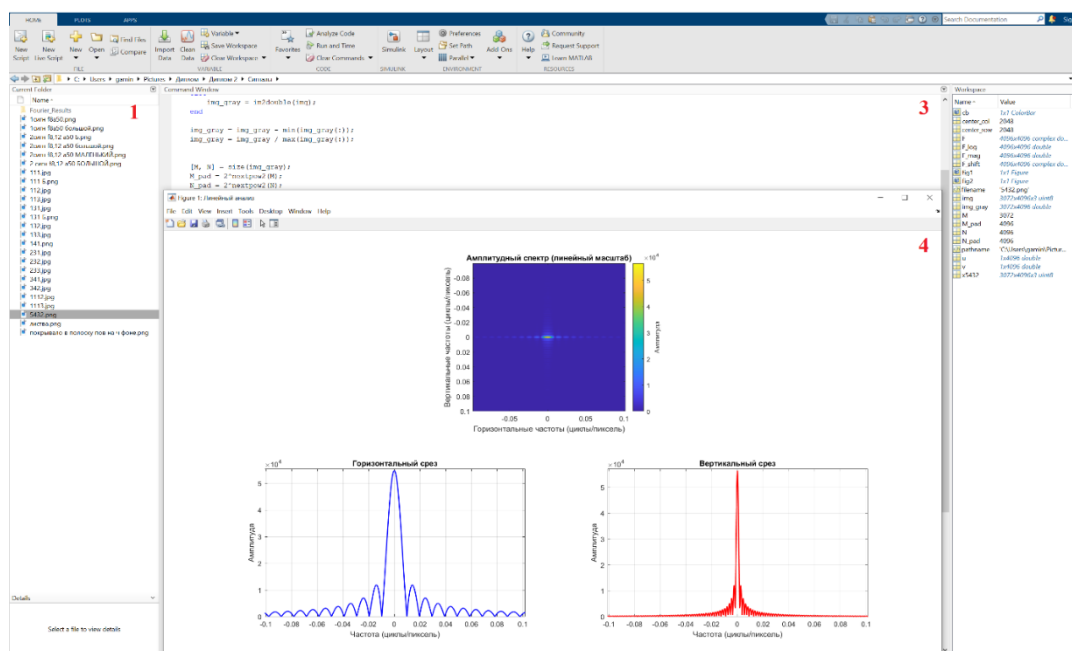


Рис. 2. Интерфейс программы Matlab

При исследовании работы программы оказалось, что разрешающая способность и точность формирования выходных данных были недостаточны. Улучшить эти параметры удалось увеличением темного поля во входном изображении за пределами отличного от нуля входного сигнала, например, до размеров 4092x3072 пикселей. Это не противоречит используемой модели оптического процессора, так как за пределами ЖК ПМС оптический сигнал системы равен нулю. На рис. 3. показано сечение по одной из ортогональных координат моделируемого выходного сигнала при исходном и увеличенном числе пикселей для входного сигнала в виде изображения прямоугольника. При увеличенном размере входного поля сечение сигнала отлично совпадает с теоретически ожидаемым.

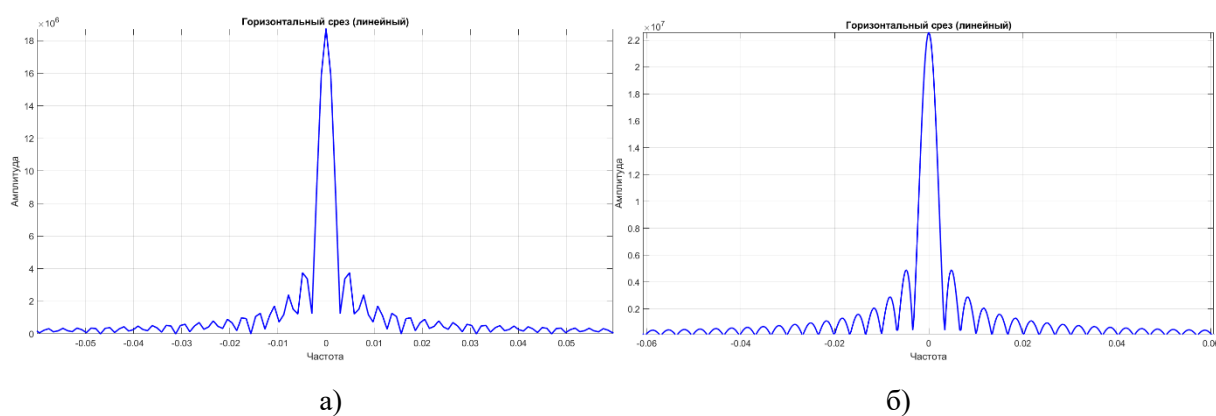


Рис. 3. Сечение выходного сигнала по горизонтальной координате при числе пикселей входного сигнала 1024 (а) и 4096 (б)

Для получения спектров одномерных (электрических) сигналов, в ЖК ПМС они также могут быть представлены в виде двумерных изображений, уровень сигнала в которых по одной координате повторяет форму входного сигнала на подставке постоянного уровня (чтобы можно было вводить двухполярный сигнал), а по второй координате уровень сигнала не меняется. Пример обработки одномерного сигнала, являющегося суммой двух радиоимпульсов разной частоты на видеоимпульсе подставки, показан на рис. 4.

Как и следует из теории [1], спектр такого сигнала состоит из пяти максимумов: спектру каждого радиоимпульса соответствуют два максимума, а один (на нулевой частоте) – спектру видеоимпульса подставки. Следует заметить, что без учета шумов в оптическом процессоре с помощью оптического моделирования можно получать выходные сигналы с высокой точностью, что позволяет, например, наблюдать взаимодействие боковых лепестков сигналов нулевого и первого порядков в спектре, как видно из рис. 4 г.

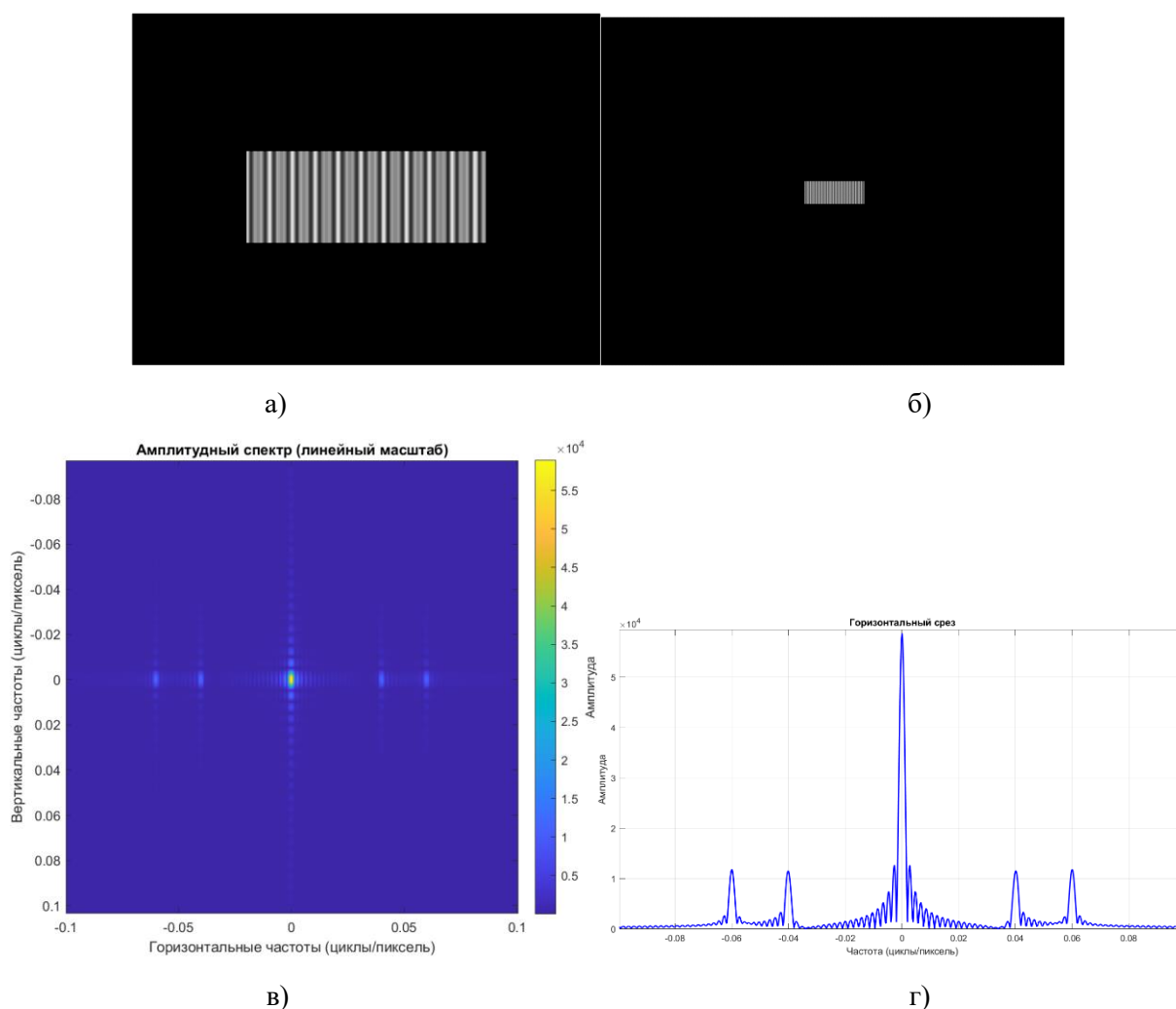


Рис. 4. Результат моделирования работы оптического Фурье-процессора при обработке одномерного сигнала. Входной сигнал оптического Фурье-процессора 1024 x 768 пикселей (а); входной сигнал программы БПФ 4096 x 3072 пикселей (б); выходной сигнал программы БПФ (в); сечение модуля выходного сигнала по горизонтальной координате (г)

Оптический процессор интересен не только сам по себе, когда он используется в различного типа анализаторах спектра сигналов, в системах обработки сигналов антенных решеток, в оптико-цифровых устройствах распознавания образов и т.п., но и тем, что он является типовым элементом более сложных оптических схем в Фурье-оптике, например, конвольверах и корреляторах, имеющих широкое применение. Рассмотренный подход математического моделирования может быть также использован при анализе подобных устройств.

#### Список используемых источников

1. Рогов С. А. Основы оптоинформатики оптические методы и устройства обработки информации: учебное пособие. Санкт-Петербург 2016

*Статья представлена научным руководителем, доктором физико-математических наук, профессором кафедры ОКСС Роговым С. А.*

УДК 621.396

**Е. В. Кравец** (к.т.н., доцент, доцент кафедры БТС, СПбГУТ)

**В. П. Подсветова** (студент группы РМ-23, СПбГУТ), [podsvetova.vp@sut.ru](mailto:podsvetova.vp@sut.ru)

## МЕТОДЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ (QoS)

*В условиях стремительного роста сетевого трафика и повышения требований к качеству передачи данных технологии обеспечения качества обслуживания (QoS, Quality of Service) приобретают особую значимость. В статье рассматриваются основные цели и принципы работы QoS, включая приоритизацию трафика, контроль пропускной способности, управление задержками и маркировку пакетов. Описаны методы реализации QoS в IP-сетях, мобильных сетях, приложениях реального времени и системах Интернета вещей. Также выделены ключевые недостатки, связанные со сложностью настройки, совместимостью оборудования и масштабируемостью решений. Материал ориентирован на технически подкованную аудиторию и предназначен для общего понимания роли QoS в современных сетевых инфраструктурах.*

*QoS, качество обслуживания, сетевые технологии, приоритизация трафика, задержка, пропускная способность, IP-сети, мобильные сети, VoIP, видеоконференции, управление трафика*

Качество обслуживания (QoS, Quality of Service) – это совокупность оценок характеристик качества предоставляемой телекоммуникационной услуги, которые определяют способность удовлетворить установленные и предполагаемые потребности пользователя (или «суммирующая оценка качества услуги, определяющая степень удовлетворенности пользователя предоставленной услугой»). В последние годы, с развитием сетей пятого поколения (5G) и сетей следующего поколения (NGN), требования к QoS значительно возросли. С увеличением объема данных, числа подключаемых устройств и появления новых приложений важно обеспечить стабильное и высококачественное предоставление услуг в условиях перегрузок и разнообразных требований пользователей. В этом докладе рассматриваются методы обеспечения QoS в современных и будущих телекоммуникационных сетях, а также плюсы и минусы их применения в сетях NGN и 5G.



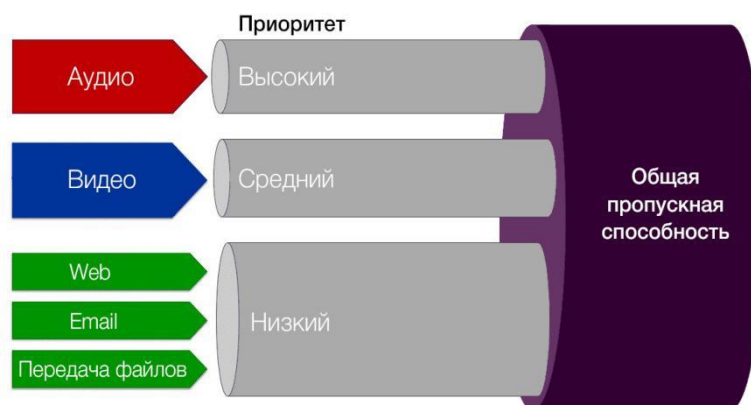


Рис. 1. Приоритеты QoS

## Основные понятия и принципы QoS

QoS включает в себя несколько аспектов, таких как управление пропускной способностью, задержками, джиттером (нестабильность задержки), потерей пакетов и обеспечением надежности связи. Все эти параметры играют ключевую роль в качестве предоставляемых телекоммуникационных услуг.

Для обеспечения качественного сервиса операторы сетей используют различные механизмы управления трафиком, такие как классификация трафика, управление очередями, предсказание нагрузки и приоритизация пакетов. Эти методы позволяют эффективно распределять ресурсы сети в зависимости от потребностей пользователей и типов обслуживаемых приложений.

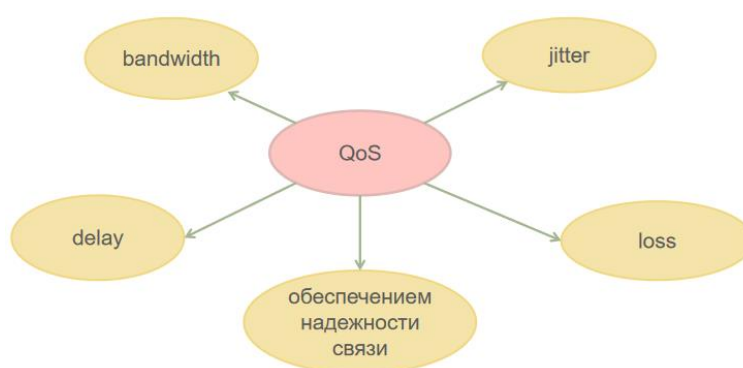


Рис. 2. Аспекты QoS

## Механизмы обеспечения QoS

### 1. Классификация и маркировка трафика

Классификация трафика включает в себя разделение пакетов данных на категории в зависимости от их типа или назначения. Например, видео или

голосовые данные могут быть классифицированы как трафик реального времени и иметь более высокий приоритет по сравнению с другими видами трафика, такими как электронная почта или веб-серфинг. Маркировка пакетов используется для обозначения их приоритетности, что позволяет операторам эффективно управлять трафиком и обеспечивать требуемое качество обслуживания.

## 2. Управление очередями

Очереди – это структуры данных, в которых хранятся пакеты до того, как они будут переданы по сети. В условиях перегрузки сети важно эффективно управлять очередями, чтобы минимизировать задержки для приоритетных пакетов. Один из распространенных методов – это взвешенное циклическое расписание (WRR), которое регулирует порядок обработки пакетов в очереди в зависимости от их приоритета. Алгоритм WFQ (Weighted Fair Queuing) помогает справедливо распределять доступную пропускную способность между различными потоками данных, принимая во внимание их приоритеты.

## 3. Резервирование ресурсов

Резервирование пропускной способности для определенных типов трафика помогает гарантировать, что важные приложения, такие как видеоконференции или VoIP-связь, получают необходимое количество ресурсов в условиях перегрузки сети. Протокол RSVP (Resource Reservation Protocol) позволяет резервировать пропускную способность для конкретных потоков данных, обеспечивая тем самым стабильность и высокое качество обслуживания для критичных сервисов.

## 4. Методы управления задержками и джиттером

Для приложений, чувствительных к задержкам, таких как видеозвонки или онлайн-игры, важно минимизировать задержки и поддерживать их на постоянном уровне. Одним из методов управления задержками является использование алгоритмов взвешенного случайного раннего обнаружения (WRED), которые регулируют очередь с учетом вероятности потери пакетов при перегрузке.

## QoS в сетях следующего поколения (NGN)

Сети NGN – следующая эволюция в области телекоммуникаций, объединяющая различные сетевые технологии для обеспечения услуг с высокими требованиями к QoS. В таких сетях QoS управляется не только на

уровне передачи данных, но и на уровне предоставления услуг. Важным аспектом является возможность сквозного обеспечения QoS, что означает поддержание требуемого уровня обслуживания на всем пути передачи данных от источника до получателя.

Для сетей NGN характерно использование концепции мульти-услуг, где различные типы трафика (например, голосовые и видео-сервисы) могут быть обслуживаемы с разными приоритетами. Это позволяет более гибко управлять сетью и минимизировать влияние перегрузок на чувствительные к задержкам приложения.

Сети NGN – следующая эволюция в области телекоммуникаций, объединяющая различные сетевые технологии для обеспечения услуг с высокими требованиями к QoS. В таких сетях QoS управляется не только на уровне передачи данных, но и на уровне предоставления услуг. Важным аспектом является возможность сквозного обеспечения QoS, что означает поддержание требуемого уровня обслуживания на всем пути передачи данных от источника до получателя.

Для сетей NGN характерно использование концепции мульти-услуг, где различные типы трафика (например, голосовые и видео-сервисы) могут быть обслуживаемы с разными приоритетами. Это позволяет более гибко управлять сетью и минимизировать влияние перегрузок на чувствительные к задержкам приложения.

Плюсы использования QoS в сетях NGN:

- гибкость в управлении трафиком. Механизмы QoS позволяют гибко управлять трафиком, распределяя ресурсы в зависимости от потребностей разных типов приложений;
- обеспечение качества для мультимедийных услуг. QoS гарантирует, что услуги реального времени, такие как видеозвонки и VoIP, будут обеспечены минимальными задержками и высокой надежностью;
- интеграция различных сервисов. NGN позволяет интегрировать голосовые, видеосервисы и данные в единую сеть, предоставляя универсальные услуги;

Минусы использования QoS в сетях NGN:

- сложность настройки и управления. Различные механизмы QoS требуют сложной настройки и могут потребовать значительных вычислительных ресурсов;

- ограниченная масштабируемость. С увеличением количества подключаемых устройств и пользователей на сети может возникнуть необходимость в модернизации инфраструктуры для поддержания высококачественного обслуживания.

## QoS в сетях 5G

С развитием технологий 5G требования к QoS становятся еще более сложными из-за увеличившегося количества устройств и разнообразия приложений, от мобильной связи до интернета вещей (IoT). В сетях 5G применяется технология слайсинга (она же сегментация) сети (network slicing), которая позволяет разделить сеть на несколько виртуальных сегментов (срезов), каждый из которых может обслуживать различные типы приложений с различными требованиями к QoS. Слайсинг сети – это создание изолированных логических сетей или сегментов.

Например, для приложений с низкими требованиями к задержке (например, дистанционное управление или автономные автомобили) будет выделен отдельный срез с минимальной задержкой. В то же время для высокоскоростной передачи данных (например, для потокового видео) будет создан срез с максимальной пропускной способностью.

Плюсы использования QoS в сетях 5G:

- высокая производительность. QoS позволяет эффективно распределять ресурсы сети для обеспечения высокой скорости передачи данных и минимальной задержки, что критично для приложений реального времени;
- поддержка множества сценариев использования. Благодаря слайсингу, 5G может поддерживать различные типы услуг с различными требованиями, от IoT до мультимедийных сервисов;
- оптимизация ресурсов. Сетевой слайсинг и виртуализация сетевых функций (NFV) позволяют эффективно использовать ресурсы сети, обеспечивая динамическое распределение в зависимости от текущих потребностей.

Минусы использования QoS в сетях 5G:

- сложность архитектуры. Разделение сети на срезы и управление ими требует сложной инфраструктуры и интеграции новых технологий, что может увеличить затраты на развертывание и обслуживание.

- проблемы безопасности. Для каждого среза требуется отдельное обеспечение безопасности, что усложняет управление рисками и уязвимостями, особенно с учетом огромного количества подключаемых устройств и сервисов.

## Выводы

Методы обеспечения качества обслуживания (QoS) являются ключевыми для поддержания высокой производительности и удовлетворенности пользователей в современных и будущих телекоммуникационных сетях. Сети следующего поколения, такие как NGN и 5G, требуют новых подходов и технологий, таких как управление очередями и слайсинг сети, для эффективного распределения ресурсов и обеспечения стабильного качества обслуживания. Несмотря на преимущества (гибкость и высокая производительность), внедрение QoS также сопровождается определенными сложностями (включая настройку инфраструктуры, масштабируемость и безопасность).

## Список используемых источников

1. ITU-T Recommendation G.709/Y.1331. ITU-T Interfaces of the optical transport network. Digital terminal equipment. – General. Series Y. Global information infrastructure, Internet protocol aspects, next generation network, Internet of things and smart cities. Internet protocol aspects – Transport, 2020.
2. Иткин А. Стандартизация QoS и понятие качества услуг // Семинар ФГУП ЦНИИС «Подходы по тестированию параметров функционирования сети в целях обеспечения качества услуг связи», 2019.
3. ITU-T Recommendation G.872. Architecture of the optical transport network. Digital networks–Optical transport networks, 2019.
4. Рекомендация МСЭ-Т E.800. Определение терминов, относящихся к качеству обслуживания. Качество услуг электросвязи: концепции, модели, цели и планирование надежности работы. Термины и определения, связанные с качеством услуг электросвязи, 2009.
5. Рекомендация МСЭ-Т J.241. Распределение качества обслуживания по классам и методы измерения для услуг цифрового видео, доставляемых по широкополосным сетям IP. Измерение качества обслуживания, 2005.

*Статья представлена научным руководителем, доцентом кафедры БТС СПбГУТ, кандидатом технических наук, доцентом Кравец Е. В.*

УДК 621.396

**Е. В. Кравец** (к.т.н., доцент, доцент кафедры БТС, СПбГУТ),  
[kravec.ev@sut.ru](mailto:kravec.ev@sut.ru)

**В. П. Подсветова** (студент группы РМ-22, СПбГУТ), [podsvetova.vp@sut.ru](mailto:podsvetova.vp@sut.ru)

## УПРАВЛЕНИЕ ГОРОДСКИМ ОСВЕЩЕНИЕМ

*В данной работе рассматриваются интеллектуальные системы управления городским освещением как неотъемлемый элемент «умного города», с учетом наиболее частых и основных задач, которые играют значительную роль и возникают в ходе планирования перед разработчиками, таких систем и функций, включая автоматизацию, мониторинг и энергоэффективность. Был проведен краткий обзор и рассмотрены основные особенности следующих технологий и протоколов связи: LoRa, NB-IoT, Wi-Fi, Bluetooth, «Стриж», LoRaWAN, Bluetooth Mesh, Matter, ZigBee и Thread. Отдельное внимание уделено сравнительному анализу, а также целесообразности интеграции и ее возможности использования при различных технологиях и протоколах связи для повышения соответствия ключевым параметрам, например, таких как энергоэффективность, масштабируемость и другим. Были обозначены выводы о значимости использования и применения комбинирования нескольких технологий в условиях цифровизации городской инфраструктуры.*

*умный город, городское освещение, LoRa, NB-IoT, Wi-Fi, Bluetooth, ZigBee, Matter, Thread, автоматизация, энергоэффективность, интеграция, мониторинг*

Современные города все активнее внедряют цифровые технологии для повышения комфорта, безопасности и энергоэффективности. Одной из важнейших инфраструктурных задач является организация и управление городским освещением. Переход от традиционных уличных светильников к интеллектуальным системам управления позволяет не только значительно снизить энергопотребление, но и создать основу для развития «умного города» через интеграцию с другими сервисами [1].

### Назначение и задачи интеллектуальных систем освещения [2]

Интеллектуальные системы освещения решают широкий круг задач:

- энергосбережение;
- мониторинг и диагностика позволяют уменьшить эксплуатационные расходы благодаря удаленному управлению и автоматическому оповещению о неисправностях;
- гибкое управление;
- интеграция с другими системами – взаимодействие с видеонаблюдением, мониторингом, системами безопасности;
- аналитика и отчетность.

## Технологии и протоколы связи

Для функционирования интеллектуального освещения используются различные технологии связи и протоколы.

Технология связи:

1. LoRa (Long Range) – это технология беспроводной связи, предназначенная для передачи данных на большие расстояния с низким энергопотреблением. Данная технология используется для построения сетей с большой дальностью связи и низким энергопотреблением. Является основой протокола LoRaWAN.

Преимущества: дальность до 15 км, энергоэффективность, независимость от операторов связи.

Недостатки: низкая скорость передачи (до 50 кбит/с), чувствительность к помехам в городской застройке.

Интеграция: через LoRaWAN с NB-IoT, Ethernet и облачными платформами.

Пример: сбор телеметрии со светильников в Астане.

2. NB-IoT – технология сотовой связи, обеспечивающая стабильную и надежную связь с низким энергопотреблением. За счет ее использования обеспечиваются: большая дальность и проникающая способность сигнала, использование существующей мобильной инфраструктуры.

Преимущества: стабильное соединение, хорошая проникающая способность, подходит для городской застройки.

Недостатки: требует операторской инфраструктуры, возможна задержка передачи, абонентская плата.

Интеграция: сочетается с LoRaWAN, Zigbee и Wi-Fi в гибридных системах.

Пример: В Москве реализован пилотный проект на базе NB-IoT, в рамках которого установлены "умные" фонари с контролем и управлением через сотовую сеть.

3. Wi-Fi – это технология беспроводной связи, позволяющий устройствам обмениваться данными, которая обеспечивает высокоскоростную передачу данных на короткие расстояния.

Преимущества: высокая пропускная способность, распространенный.

Недостатки: энергозатратность, малая дальность.

Интеграция: применяется как шлюз для протоколов Matter, Bluetooth Mesh.

Пример: шлюзы в Bluetooth Mesh-сетях для передачи данных в облако.

4. «Стриж» – российская LPWAN-технология с низким энергопотреблением и длительным сроком автономной работы. Данная технология была разработана для автономных IoT-устройств.

Преимущества: высокая помехозащищенность, малое энергопотребление.

Недостатки: ограниченная совместимость и распространение.

Пример: освещение в Тюмени и Санкт-Петербурге.

5. Bluetooth – технология беспроводной связи, предназначенная для обмена устройствами данными на малых расстояниях.

Преимущества: малое энергопотребление, массовость поддержки, высокая скорость (до 2 Мбит/с).

Недостатки: низкая дальность (до 30 м), малая помехоустойчивость.

Интеграция: на его основе работает Bluetooth Mesh, используется с Matter.

Пример: управляемое посредством телефона освещение помещений.

Протокол связи:

6. LoRaWAN – беспроводной протокол связи с технологией широкополосного распространения сигнала. Обеспечивает, дальностью до 15 км, связь, подходит для использования в крупных городах и пригородах.

Преимущества: высокая дальность, низкое энергопотребление, подходит для распределенных сетей.

Недостатки: низкая скорость передачи данных, чувствительность к плотной застройке.

Интеграция: легко объединяется с NB-IoT и Ethernet через шлюзы.

Пример: Система Smart Lighting в городе Нур-Султан (Казахстан), где применяется LoRaWAN для сбора телеметрии со светильников и передачи на облачную платформу.

7. Bluetooth Mesh – это протокол, основанный на технологии Bluetooth Low Energy, позволяющий организовать сетевое взаимодействие большого числа устройств на малых расстояниях (до 100 метров). Он особенно эффективен для освещения общественных пространств и зданий.

Преимущества: низкая стоимость, высокая скорость локального взаимодействия, простая установка.

Недостатки: малая дальность, чувствительность к помехам, требует плотной установки устройств.

Интеграция: сочетается с Wi-Fi и Matter.

Пример: связь между светильниками, активирующаяся в зависимости от движения пешеходов и велосипедистов в парках Амстердама.



8. Matter – стандарт IoT-устройств, поддерживает совместимость разных производителей. Обеспечивает высокую безопасность, прост в эксплуатации.

Преимущества: совместимость разных производителей, высокая безопасность.

Недостатки: пока ограничена в промышленной реализации, преимущественно используется в бытовых и офисных IoT-системах.

Интеграция: работает на базе Wi-Fi, Thread и Bluetooth.

Пример: Matter применяется в проектах по созданию умных кварталов в Южной Корее, где управление освещением интегрировано с домашней автоматикой и городской инфраструктурой.

9. ZigBee – это протокол беспроводной связи, предназначенный для построения сетей между устройствами умного дома, промышленной автоматизации и других IoT-приложений. Позволяет устройствам обмениваться данными и управлять друг другом, образуя сеть, где каждое устройство может выступать в качестве маршрутизатора.

Преимущества: низкое энергопотребление, устойчивая связь, mesh-архитектура.

Недостатки: ограниченная дальность (до 100 м), умеренная скорость.

Интеграция: может взаимодействовать с Matter через шлюзы.

Пример: системы освещения Philips Hue, освещение улиц в Барселоне [3].

10. Thread – протокол беспроводной связи, предназначенный для устройств умного дома, использует ячеистую топологию. Позволяет устройствам взаимодействовать друг с другом, интернетом напрямую, без использования узла сети (hub), хоть может и понадобится пограничный маршрутизатор (Thread Border Router) для связи с облаком/смартфоном.

ТАБЛИЦА 1. Сравнительный анализ технологий связи

| Технология | Энергопотребление | Дальность | Скорость передачи | Надежность | Масштабируемость | Стоимость |
|------------|-------------------|-----------|-------------------|------------|------------------|-----------|
| LoRa       | Низкое            | До 15 км  | До 50 кбит/с      | Средняя    | Высокая          | Низкая    |
| NB-IoT     | Низкое            | До 10 км  | До 250 кбит/с     | Высокая    | Высокая          | Средняя   |
| Wi-Fi      | Высокое           | До 100 м  | До 600 Мбит/с     | Средняя    | Средняя          | Средняя   |
| Стриж      | Низкое            | До 10 км  | До 100 кбит/с     | Высокая    | Средняя          | Средняя   |
| Bluetooth  | Низкое            | До 30 м   | До 2 Мбит/с       | Средняя    | Низкая           | Низкая    |

ТАБЛИЦА 2. Сравнительный анализ протоколов связи

| Протокол       | Энергопотребление | Дальность | Скорость передачи                | Надежность | Масштабируемость |
|----------------|-------------------|-----------|----------------------------------|------------|------------------|
| LoRaWAN        | Низкое            | До 15 км  | До 50 кбит/с                     | Средняя    | Высокая          |
| Bluetooth Mesh | Среднее           | До 100 м  | До 1 Мбит/с                      | Средняя    | Средняя          |
| Matter         | Среднее           | До 150 м  | До 1 Мбит/с<br>(и выше по Wi-Fi) | Средняя    | Средняя          |
| ZigBee         | Низкое            | До 100 м  | До 250 кбит/с                    | Средняя    | Средняя          |
| Thread         | Низкое            | До 100 м  | До 250 кбит/с                    | Высокая    | Средняя          |

### Интеграция протоколов и технологий

Единых технологии или протокола, закрывающих все требования нет, но можно использовать интеграции различных решений между собой. Гибридные решения позволяют использовать преимущества нескольких технологий и протоколов, решая большее количество задач. Примеры:

LoRaWAN + NB-IoT – передача телеметрии по LoRa, централизованное управление по NB-IoT. Обеспечивать связь с центральным сервером.

Bluetooth Mesh + Wi-Fi – локальное управление светильниками через Mesh, выход в интернет через Wi-Fi-шлюз. Подходит для плотной локальной сети внутри микрорайона.

Интеграция протоколов способствует лучшему масштабированию инфраструктуры: локальные сети подключают к облачным платформам, автоматически распределяя нагрузку. Внедрение многоуровневой архитектуры снижает риски отказов, увеличивает управляемость. Интеграционные шлюзы позволяют объединять Wi-Fi и другие сети, обеспечивая единую точку доступа и координации. Подобные решения находят применение в проектах «умных районов», где различные протоколы служат разным функциям в рамках одной системы. Мультипротокольность актуальна при масштабировании систем, адаптации под существующую инфраструктуру города.

### Выводы

Интеллектуальные системы управления городским освещением играют важную роль в формировании устойчивой и безопасной умной среды [4]. Они позволяют существенно экономить ресурсы и повышать качество

жизни граждан за счет гибкости, адаптивности и интеграции с другими системами. Выбор технологии зависит от задач проекта, плотности застройки, бюджета и возможностей инфраструктуры, а наилучшие результаты достигаются при комбинировании нескольких подходов.

#### Список используемых источников

1. Умное освещение городских улиц // ServiceEnergy.ru. URL: <https://www.serviceenergy.ru/solutions/umnое-osveshchenie/osveshchenie-gorodskikh-ulits/> (дата обращения 23.04.2025).
2. Водовозов А. М., Бурцев А. В. Интеллектуальная система уличного освещения на основе парадигмы Интернета вещей // Вестник Череповецкого государственного университета. 2021. № 3 (102). С. 7–17. DOI:10.23859/1994-0637-2021-3-102-1 (<https://doi.org/10.23859/1994-0637-2021-3-102-1>).
3. Перспективы IoT для систем умного освещения // Электроэнергия. URL: <https://smartlight.elec.ru/article/perspektivy-iot-dlya-sistem-umnogo-osvesheniya.html> (дата обращения 23.04.2025).
4. Умное освещение как основа «умного города» // LED-E.ru. URL: <https://led-e.ru/sys/osnova-umnogo-goroda/> (дата обращения 23.04.2025).

*Статья представлена научным руководителем, доцентом кафедры БТС СПбГУТ, кандидатом технических наук, доцентом Кравец Е. В.*

УДК 534.213

**А. А. Кропанина** (студент группы РЦТ-31, СПбГУТ),  
[kropanina.aa@sut.ru](mailto:kropanina.aa@sut.ru)

## ОСОБЕННОСТИ ПЕРЕДАЧИ ИНФОРМАЦИОННЫХ СООБЩЕНИЙ ЧЕРЕЗ КАНАЛ АКУСТИЧЕСКОГО ТРАНСФОРМАТОРА

*Целью работы является обзор особенностей передачи детерминированных и дискретных сигналов через канал акустического трансформатора. Показана возможность применения различных видов амплитудной модуляции для передачи информации. Приведена оценка возможной скорости передачи информации при использовании пятипозиционной амплитудной манипуляции. Так же показаны особенности использования дискретных сигналов в трактах акустического трансформатора. Представлены результаты лабораторной апробации передачи указанных выше сигналов.*

*акустический трансформатор, беспроводная передача информации, пьезокерамические излучатели, скорость передачи данных*

Существует проблема передачи информации с датчиков из изолированных помещений, которые имеют металлические стенки. Например, климат камеры и комнаты с химическим производством. Существует несколько способ организации такого канала связи [1]. Одно из решений данной проблемы – акустический трансформатор, состоящий из передатчика, двух пьезоэлектрических преобразователей, разделенных металлическим барьером и приемника [2, 3].

Прежде чем проверять передачу аналоговых и дискретных сигналов через акустический трансформатор, необходимо исследовать его амплитудно-частотную характеристику (АЧХ) амплитудную характеристику (АХ).

АЧХ пьезопреобразователя имеет ярко выраженный резонансный характер. Из этого можно сделать вывод, что через акустический трансформатор возможна передача только узкополосных сигналов.

Исследуем АХ данного акустического трансформатора на частотах 39 кГц, 40 кГц и 41 кГц, так как это частоты вблизи резонанса и антирезонанса используемых в испытаниях пьезопреобразователя.

На рис. 1 видно, что АХ имеет явный линейный характер. Из этого можно сделать вывод, что на выходе будет сигнал той же формы, что и на входе. Проверим передачу информации с использованием амплитудной мо-

дуляции (АМ). Для этого добавим к акустическому трансформатору генератор АМ сигнала и осциллограф, который контролирует выходной сигнал.

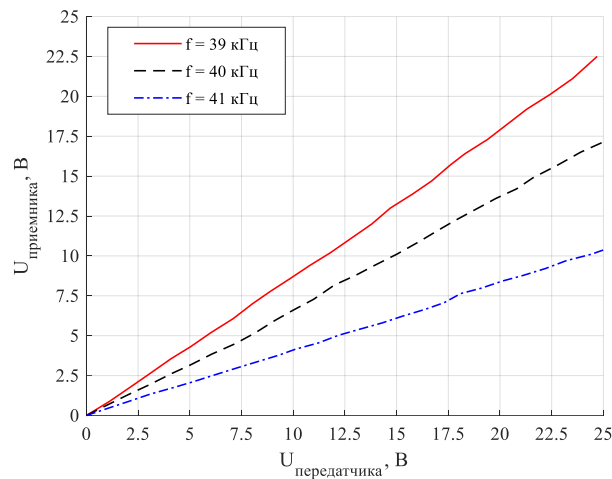


Рис. 1. Амплитудная характеристика акустического трансформатора на частотах 39 кГц, 40 кГц и 41 кГц

На рис. 2 изображены осциллограммы выходных сигналов с разными видами огибающих. На рис. 2 (б) наблюдается два значения амплитуды, соответственно их можно приравнять к логическим уровням. Соответственно через акустический трансформатор возможна передачи информации с использованием дискретных сигналов.

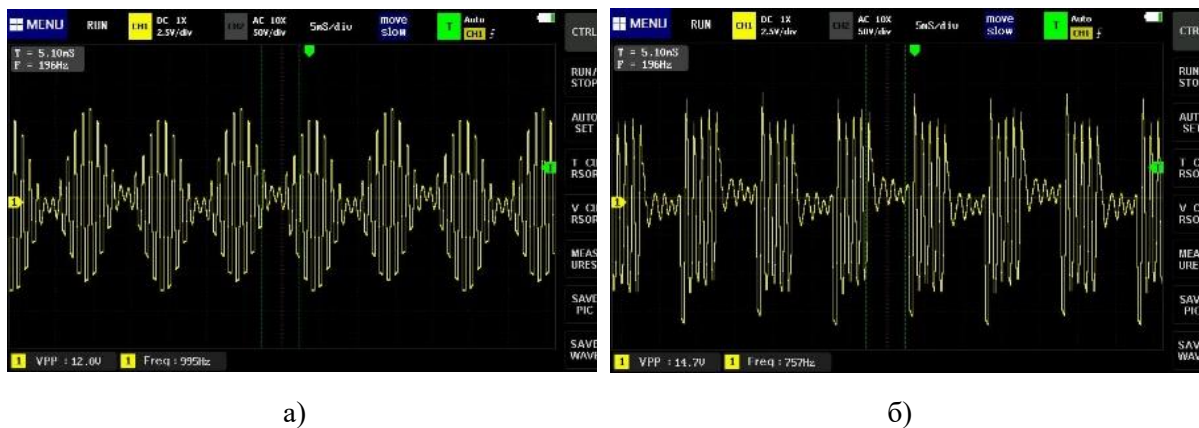


Рис. 2. Осциллограмма выходного сигнала а) с гармонической огибающей; б) с прямоугольной огибающей

Для проверки передачи дискретных сигналов подключим к одному пьезоэлементу ардуино и преобразователь UART-RS485, которые будут выступать имитацией современного датчика, подающего дискретный сигнал на акустический трансформатор. Ко второму пьезопреобразователю подключим с помощью преобразователя USB-RS485 персональный компьютер (ПК) на котором будем записывать принимаемые послышки. Стоит отметить, что в соответствии со стандартом EIA/TIA-485 передача данных осуществляется с использованием дифференциальных сигналов. В связи с этим для

организации канала связи обязательно нужен опорный уровень, относительного которого и происходит оценка уровня напряжения на каждой линии. В сети связи, построенной на основе RS-485 таким уровнем является общий провод или шина заземления.

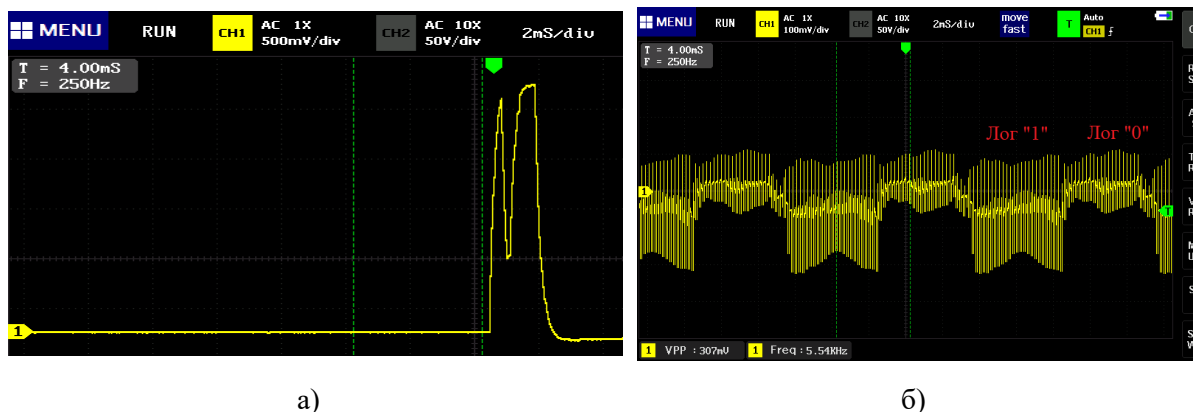


Рис. 3. Осциллограммы а) принятой посылки; в) принятые биты RS-485

На рис. 3(а) представлена принимаемая посылка, на которой видны явные логические «1» и «0». Если увеличить масштаб принимаемой посылки, то будет видна последовательность передаваемых битов (рис. 3(б)). Осциллограммы были сняты в разные моменты времени.

Для оценки передачи дискретных сообщений необходимо оценить вероятность возникновения ошибки в передаваемой ошибке и скорость передачи.

Чтобы оценить скорость передачи, по формуле (1) рассчитаем максимальную теоретическую скорость передачи для 1, 3 и 5 передаваемых битов, которая может быть обеспечена в данном канале при полосе пропускания 300 Гц.

$$C = \frac{1}{T_c} \log_2 M = \Delta F \log_2 M \quad (1)$$

где  $c$  – пропускная способность,  $T_c$  – период сигнала,  $M = 2^n$  ( $n$  – количество передаваемых битов),  $\Delta F$  – полоса пропускания.

ТАБЛИЦА 1. Пропускная способность

| М  | С, бит/с |
|----|----------|
| 2  | 300      |
| 8  | 900      |
| 32 | 1500     |

Вовремя испытаний передачи дискретного сигнала была выставлена скорость передачи 4800 бит/с, что больше теоретических расчетов (таблица 1).

При передаче дискретного сигнала на ПК в специализированной программе «Terminal» осуществлялась запись всех принимаемых посылок. После чего было посчитано: из 6592 переданных сообщений было принято 40 ошибочных сообщений, что составляет менее 1 % и удовлетворяет нашим задачам.

Таким образом, при передаче сигналов через акустический трансформатор существуют следующие особенности: передача только узкополосных сигналов для аналоговых сигналов и обязательное наличие общей земли для дискретных сигналов.

#### **Список используемых источников**

1. Качнов А. В. Формирование требований к системе беспроводной передачи данных и электроэнергии сейсмических донных станций комплекса «краб» / А. В. Качнов, А. А. Кропанина // 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. 159-163. EDN OBXNXM.

2. Воробьев О. В. Исследования применения пьезоэлектрических преобразователей для одновременной передачи данных и заряда аккумулятора донной станции / О. В. Воробьев, А. В. Качнов, Е. А. Пышкин // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024): Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах, СПб.: СПбГУТ, 2024. С. 117-121. EDN LTWDIJ.

3. Бабичева И. И. Оценка методов беспроводной передачи энергии и информации через металлический корпус / И. И. Бабичева, О. В. Воробьев, А. В. Качнов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024): Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах, СПб.: СПбГУТ, 2024. С. 40-45. EDN EEWVUU.

*Статья представлена научным руководителем,  
ведущим инженером кафедры БТС СПбГУТ Качновым А. В.*

УДК 004.032.6

А. А. Мочалов (студент группы Р-41м, СПбГУТ), [mochalov.aa@sut.ru](mailto:mochalov.aa@sut.ru)

## МЕТОДЫ ОБУЧЕНИЯ НЕЙРОСЕТИ DTLN В ЗАДАЧЕ ШУМОПОДАВЛЕНИЯ

*Исследование направлено на рассмотрение методов обучения нейронной сети DTLN. В ходе исследования в нейронную сеть загружаются чистые аудиосигналы, впоследствии аугментированные разными видами шумов. При обучении нейросеть тренируется анализировать аудиосигналы и выявлять в них нежелательные шумы. Результатом работы является модель, обученная на собственной библиотеке данных, и образцы аудиосигналов, очищенных от шумов.*

*нейросети, обучение, шумоподавление, аудиосигналы*

DTLN (Dual-Signal Transformation LSTM Network) – нейронная сеть для удаления шумов из аудиосигнала, использующая комбинацию рекуррентной нейронной сети для обработки последовательных данных и временных преобразований [1]. Готовые обученные нейросети не всегда могут обеспечить эффективное шумоподавление. Для повышения качества следует обучать модель самостоятельно на собственном наборе данных.

Этапы обучения нейронной сети DTLN представлены на рис. 1:

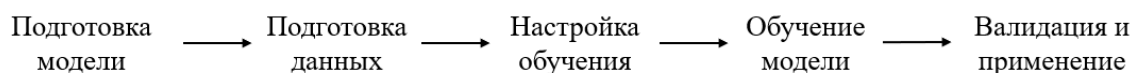


Рис. 1. Этапы обучения нейросети DTLN

Для подготовки модели следует установить необходимые зависимости: TensorFlow для обучения на наборе данных, Librosa для загрузки и преобразования аудиосигнала в спектрограмму и Wavinfo для валидации файлов.

При подготовке данных нужно знать, из чего состоит набор данных и требования к аудиофайлам набора. Датасет состоит из набора чистых записей речи и аудиофайлов, содержащих образцы шумов. От набора данных будет зависеть качество дальнейшего шумоподавления, поэтому важно чтобы в нем содержались реальные записи шумов, а не синтезированные. Также для повышения эффективности шумоподавления следует загружать образцы речи разных голосов. Требования к аудиофайлам: формат WAV (16



бит, моно) с частотой дискретизации 16 кГц [2]. В ходе исследования в качестве набора данных будет использоваться готовый набор данных на 40 часов. К нему будут добавлены новые образцы речи ведущих и обозревателей радиостанции в качестве эталона. Речь будет аугментирована записанными шумами городского транспорта, ветра и музыкой уличных музыкантов.

На этапе настройки обучения следует изучить параметры, с которыми предстоит работать. Epochs – количество эпох [3]. Параметр задает, сколько раз модель осуществит полный проход всего обучающего набора данных. На первых эпохах модель учится грубым закономерностям, на поздних – анализирует мелкие детали. При выставлении большого количества эпох можно столкнуться с эффектом переобучения, при котором модель запоминает шумы из датасета и эффективно работает только с ними, но при этом будет плохо работать с новыми данными. При слишком низком значении параметра Epochs модель не успевает выучить полезные признаки, вследствие чего эффективность шумоподавления также снизится. Оптимальными значениями параметра считаются значения от 50 до 100. В ходе исследования будет использовано значение 50. Batch size (размер пакета) – количество обрабатываемых файлов за один шаг перед обновлением весов [4]. При больших значениях размера пакета обучение будет проходить более стабильно, требуя при этом большее количество памяти графического адаптера. При низких значениях модель быстрее адаптируется, но возникает риск нестабильного обучения. Рекомендуемые значения параметра: 16-32. В ходе исследования будет использовано значение 16.

В процессе обучения модель на входе получает образец речи, аугментированный шумами, и пытается восстановить чистый сигнал. После восстановления модель сравнивает полученный результат с эталоном (аудиосигнал чистой речи) через функции потерь MSE и MAE. Среднеквадратичная ошибка MSE чувствительна к резким шумам, поэтому хороша для подавления заметных артефактов в аудиосигнале. Средняя абсолютная ошибка MAE дает более равномерное обучение и менее чувствительна к резким шумам. Она позволяет лучше сохранять детали звука, например, тихие гласные.

Затем алгоритм оптимизации Adam (Adaptive Moment Estimation) корректирует веса нейросети для минимизации ошибки. Алгоритм представляет собой гибрид двух методов: Momentum для учета инерции градиента и

RMSprop для адаптивной настройки шага обучения каждого параметра модели [5].

Последним этапом обучения модели DTLN перед применением является валидация, т.е. проверка обученной нейросети на отдельном наборе данных для выявления недочетов обучения. На данном этапе можно выяснить, следует ли обучать модель заново с выбором других наборов данных и параметров или достигнутый уровень обучения достаточен для применения модели в реальных задачах шумоподавления.

При работе с моделью DTLN изначально предоставлено два набора данных – DNS-challenge на 500 часов с шумной речью и несбалансированными данными и набор на 40 часов, содержащий в себе более чистые образцы речи и разнообразные шумы. С их помощью можно наглядно сравнить новую обученную модель с представленными и проанализировать результат. На рисунке 2 представлены спектрограммы исходного речевого сигнала, аугментированного шумом городского транспорта (Bus), спектрограммы сигнала обработанного моделями, обученными на наборе данных 40 и 500 часов (40h и 500h соответственно), а также спектрограмма сигнала обработанного моделью, обученной в ходе исследования (NEW).

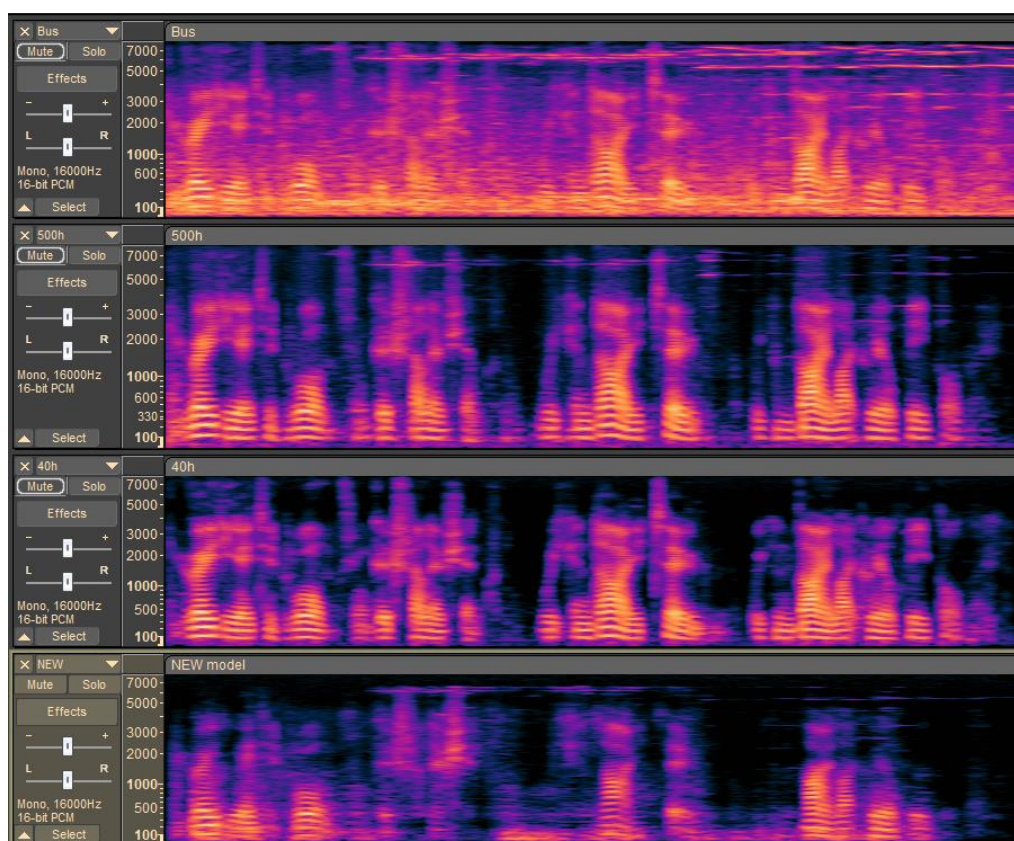


Рис. 2. Спектрограммы полученных аудиофайлов

Анализ результатов шумоподавления показал следующее. Модель, обученная на 500 часах данных, обеспечивает базовое подавление шума, однако оставляет артефакты и остаточный шум в области речевых частот. Обученная на 40 часах данных, содержащих в себе более чистые образцы речи и большее разнообразие шумов, позволяет значительно повысить качество шумоподавления и лучше сохранить речевые характеристики. Модель, обученная в ходе исследования, обладает промежуточным по качеству результатом между наборами на 40 и 500 часов. Присутствуют артефакты в области высоких частот, однако подавление шума выполнено на удовлетворительном уровне. В связи с чем можно сделать вывод о недостаточном обучении нейросети и рекомендуется расширить набор данных для достижения более эффективного шумоподавления после обучения.

#### **Список используемых источников**

1. Nils L. Westhausen, Bernd T. Meyer. Dual-Signal Transformation LSTM Network for Real-Time Noise Suppression // Interspeech. 2020
2. Nilesh Verma. Speech Enhancement Noise Suppression Using DTLN . URL: <https://github.com/TechyNilesh/Speech-Enhancement-Noise-Suppression-Using-DTLN?tab=readme-ov-file> (дата обращения 30.04.2025).
3. Epochs, Batch Size, Iterations – How are They Important to Training AI and Deep Learning Models. URL: <https://www.sabrepc.com/blog/Deep-Learning-and-AI/Epochs-Batch-Size-Iterations?srsltid=AfmBOooZ6ogcRfHiesTOIFevG8H0s-cKXLYWfri1lrKrOdgnyEhMNU90> (дата обращения 30.04.2025).
4. Jun Qi, Jun Du, Sabato Marco Siniscalchi, Xiaoli Ma, Chin-Hui Lee. On Mean Absolute Error for Deep Neural Network Based Vector-to-Vector Regression // IEEE Signal Processing Letters. 2020.
5. Diederik P. Kingma, Jimmy Lei Ba. Adam: A Method for Stochastic Optimization // International Conference for Learning Representations. 2015.

*Статья представлена научным руководителем, старшим преподавателем кафедры ЦТМ СПбГУТ Свинойной О. А.*

УДК 621.396

В. О. Орехова (студент группы РД-11, СПбГУТ), [orekhova.vo@sut.ru](mailto:orekhova.vo@sut.ru)

## ВЛИЯНИЕ ПАРАМЕТРОВ КОНФИГУРАЦИИ СЕТИ 5G NR НА СПЕКТРАЛЬНЫЕ ХАРАКТЕРИСТИКИ СИГНАЛОВ

*Сети мобильной связи пятого поколения продолжают активно развиваться, предлагая высокие скорости передачи данных, низкие задержки и широкие возможности конфигурации параметров сигнала. Одним из ключевых направлений является организация восходящей линии связи, обеспечивающей стабильный и эффективный обмен данными между пользовательскими устройствами и базовыми станциями. Использование современных методов модуляции, технологий синхронизации сигнала и оптимизации спектральных характеристик повышает надежность связи и адаптирует ее к различным условиям распространения. Гибкость конфигурации параметров дает возможность адаптировать систему как для сценариев с ограниченными ресурсами, так и для задач, требующих высокой скорости и надежности. Это открывает широкие перспективы для применения технологии в различных сферах – от систем умного города до промышленной автоматизации.*

*5G NR, PUSCH, DM-RS, PT-RS, SCS, BWP, спектрограмма*

В работе рассмотрен процесс создания сигналов в восходящей линии связи. На примере спектрограмм для нескольких технологий будет показано, как изменяются спектральные характеристики в зависимости от выбора конфигураций сигналов 5G NR. В сгенерированных сигналах используются:

- канал PUSCH (Physical Uplink Shared Channel) – физический канал передачи индивидуального пользовательского трафика и сопутствующей информации управления восходящим каналом (Uplink Control Information).
- опорный сигнал демодуляции (DM-RS), который используется для оценки характеристик канала и синхронизации приемника с передатчиком.
- опорный сигнал отслеживания фазы (PT-RS), используемый для оценки и минимизации влияния общей фазовой ошибки (CPE), которая возникает из-за фазового шума, нарушающего ортогональность поднесущих.

Для создания сигналов, в первую очередь, необходимо задать конфигурацию несущей восходящего сигнала. Она позволяет использовать параметры для несущей NR. К этим данным относятся дополнительные объекты конфигурации: идентификатор соты, пропускная способность канала, количество подкадров, частота дискретизации и несущая частота.

Далее нужно задать конфигурацию несущей разноса поднесущих радиочастот сигнала (*SCS*). С помощью заданного объекта конфигурации можно добавить дополнительные параметры для того, чтобы управлять расстоянием между поднесущими сигнала, а также количеством ресурсных блоков (*RBS*) в сетке ресурсов несущей и смещением начала сетки ресурсов относительно нулевого *RB*.

В таблице 1 показано, как количество ресурсных блоков (*NRB*) изменяется в зависимости от расстояния между поднесущими и полосы пропускания [1]. Исходя из представленной таблицы можно сделать вывод: чем шире полоса пропускания, тем большее количество ресурсных блоков можно использовать, поскольку большая полоса пропускания позволяет передавать больше данных одновременно.

Для определенных комбинаций *SCS* и полосы пропускания значения *NRB* не доступны (*N/A*). Например, *SCS* = 15 кГц не поддерживается для полосы пропускания 3 и 5 МГц. Это указывает на ограничения в конфигурациях системы.

ТАБЛИЦА 1. Конфигурация полосы пропускания *NRB* для FR1

| SCS<br>(кГц) | 3<br>МГц              | 5<br>МГц              | 10<br>МГц             | 15<br>МГц             | 20<br>МГц             | 25<br>МГц             | 30<br>МГц             | 35<br>МГц             | 40<br>МГц             |
|--------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
|              | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> | <i>N<sub>RB</sub></i> |
| 15           | 15                    | 25                    | 52                    | 79                    | 106                   | 133                   | 160                   | 188                   | 216                   |
| 30           | N/A                   | 11                    | 24                    | 38                    | 51                    | 65                    | 78                    | 92                    | 106                   |
| 60           | N/A                   | N/A                   | 11                    | 18                    | 24                    | 31                    | 38                    | 44                    | 51                    |

Также для генерации сигналов 5G создается структура конфигурации части полосы пропускания (*BWP*). Использование конфигурации нужно для того, чтобы управлять полосой пропускания, разделяя ее на несколько частей или сегментов. Установить параметры *BWP* необходимо в определенной несущей с интервалом поднесущей (*SCS*).

Следующий шаг для генерации сигнала NR восходящей линии связи – задание конфигурации и инициализация параметров PUSCH, а также определение необходимых свойств, связанных с ним физических опорных сигналов демодуляции (*DM-RS*) и отслеживания фазы (*PT-RS*). Конфигурация

физического канала передачи пользовательских данных задается с использованием массива ячеек. Каждый элемент массива определяет последовательность фрагментов передачи PUSCH.

Для демодуляции PUSCH UE используются опорные сигналы демодуляции (DM-RS). Они необходимы для оценки состояния радиоканала и для синхронизации приемника с передатчиком. Следует отметить, что позиции DM-RS варьируются в зависимости от выбранного частотного диапазона. В частотном диапазоне 1 (FR1, 410 МГц-7.125 ГГц) используются две позиции DM-RS на слот, что обеспечивает более надежную оценку канала в условиях потенциально более высокой дисперсии и интерференции. В частотном диапазоне 2 (FR2, 24.25 ГГц-52.6 ГГц) используется одна позиция DM-RS на слот, что позволяет увеличить спектральную эффективность, учитывая, что на более высоких частотах канал может изменяться более быстро, и избыточное количество опорных сигналов не приводит к существенному улучшению качества демодуляции [2].

Затем настраивается генерация символов опорного сигнала отслеживания фазы (PT-RS), используемого для оценки и минимизации влияния общей фазовой ошибки (CPE).

Спектрограмма на рисунке 1 показывает, что сигнал NB-IoT занимает ограниченную полосу частот и передается периодически. Интенсивность цвета указывает на мощность сигнала в данной точке частотно-временной области. Пропуски между всплесками показывают, что передача данных происходит не непрерывно, а с заданным периодом.

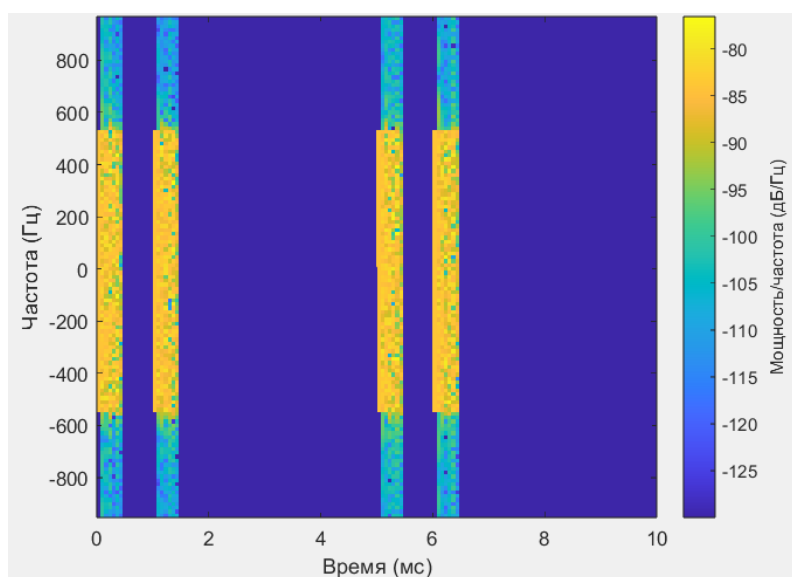


Рис. 1. Спектрограмма сигнала 5G NR для NB-IoT



Спектрограмма сигнала 5G NR V2X, представленная на рисунке 2, демонстрирует передачу сигнала в диапазоне 20-30 МГц. Интенсивность цвета визуализирует спектральную плотность мощности сигнала (дБ/Гц) в частотно-временной области, где желтый цвет соответствует максимальной мощности сигнала. Вертикальные полосы, отражающие кратковременные всплески высокой мощности, перемежаются периодами отсутствия активности, что свидетельствует о не непрерывной передаче данных, характерной для сценариев V2X, подразумевающих периодический обмен информацией.

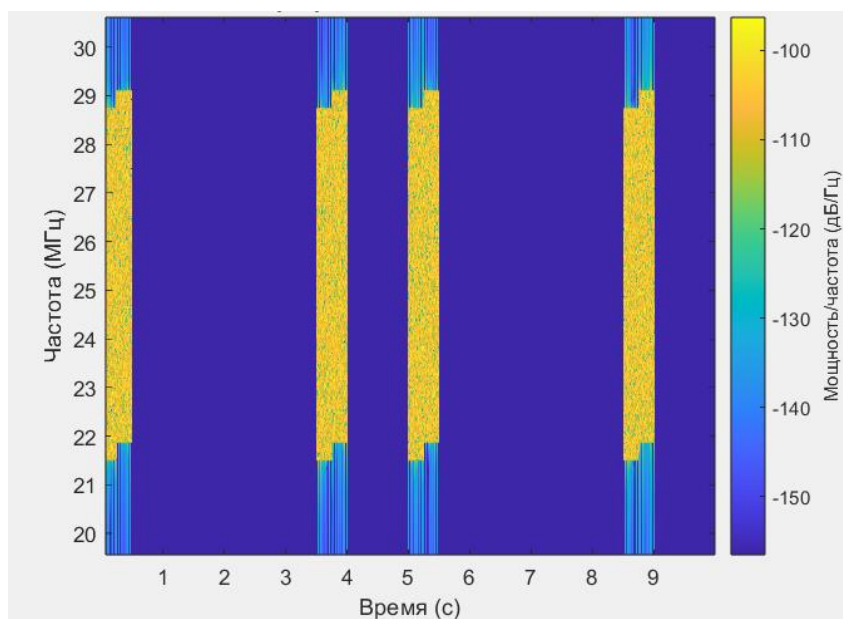


Рис.2. Спектрограмма сигнала 5G NR для V2X

Спектрограммы на представленных рисунках наглядно демонстрируют ключевые различия между NB-IoT и V2X. NB-IoT характеризуется узкополосной передачей данных, что отражается в ограниченном количестве выделенных поднесущих и OFDM символов для PUSCH [3]. Плотное распределение DM-RS обеспечивает надежную оценку канала в условиях ограниченной полосы и мощности. Отсутствие PT-RS указывает на то, что компенсация фазового шума не является критичным требованием для данного стандарта.

V2X, напротив, демонстрирует использование более широкой полосы частот, что позволяет достичь более высокой скорости передачи данных. Распределение ресурсов PUSCH охватывает большее количество поднесущих. Наличие PT-RS, распределенных по всей сетке ресурсов, подчеркивает важность компенсации фазового шума для обеспечения надежной связи в условиях быстро меняющихся каналов и высоких частот, характерных для V2X-приложений.

В таблице 2 показаны основные различия в параметрах, а именно, в ширине полосы пропускания канала, частоте дискретизации, масштабах сетки и BWP, а также в общей структуре спектра.

ТАБЛИЦА 2. Различия параметров NB-IoT и V2X

| Параметр                     | NB-IoT    | V2X         |
|------------------------------|-----------|-------------|
| Полоса пропускания канала    | 5 МГц     | 20 МГц      |
| Частота дискретизации        | 1,92 МГц  | 30,72 МГц   |
| Расстояние между поднесущими | 15 кГц    | 30 кГц      |
| Размер сетки                 | 6         | 51          |
| Размер BWP                   | 6         | 51          |
| Модуляция                    | 'QPSK'    | '64QAM'     |
| Частотный скачок             | 'neither' | 'intraSlot' |

В ходе работы был изучен процесс создания основных конфигураций для сигналов 5G NR в восходящей линии связи. Анализ распределения ресурсов и структуры опорных сигналов наглядно демонстрирует различия в подходах к организации связи в NB-IoT и V2X, обусловленные разными требованиями к пропускной способности, надежности и устойчивости к фазовому шуму, диктуемыми их сценариями использования.

#### Список используемых источников

1. 3GPP TS 38.104. NR; Base Station (BS) radio transmission and reception. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network.
2. 3GPP TS 38.211. NR; Physical channels and modulation. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network.
3. 3GPP TS 38.214. NR; Resource allocation; 3rd Generation Partnership Project; Physical layer procedures for data.

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



УДК 004.932

Д. А. Татаренков (ст. преподаватель кафедры ЦТМ, СПбГУТ)

Е. А. Трапезникова (магистрант группы Р-41м, СПбГУТ), [katu.ush@sut.ru](mailto:katu.ush@sut.ru)

## ПРИМЕНЕНИЕ ГЕНЕРАТИВНЫХ НЕЙРОСЕТЕЙ ДЛЯ ФОРМИРОВАНИЯ ВИРТУАЛЬНЫХ РАКУРСОВ

*В статье рассматривается применение генеративных нейросетей для построения виртуальных ракурсов на основе набора двумерных изображений, что особенно актуально в свете развития систем виртуальной и дополненной реальности. Виртуальные ракурсы позволяют формировать альтернативные точки обзора сцены без физического перемещения камеры за счет синтеза недостающих фрагментов изображения. В статье приведен обзор архитектуры модели Stable Virtual Camera, способной реконструировать 3D-пространство, и рассмотрены возможности ее практического применения в интерфейсных решениях.*

*генеративные нейросети, визуализация, виртуальный ракурс, 3D-реконструкция*

В последние годы наблюдается стремительное развитие технологий виртуальной и дополненной реальности, что требует все более точных и реалистичных методов визуализации трехмерных сцен. Одним из ключевых направлений в этой области является построение виртуальных ракурсов – альтернативных точек обзора сцены, создаваемых без физического перемещения камеры.

Создание виртуальных ракурсов на основе ограниченного количества двумерных изображений требует высокой степени обобщения и способности модели «дорисовывать» недостающие элементы сцены. Этой задаче в полной мере соответствует применение генеративных нейросетей, способных не только интерпретировать пространственные отношения между изображениями, но и реконструировать недостающие фрагменты, опираясь на вероятностные представления [1].

Одним из современных решений является модель Stable Virtual Camera – генеративная архитектура для синтеза новых ракурсов сцены на основе набора входных изображений [2, 3]. Модель опирается на диффузионные методы генерации и включает в себя несколько ключевых компонент: энкодер, модуль пространственного сопоставления, латентную диффузионную модель и декодер. В ходе работы был разработан пользовательский интерфейс (рис. 1), позволяющий задавать ряд параметров: тип движения виртуальной камеры (preset trajectory), стратегию обработки кадров (chunk

strategy), значение контроля генерации (CFG value), начальное значение генератора случайных чисел (random seed), масштаб камеры (camera scale).

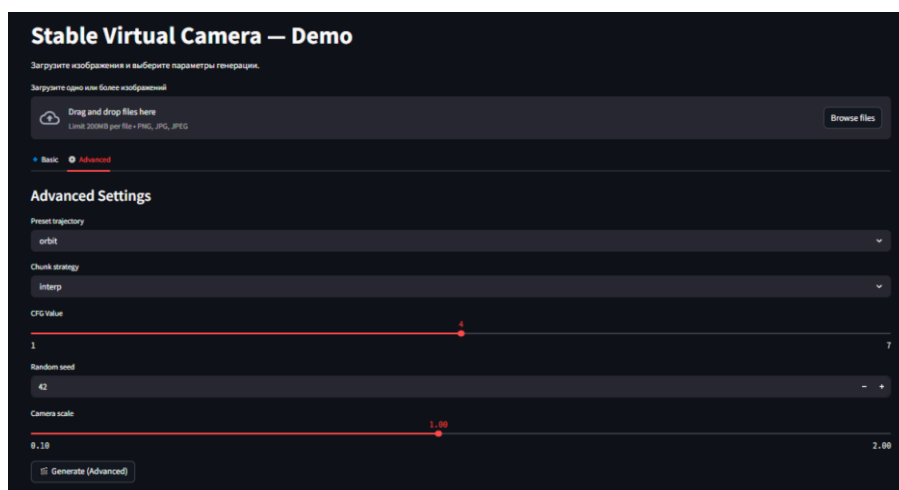


Рис. 1. Пользовательский интерфейс для формирования виртуальных ракурсов

На вход модель получает от 1 до 32 изображений, снятых с различных точек обзора. Каждый кадр проходит через энкодер, преобразующий его в латентное представление – сжатую форму данных, сохраняющую ключевые признаки сцены. На рис. 2 слева показан общий вид сцены с исходными изображениями, справа – соответствующее латентное представление, сформированное моделью на основе входных данных.



Рис. 2. Визуализация реконструкции сцены на основе входных изображений

После преобразования входных изображений в латентные представления, модель выполняет их пространственное выравнивание при помощи механизма сопоставления, который учитывает положение каждой камеры относительно сцены. Сопоставление позволяет определить взаимосвязи между кадрами, скорректировать геометрические искажения и синхронизировать элементы сцены. Полученные данные объединяются в единое многомерное представление, которое моделирует структуру сцены в латентном пространстве, что обеспечивает полноту пространственной информации,

включая глубинные уровни, перспективные смещения и детали, не присутствующие во всех кадрах. Это позволяет диффузионной модели на следующих этапах использовать полноценный контекст и восстанавливать отсутствующие области с высокой достоверностью.

Диффузионная генеративная модель обучается синтезировать изображения в латентном пространстве посредством поэтапного устранения шума из случайного начального состояния. На каждом шаге итерации она уточняет детали, опираясь на распределение вероятностей, извлеченное из обучающих данных. Такой подход обеспечивает высокое качество генерации, поскольку процесс построения изображения идет от грубой структуры к более детализированной, приближая результат к реалистичному ракурсу сцены [4, 5].

В результате работы модели создается последовательность новых изображений, имитирующих движение камеры в виртуальной сцене. На рис. 3 слева представлена исходная сцена, где серым цветом окрашены пустые области, которые впоследствии будут заполнены сгенерированными ракурсами, а также траектория движения камеры, где красным цветом выделены исходные ракурсы, а черным те, которые в ходе генерации должна сформировать модель. Справа представлено одно из изображений, полученное на выходе модели.

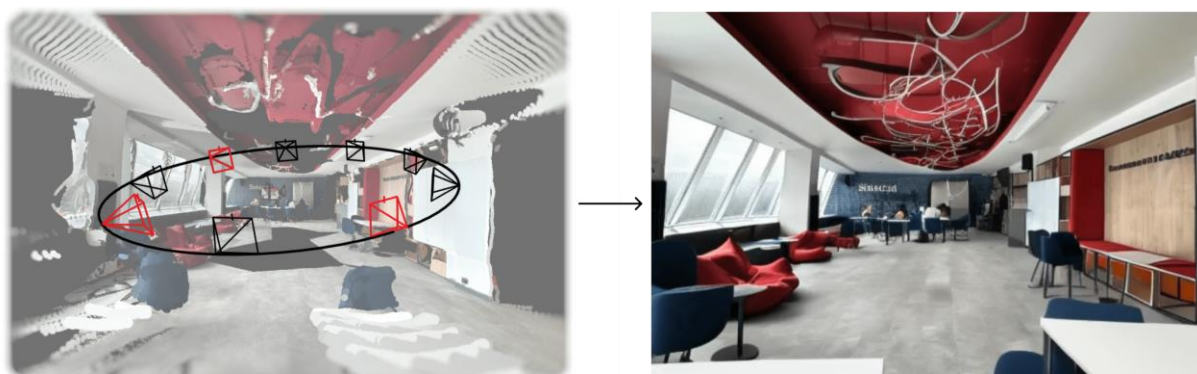


Рис. 3. Визуализация процесса формирования виртуальных ракурсов: компоновка входных данных (слева) и пример результата (справа)

Таким образом, модель способна плавно интерполировать движение между заданными ракурсами, формируя иллюзию непрерывного перемещения камеры.

Модель находит применение в постпродакшне, создании телевизионной графики, реставрации архивных записей, а также подходит для удаленного предварительного осмотра локаций для съемок. Несмотря на высокую

точность генерации, технология пока ограничена рядом факторов: значительными требованиями к видеопамяти, максимальным числом входных изображений (32) и отсутствием поддержки рендера в режиме реального времени, что оставляет пространство для дальнейшего совершенствования. Тем не менее, применение диффузионных генеративных моделей позволяет решать задачу реконструкции виртуальных ракурсов с высокой степенью достоверности [6], что подтверждает потенциал подобных архитектур в области трехмерной визуализации и поддерживает целесообразность их дальнейшего внедрения в мультимедийные и интерфейсные решения.

#### Список используемых источников

1. Применение генеративных адверсариальных сетей (GANs) для синтеза данных. URL: <https://habr.com/ru/companies/otus/articles/754978/> (дата обращения 29.05.2025).
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 29.05.2025).
4. Kim S. W. et al. Neuralfield-ldm: Scene generation with hierarchical latent diffusion models // Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. – 2023. – С. 8496-8506.
5. Nam, G., Khlifi, M., Rodriguez, A., Tono, A., Zhou, L., & Guerrero, P. 3d-ldm: Neural implicit 3d shape generation with latent diffusion models // arXiv preprint arXiv:2212.00842. 2022.
6. Stable Virtual Camera: Generative View Synthesis with Diffusion Models. URL: <https://stable-virtual-camera.github.io/> (дата обращения 29.05.2025).

*Статья представлена научным руководителем,  
старшим преподавателем кафедры ЦТМ СПбГУТ Татаренковым Д. А.*

УДК 004.921

Д. А. Татаренков (ст. преподаватель кафедры ЦТМ СПбГУТ)

П. В. Фомин (магистрант группы Р-41м, СПбГУТ), [fomin.pv@sut.ru](mailto:fomin.pv@sut.ru)

## РОЛЬ РОТОСКОПИИ В ОБЕСПЕЧЕНИИ РЕАЛИСТИЧНОСТИ КОМБИНИРОВАННЫХ СЪЕМОК С 3D-ОБЪЕКТАМИ

*Развитие технологий визуальных эффектов повысило требования к реалистичности комбинированных съемок, где живая съемка сочетается с трехмерной графикой. Ротоскопия представляет собой ключевой процесс для создания точных масок и контуров при комбинировании живого видео с компьютерной графикой. Этот процесс играет важную роль в обеспечении органичного взаимодействия 3D-объектов с реальной съемкой. Использование современных инструментов ротоскопии значительно повышает качество композитинга и визуальную достоверность сцены. В статье описан алгоритм применения ротоскопии для композиции сцен с участием трехмерных объектов, обеспечивающий точное совмещение элементов живой съемки и компьютерной графики.*

ротоскопия, комбинированные съемки, визуальные эффекты, 3D-графика, композитинг.

### Этапы выполнения ротоскопии

Ротоскопия – это высокоточная методика сегментации движущихся объектов в видеопоследовательностях, опирающаяся на контурные или трековые методы с учетом временной согласованности [1]. Ротоскопия важный инструмент для прецизионной сегментации изображений, особенно в тех случаях, когда автоматические алгоритмы, включая хромакей или оптический трекинг, оказываются недостаточно точными. Применение ротоскопии становится особенно актуальным в условиях сложного освещения, наличия пересечений объектов или прозрачных/полупрозрачных материалов, когда компьютерные методы дают сбой, и необходимо ручное управление [2].

Процесс ротоскопии включает несколько логически взаимосвязанных этапов:

1. Импорт и подготовка исходного материала. Художник загружает видеоряд в специализированное программное обеспечение (Nuke, After Effects, Silhouette и др.) и проверяет его на наличие артефактов, резких движений или изменений освещения, которые могут повлиять на точность маски.

2. Создание маски. На выбранных кадрах создаются маски, описывающие границы нужного объекта (например, актера или части тела). Эти контуры определяют форму объекта и служат основой для интерполяции. В

промежуточных кадрах контуры трансформируются согласно движению объекта. Это может осуществляться вручную или с помощью трекинга – автоматического отслеживания движения по характерным точкам (feature tracking, planar tracking) [3]. На этой стадии часто используется планарный трекинг, что позволяет «привязать» маску к движущейся поверхности (например, лицо или автомобильная дверь). Из-за изменений перспективы, теней, освещения и неидеальности трекинга контуры часто приходится ретрактить вручную. Особое внимание уделяется анимации кривых Безье, так как именно от их точности зависит органичность последующего наложения 3D-графики [4]. В сценах с большим количеством кадров может применяться техника сплит-масок, при которой объект разбивается на функциональные зоны – голову, торс, конечности – для удобства отслеживания. Качественная ротоскопия не только определяет края объекта, но и передает тонкие нюансы – волосы, тени, отражения – что критически важно при внедрении 3D-моделей. Например, в случае наложения CGI-объекта (автомобиля, фантастического существа) на улицу, где присутствуют актеры, ротоскопия позволяет добиться перекрытия – один из главных признаков реалистичного взаимодействия.

3. Сглаживание и очистка. Для устранения «дерганья» (jitter) маски между кадрами проводится сглаживание ключевых точек и их движения, чтобы сохранить визуальную непрерывность.

4. Экспорт масок. Маски сохраняются в формате черно-белых изображений, которые затем используются на этапе композитинга – объединения живого и синтетического материала.

Интеграция трехмерных элементов в комбинированную съемку требует высокой точности не только в позиционировании объектов, но и в их взаимодействии со средой – тенях, отражениях, эффекте глубины резкости. Маски, полученные методом ротоскопии, становятся основой для создания occlusion-проекций – корректного визуального перекрытия объектов. Благодаря им CGI-объект логично исчезает за спиной актера или наоборот перекрывает его. Помимо этого, ротоскопия активно используется в задачах светокоррекции: зоны, замаскированные вручную, могут обрабатываться с точки зрения экспозиции, контраста, цветокоррекции для достижения равномерности между живой и синтетической съемкой. Современные подходы предполагают использование нейросетевых методов ускоренного обвода (например, с применением инструментов, основанных на convolutional

neural networks), но они пока не способны заменить точность профессиональной ручной ротоскопии в коммерческих проектах [5].

### Методы оценки качества ротоскопии

Оценка качества ротоскопической маски сводится к сравнению предсказанной маски с эталонной (ручной) маской. В компьютерном зрении стандартными мерами служат метрика перекрытия (IoU) и коэффициент Дайса [6]. Эти метрики основаны на количествах истинных и ложных срабатываний по пикселям.

Intersection over Union (IoU) – отношение площади пересечения двух масок к площади их объединения:

$$IoU = \frac{|Mask_{pred} \cap Mask_{true}|}{|Mask_{pred} \cup Mask_{true}|} \quad (1)$$

В терминах TP/FP/FN формула записывается как:

$$IoU = \frac{TP}{TP+FP+FN} \quad (2)$$

где: True Positive (TP) – количество истинно положительных пикселей, False Positive (FP) – количество ложно положительных пикселей, False Negative (FN) – количество ложно отрицательных пикселей. Метрика IoU принимает значение от 0 до 1: значение 1 соответствует полному совпадению масок, 0 – полному расхождению.

Коэффициент Дайса (Dice, F1-score) – гармоническое среднее точности и полноты либо удвоенная площадь пересечения, деленная на сумму площадей масок:

$$Dice = \frac{2|Mask_{pred} \cap Mask_{true}|}{|Mask_{pred}| + |Mask_{true}|} \quad (3)$$

Эквивалентная запись через TP/FP/FN:

$$IoU = \frac{2*TP}{2*TP+FP+FN} \quad (4)$$

Коэффициент Дайса также лежит в  $[0,1]$ , причем  $Dice = 1$  при идеальном совпадении масок. По сути, метрики IoU и Dice тесно связаны, поэтому обычно достаточно вычислять лишь одну из них.

Пиксельная точность – доля правильно классифицированных пикселей (как положительных, так и отрицательных) относительно общего числа пикселей:

$$Pixel\ Accuracy = \frac{TP+TN}{N} \quad (5)$$

где: N – общее количество пикселей в изображении.

Расстояние Хаусдорфа – максимальное расстояние от точки контура одной маски до ближайшей точки контура другой. Эта метрика (мера максимальной погрешности по контуру) полезна для оценки точности краев сегмента.

Методы оценки обычно применяются ко всем кадрам в наборе: вычисляется среднее значение (Mean IoU) или усредненная Dice по всем объектам и кадрам. При этом часто исключают фоновые классы и размытие краев, фокусируясь на видимых контурах объекта. Хорошая ротоскопическая маска должна одновременно давать высокие значения IoU/Dice и минимизировать погрешность границ, что обеспечивает органичное наложение CG-объектов.

## Программное обеспечение

Эффективность ротоскопии во многом определяется качеством и функциональностью программного обеспечения, применяемого в производственном процессе. Современные инструменты не только позволяют ускорить выполнение рутинных задач, но и обеспечивают высокий уровень точности, что особенно важно при интеграции 3D-объектов в живую съемку. Наиболее распространенным решением в индустрии визуальных эффектов является The Foundry Nuke – профессиональный композитинговый пакет, обладающий развитой системой нод, поддержкой глубины резкости, 3D-камер и стереоскопии. Он используется в крупных голливудских студиях за счет гибкости и модульности, позволяющих выстраивать сложные пайплайны ротоскопии, композитинга и трекинга в едином пространстве.

Adobe After Effects занимает лидирующее положение в сегменте телевидения, онлайн-контента и рекламы. Хотя его возможности в области сложной ротоскопии несколько уступают Nuke, благодаря инструменту Rotobrush и интуитивно понятному интерфейсу программа позволяет эффективно решать задачи средней сложности. Она особенно удобна для художников, не работающих в глубоко технической среде, и ценится за широкую интеграцию с другими продуктами Adobe.



Silhouette FX считается специализированным программным обеспечением для высокоточной ручной и автоматизированной ротоскопии. Программа поддерживает работу с изображениями большого разрешения, стерео-проектами и множеством форматов масок, а также обладает развитой системой инструментов для сглаживания, деформации и анимации масок. Она особенно востребована в проектах, где требуется прецизионная детализация и глубинная работа с объектами на длительных временных отрезках.

Mocha Pro отличается от остальных своим уникальным подходом к трекингу – здесь используется планарная система отслеживания, которая позволяет «прикрепить» маску к движущейся поверхности, даже если она частично выходит за пределы кадра или подвергается деформациям. Mocha активно применяется как в крупных студиях, так и в среде фрилансеров благодаря своей точности, высокой скорости работы и возможности интеграции в другие приложения через плагины.

Помимо традиционных решений, в последние годы получают распространение гибридные программы с элементами искусственного интеллекта, такие как Runway ML и EbSynth. Они используют нейросетевые подходы для автоматического обвода объектов, что значительно сокращает время на начальный этап создания масок. Однако при всех преимуществах нейросетевой ротоскопии на текущем этапе ее результат требует обязательной ручной коррекции, особенно при работе со сложными текстурами, движением камеры и взаимодействием объектов. Такие инструменты становятся удобным вспомогательным решением, но пока еще не заменяют точность, достигаемую при традиционном подходе.

Таким образом, выбор программного обеспечения напрямую зависит от задач проекта, требуемого уровня детализации, масштаба производства и квалификации художника. В профессиональных студиях чаще всего используется комбинация нескольких решений, что позволяет сочетать преимущества ручной и автоматизированной ротоскопии для достижения наилучшего результата.

## **Заключение**

Ротоскопия продолжает оставаться важнейшим инструментом в арсенале специалистов по визуальным эффектам, несмотря на развитие автоматических технологий. Прогресс в области искусственного интеллекта, машинного зрения и облачных вычислений открывает путь к частичной автоматизации этого процесса, но сохранение высокого качества требует

участия квалифицированных художников. В будущем ожидается интеграция ротоскопии с нейросетевыми трекерами, гибридными 2D/3D системами и адаптивными масками, что значительно сократит время производства без ущерба для визуального результата. Это делает технологию ротоскопии перспективным направлением не только для киноиндустрии, но и для сферы виртуальной и дополненной реальности, где реалистичное взаимодействие цифровых и реальных элементов имеет критическое значение.

#### **Список используемых источников**

1. Радке Р. Компьютерное зрение для визуальных эффектов / Пер. с англ. М.: ДМК Пресс, 2013. 360 с.
2. Смит Р. Основы визуальных эффектов. Практическое руководство. СПб.: Питер, 2020. 512 с.
3. Гусев А. В. Методы и средства трекинга в системах компьютерного зрения: учеб. пособие. М.: МГТУ им. Баумана, 2021. 88 с.
4. Алексеев И. М., Захаров А. И. Методы анализа границ объектов на изображениях // Вестник Томского государственного университета. Математика и механика. 2022. № 76. С. 101–112.
5. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge: MIT Press, 2016. 775 p.
6. He K., Gkioxari G., Dollár P., Girshick R. Mask R-CNN // IEEE International Conference on Computer Vision (ICCV), 2017. PP. 2961–2969.

УДК 654.195

С. А. Терентьева (магистрант группы Р-41м, СПбГУТ), [terenteva.sa@sut.ru](mailto:terenteva.sa@sut.ru)

## РАЗРАБОТКА ПСИХОАКУСТИЧЕСКОЙ МОДЕЛИ PERCEPTUAL EVALUATION OF AUDIO QUALITY

*В данной статье рассматривается процесс разработки психоакустической модели, используемой в Perceptual Evaluation of Audio Quality (PEAQ), на основе быстрого преобразования Фурье. Разработаны и проанализированы основные этапы работы психоакустической модели. На основании проведенного анализа реализована психоакустическая модель в программном обеспечении MatLab, включающая модель периферийной части уха и предварительную обработку образцов возбуждения.*

*психоакустическая модель, Perceptual Evaluation of Audio Quality, преобразование Фурье, MatLab, образцы возбуждения*

Психоакустическая модель, применяемая в методе PEAQ, имеет две независимые реализации. Первая из них основана на использовании кратковременного спектрального анализа с применением быстрого преобразования Фурье (БПФ-модель), а вторая – на спектральном анализе с использованием банка фильтров (БФ-модель) [1].

Ключевое различие между этими моделями заключается в способе реализации кратковременного спектрального анализа: в БПФ-модели применяется быстрое преобразование Фурье, тогда как в БФ-модели используются фильтрационные методы. Кроме того, в отличие от БПФ-модели, БФ-модель включает этап учета эффекта предмаскировки. Использование различных математических подходов обуславливает отличия моделей по частотному и временному разрешению.

В рамках данной работы была выбрана реализация психоакустической модели на основе быстрого преобразования Фурье, представленная на рисунке 1.

Входными данными для психоакустической модели являются эталонный и тестируемый аудиосигналы, которые предварительно синхронизируются по времени и приводятся к одинаковой частоте дискретизации, составляющей 48 кГц. После этого оба сигнала разбиваются на последовательные блоки (фреймы) длиной приблизительно 2048 отсчетов, с перекрытием между соседними фреймами на 50 %.



Рис. 1. Психоакустическая модель на основе БПФ

Для каждого фрейма применяется окно Ханна, позволяющее сгладить переходы на границах блока и уменьшить спектральные искажения, после чего осуществляется вычисление дискретного спектра с использованием быстрого преобразования Фурье (БПФ). Полученные спектральные данные масштабируются в соответствии с заданным уровнем воспроизведения, что позволяет учесть влияние громкости сигнала на восприятие [2].

На следующем этапе производится моделирование прохождения звукового сигнала через наружное и среднее ухо человека [3]. Этот процесс реализуется с помощью спектрального взвешивания, учитывающего передаточные характеристики соответствующих участков слуховой системы, что позволяет приблизить модель к реальному физиологическому восприятию.

Далее осуществляется расчет энергетических характеристик сигнала в отдельных частотных полосах, параметры которых (ширина и интервал) выбраны с учетом частотного разрешения слуха и составляют 0,25 Барк.

Для моделирования внутреннего шума слуховой системы к рассчитанным значениям энергии добавляется частотно-зависимое смещение, которое отражает спектральное распределение собственной шумовой активности слуха и позволяет учесть ее влияние на восприятие слабых сигналов. Эффект частотной маскировки реализуется путем так называемого «развертывания» энергии в частотной области [3]. Этот процесс представляет собой свертку спектра с функцией развертывания, которая аппроксимирует маскирующий порог слышимости. Развертывание выполняется отдельно для каждой частотной полосы, после чего полученные значения объединяются с применением степенного закона суммирования с показателем степени 0,4. На этом этапе формируются начальные образцы возбуждения.

Далее следует этап временной адаптации возбуждения, необходимый для учета эффекта постмаскировки, при котором слышимость сигнала зависит от его временного контекста. Этот эффект моделируется с использованием биэкспоненциального импульсного отклика, реализованного через бесконечный импульсный отклик (БИХ) фильтр нижних частот, что обеспечивает размазывание возбуждения во времени. Результатом данной процедуры являются финальные образцы возбуждения, которые используются на последующих этапах перцепционной оценки качества аудиосигнала [4].

Программная модель была реализована с помощью ПО MatLab. На рисунке 2 представлен график амплитудного спектра сигнала для тестового музыкального сигнала фортепиано. График показывает преобладание низкочастотных компонентов – типично для музыкального сигнала (фортепиано). Снижение амплитуды на высоких частотах – результат как особенностей сигнала, так и фильтрации Ханна.

В разработанной модели были учтены те особенности слухового аппарата (частотная и временная избирательность, инерционность, передаточная характеристика и т.п.), которые наиболее существенно влияют на восприятие человеком аудиосигналов.

После завершения всех вычислений в программном обеспечении необходимо выполнить предварительную обработку полученных образцов возбуждения.

В первую очередь определяются значения удельной громкости и ее абсолютные изменения. Для приближенной оценки удельной громкости

используется формула, предполагающая возведение значений возбуждения в степень 0,3 [1].

Расчет порога маскировки осуществляется путем применения весовой функции к образцам возбуждения. Эта функция представляет собой аппроксимацию коэффициента маскировки и отражает способность слуховой системы подавлять менее интенсивные сигналы в присутствии более сильных [3].

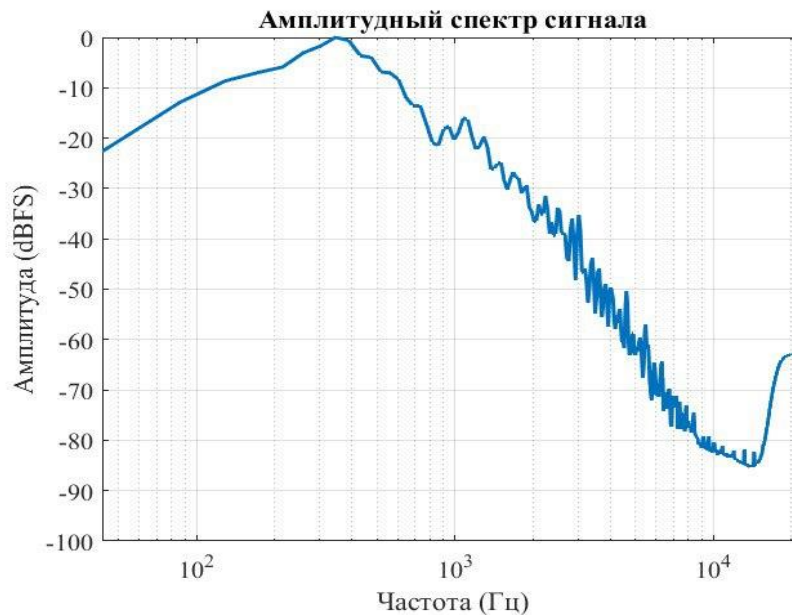


Рис. 2. Амплитудный спектр музыкального сигнала (фортепиано)

Регистрацию некоторых типов искажений, в частности аддитивных, удобнее осуществлять посредством анализа временной огибающей сигналов, приходящихся на каждую критическую полосу слуха. Модель обнаружения аддитивных искажений в установившихся сигналах позволяет вычислить величину модуляции (modulation measure), как некоторую оценку формы временных огибающих [3]. Образцы модуляции вычисляются на основе образцов возбуждения. С помощью значений уже полученной удельной громкости и рассчитанного значения ее абсолютного изменения, которые подверглись «размазыванию» во времени с помощью БИХ ФПЧ первого порядка [5], получим формулу для оценки величины модуляции:

$$Mod[k, n] = \frac{\bar{E}_{der}[k, n]}{1 + \bar{E}[k, n]/0.3}, \quad (1)$$

где  $\bar{E}[k, n]$  – удельная громкость,  $\bar{E}_{der}[k, n]$  – значение абсолютного изменения удельной громкости.

В таблице 1 приведены значения предварительной обработки, сделанные с помощью ПО MatLab, для трех типов звуковых сигналов.

Согласно таблице 1 можно сделать выводы, что электронная музыка демонстрирует наибольшие значения удельной громкости (0.3821 сон) и средней модуляции (0.0524), что связано с ее насыщенной спектральной структурой, ритмическими пульсациями и активным использованием амплитудных эффектов. Маскирующий порог у данного сигнала также выше (–16.12 dBFS), что указывает на его высокую способность подавлять восприятие слабых звуков вследствие спектральной плотности.

Фортепиано занимает промежуточное положение: умеренная удельная громкость (0.2508 сон) и невысокий уровень модуляции (0.0297) соответствуют более плавному и гармоничному характеру звучания. Маскирующий порог ниже, чем у электронной музыки (–25.68 dBFS), что объясняется более разреженным спектром.

Речевой сигнал имеет наименьшую удельную громкость (0.1732 сон), что отражает естественную динамику речи, а также средний уровень модуляции (0.0300), характерный для чередования гласных и согласных звуков. Самый низкий маскирующий порог (–31.25 dBFS) свидетельствует о наименьшей способности речи подавлять другие звуки, что обусловлено ее переменной спектральной структурой и кратковременными импульсами.

ТАБЛИЦА 1. Значения предварительной обработки образцов возбуждения

| Значение                | Фортепиано | Электронная музыка | Речевой сигнал |
|-------------------------|------------|--------------------|----------------|
| Удельная громкость, сон | 0.2508     | 0.3821             | 0.1732         |
| Оценка модуляции        | 0.0297     | 0.0524             | 0.0300         |
| Маскирующий порог, dBFS | -25.6770   | -16.1195           | -31.2474       |

Таким образом, различия в значениях параметров обусловлены спектральными и временными характеристиками каждого типа сигнала, а полученные данные подтверждают корректность работы, разработанной психоакустической модели. В дальнейшей работе над магистерской диссертацией, разработанный код и полученные значения будут необходимы для конечного разработки и получения объективной оценки качества.

**Список используемых источников**

1. ITU-R. Recommendation BS.1387, Method for Objective Measurement of Perceived Audio Quality. International Telecommunications Union Radiocommunication Assembly, 1998.
2. Аудиотехника. Учебник для вузов / Ю. А Ковалгин, Э. И Вологдин/ М.: Горячая линия – Телеком, 2013. 742 с., ил.
3. Иванов А. С. Разработка и исследование метода объективной оценки качества кодексов с компрессией цифровых аудиоданных: дис. ... канд. техн. наук: спец. 05.12.04 - Радиотехника, в том числе системы и устройства телевидения / науч. рук. д-р техн. наук, проф. Ю. А. Ковалгин; СПбГУТ им. проф. М. А. Бонч-Бруевича. СПб., 2007. 206 с
4. Электроакустика и звуковое вещание: учебное пособие для вузов / И. А. Алдошина, Э. И. Вологдин, А. П. Ефимов, Г. П. Катунин, Л. Н. Кацнельсон, Ю. А. Ковалгин, А. А. Фадеев; под ред. Ю. А. Ковалгина. М.: Горячая линия – Телеком, Радио и связь, 2007. 872 с.; ил.
5. Perceptual Audio Evaluation – Theory, Method and Application / Søren Bech и Nick Zacharov, 2013. 464 с

*Статья представлена научным руководителем, старшим преподавателем кафедры ЦТМ СПбГУТ О. А. Свиньиной.*



УДК 534.6

Р. Т. Хафизов (магистрант группы Р-41м, СПбГУТ), [khafizov.rt@sut.ru](mailto:khafizov.rt@sut.ru)

## ПРОСТРАНСТВЕННЫЙ ЗВУК В ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

*Статья посвящена вопросам создания и применения пространственного звука в виртуальной и дополненной реальности. Рассматриваются теоретические основы восприятия трехмерного звука человеком, современные технологии его реализации, такие как бинауральный звук и объектно-ориентированное аудио. Особое внимание уделено основным вызовам, связанным с персонализацией HRTF, ограничениями вычислительных ресурсов и точностью трекинга движений пользователя. Проанализированы области применения пространственного звука в индустрии развлечений, образовании, медицине и социальных коммуникациях. В заключении обозначены перспективные направления развития технологий пространственного аудио в контексте медиатехнологий и теле-радиовещания.*

*пространственный звук, виртуальная реальность, дополненная реальность, бинауральный звук, объектно-ориентированное аудио, медиа*

Пространственный звук играет важную роль в создании эффекта присутствия в системах виртуальной и дополненной реальности. В реальной жизни человеческий слух помогает определить положение звуков в пространстве относительно слушателя, аналогично в AR/VR пространственный звук помогает дополнить визуальную сцену, усиливая погружение пользователя.

Система человеческого слуха определяет направление и расстояние до источника звука опираясь на ряд акустических «подсказок». Ключевую роль играют междушумные различия: разница во времени прихода звука и его уровне между левым и правым ухом. Не менее важный фактор – спектральные искажения [1]. Звук по-разному взаимодействует с формой ушной раковины левого и правого уха, а также изменяется в зависимости от тонкостей формы головы и особенностей строения лица человека. Звук искажается, отражаясь от волос и затеняясь в ушной раковине, это создает резонансы и провалы в спектре – эти признаки помогают определять высоту источника относительно головы, а также его положение спереди или сзади от слушателя.

Все перечисленные эффекты формализуются понятием HRTF – head related transfer function – функция передачи звука от источника до барабан-

ной перепонки слушателя. Обычно она описывается спектрально. Также существует и импульсная характеристика HRIR – head related impulse response [2, 3].

Также на восприятие звука влияет и его расстояние от слушателя. Более близкие звуки воспринимаются громче, чем те же звуки, но изданные далеко. Помимо этого, с увеличением расстояния до источника звука, увеличивается и количество его переотражений от объектов окружающей среды, которые в свою очередь вызывают соответствующие спектральные и импульсные искажения для слушателя. Эти тонкости тоже учитываются при моделировании акустической среды в системах VR/AR [4].

Один из способов реализации пространственного звука для восприятия в наушниках – бинауральный рендеринг каждого источника. Метод заключается в пересчете каждого источника звука с учетом пары спектральной и импульсной функций для разных ушей. Сумма пересчитанных стереосигналов и создает картину звуков с учетом разницы восприятия ушами слушателя реальных звуков. Такой метод показывает высокую точность локализации, однако вычислительно затратен, так как с увеличением количества источников звука возрастает и количество необходимых пересчетов сигнала. В тяжелых сценах в реальном времени эти пересчеты создают большую нагрузку на вычисляющее устройство.

Альтернативный метод – микширование с помощью ambisonics. Суть этого способа противоположна вышеописанному. Прежде всего все звуки объединяются в общую звуковую сцену, а затем вся сцена преобразуется в бинауральный сигнал. На практике это реализуется благодаря кодированию каждого источника в сферические гармоники [5]. Полученные компоненты суммируются, а затем к их сумме и применяется пересчет с учетом спектральной и импульсной функции для каждого уха. Поскольку пересчет сигнала производится всего один раз, в реальной жизни такой процесс не сильно нагружает вычисляющее устройство, а значит сложность реализуемых сцен может быть выше, чем у вышеописанного метода, однако на практике использование такого метода показывает ухудшение точности локализации близких звуков.

Существуют также и модели учета акустики помещения. Ведь виртуальные миры, как и реальные, содержат поверхности, от которых звук отражается или при взаимодействии с которыми всячески изменяется. Простая акустическая модель учитывает лишь ослабление уровня звукового сигнала в зависимости от расстояния, однако для правдоподобности желательно

учитывать и ослабление звука в следствие встречи с препятствием на пути к слушателю и отражения от объектов. Существует несколько способов реализации этой идеи – от простых до сложных. Более простые методы используют автоматизацию фильтров низких частот и затухания громкости. Более сложные способы реализации подразумевают моделирование реального распространения волн в звуковой сцене. Делается это благодаря технологии трассировки лучей, то есть вычисление пути отраженной волны, как это делается с лучами света в графическом рендеринге. На практике широко применим гибридный способ – особо важные звуки трассируются, а фоновая сцена обрабатывается автоматизацией фильтров, эквализации и реверберации.

Для реализации пространственного звука в наше время существует несколько готовых решений. Рассмотрим Steam audio, воспроизводящий бинауральные записи и просчитывающий физическую модель распространения звука в реальном времени. Он предоставляется в форме плагина для Unity, Unreal и других. Его работа может происходить и в реальном времени и быть просчитана заранее. Применяется эта технология в основном в игровой индустрии [6].

Google Resonance Audio использует в основном идею микширования с ambisonics. Он также предоставляется в форме плагина для игровых движков. Его особенность – представление звука в виде высокопорядкового ambisonics, где все источники звука суммируются в глобальное поле, которое далее пересчитывается с учетом HRTF и HRIR [7].

Существует еще множество технологий, ведь сфера пространственного звука сегодня активно развивается. Одной из основных перспектив является возможность создания индивидуального звучания. Идея заключается в создании персональных функций HRTF и HRIR для пользователя с целью последующего их применения к воспроизводимому контенту. Некоторые компании реализуют начальные этапы воплощения этой идеи уже в наше время.

С ростом вычислительных мощностей персональной техники в будущем может возрасти и точность расчетов и моделирования распространения звука и пересчета сигнала с применением функций HRTF и HRIR [8].

Пространственный звук в виртуальной и дополненной реальности – динамично развивающаяся область, лежащая на пересечении акустики и компьютерных технологий. Особенности восприятия звуков человеческим ухом в дальнейшем будут изучены глубже, а стремительно растущие вычис-

лительные мощности позволяют все быстрее и быстрее просчитывать пространство и изменение звуковых волн в пространстве для локализации источников звука [9]. Инженерам, разрабатывающим эти системы, предстоит решить такие проблемы, как индивидуальные особенности слуха пользователей, необходимость мгновенной реакции системы на изменение движения или окружения, большой спрос на вычислительные ресурсы и другие.

В заключение, можно сделать вывод, что пространственный звук уже развился из нишевой отрасли в неотъемлемую часть VR/AR и других систем воспроизведения контента. Для исследователей звука будущее открывает множество возможностей для развития существующих идей и внедрения новых, ныне невообразимых технологий.

#### Список используемых источников

1. «Объемная» музыка: как VR-технологии передают звук // Хабр, 2016. URL: <https://habr.com/ru/companies/audiomania/articles/397147/> (дата обращения 10.06.2025).
2. Begault D. R. 3D Sound for Virtual Reality and Multimedia. Moffett Field, CA: NASA Ames Research Center, 2000. 160 с. URL: [https://human-factors.arc.nasa.gov/publications/Begault\\_2000\\_3d\\_Sound\\_Multimedia.pdf](https://human-factors.arc.nasa.gov/publications/Begault_2000_3d_Sound_Multimedia.pdf) (дата обращения 10.06.2025).
3. Blauert J. Spatial Hearing: The Psychophysics of Human Sound Localization. Revised edition. Cambridge, MA: MIT Press, 1997. 512 с. URL: [https://www.researchgate.net/publication/200045092\\_Spatial\\_hearing\\_the\\_psychophysics\\_of\\_human\\_sound\\_localization](https://www.researchgate.net/publication/200045092_Spatial_hearing_the_psychophysics_of_human_sound_localization) (дата обращения 10.06.2025).
4. Виртуальная реальность: видео 360 и бинауральный звук // Хабр. 2015. URL: <https://habr.com/ru/articles/379405> (дата обращения 10.06.2025).
5. Lokki T. Physically-Based Auralization—Design and Evaluation of Listening Environments. Doctoral dissertation. Helsinki University of Technology, 2002. 185 с. URL: <http://lib.tkk.fi/Diss/2002/isbn9512261588/isbn9512261588.pdf> (дата обращения 10.06.2025).
6. Valve Corporation. Steam Audio SDK Documentation. 2023. URL: <https://valvesoftware.github.io/steam-audio/> (дата обращения 10.06.2025).
7. Google Developers. Resonance Audio Overview. 2022. URL: <https://resonance-audio.github.io/> (дата обращения 10.06.2025).

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

## РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА

УДК 621.396

А. Э. Алексеев (магистрант группы РТ-42м, СПбГУТ), [alekseev.ae@sut.ru](mailto:alekseev.ae@sut.ru)

### ПЛАНИРОВАНИЕ И ОПТИМИЗАЦИЯ ТРАНСПОРТНОЙ СЕТИ ОПЕРАТОРА ДЛЯ УЛУЧШЕНИЯ ПОКАЗАТЕЛЕЙ GTP LOSS

*В статье рассматриваются методы мониторинга и оптимизации транспортной сети оператора мобильной связи на примере сегмента сети в Тосненском районе Ленинградской области. Основное внимание уделено анализу показателя GTP Loss, который отражает потери пакетов на интерфейсе S1-U. Приведены результаты исследования, включая сравнение методов мониторинга (GTP Loss, IPPM Huawei, TWAMP), а также технические решения для улучшения качества сети, такие как расширение радиорелейных линий, аренда каналов и оптимизация маршрутизации трафика. Показано, что реализация предложенных мероприятий позволила значительно снизить потери пакетов и улучшить качество обслуживания абонентов.*

*транспортная сеть, GTP Loss, мониторинг, оптимизация, радиорелейные линии, пропускная способность*

#### Введение

Транспортная сеть оператора мобильной связи – это сложная система, обеспечивающая передачу трафика между базовыми станциями (БС) и узлами ядра сети. Ее надежность и пропускная способность напрямую влияют на качество услуг, предоставляемых абонентам. Одним из ключевых показателей качества является GTP Loss, характеризующий потери пакетов на интерфейсе S1-U. Высокие значения GTP Loss приводят к снижению скорости передачи данных, увеличению задержек и ухудшению пользовательского опыта.

Актуальность исследования обусловлена ростом трафика в сетях LTE и необходимостью поддержания высоких стандартов качества обслуживания [1]. В статье анализируются методы мониторинга GTP Loss, причины его возникновения и технические решения для оптимизации сети на примере Тосненского района Ленинградской области.

## Методы мониторинга

Для контроля потерь на интерфейсе S1-U (рис. 1) применяются три основных метода:

1. GTP Loss – анализ потерь на основе «живого» абонентского трафика.

Преимущества: совместимость с большинством вендоров (Huawei, Nokia, Ericsson).

Недостатки: ограниченный набор метрик.

2. IPPM Huawei – сквозное тестирование качества IP-сети.

Преимущества: широкий набор метрик.

Недостатки: работает только с оборудованием Huawei.

3. TWAMP – активные измерения с использованием тестового трафика.

Преимущества: поддержка всеми вендорами.

Недостатки: требует дополнительного оборудования (IP Probe).

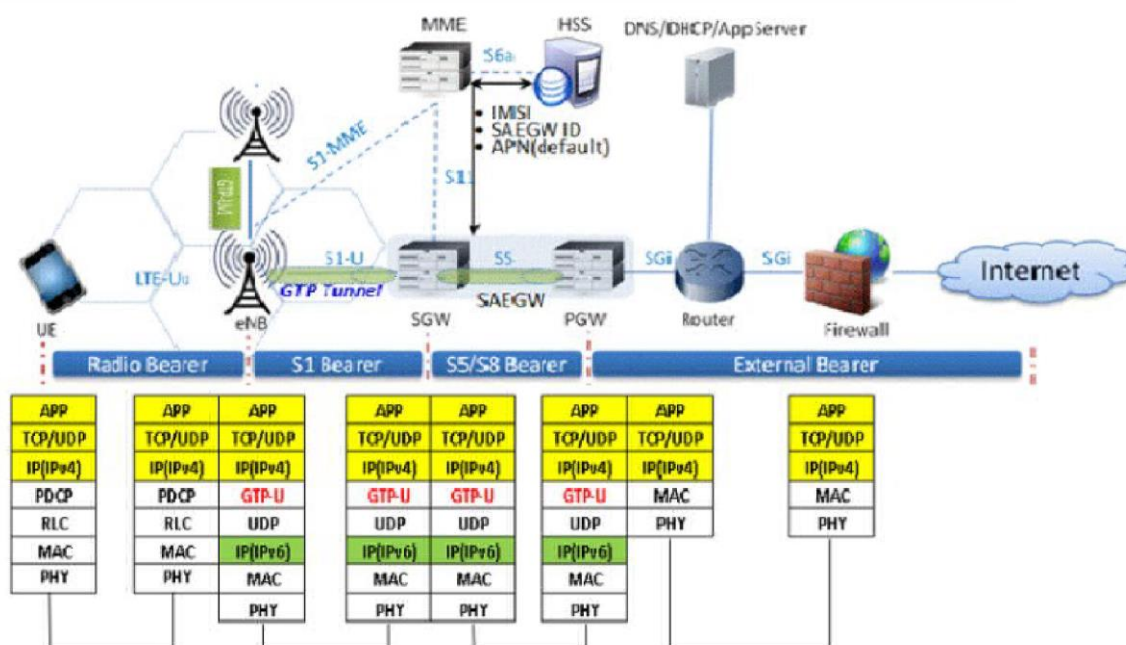


Рис. 1. GTP-туннель на интерфейсе S1-U  
[<https://vbook.pub/documents/gtp-loss-troubleshooting-9odny418jjwy>]

В таблице 1 приведено сравнение трех методов.

ТАБЛИЦА 1. Способы мониторинга потерь S1-U

| Метод       | Вендор RAN              | Вендор PS Core (SGW) | Основан на              | Стандарт                                       |
|-------------|-------------------------|----------------------|-------------------------|------------------------------------------------|
| GTP Loss    | Huawei, Nokia, Ericsson | Cisco, ZTE           | Пользовательский трафик | 3GPP TS 29.281(based on GTPSequence number)    |
| IPPM Huawei | Huawei (только)         | Huawei (только)      | Пользовательский трафик | Собственный                                    |
| TWAMP       | Huawei, Nokia, Ericsson | Не важно             | Тестовый трафик         | RFC 5357 (Two-Way Active Measurement Protocol) |

Сравнение методов показало, что GTP Loss является оптимальным выбором для операторов с разнородным оборудованием, так как не требует дополнительных затрат на инфраструктуру. [0]

### Анализ проблемного сегмента сети

В 2023 году в Тосненском районе наблюдался резкий рост трафика из-за увеличения абонентской базы LTE и повышения активности пользователей. Можно предположить несколько факторов, которые привели к увеличению числа абонентов в регионе:

- близость к Санкт-Петербургу,
- экономический рост и развитие промышленности,
- развитие инфраструктуры,
- улучшение качества жизни,
- привлечение инвестиций.

Это привело к перегрузке транспортной сети и росту показателя GTP Loss. На 1-й неделе 2023 года зафиксировано (рис. 2):

- 18 БС с состоянием «критично» (GTP Loss >5 %).
- 23 БС с состоянием «плохо» (GTP Loss 0,5–5 %).

Основные причины:

- Перегрузка радиорелейных линий (РРЛ).
- Недостаточная пропускная способность арендованных каналов.



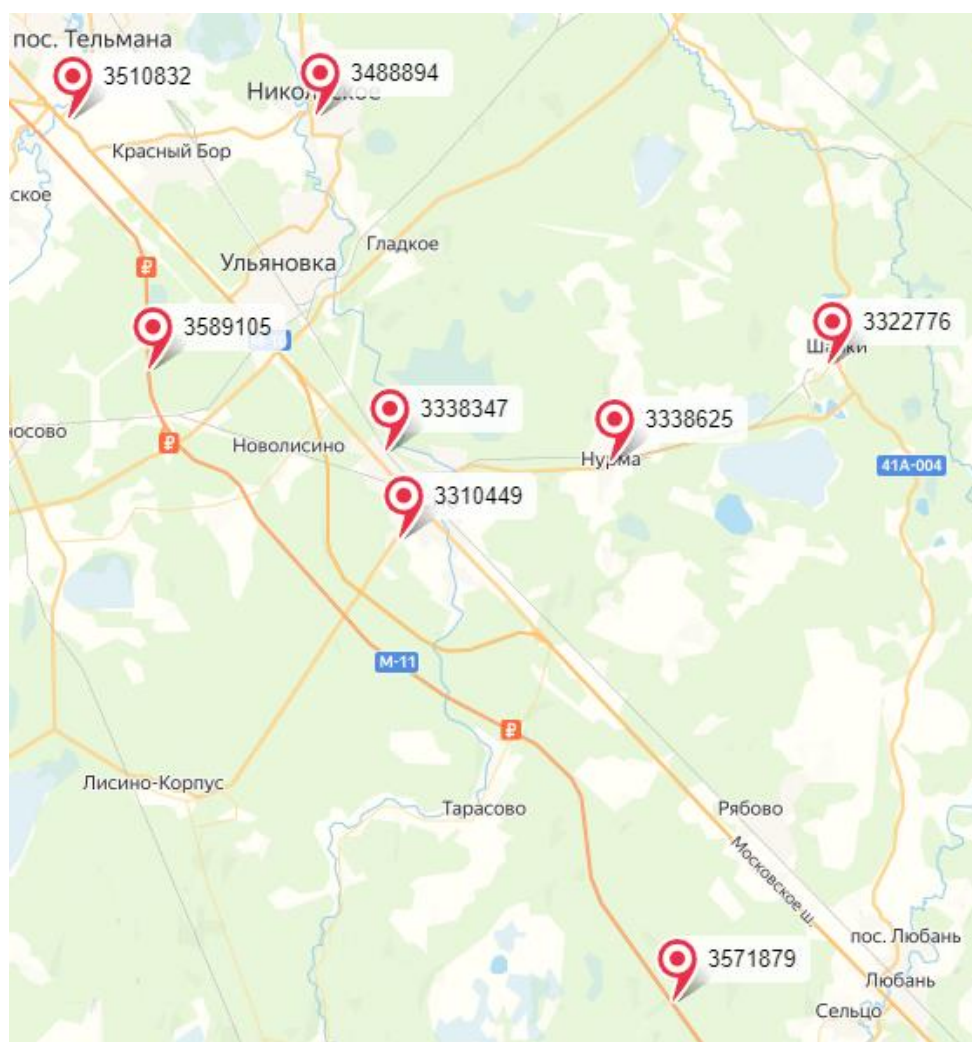


Рис. 2. Местоположения нескольких пораженных станций

## Технические решения и результаты

Для устранения проблем реализованы следующие мероприятия:

1. Расширение РРЛ: модернизация пролета с конфигурации 1 + 0 до 2 + 0, установка оборудования Ericsson RAU 2X.

Результат: снижение потерь до 0,1 %, увеличение пропускной способности с 400 Мбит/с до 800 Мбит/с.

2. Аренда каналов: организация дополнительного канала 2GE.

Результат: улучшение показателей на 12 смежных БС.

3. Оптимизация маршрутизации: построение новой точки слива трафика.

Результат: снижение утилизации каналов до 60 %.

Влияние проделанных мероприятий наглядно представлено на рис. 3.



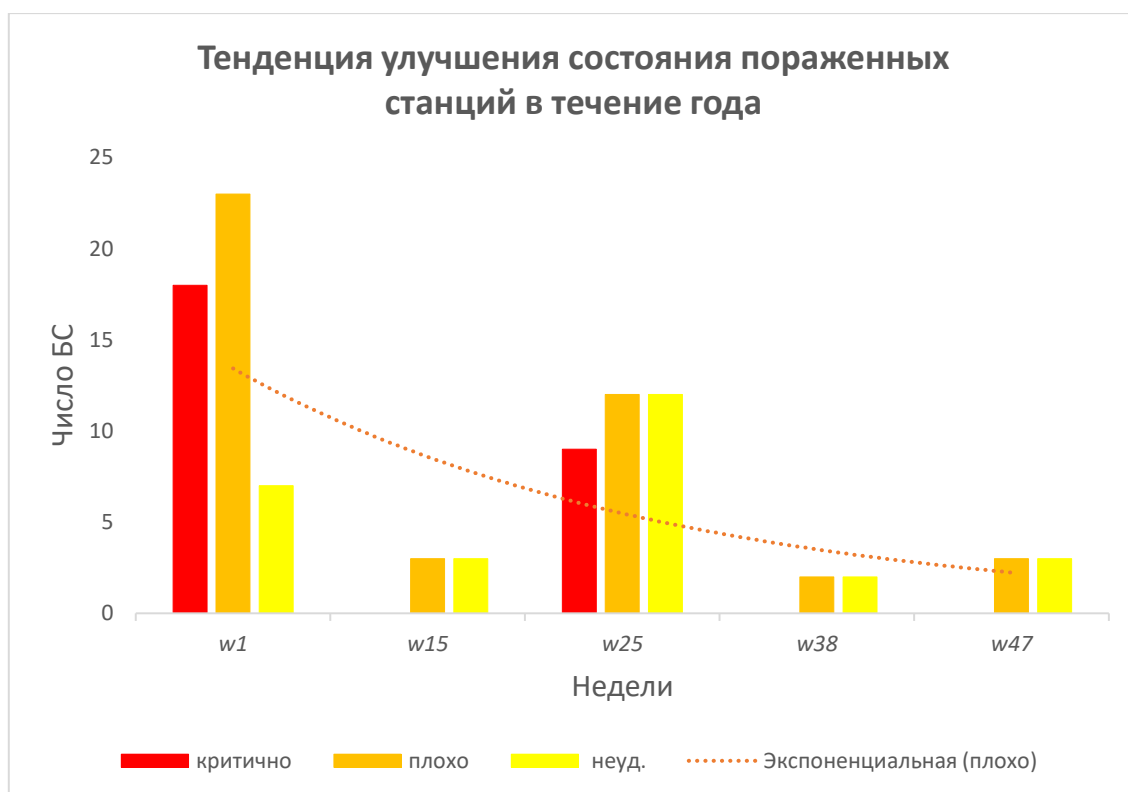


Рис. 3. Тенденция улучшения состояния пораженных станций в течение года

## Заключение

Реализованные мероприятия позволили сократить количество «критичных» БС на 85 % и повысить среднюю скорость передачи данных на 20–35 %. Для дальнейшего развития сети рекомендуется увеличивать долю ВОЛС, проектировать новые участки с запасом пропускной способности не менее 40 % и внедрять технологии IP MPLS и DWDM.

## Список использованных источников

1. Приказ №113 Министерства информационных технологий и связи РФ от 27.09.2007.
2. Kumar R. GTP Loss and Impact of Transport Bandwidth. URL: <https://mytelcolearning.blogspot.com> (дата обращения 08.04.2025).

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры БТС СПбГУТ Чернышовым А. Г.*

УДК 621.3.088.3

В. В. Гмырин (магистрант группы РТ-42м, СПбГУТ), [gmyrin.vv@sut.ru](mailto:gmyrin.vv@sut.ru)

## ОЦЕНКИ ТОЧНОСТИ ПАРАМЕТРОВ РАДИОНАВИГАЦИОННОГО СИГНАЛА

*В статье рассматриваются практические методы оценки нестабильности параметров сигналов как на передающей, так и на приемной стороне. Особое внимание уделено применению Вариации Аллана для выделения и оценивания составляющих погрешностей в области навигационного приборостроения. В частности, приведены методы оценивания среднего значения относительной нестабильности частоты в опорных генераторах. Также рассмотрены соотношения для анализа точности параметров радиосигнала на приемной стороне. Приведено практическое использование границы Рао-Крамера как минимального среднего квадрата ошибки при оценке доплеровского смещения частоты, фазы радиосигнала и его задержки по фазе.*

*вариация Аллана, опорные генераторы, оценка параметров радионавигационного сигнала*

Для определения координат потребителя, как известно, используется измерение времени прохождения радиосигнала от спутника до наземной станции. В качестве источников высокоточных колебаний для формирования различных шкал времени, таких как бортовая шкала времени, шкала времени потребителя используются высокоточные опорные генераторы гармонических колебаний.

Однако, присущая им нестабильность частоты, одной из основных причин которой являются шумы, накладывает определенные погрешности в измерениях и определении координат. Как решение, методы определения дисперсии сигналов опорных генераторов могут дать оценку погрешности измерения навигационных данных.

В качестве оценки дисперсии широкое применение нашла Вариация Аллана [1].

Для определения параметров радионавигационного сигнала (фаза, задержка фазы, смещение частоты) используют нижнюю границу Рао-Крамера [2].

Рассмотрим влияние нестабильности фазы опорного генератора на нестабильность времени.

Общее уравнение реального опорного генератора

$$U_{ог}(t) = U_0 \sin((2\pi f_0 t + \varphi_0) + \varphi(t) + \vartheta(t)), \quad (1)$$

где  $f_0$  – номинальная частота опорного генератора,  $\varphi_0$  – начальная фаза,  $\varphi(t)$  – систематический уход фазы,  $\vartheta(t)$  – случайные флуктуации фазы сигнала. Если  $\varphi(t)$  – прогнозируемы и могут быть использованы при формировании и передаче сигнала, то  $\vartheta(t)$  – случайные флуктуации фазы сигнала.

Можно показать, что при наличии таких флуктуаций реальная шкала времени потребителя будет выглядеть как

$$t_{\pi} = t + t'(t), \quad (2)$$

где  $t_{\pi}$  – время потребителя,  $t'(t) = \frac{\vartheta(t)}{2\pi f_{0\text{ог}}}$

Принимая во внимание выражение для мгновенного относительного отклонения частоты опорного генератора

$$\sigma\omega_{\text{ог}} = \frac{1}{\omega_0} \frac{d\vartheta(t)}{dt} \quad (3)$$

получаем, что нестабильность времени определяется нестабильностью частоты опорного генератора, то есть

$$\frac{dt'(t)}{dt} = \sigma\omega_{0\text{ог}}(t) \quad (4)$$

где  $\sigma\omega_{0\text{ог}}$  – мгновенное относительное отклонение частоты ОГ.

Величины  $d\vartheta(t)$  и  $\sigma\omega_{0\text{ог}}(t)$  есть случайные нестационарные величины, для описания которых применима Вариация Аллана [2].

Вариация Аллана служит для оценки стабильности параметров, которые могут быть подвержены не систематическим ошибкам, таким как дрейф частоты, температурные отклонения, а случайным шумовым процессам.

Согласно ГОСТ 8.567–2014, количественная характеристика нестабильности частоты определяется по следующей формуле:

$$\sigma^2 = \frac{\sum_{i=1}^n \sigma_{0i}^2}{n-1} \quad (5)$$

где  $\sigma_{0i} = \frac{f_{i+1} - f_i}{f_{\text{ном}}}$  – относительная вариация частоты,  $f_{i+1} - f_i$  – разность между соседними в ряду наблюдаемыми частотами [3].

Если рассматривать разность частот через приращение фазы, которая обусловлена случайными флуктуациями, то можно получить следующие выражения для вариации Аллана.

Пусть  $\overline{\sigma\omega_k} = \frac{\vartheta(t_k - \tau) - \vartheta(t_k)}{\omega_0 \tau}$  – среднее значение относительной нестабильности частоты на некотором интервале  $[t_k, t_k + \tau]$ . Разность в числителе есть приращение фаз сигнала на данном интервале.

Тогда для двухвыборочной дисперсии получим следующий вид

$$\sigma_{\text{Ал}}^2 = \frac{1}{2} \langle (\overline{\sigma\omega_2} - \overline{\sigma\omega_1})^2 \rangle, \quad (6)$$

где  $\overline{\sigma\omega_1}$  и  $\overline{\sigma\omega_2}$  среднее значение относительной нестабильности частоты на двух соседних промежутках времени.

Таким образом, при измерении приращения фаз сначала вычисляются их приращения на двух соседних участках  $\overline{\sigma\omega_1}$  и  $\overline{\sigma\omega_2}$ , а затем приращение для найденных первых разностей  $\overline{\sigma\omega_2} - \overline{\sigma\omega_1}$ .

Применение вариация Аллана находит, в первую очередь, в сфере навигационного приборостроения для выделения и оценивания составляющих погрешностей и шумов компонентов аппаратуры, которые служат в качестве частотоподающих источников гармонических колебаний для формирования радионавигационного сигнала.

При приеме для определения точности позиционирования необходимо дать оценку параметрам самого радионавигационного сигнала таким, как доплеровское смещение частоты, фазы и смещения фазы.

Пусть на входе приемника будет реализация сигнала в виде

$$y(t) = s(t, \lambda) + n(t), \quad (7)$$

где  $s(t, \lambda)$  – радиосигнал с параметрами  $t$  и  $\lambda$ ,  $\lambda$  – оцениваемый случайный параметр,  $n(t)$  – белый гауссовский шум.

В качестве оценки параметра  $\lambda$  применимы Границы Рао-Крамера для определения минимального среднего квадрата ошибки.

Принимая во внимание, что средний квадрат ошибки  $D_\lambda$  не может превышать величину

$$-\left( M \left[ \frac{d^2 \ln P(Y_0^T | \lambda)}{d\lambda^2} \right] \right)^{-1} \leq D_\lambda, \quad (8)$$

где  $P(Y_0^T | \lambda)$  – апостериорная плотность вероятности параметра  $\lambda$ ,  $Y_0^T$  – реализация самого сигнала, то можно дать количественную оценку параметрам радионавигационного сигнала.

Рассмотрим более подробно некоторые реализации.

Граница Рао-Крамера для дисперсии ошибки оценки доплеровского смещения частоты радиосигнала:

Пусть  $s(t, f_d) = A(t)\cos(2\pi(f + f_d)t + \varphi_0)$  – реализация сигнала где  $A(t)$  – амплитуда сигнала,  $\varphi_0$  – начальная фаза,  $f$  – несущая частота,  $f_d$  – доплеровское смещение частоты.

Используя формулу для нахождения границы Рао-Крамера можно получить, что минимальный средний квадрат ошибки оценки доплеровского смещения частоты будет выражаться, как

$$D_{f_d} = \frac{3}{2q(2\pi)^2 T^2}, \quad (9)$$

где  $q = \frac{E_c}{N_0}$  – отношение сигнал/шум,  $T$  – длительность наблюдаемого радиосигнала.

В результате, граница Рао-Крамера для среднего квадрата ошибки оценки доплеровского смещения частоты определяется только величиной отношения сигнал/шум и длительностью  $T$  наблюдаемого радиосигнала.

Граница Рао-Крамера для дисперсии ошибки оценки фазы радиосигнала:

Пусть  $s(t, \varphi_0) = A\cos(\omega t + \varphi_0)$  – реализация сигнала.

Тогда минимальный средний квадрат ошибки оценки фазы радионавигационного сигнала будет выражаться, как

$$D_\varphi = \frac{1}{2q}, \quad (10)$$

где  $q = \frac{E_c}{N_0}$  – отношение сигнал/шум.

В данном случае, минимальный средний квадрат ошибки оценки фазы будет зависеть только от отношения сигнал/шум.

Граница Рао-Крамера для дисперсии ошибки оценки задержки по фазе радионавигационного сигнала:

Пусть  $s(t, \tau) = A(t)\cos(\omega(t - \tau) + \varphi_0)$  – реализация сигнала,

Тогда минимальный средний квадрат ошибки оценки задержки по фазе радионавигационного сигнала будет выражаться, как

$$D_{\tau/\varphi} = \frac{1}{2q(2\pi f)^2}, \quad (11)$$

где  $q = \frac{E_c}{N_0}$  – отношение сигнал/шум.

Таким образом видно, что граница Рао-Крамера при оценке среднего квадрата ошибки оценки задержки по фазе зависит от отношения сигнал/шум и несущей частоты радионавигационного сигнала [2].

#### **Список используемых источников**

1. Сирая Т. Н. Статистическая интерпретация Вариации Аллана как характеристики измерительных и навигационных устройств // Гироскопия и навигация. 2020. Том 28. № 1 (108).
3. ГЛОНАСС. Модернизация и перспективы развития. Монография. Под ред. А. И. Перова. М.: Радиотехника, 2020 г. 1072 с. ISBN: 978–5–93108–198–4.
4. ГОСТ 8.567– 2014. Измерение времени и частоты. Термины и определения. М.: Москва, Стандартиформ, 2019. II, 16 с.

*Статья представлена научным руководителем, профессором кафедры РТ СПбГУТ, доктором технических наук, профессором Глушанковым Е. И.*

УДК 654.739

**В. М. Деткова** (к.ф-м.н., доцент кафедры Ф, СПбГУТ)

**М. Б. Надаршин** (студент группы ИКТ-414, СПбГУТ)

**М. В. Слюсаренко** (студент группы ИКТ-414, СПбГУТ),

[slyusarenko.mv@sut.ru](mailto:slyusarenko.mv@sut.ru)

## ПРИМЕНЕНИЕ ФЕРРОМАГНИТНОГО РЕЗОНАНСА В ФЕРРИТОВЫХ ФИЛЬТРАХ

*Ферритовые фильтры, основанные на явлении ферромагнитного резонанса (ФМР), находят широкое применение в современных электронных устройствах для подавления высокочастотных электромагнитных помех. Преимущество использования таких фильтров заключается в их компактности, экономичности и способности эффективно устранять помехи без искажения полезного сигнала. В работе рассматриваются физические основы ФМР, экспериментальная установка для его исследования, а также области применения ферритовых фильтров и их преимущества по сравнению с традиционными методами экранирования.*

*ферромагнитный резонанс, ферритовые фильтры, электромагнитные помехи, магнитная анизотропия*

### Введение

Современные электронные устройства постоянно сталкиваются с проблемой электромагнитных помех, которые могут приводить к сбоям в работе и ухудшению качества сигнала. Одним из эффективных решений является использование ферритовых фильтров, принцип работы которых основан на явлении ферромагнитного резонанса (ФМР) [1, 2]. В данной статье мы рассмотрим физическую сущность ФМР, экспериментальные методы его изучения и объясним, почему ферритовые фильтры являются предпочтительным способом защиты от помех по сравнению с традиционным экранированием.

Исследования, приведшие к открытию ферромагнитного резонанса (ФМР), начались в начале XX века. В 1911–1913 годах В. Аркадьев впервые наблюдал избирательное поглощение электромагнитных волн ферромагнетиками. В 1923 году Я. Дорфман предложил квантовое объяснение этого явления. Теоретическую основу ФМР заложили Л. Ландау и Е. Лифшиц в 1935 году, сформулировав уравнение динамической магнитной восприимчивости. В 1946 году Дж. Гриффитс экспериментально обнаружил ФМР в металлах, а в 1948 году Ч. Киттель описал влияние формы образца и магнитной

анизотропии на частоту резонанса [5]. В 1949 году У. Хьюитт наблюдал ФМР в ферритах.

### Теоретические основы ферромагнитного резонанса

Ферромагнитный резонанс – это резонансное поглощение электромагнитной энергии ферромагнетиком на определенной частоте, связанной с прецессией магнитных моментов в магнитном поле [1, 2]. В ферромагнитных материалах (например, ферритах) магнитные моменты электронов выстраиваются параллельно, образуя домены – области с одинаковой намагниченностью. Под действием внешнего магнитного поля домены могут менять ориентацию, а магнитные моменты начинают прецессировать вокруг направления поля.

Внешнее магнитное поле оказывает крутящий момент на намагниченность  $M$  ферромагнетика, заставляя ее прецессировать вокруг направления поля. Частота прецессии определяется свойствами материала и величиной поля. Если на материал подать переменное электромагнитное поле с частотой, совпадающей с собственной частотой прецессии, происходит резонансное поглощение энергии – аналогично тому, как качели раскачиваются сильнее, если толкать их в резонанс.

Частота ферромагнитного резонанса для тонкой пленки в параллельном поле рассчитывается по формуле Киттеля [2]:

$$f = \frac{\gamma}{2\pi} \sqrt{B(B + \mu_0 M)} \quad (1)$$

где  $\gamma$  – гиромагнитное отношение,  $\mu_0$  – магнитная постоянная,  $M$  – намагниченность,  $B$  – внешнее магнитное поле.

В ферритовых фильтрах резонансная частота определяется внутренними свойствами материала и его геометрией, так как внешнего магнитного поля обычно нет.

### Экспериментальная установка для исследования ФМР

Для изучения ФМР используется специальная лабораторная установка (рис. 1), включающая СВЧ-резонатор и электромагнит [1]. Ферромагнитный образец помещается в резонатор, а электромагнит создает регулируемое магнитное поле. Измеряется поглощение микроволновой энергии при изменении магнитного поля или частоты. Резонанс проявляется как резкий пик на графике зависимости поглощения от поля или частоты, что позволяет



определять резонансные частоты, ширину линий и релаксационные процессы в материале.

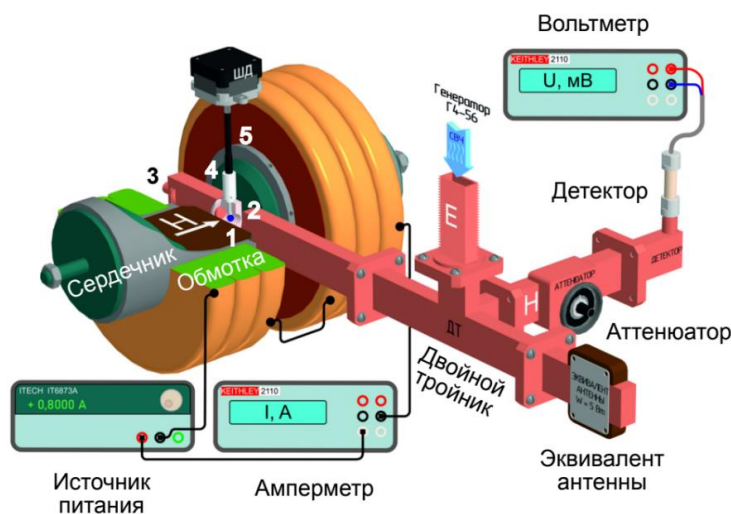


Рис. 1. Основные элементы экспериментальной установки [1]

## Применение ферромагнитного резонанса в ферритовых фильтрах

Ферритовые фильтры – это пассивные компоненты, изготовленные из ферритов (смесей оксидов железа и других металлов), которые используются для подавления высокочастотных электромагнитных помех. Наиболее распространены ферритовые бусинки, надеваемые на кабели (USB, HDMI, аудио и др.).

Принцип работы основан на ФМР: феррит поглощает энергию электромагнитных волн на определенных частотах, превращая ее в тепло [1, 3]. Это позволяет фильтровать высокочастотный шум, не влияя на полезный сигнал.

Ферритовые фильтры действуют как избирательные поглотители высокочастотного шума. При прохождении сигнала по кабелю вместе с ним могут передаваться паразитные высокочастотные помехи. Ферритовая бусинка увеличивает индуктивность участка провода и резонансно поглощает энергию помех, преобразуя ее в тепло. Полезный сигнал при этом практически не искажается.

Примеры применения:

- в HDMI-кабелях (рис. 2) предотвращают появление «снега» и полос на экране телевизора;
- в USB-кабелях (рис. 3) обеспечивают стабильную передачу данных и питания;
- В аудиокабелях устраняют треск и шум.
- На печатных платах подавляют помехи между компонентами.



Рис 2. HDMI-кабель с ферритовыми фильтрами



Рис 3. Кабель Mini-USB с ферритовым фильтром

## Преимущества и сравнительный анализ ферритовых фильтров

Преимущества:

- компактность – легко устанавливаются на существующие кабели;
- настраиваемость – разные составы ферритов позволяют фильтровать нужные диапазоны частот;
- экономичность – не требуют питания, дешевы в производстве;
- простота установки – не требуют модификации устройства.

ТАБЛИЦА 1. Сравнение с экранированием [4]

| Параметр           | Ферритовый фильтр | Сплошное экранирование |
|--------------------|-------------------|------------------------|
| Размер             | Компактный        | Часто громоздкий       |
| Стоимость          | Низкая            | Высокая                |
| Настраиваемость    | Есть              | Нет                    |
| Простота установки | Очень простая     | Сложная                |
| Эффективность      | Избирательная     | Универсальная          |

ТАБЛИЦА 2. Типы ферритов [4]

| Тип феррита | Основные применения                | Диапазон частот подавления |
|-------------|------------------------------------|----------------------------|
| MnZn        | Блоки питания, силовые кабели      | 0,1–2 МГц                  |
| NiZn        | Дата-кабели, высокочастотные линии | 1 МГц–2,45 ГГц             |

## Заключение

Ферромагнитный резонанс – фундаментальное явление, лежащее в основе работы ферритовых фильтров, которые сегодня широко применяются для защиты электроники от помех. Благодаря своим преимуществам – компактности, экономичности и простоте применения – ферритовые фильтры становятся незаменимыми компонентами в современной электронике. Экспериментальное изучение ФМР позволяет оптимизировать составы и конструкции фильтров для различных задач, обеспечивая надежную работу устройств в условиях электромагнитных помех.

## Список используемых источников

1. Ферромагнитный резонанс: Лабораторный практикум / А. Н. Егоров, А. В. Кузнецов, О. Б. Маврицкий. М.: НИЯУ МИФИ, 2021.
2. Перов Н. С., Ковалева И. Ю. Магнитный резонанс. Упражнение 2. Ферромагнитный резонанс в монокристалле феррита-граната иттрия: Лабораторный практикум. М.: Изд-во МГУ, 2015.
3. Ильченко М. Е., Мелкова Г. А., Мирских Г. А. Твердотельные СВЧ фильтры. М.: Наука, 1977.
4. Гуревич В. Ферритовые фильтры // Компоненты и технологии. 2015. № 10.
5. Ферромагнитный резонанс // Вестник ММИ Сыктывкарского гос. университета, вып. 21.

*Статья представлена научным руководителем, доцентом кафедры Ф СПбГУТ, кандидатом физико-математических наук Детковой В. М.*

УДК 621.3.062.9

**А. Н. Коробейников** (магистрант группы ФП-41м, СПбГУТ),  
[korobeinikov.an@sut.ru](mailto:korobeinikov.an@sut.ru)

**Е. И. Носенко**, (магистрант группы ФП-41м, СПбГУТ), [nosenko.ei@sut.ru](mailto:nosenko.ei@sut.ru)

**Э. Ю. Седышев** (к.т.н., доцент, доцент кафедры Э СПбГУТ)

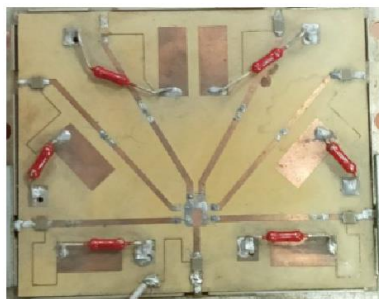
## МЕХАНИЧЕСКИЙ КОММУТАТОР ДЛЯ ПЕРЕДАЮЩИХ ЛИНИЙ СВЧ ДИАПАЗОНА

*В статье представлены результаты экспериментов с двумя устройствами коммутации сигналов СВЧ диапазона на основе р-і-п структур и геркона. Предложено оригинальное электромеханическое устройство для коммутации микрополосковых линий. Представлен его эскиз, описаны некоторые преимущества и потенциально слабые стороны, а также возможные области применения.*

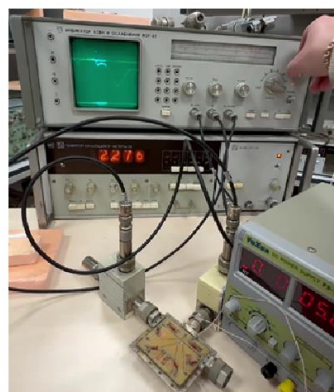
*СВЧ, механические коммутаторы*

Микрополосковая линия благодаря своей простоте на сегодняшний день является одной из самых популярных передающих линий в нижней области СВЧ диапазона (0,3-10 ГГц). Коммутаторы для данных линий зачастую строятся на р-і-п диодах, которые весьма быстродействующие и мощные [1, 3]. Другим вариантом могут служить герконовые реле, которые имеют свои преимущества, но также не лишены недостатков.

Был проведен эксперимент с р-і-п диодом 2А546А-5. Устройство коммутации (Рисунок 1а) с двумя диодами было подключено к измерительному комплексу, состоящему из индикатора КСВН и ослабления Я2Р-67 и генератора качающей частоты 2-4 ГГц. Напряжение смещения подавалось с внешнего лабораторного блока питания (рис. 1б).



а)



б)

Рис. 1. Измерение ослабления передающего тракта с двумя последовательно включенными 2А546А-5. Фото исследуемого устройства (а), фотография макета (б)

В RFSim99 была составлена принципиальная схема на основе геометрических параметров линий и документации на диод 2A546A-5 [2] (рис. 2).

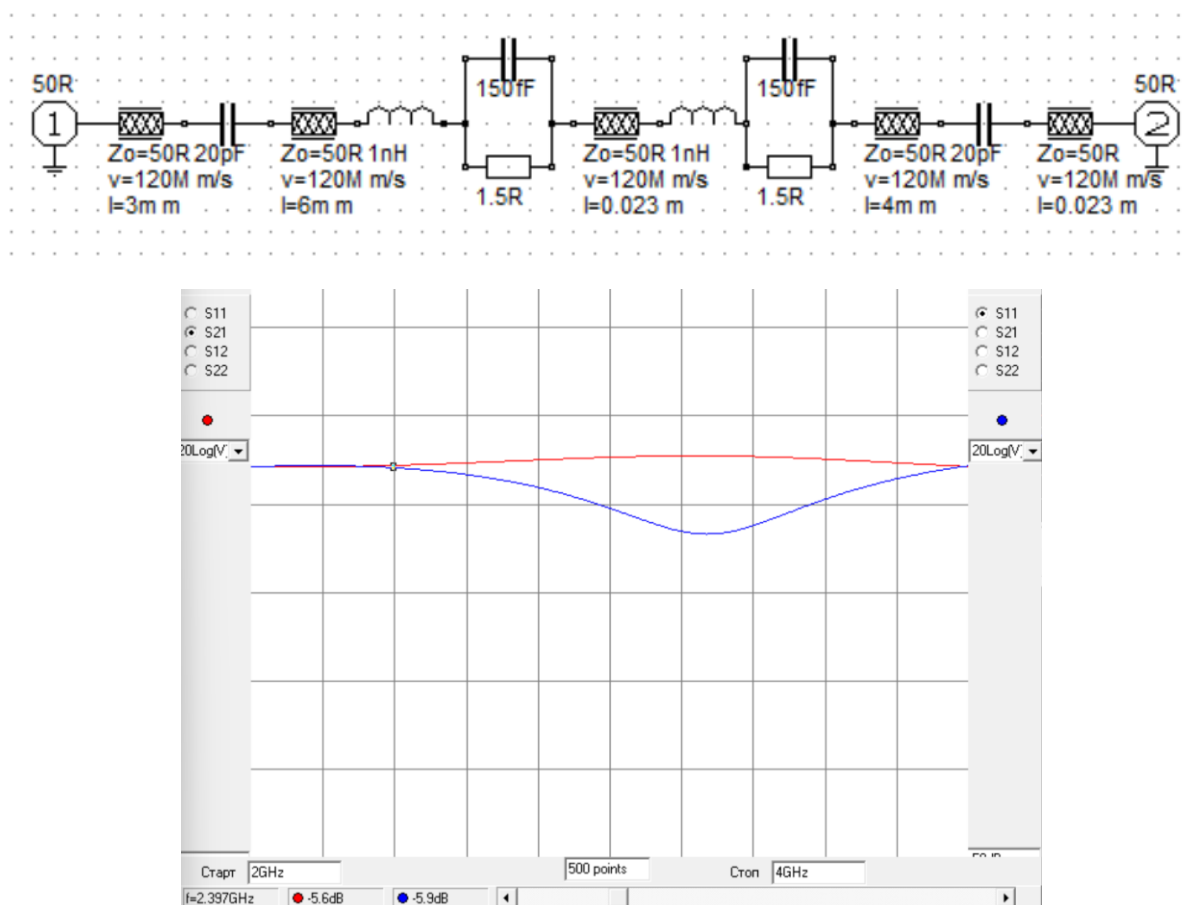


Рис. 2. Идеализированная принципиальная схема открытого канала в RFSim99 и результаты ее моделирования

При измерении прохождения сигнала потери в части рабочего диапазона составляли порядка -5 дБ, что является достаточно низким показателем для коммутатора и для р-і-п диодов, в частности. При закрытии канала изоляция составила порядка -25 дБ.

Также был исследован геркон, который можно отнести к электромеханическому типу переключателей (рис. 3). С помощью того же измерительного комплекса было измерено прохождение сигнала через геркон и изоляция при размыкании цепи (рис. 4).

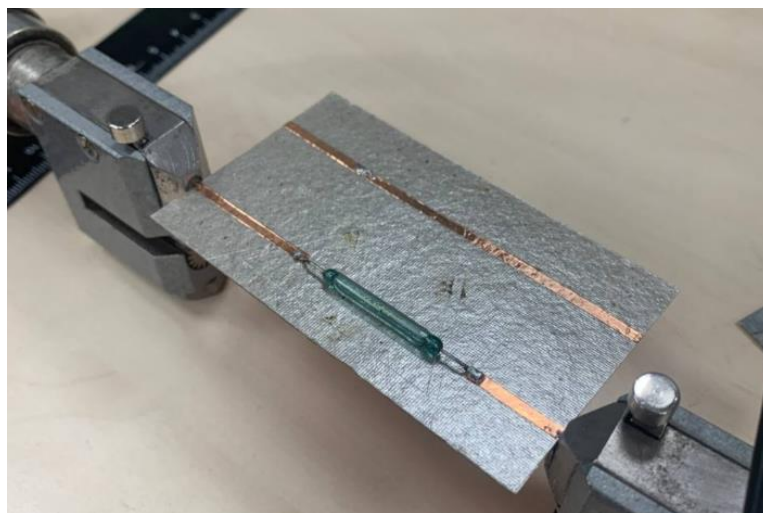


Рис. 3. Геркон, установленный в микрополосковую линию



Рис. 4. Прохождение сигнала при разомкнутом (а) и замкнутом (б) контакте геркона

Как нетрудно заметить, в качестве коммутационного прибора на 2-4 ГГц выбранный геркон не работает, характеристики при разомкнутом и замкнутом контакте имеют пологие спады и уровень в среднем -15 дБ. Такие показатели могут быть обусловлены в том числе и неравномерностью волнового сопротивления (проводник в корпусе поднят на 1-2 мм относительно поверхности платы), а также паразитной емкостью между контактами геркона. Однако, изменение полосы пропускания все же наблюдается, поэтому можно сделать вывод, что данный элемент мог быть спроектирован для решения более узкоспециализированных задач.

Возможной альтернативой является использование механического коммутатора в виде отрезка микрополосковой линии. Эскиз такого коммутатора представлен на рисунке 5.

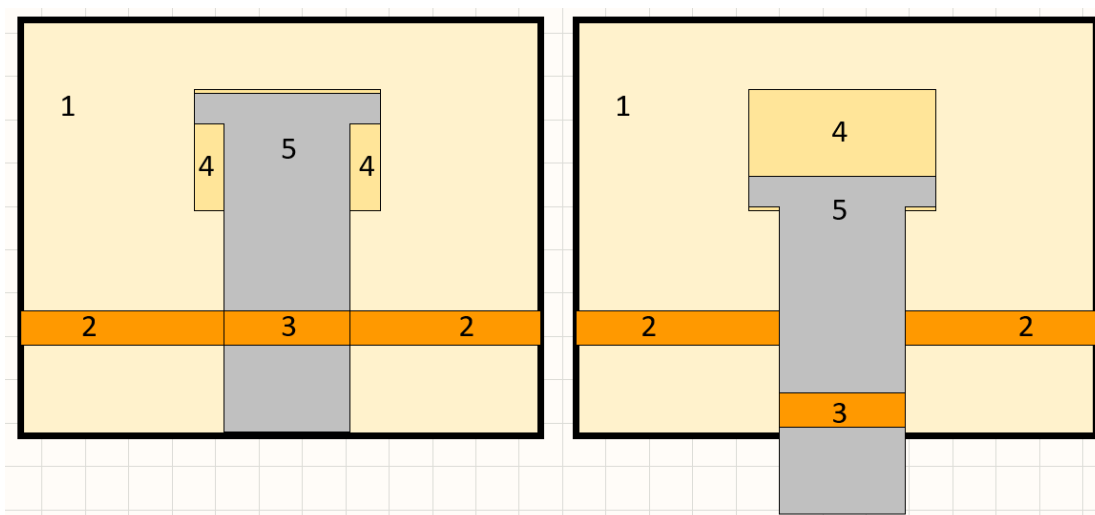


Рис. 5. Эскиз механического коммутатора. 1 – подложка платы; 2 – микрополосковая линия передачи; 3 – коммутирующий отрезок МПЛ; 4 – паз, фрезерованный в глубину подложки; 5 – подвижный переключатель

Установка отрезка линии на одном уровне с поверхностью платы позволяет избежать скачков волнового сопротивления, а увеличение хода позволяет уменьшить паразитную емкость между контактами. Также, на скользящую пластину могут быть нанесены несколько отрезков линий с различными параметрами, например с заданным затуханием, что позволит использовать данное устройство как сборку резисторов. Эскиз резисторной сборки представлен на рисунке 6.

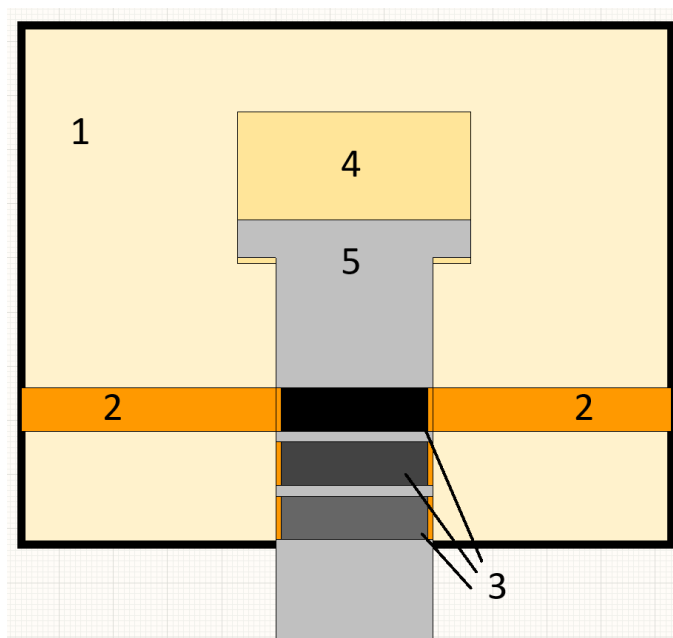


Рис. 6. Вариант исполнения резисторной сборки: 1 – подложка платы; 2 – микрополосковая линия передачи; 3 – различные резистивные пленки; 4 – паз, фрезерованный в глубину подложки; 5 – подвижный переключатель



Однако, данный вариант коммутатора не лишен недостатков:

1. Поскольку коммутатор имеет подвижные части, он будет подвержен износу. Чтобы уменьшить износ возможно использовать устойчивые к трению материалы, например фторопласт.

2. Коммутатор имеет относительно массивные подвижные части, поэтому максимальная частота коммутации на данном этапе не превышает единицы герц.

3. Так как толщина МПЛ обычно не превышает 0.1 мм, необходимо делать отрезок на подвижной части либо большей толщины, чтобы обеспечить гальваническое соединение торец в торец, либо большей длины, чтобы края медного отрезка выступали за пределы подвижного переключателя и обеспечивали соединение внахлест.

Таким образом, были проведены эксперименты с реальными коммутаторами, на основе которых было выдвинуто предположение об эффективности коммутации с помощью отрезка микрополосковой линии. Был создан эскиз такого коммутатора, описаны его возможные применения, потенциальные достоинства и недостатки. Следующим этапом может быть создание чертежа и изготовление макета с последующим тестированием и доработкой.

#### **Список используемых источников**

1. Седышев Э. Ю., Бочаров Е. И., Кулаков Н. С. Коммутационные диоды СВЧ при обратном смещении // III Всероссийская научно-техническая конференция «Электроника и микроэлектроника СВЧ»: материалы конф. СПб.: ЛЭТИ, 2014. С. 534–536.
2. Диоды СВЧ типа 2А546А-5. Технические условия аА0.339.286 ТУ. 11 с.
3. Вайсблат А. В. Коммутационные устройства СВЧ на полупроводниковых диодах. М.: Радио и связь, 1987. 116 с.



УДК 629.78

**М. А. Мельникова** (магистрант группы РТ-42м, СПбГУТ),  
[melnikova.ma@sut.ru](mailto:melnikova.ma@sut.ru)

## **СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ВНУТРИСИСТЕМНОЙ ЭМС В НИЗКООРБИТАЛЬНЫХ СПУТНИКОВЫХ СИСТЕМАХ СВЯЗИ**

*Современные низкоорбитальные спутниковые системы (НОСС) стремительно развиваются: к 2025 году на орбите работает свыше 20 тыс. спутников. Такая плотность вызывает проблемы электромагнитной совместимости (ЭМС), ухудшая качество связи. Исследование актуально из-за дефицита частотного ресурса и необходимости оптимизации методов ЭМС, которые различаются у каждой системы. Цель работы – сравнить эти методы и предложить рекомендации по их выбору для конкретных архитектур НОСС.*

*низкоорбитальные спутниковые системы (НОСС), электромагнитная совместимость (ЭМС), методы разделения сигналов, сравнительный анализ, оптимизация частотного ресурса, помехоустойчивость*

Современные низкоорбитальные спутниковые системы связи (НОСС), такие как Starlink, OneWeb и Iridium, переживают период бурного роста. По данным на 2025 год, только в системе Starlink работает более 12 тысяч активных спутников, а общее количество аппаратов на низкой околоземной орбите превысило 20 тысяч. Такой резкий рост спутниковой группировки создает серьезные проблемы электромагнитной совместимости (ЭМС), когда сигналы от разных спутников могут создавать взаимные помехи, снижая общую пропускную способность системы и качество связи.

В настоящее время используют шесть основных методов обеспечения ЭМС, каждый из которых имеет свои преимущества и ограничения. В данной статье будет исследован каждый из методов и на основе проведенного исследования осуществлен сравнительный анализ (1-13).

Метод частотного разделения (FDMA):

Принцип метода основан на выделении каждому спутнику или группе спутников отдельных частотных каналов. Основное преимущество - простота реализации. Однако метод характеризуется низкой спектральной эффективностью и плохой масштабируемостью.

Метод временного разделения (TDMA):

В данном случае разные спутники используют один частотный канал, передавая сигналы в строго определенные временные интервалы. Метод требует точной синхронизации всех элементов системы, но обеспечивает хорошую защиту от коллизий.

Метод пространственного разделения (SDMA):

Использование узконаправленных антенн и оптимального пространственного разнесения спутников позволяет многократно использовать одни и те же частоты в разных зонах покрытия. Современные фазированные антенные решетки значительно повышают эффективность этого метода.

Метод кодового разделения (CDMA):

Метод основан на применении ортогональных кодов для разделения сигналов. Отличается высокой помехоустойчивостью, но требует значительных вычислительных ресурсов.

Метод поляризационного разделения:

Использование сигналов с разной поляризацией позволяет удвоить пропускную способность системы без расширения полосы частот. Однако на эффективность метода влияют атмосферные явления.

Метод адаптивного управления мощностью:

Динамическая регулировка мощности передачи в зависимости от текущих условий связи. Современные реализации используют алгоритмы машинного обучения для оптимизации этого процесса.

Для наглядного сравнения методы сведены в таблицу 1.

ТАБЛИЦА 1. Сравнительный анализ методов

| Метод                 | Спектральная эффективность | Сложность реализации | Устойчивость к помехам |
|-----------------------|----------------------------|----------------------|------------------------|
| FDMA                  | Низкая                     | Низкая               | Средняя                |
| TDMA                  | Средняя                    | Средняя              | Высокая                |
| SDMA                  | Высокая                    | Высокая              | Очень высокая          |
| CDMA                  | Высокая                    | Очень высокая        | Очень высокая          |
| Поляризация           | Очень высокая              | Средняя              | Средняя                |
| Адаптивное управление | Средняя                    | Высокая              | Высокая                |

По результатам сравнительного анализа сделан вывод, что ни один из методов не является универсальным решением всех проблем ЭМС. Каждый метод имеет свои оптимальные области применения и ограничения, что приводит к необходимости их комбинирования в реальных системах.

Среди наиболее перспективных направлений развития технологий ЭМС можно выделить:

1. Гибридные методы, сочетающие преимущества различных подходов. Например, комбинация SDMA и FDMA позволяет достичь высокой спектральной эффективности при относительно невысокой сложности реализации.

2. Применение искусственного интеллекта (ИИ) и машинного обучения для: прогнозирования помеховой обстановки, оптимального распределения ресурсов, автоматической адаптации параметров передачи.

3. Освоение миллиметрового диапазона частот (30-300 ГГц), что открывает новые возможности для: увеличения пропускной способности, реализации сверхузконаправленной связи, дальнейшего развития пространственного разделения.

Проведенное исследование позволяет сделать следующие выводы:

1. Ни один из рассмотренных методов не является универсальным решением всех проблем ЭМС. Выбор оптимального подхода должен основываться на конкретных требованиях и архитектуре системы.

2. Современные НОСС демонстрируют тенденцию к использованию комбинированных методов, что позволяет преодолеть ограничения отдельных технологий.

3. Наиболее перспективными направлениями являются развитие гибридных методов, внедрение технологий искусственного интеллекта и освоение новых частотных диапазонов.

Одним из удачных примеров использования комплексного подхода в обеспечении ЭМС в НОСС является Starlink от компании SpaceX, которая является одной из самых передовых и масштабных НОСС. Комплексное решение включает в себя:

1. SDMA–использование фазированных антенных решеток с формированием узких управляемых лучей.

2. FDMA–разделение частот между разными орбитальными плоскостями и группами спутников.

3. Адаптивное управление мощностью – динамическая регулировка мощности передачи в зависимости от нагрузки и условий связи.

Такой комплексный подход позволяет системе эффективно работать при невероятно высокой плотности спутников–более 2000 аппаратов на одной орбитальной плоскости.

Оптимальный метод обеспечения ЭМС зависит от архитектуры конкретной спутниковой системы. Современные НОСС, такие как Starlink,

OneWeb и Iridium, используют комбинации методов для достижения высокой эффективности. Перспективы развития связаны с гибридными технологиями, применением ИИ и освоением миллиметровых волн.

Исследование подтверждает, что комбинирование методов ЭМС является наиболее эффективным решением для современных спутниковых систем, обеспечивая устойчивую связь в условиях высокой плотности спутников на орбите.

Дальнейшие исследования в этой области должны быть направлены на разработку интеллектуальных систем управления ЭМС, способных адаптироваться к постоянно изменяющимся условиям на орбите. Особое внимание следует уделить вопросам международной координации использования частотного ресурса.

#### Список используемых источников

1. Козлов Д. В., Курдюмов С. В. Электромагнитная совместимость радиоэлектронных средств. М.: Радио и связь, 2013. 352 с.
2. Никаноров А. И. Электромагнитная совместимость в радиосвязи: учебное пособие. СПб.: Политехника, 2017. 288 с.
3. Мельников В. П., Карпов А. И., Чернов С. М. Низкоорбитальные спутниковые системы: архитектура, особенности, тенденции // Вестник связи. 2020. № 5. С. 10–17.
4. Rappaport T. S. Wireless Communications: Principles and Practice. 2nd ed. Upper Saddle River: Prentice Hall, 2002. 707 p.
5. Proakis J. G. Digital Communications. 5th ed. New York: McGraw-Hill, 2001. 1080 p.
6. International Telecommunication Union. Technical and operational characteristics of non-geostationary satellite systems in the FSS. ITU-R Report M.2225-2. Geneva: ITU, 2021. 74 p.
7. Zhang Y., Zhang H., Zhang Y., Wang M. AI-based dynamic resource allocation in LEO satellite systems // IEEE Communications Surveys & Tutorials. 2021. Vol. 23. № 1. PP. 182–203.
8. Li W., Han Z., Vasilakos A. Machine learning for satellite communication: A review // IEEE Access. 2020. Vol. 8. P. 73064–73099.
9. Kaplan E. D., Hegarty C. J. Understanding GPS/GNSS: Principles and Applications. 3rd ed. Boston: Artech House. 2017. 878 p.
10. ITU-R Recommendation SM.1132-2. General principles and methods of spectrum management. Geneva: ITU, 2015.
11. ESA Telecommunications & Integrated Applications. Mega-Constellations: Opportunities and Challenges. ESA Report TEC-SAT/2020. Noordwijk: ESA, 2020. 58 p.
12. Han Y., Zhang X., Lu J. Adaptive Beamforming Techniques for LEO Satellite Communication Using AI // IEEE Access. 2021. Vol. 9. P. 119870–119884.
13. Zheng C., Guo L., Yan F. Inter-satellite interference analysis in large-scale LEO constellations // International Journal of Satellite Communications and Networking. 2021. Vol. 39. № 3. PP. 235–250.

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры PCuB СПбГУТ, доцентом Симониной О. А.*

УДК 621.396

Н. С. Пирогов (магистрант группы РТ-42м, СПбГУТ), [pirogov.ns@sut.ru](mailto:pirogov.ns@sut.ru)

## ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ РАСПРОСТРАНЕНИЯ СВЧ СИГНАЛОВ НАД ВОДНОЙ ПОВЕРХНОСТЬЮ

*Исследование посвящено особенностям распространения СВЧ сигналов над водной поверхностью, что является критически важной задачей для морских радиолокационных систем, спутникового мониторинга и корабельной связи. Основное внимание уделено анализу влияния электродинамических и гидрофизических факторов, таких как высокая диэлектрическая проницаемость воды, интерференционные замирания, аномальная рефракция и воздействие волнения. Предложена математическая модель затухания сигнала, включающая потери в свободном пространстве, атмосферные эффекты, отражения от воды и влияние осадков. На основе экспериментальных данных для частот 2.4 ГГц и 5 ГГц показано воздействие волнения водной поверхности на качество связи: при высоте волн более 1 м наблюдаются глубокие замирания (до 30–40 дБ) и снижение дальности.*

*СВЧ – сигнал, распространение, затухания, замирания*

Распространение СВЧ-сигналов над водной поверхностью представляет собой критически важную техническую задачу, обусловленную уникальными электродинамическими свойствами и широким спектром практических приложений в морских радиолокационных комплексах, спутниковых системах мониторинга и корабельных системах связи. Физические особенности СВЧ-диапазона, включая малую длину волны (1 мм - 30 см) и высокую направленность излучения, обеспечивают принципиальные преимущества для задач обнаружения и идентификации объектов.

Распространение сверхвысокочастотных (СВЧ) волн в приграничной зоне "воздух-вода" определяется комплексом электродинамических и гидрофизических явлений, например, таких как: высокая диэлектрическая проницаемость воды ( $\epsilon \approx 80$  при 3 ГГц) вызывает существенное изменение импеданса на границе раздела; коэффициент отражения Френеля для вертикальной поляризации демонстрирует минимум при угле Брюстера ( $\sim 83^\circ$  для морской воды на 10 ГГц). Многолучевая интерференция в условиях распространения СВЧ-сигналов над водной поверхностью проявляется через формирование характерной интерференционной картины с выраженными минимумами, описываемой формулой Парсеваля-Вейля, где критиче-

ским параметром выступает высота антенны над поверхностью, определяющая глубину замираний в рамках классической двухлучевой модели. Особое значение имеет устойчивость СВЧ-сигналов к атмосферным помехам, что в сочетании с современными методами цифровой обработки (адаптивная фильтрация, когерентное накопление) делает их основным инструментом для построения защищенных систем связи морского базирования, где традиционные УКВ-системы демонстрируют недостаточную помехоустойчивость (1-6).

Специфические условия распространения над водной поверхностью - от формирования интерференционных минимумов при многолучевом распространении до аномальной рефракции в приграничном слое - требуют разработки специализированных компенсационных алгоритмов и аппаратных решений, что определяет актуальность дальнейших исследований в данной области.

СВЧ-диапазон (1-300 ГГц,  $\lambda = 30$  см-1 мм) характеризуется квазиоптическим распространением с выраженной направленностью излучения, малой глубиной скин-слоя и значительной зависимостью от свойств среды распространения, но над водной поверхностью существенно модифицируется за счет уникальных диэлектрических свойств воды ( $\epsilon' \approx 80$ ,  $\epsilon'' \approx 12$  при 3 ГГц), вызывающих резкое изменение импеданса на границе раздела сред и формирующих коэффициент отражения по Френелю до 0.6-0.8 для вертикальной поляризации в зависимости от угла падения. Ключевые эффекты распространения включают: аномальную рефракцию из-за градиента диэлектрической проницаемости в приповерхностном слое (модифицированный показатель преломления  $n = 1.00025-1.00045$  для морского воздуха), интерференционные замирания при сложении прямого и отраженного лучей (двухлучевая модель с глубиной замираний до 30-40 дБ), а также дополнительные потери 0.5-3 дБ/км в зависимости от частоты из-за поглощения в водяном паре и рассеяния на капиллярных волнах, что требует применения специализированных методов компенсации при проектировании морских радиосистем.

Распространение СВЧ-сигналов над водной поверхностью подвержено комплексному влиянию четырех ключевых групп факторов. Во-первых, рельеф поверхности капиллярные волны, рябь, волнение до 5-6 баллов, которые вызывают рассеяние излучения с модуляцией фазового фронта, приводя к увеличению эквивалентной шумовой температуры антенны на 15-20 % при высоте волн больше одного метра. Во-вторых, атмосферные параметры

такие как градиенты влажности 0-100 %, температурные инверсии, скорость ветра, формируют неоднородный профиль диэлектрической проницаемости, вызывающий как траекторные искривления (эффект сверхрефракции), так и образование испарительных волноводов в миллиметровом диапазоне. В-третьих, многолучевое распространение с дифракцией на неоднородностях создает интерференционные замирания глубиной до 30-40 дБ, при этом дифракционные потери на краях волн могут достигать 6-8 дБ/длина волны. Наконец, электрофизические параметры воды: соленость и температура, которые существенно изменяют комплексную диэлектрическую проницаемость, что приводит к вариациям коэффициента отражения и требует адаптивной коррекции параметров излучения в реальном времени.

Математическая модель, которая использовалась для исследования и моделирования затуханий сигнала над водной поверхностью:

$$L = L_{\text{прст}} + L_{\text{атм}} + L_{\text{дождь}} + L_{\text{вода}}$$

где  $L$  – общее затухания сигнала;

$L_{\text{прст}}$  – затухания в свободном пространстве:

$$L_{\text{прст}} = 20 \log_{10} \left( \frac{4\pi d}{\lambda} \right),$$

$d$  – расстояние (м);  $\lambda$  – длина волны (м);

$L_{\text{атм}}$  – атмосферные затухания:

$$L_{\text{атм}} = \gamma_{\text{атм}} \left( \frac{H}{H_{\text{норм}}} \right) \cdot \frac{d}{1000},$$

$\gamma_{\text{атм}}$  – удельный коэффициент атмосферного затухания (дБ/км);  $H$  – относительная влажность воздуха (%);  $H_{\text{норм}}$  – нормативная влажность (80 %);  $d$  – расстояние между передатчиком и приемником (м);  $L_{\text{вода}}$  – затухания из – за отражений от воды:

$$L_{\text{вода}} = -10 \log_{10} \left[ \left( \frac{\lambda}{4\pi d} \right)^2 \cdot 2(1 - |\Gamma| \cos \left( \frac{2\pi \Delta d}{\lambda} \right)) \right]$$

$\Gamma$  – коэффициент отражения Френеля;  $\Delta d$  – разность хода лучей;

$L_{\text{дождь}}$  – затухания в дожде (ITU – R P. 838).

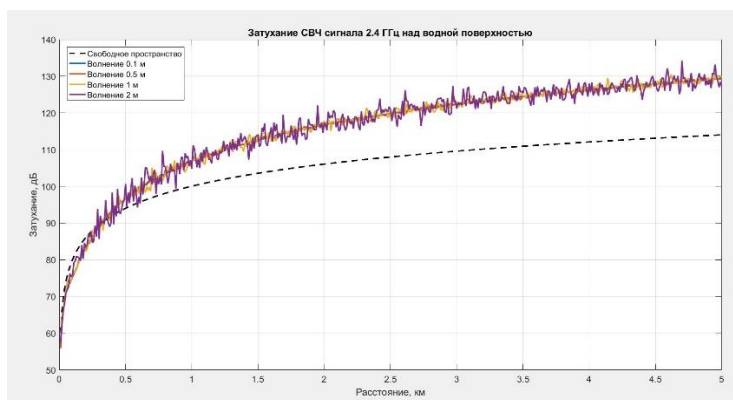


Рис. 1. Затухания СВЧ сигнала 2.4 ГГц над водной поверхностью

Сравнение затухания в свободном пространстве и при разной высоте волн (0.1 м, 0.5 м, 1 м, 2 м). Из графика видно, что в свободном пространстве затухание растет плавно по логарифмическому закону. При влиянии волны в 0.1 метр затухание близко к графику свободного пространства, но с небольшими колебаниями из-за слабых отражений. При волнах 0.5-1 метр появляются выраженные "провалы" сигнала на дистанциях 1–3 км из-за интерференции прямого и отраженного лучей. Затухание при крупных волнах (2 метра) усиливается на 10–15 дБ, а связь на расстояниях больше 2 км становится нестабильной. Исходя из этого можно сделать вывод – чтобы минимизировать влияние волн до 1 м для частоты 2.4 ГГц необходимо выбирать оптимальную высоту антенн от 3 до 5 м.

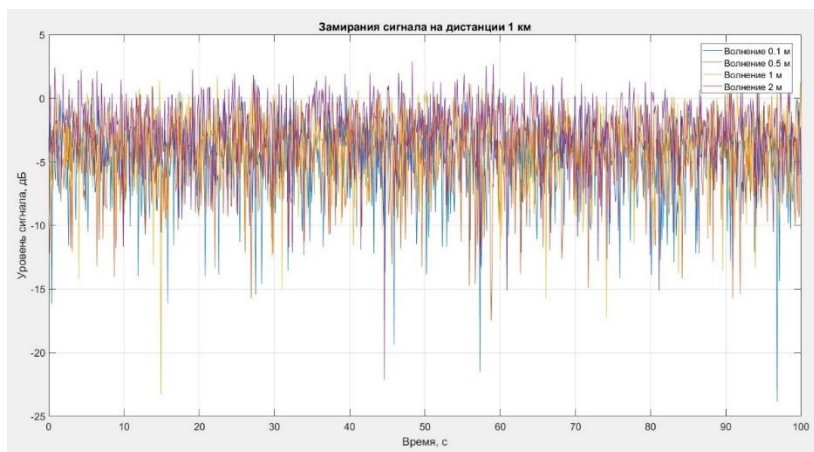


Рис. 2. Замирания сигнала на дистанции 1 км

Изменение уровня сигнала во времени для разных высот волн говорит о том, что при волнении 0.1 м сигнал стабилен ( $\pm 5$  дБ), замирания редкие, при волнении 0.5–1 м замирания глубокие до 20–30 дБ с периодичностью 2–5 секунд, что соответствует скорости волн. Волнение 2 м делает сигнал критически нестабильным, из-за чего возможны полные потери связи на 1–



3 секунды. Исходя из этого можно сказать, что при волнении более 1 м требуется адаптивная модуляция или ММО-антенны.

Далее представлены графики затухания СВЧ сигнала на частоте 5 ГГц.

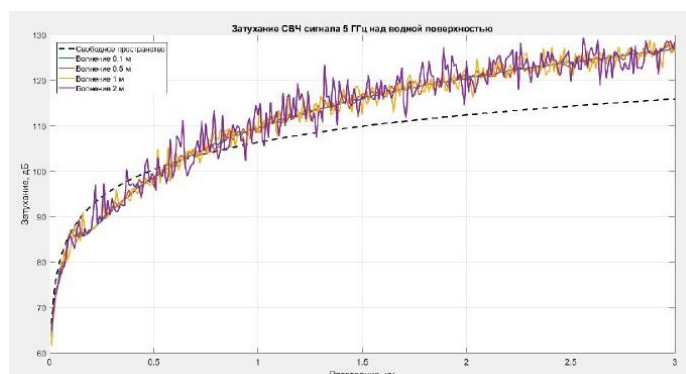


Рис. 3. Затухания СВЧ сигнала 5 ГГц над водной поверхностью

Затухание на 5 ГГц выше, чем на 2.4 ГГц, примерно 100 дБ на 1 км. При высоте волн 0.5 м наблюдаются дополнительные потери 8–12 дБ на дистанциях свыше 500 м. Волны 2 м: максимальная дальность падает до 700 м, по сравнению с 1.5 км для 2.4 ГГц. Для 5 ГГц критично уменьшать расстояние или повышать мощность. В условиях волнения свыше 1 м предпочтительнее использовать 2.4 ГГц.

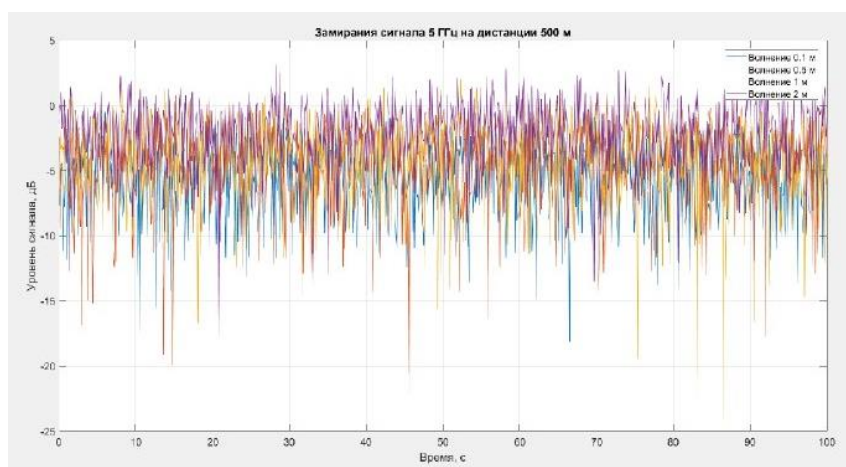


Рис. 4. Замирания сигнала на дистанции 500 м

Глядя на динамику сигнала при разном волнении, можно сказать, что 5 ГГц более чувствителен к волнам, даже при 0.3 м замирания достигают 15–20 дБ. Из-за меньшей длины волны провалы сигнала чаще и глубже, чем на 2.4 ГГц. 5 ГГц подходит только для коротких дистанций до 1 км или систем с разнесенным приемом.

Сравнение графиков для 2.4 ГГц и 5 ГГц демонстрирует ключевой компромисс между дальностью и устойчивостью сигнала. На 2.4 ГГц затухание растет плавно, обеспечивая стабильную связь до 5 км даже при волнении

0.5–1 м, но с периодическими замираниями до 20–30 дБ. В отличие от этого, 5 ГГц критически зависит от условий: уже при волнении 0.3 м замирания достигают 15–20 дБ, ограничивая рабочую дистанцию 1 км.

Подводя итоги можем наблюдать, что диапазон 2.4 ГГц – выбор для протяженных линий с умеренным волнением, но требует запаса мощности, в то время как диапазон 5 ГГц применим только на коротких дистанциях с антеннами высотой больше или равной 3 м. Волны свыше 1 м дестабилизируют любую частоту, требуя ММО или адаптивных модуляций. Оптимальная стратегия – комбинация 2.4 ГГц для дальних линий и 5 ГГц для высокоскоростных сегментов с жестким контролем высоты антенн.

### Список используемых источников

1. ITU-R P.838 – Рекомендация МСЭ-R по удельным коэффициентам затухания сигнала в дожде для моделей прогнозирования.
2. ITU-R P.676 – Атмосферное затухание электромагнитных волн в диапазоне 1–350 ГГц.
3. Курикша А. А., Логачев А. А. Распространение радиоволн над морской поверхностью. – М.: Радио и связь, 1987. 248 с.
4. Бреховских Л. М. Волны в слоистых средах. М.: Наука, 1973. 343 с.
5. Ismail T., Jawhar I. Microwave Propagation over Sea: A Review // IEEE Communications Surveys & Tutorials. 2010. Vol. 12. № 3. PP. 376–387.
6. ITU-R P.530 – Рекомендация МСЭ-R по распространению радиоволн и доступности для наземных линий связи.

*Статья представлена научным руководителем, доцентом кафедры РСuВ СПбГУТ, кандидатом технических наук, доцентом Симониной О. А.*

УДК 004.032.2

Д. Г. Попугаев (студент группы ИСТ-261, СПбГУТ), [pdg@sut.ru](mailto:pdg@sut.ru)

А. П. Шабанов (преподаватель кафедры САР, СПбГУТ), [aps@sut.ru](mailto:aps@sut.ru)

## АНАЛИЗ ПРАВОВЫХ АСПЕКТОВ ТЕХНОЛОГИЙ БЛОКЧЕЙН В УПРАВЛЕНИИ ПРЕДПРИЯТИЕМ

*В статье представлены действующие правовые основы взаимодействия с технологией блокчейн в рамках систем управления предприятием. Проанализированы основные нормативно-правовые акты, стандарты и международные документы, регулирующие использование распределенных реестров и криптографических технологий. Особое внимание уделено Российскому законодательству в сфере цифровых финансовых активов, международным стандартам информационной безопасности (ISO/IEC 27001, ISO 22739:2024) и регламенту Европейского Союза MiCA.*

*блокчейн, распределенный реестр, смарт-контракты, правовое регулирование, информационная безопасность*

В настоящее время технология блокчейн привлекает значительное внимание со стороны правительств как экономически развитых, так и развивающихся стран, а также активно обсуждается в научном сообществе. Отправной точкой в развитии данной технологии стало создание в 2009 году программистом под псевдонимом Сатоши Накамото первой криптовалюты – биткойна [1].

Во многих исследованиях блокчейн рассматривается как неотъемлемая часть четвертой промышленной революции, и благодаря своим основным свойствам, технология обладает широким спектром потенциальных применений в различных сферах.

В Российской Федерации системное развитие блокчейн-технологий на государственном уровне началось сравнительно недавно. В 2019 году Министерство цифрового развития, связи и массовых коммуникаций РФ представило дорожную карту по развитию «сквозной» цифровой технологии «Системы распределенного реестра». Документ определяет стратегические направления развития блокчейн в России, фиксирует предполагаемые результаты внедрения и выделяет приоритетные области для международного сотрудничества [2].

В связи с тем, что развитие технологии началось относительно недавно, нормативно-правовая база в данной сфере ограничена. На данный момент специализированного, утвержденного ГОСТа исключительно по технологиям блокчейн в России пока нет, однако ведутся разработки в данном направлении. При применении технологии блокчейн можно выделять ряд нормативных требований, а именно: ГОСТ Р 57580.1-2017, ГОСТ Р ИСО/МЭК 27001-2012:

- ГОСТ Р 57580.1-2017 «Безопасность финансовых (операционных) систем. Защита информации финансовых организаций. Общие положения». ГОСТ напрямую не упоминает блокчейн, он задает универсальные требования к системам, работающим с важной финансовой информацией, в частности с распределенными реестрами. Среди требований выделяются: Требования к обеспечению целостности информации, наличие аутентификации и управление доступом, журналирование и контроль действий пользователей. Все указанные требования являются основой для обеспечения информационной безопасности любых финансовых ИТ-систем, включая блокчейн [3];

- ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» представляет собой базовый международный стандарт по управлению информационной безопасностью, что необходимо для любых блокчейн-систем, особенно корпоративных и финансовых. Основные требования к системе управления информационной безопасностью: 1) Управление рисками информационной безопасности; 2) Управление доступом; 3) Управление криптографическими средствами; 4) Управление инцидентами информационной безопасности; 5) Обеспечение целостности информации.

На международном уровне имеются специальные нормативные документы, направленные на создание качественных блокчейн решений и безопасных смарт-контрактах. Можно выделить следующий ряд документов: ISO/IEC 27001, ISO 22739:2024, ЕС – MiCA.

- ISO/IEC 27001 идентичен вышеуказанному ГОСТ Р ИСО/МЭК 27001-2021.

- ISO 22739:2024 представляет собой международный стандарт, устанавливающий терминологию в области блокчейн и распределенных реестров. Основная цель стандарта – предоставить согласованную терминологию для всех участников экосистемы блокчейн, включая разработчиков, архитекторов решений, регуляторов, аудиторов и стандартизаторов. Являясь определяющей базой, стандарт указывает ключевые термины и их определения, используемые в документах, проектах и правовом регулировании, связанных с технологиями распределенных реестров. Например, согласно стандарту, термин «asset» (актив) определяется как все, что имеет ценность для заинтересованной стороны. Термин «block» (блок) определяется как, структурированные данные, включающие заголовок блока и данные блока [4].

- MiCA (Markets in Crypto-Assets) представляет собой законодательный акт Европейского Союза, направленный на регулирование рынка криптоактивов. Регламент разработала Европейская комиссия в котором, основные задачи

направлены на обеспечение юридической ясности для криптопроектов и защиты права криптоинвесторов. Для блокчейн-экосистемы и корпоративного управления регламент важен, поскольку определяет правовой статус криптоактивов, эмитентов токенов, операторов платформ, провайдеров кошельков и бирж, а также устанавливает требования к публичным предложениям и листингу токенов [5].

Технология блокчейн постепенно внедряется в практику корпоративного управления и финансовых систем и становится частью современных цифровых преобразований. Несмотря на то, что нормативно-правовое регулирование в этой сфере находится на стадии формирования, как в России, так и на международном уровне, уже существуют базовые стандарты и регламенты, определяющие ключевые требования и метрики к безопасности, терминологии и правовому статусу криптоактивов, а также систем на основе распределенных реестров.

В дальнейшем для успешного внедрения технологии блокчейн в систему корпоративного управления предприятий потребуется как развитие национальной нормативной базы, так и гармонизация российского законодательства с международными правовыми актами и стандартами в этой области.

#### Список используемых источников

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system // Bitcoin.org. 2008. URL: <https://bitcoin.org/bitcoin.pdf> (дата обращения 10.02.2024).
2. Попугаев Д. Г., Шабанов А. П. Применение технологии блокчейн при создании единого информационного пространства виртуального предприятия // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2023): Сборник лучших докладов: в 2 т. Т.2. / сост. Н. Н. Иванов. СПб.: СПбГУТ. 2024. С. 376-379.
3. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций // URL: <https://itglobal.com/wp-content/uploads/2021/05/gost-57580.1-1.pdf> (дата обращения 10.06.2025).
4. ISO 22739:2024(en), Blockchain and distributed ledger technologies – Vocabulary // URL: <https://www.iso.org/obp/ui/en/#iso:std:82208:en> (дата обращения 10.06.2025).
5. Обзор Европейского регламента о криптоактивах (MiCA) // URL: [https://www.magenta.legal/ru/news/European-crypto-assets-regulation-\(MiCA\)-overview](https://www.magenta.legal/ru/news/European-crypto-assets-regulation-(MiCA)-overview) (дата обращения 10.06.2025).

*Статья представлена научным руководителем, и.о. заведующим кафедрой САР СПбГУТ, кандидатом технических наук, доцентом Акимовым С. В.*

УДК 004.3 + 004.7:004.4 + 004.62 + 004.8

П. А. Процкий (студент группы ИКПИ-33, СПбГУТ), [protskiy.pa@sut.ru](mailto:protskiy.pa@sut.ru)

## РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ ДЕФЕКТОВ НА МЕТАЛЛИЧЕСКИХ ПОВЕРХНОСТЯХ В РЕАЛЬНОМ ВРЕМЕНИ

*На производствах и других объектах часто наблюдаются значительные убытки после непредвиденного разрушения критически-важных узлов. В статье представлена разработка автономной системы для мониторинга состояния металлических поверхностей в реальном времени на основе сети Zigbee. Проведен сравнительный анализ уже существующих методик контроля, обоснован выбор технологий и программного обеспечения, представлены результаты моделирования работы системы на схеме и в среде LabView. Обеспечивается низкое энергопотребление и масштабируемость.*

*методы анализа, радиоволновой датчик, Zigbee-сеть, анализ сигнала*

### Введение

На производствах и в системах обслуживания металлические поверхности критически важных узлов (трубопроводы, корпуса приборов и др.) подвержены износу и повреждениям. Это приводит к убыткам, особенно если дефекты не обнаружены вовремя. Факторы риска включают влажность, механические воздействия и другие неблагоприятные условия.

Целью проекта является разработка энергоэффективной и недорогой системы мониторинга металлических поверхностей в реальном времени для выявления микротрещин, коррозии и других дефектов. Необходимо проанализировать существующие решения и выбрать оптимальные технологии [1-4].

Результатом проекта будет система, снижающая материальные потери за счет своевременного обнаружения повреждений.

### Уже реализованные решения

В авиационной промышленности применяются радиоволновые сканеры, работающие в GHz-диапазоне. Эти системы используют датчики с передачей данных по Zigbee или Wi-Fi и алгоритмы машинного обучения для выявления дефектов в металлических и композитных конструкциях. Основные преимущества – бесконтактный метод и высокая скорость сканирования, однако глубина анализа ограничена, а стоимость реализации высока. Аналогичная технология адаптирована для мониторинга трубопроводов, где датчики устанавливаются на дронах или роботах, перемещающихся внутри труб.

Ультразвуковые методы широко используются при обследовании мостов и других инфраструктурных объектов. Датчики, работающие в контактном режиме, обеспечивают высокую точность и возможность глубокого анализа, но требуют точного позиционирования. Автоматизированные решения на базе роботизированных платформ повышают эффективность, однако их внедрение сопряжено со значительными затратами.

Термографические системы, основанные на инфракрасных камерах, применяются для контроля ветряных турбин и сварных швов. Они позволяют быстро анализировать большие площади без физического контакта, но их возможности ограничены поверхностными дефектами, а оборудование имеет высокую стоимость.

Вихретоковые технологии нашли применение в железнодорожной отрасли, где они эффективно выявляют поверхностные трещины в рельсах. Метод отличается высокой чувствительностью, но не подходит для глубокого анализа.

Отдельное направление – беспроводные сети датчиков (Zigbee, LoRa), используемые для мониторинга мостов. Такие системы обеспечивают масштабируемость и энергоэффективность, хотя по точности уступают другим методам.

Каждый из рассмотренных подходов имеет свои сильные и слабые стороны. Их сравнительные характеристики по ключевым параметрам представлены в таблице 1.

ТАБЛИЦА 1. Сравнение популярных методов

| Метод             | Точность | Глубина анализа     | Бесконтактность | Стоимость |
|-------------------|----------|---------------------|-----------------|-----------|
| Ультразвуковой    | Высокая  | Большая             | Нет             | Высокая   |
| Радиоволновой     | Средняя  | Малая               | Да              | Средняя   |
| Термографический  | Средняя  | Малая               | Да              | Высокая   |
| Вихретоковый      | Высокая  | Малая               | Да              | Средняя   |
| Радиографический  | Высокая  | Большая             | Да              | Высокая   |
| Беспроводные сети | Средняя  | Зависит от датчиков | Да              | Низкая    |

## Разработанное решение

Предлагаемое решение представляет собой систему мониторинга металлических поверхностей, основанную на сети беспроводных датчиков. В качестве технологической основы используется платформа Zigbee, обеспечивающая

энергоэффективную передачу данных и масштабируемость. Система включает три ключевых компонента: сеть датчиков, шлюз обработки данных и серверный анализ. На рис. 1 отображены основные устройства системы.

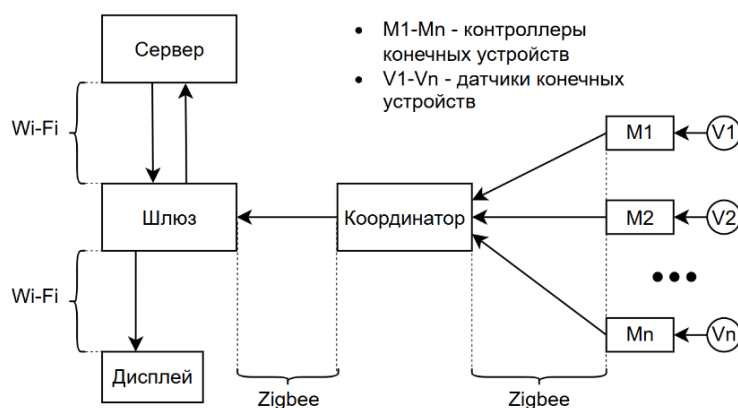


Рис. 1. Общая схема аппаратной структуры

Основу системы составляют радиоволновые датчики, которые бесконтактно измеряют параметры отраженного сигнала – амплитуду, фазовый сдвиг и временную задержку. Эти показатели позволяют выявлять микротрещины, коррозионные повреждения и другие дефекты металлических конструкций. Собранные данные передаются через Zigbee-сеть на центральный шлюз, где происходит их первичная обработка.

Для анализа полученных сигналов применяется комплекс математических методов. Быстрое преобразование Фурье переводит сигнал в частотную область, выявляя аномалии в спектральных характеристиках. Фильтрация Калмана и цифровые ФНЧ устраняют шумовые помехи, повышая точность измерений. Классификация дефектов осуществляется с помощью алгоритмов машинного обучения, включая метод опорных векторов и нейронные сети. Локализация повреждений выполняется методами триангуляции и оптимизационными алгоритмами.

Техническая реализация системы использует современные компоненты. В качестве сенсорных модулей применяются датчики AD9361 (рис. 2) с рабочим диапазоном 70 МГц – 8 GHz. Микроконтроллеры ESP32-H2 (рис. 3) обеспечивают сбор данных и беспроводную передачу по протоколу Zigbee. Также понадобится любая Zigbee-антенна (рис. 4). Центральный шлюз построен на базе Raspberry Pi 4 (рис. 5, 6) с дополнительным Zigbee-модулем CC2652P. Серверная часть, реализованная на Python с использованием библиотек NumPy, SciPy и TensorFlow, выполняет комплексный анализ данных.



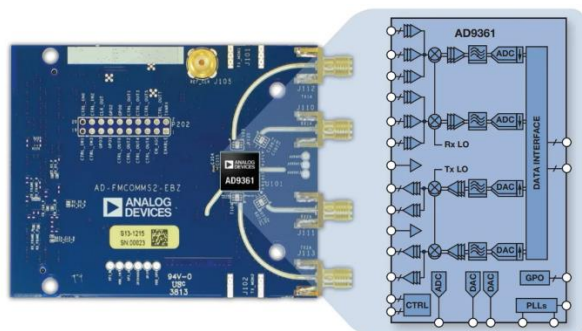


Рис. 2. Модуль AD9361

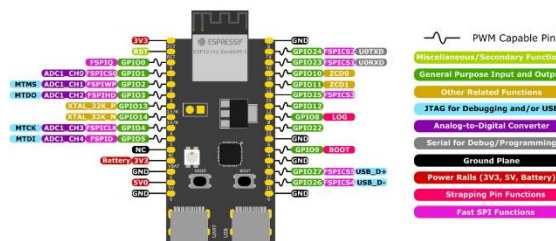


Рис. 3. Dev-kit с ESP32-H2



Рис. 4. Zigbee антенна

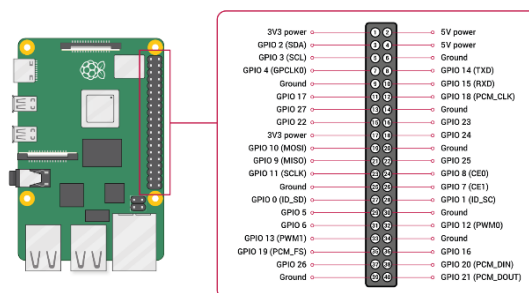


Рис. 5. Интерфейсы Raspberry Pi 4

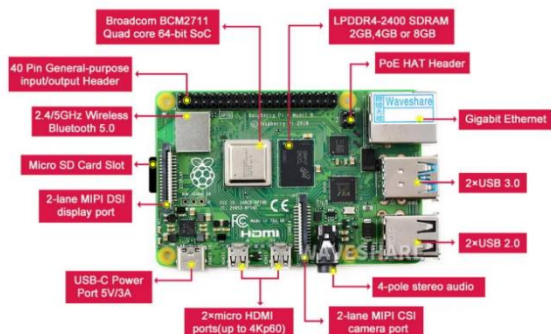


Рис. 6. Интерфейсы Raspberry Pi 4

Система демонстрирует высокую экономическую эффективность — общая стоимость аппаратных компонентов приведена в таблице 2. При этом решение обеспечивает точный мониторинг состояния металлоконструкций с возможностью раннего выявления дефектов, что позволяет значительно сократить эксплуатационные расходы и предотвратить аварийные ситуации.

При проектировании системы мониторинга металлических поверхностей необходимо тщательно рассчитать количество и расположение радиоволновых датчиков. Этот процесс требует комплексного подхода, учитывающего как технические параметры оборудования, так и особенности контролируемого объекта.

ТАБЛИЦА 2. Стоимость аппаратной части

| Оборудование                                | Количество | Стоимость за ед. | Общая стоимость |
|---------------------------------------------|------------|------------------|-----------------|
| Радиоволновой датчик (AD9361)               | 10         | \$200            | \$2000          |
| Микроконтроллер (ESP32-H2)                  | 10         | \$10             | \$100           |
| Антенна (Zigbee)                            | 10         | \$5              | \$50            |
| Координатор-шлюз (Raspberry Pi 4 и CC2652P) | 1          | \$70             | \$70            |
| Сервер (локальный или облачный)             | 1          | \$500            | \$500           |
| ИТОГО:                                      | \$2720     |                  |                 |

Основой для расчетов служат характеристики самих датчиков. Ключевыми параметрами являются рабочая частота, определяющая глубину сканирования и разрешающую способность, зона эффективного покрытия и угол обзора. Например, датчик с частотой 2.4 ГГц обеспечивает высокую точность обнаружения поверхностных дефектов, но имеет ограниченную глубину проникновения. Угол обзора варьируется от  $30^\circ$  у узконаправленных моделей до  $90^\circ$  у широкоугольных, что напрямую влияет на рекомендуемое расстояние установки от поверхности – от 10-30 см для первых до 20-50 см для вторых. Если датчик имеет угол обзора  $\theta$  и максимальное расстояние обнаружения  $R$ , то зона покрытия (площадь)  $A$  может быть рассчитана по формуле  $A = \pi \left( \frac{R \cdot \tan \frac{\theta}{2}}{2} \right)^2$  (если  $\theta = 30^\circ$ , то  $A \approx 0,07 \cdot R^2$ , если  $\theta = 90^\circ$ , то  $A \approx 0,79 \cdot R^2$ ).

Не менее важны характеристики самой поверхности: ее общая площадь, геометрическая форма (плоская, изогнутая или сложной конфигурации), а также типы и размеры дефектов, которые необходимо обнаруживать. Для плоских поверхностей оптимальным является равномерное расположение датчиков с перекрытием зон действия на 10-20 %. Такой подход не только повышает точность измерений, но и обеспечивает отказоустойчивость системы – при выходе из строя одного датчика его функции частично берут на себя соседние устройства.

Если площадь поверхности равна  $S$ , а зона перекрытия  $m$  ( $0 \leq m \leq 1$ ), то количество необходимых датчиков можно рассчитать по формуле  $N = \frac{S}{A \cdot (1-m)}$ . Для сложных геометрических форм рекомендуется увеличивать плотность размещения датчиков в зонах повышенной кривизны, где вероятность возникновения дефектов обычно выше.

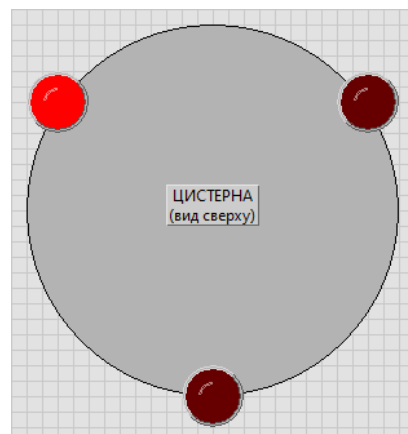


Рис. 7. Расположение датчиков на резервуаре

Для визуализации и тестирования различных конфигураций размещения датчиков была успешно применена среда LabView. На рис. 7 обозначена схема предположительного объекта наблюдения. После выявления дефекта, индикатор показывает, в каком конкретно месте обнаружилось

повреждение, для его оперативного устранения. На рис. 8, 9 приведен интерфейс и логика работы одного датчика. Здесь видно, как схема работает «под капотом». У каждого датчика есть входные параметры, график исходного сигнала, а также графики с примененным Быстрым преобразованием Фурье и фильтром Калмана. При «улавливание» датчиком какой-то аномалии, его индикатор активируется.

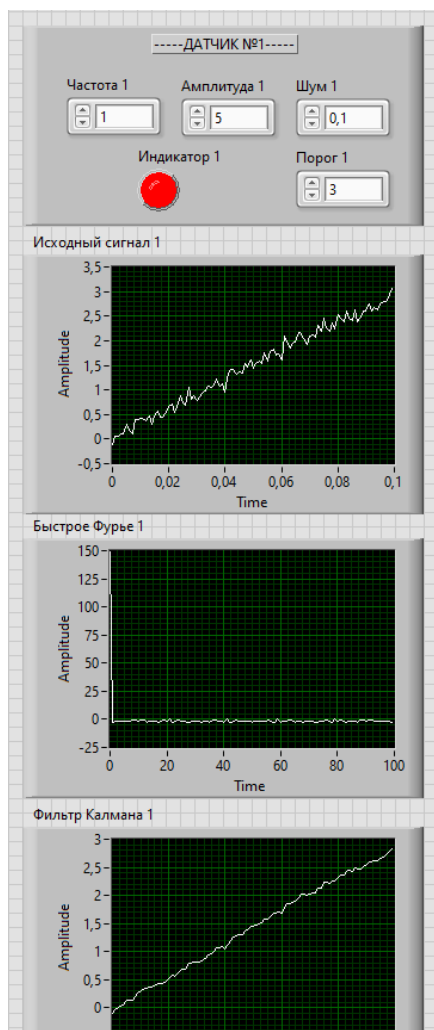


Рис. 8. Интерфейс одного датчика

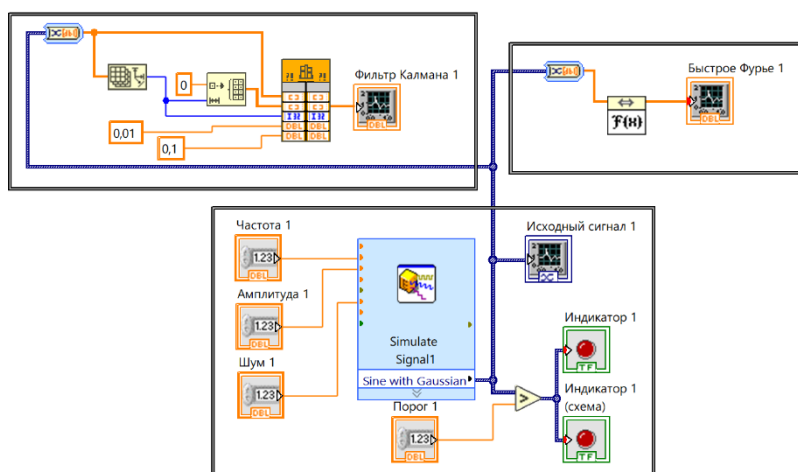


Рис. 9. Логика работы датчика

## Заключение

В ходе выполнения данной работы была разработана методика уведомления о появлении повреждений и дефектов на металлических поверхностях в реальном времени. Основывается она на анализе характера отражения радиоволн от наблюдаемых объектов. Система обладает крайне высокой автономностью и невысокой себестоимостью, имея хорошую точность и регулируемую глубину анализа. Был проанализирован рынок уже существующих продуктов и программного обеспечения в данной отрасли, а также изучены основные методы, на основе которых реализованы данные продукты. Затем были выбраны и описаны наиболее подходящие методы по цене и качеству. А в конце описана работа всей системы.

Помимо всех приведенных выше качеств данного проекта, стоит также отменить проблему, которую он решает. Описанная система способна значительно уменьшить убытки на предприятиях, возникающие из-за несвоевременного обнаружения износа разного рода на металлических поверхностях, особенно в критически важных узлах. Система заблаговременно уведомит об ухудшении состояния наблюдаемых объектов и позволит заранее позаботиться о ремонте, уменьшив риски, избавившись от неожиданных нежелательных ситуаций.

## Список используемых источников

1. Шаранова Д. А. Бесконтактные методы выявления питтинговых дефектов стенок металлических изделий // Территория «НЕФТЕГАЗ». 2016. № № 10. С. 34-40.
2. Неразрушающий контроль: способы и приборы. URL: <https://litas.ru/blog/stati/nerazrushayushchiy-kontrol-sposoby-i-pribory/> (дата обращения 02.04.2025).
3. Дефектовка металлов // URL: <https://nova78.ru/defektoskopiya-v-metallov/> (дата обращения 03.04.2025).
4. Балонин Н. А., Сергеев М. Б. Беспроводные персональные сети на основе ZigBee/ учебное пособие. СПб: ГУАП, 2012. 58 с.
5. National Instruments // Документация к среде LabView. URL: <https://www.ni.com/docs/en-US/category/labview-docs> (дата обращения 04.2025).

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Дагаевым А. В.*

УДК 531/532.1

А. Д. Сидоров (студент группы ИКТ-413, СПбГУТ), [sidorov.ad@sut.ru](mailto:sidorov.ad@sut.ru)

## **ЦИФРОВИЗАЦИЯ ЛАБОРАТОРНОЙ РАБОТЫ «ИССЛЕДОВАНИЕ АПЕРИОДИЧЕСКОГО РАЗРЯДА КОНДЕНСАТОРА. ОПРЕДЕЛЕНИЕ ЕМКОСТИ КОНДЕНСАТОРА»**

*В статье описана методика реализации программы на базе Microsoft Excel и онлайн-интерпретатора Google Colab, предназначенная для цифровизации лабораторной работы «Исследование апериодического разряда конденсатора. Определение емкости конденсатора». Основная цель работы – автоматизация и ускорение обработки экспериментальных данных, получаемых при исследовании процесса разрядки конденсатора через сопротивление, а также визуализация ключевых характеристик цепи.*

*Программа позволяет рассчитать основные параметры разряда. На основе введенных экспериментальных данных программа визуализирует графики зависимости силы тока и ее логарифма от времени, что способствует более наглядному и глубокому анализу результатов.*

*Использование цифровых инструментов значительно упрощает анализ результатов, снижает вероятность ошибок, связанных с ручными вычислениями.*

*цифровизация, лабораторная работа, разряд конденсатора, обработка данных, визуализация, Microsoft Excel, Google Colab*

### **Введение**

Цифровизация образовательного процесса требует внедрения современных инструментов для автоматизации лабораторных работ, особенно в области физики, где обработка экспериментальных данных занимает значительное время. Целью данной работы является создание программы, обеспечивающей цифровизацию лабораторного эксперимента по исследованию апериодического разряда конденсатора, что позволяет повысить качество обучения и упростить анализ данных [1].

### **Методика и программная реализация**

Цифровизация лабораторной работы реализована с помощью интеграции шаблона Microsoft Excel для ввода и предварительной обработки экспериментальных данных и набора скриптов на языке Python, выполняемых в среде онлайн интерпретатора Google Colab. Экспериментальные значения силы тока и времени вносятся в Excel, а затем импортируются в Google Colab с помощью библиотеки pandas, что обеспечивает удобную работу с табличными структурами и гибкость дальнейшей обработки [2, 3].

В ходе анализа применяется линейная регрессия из модуля `scipy.stats.linregress` для построения графика зависимости логарифма силы тока от времени, что позволяет определить временную константу цепи и емкость конденсатора [4]. Для аппроксимации экспериментальных данных и построения гладких кривых используются функции `numpy`, такие как `polyfit` и `polyval`. Это обеспечивает не только визуализацию процесса разряда, но и выделение ключевых параметров, характеризующих исследуемую цепь. Для получения промежуточных значений между экспериментальными точками применяется интерполяция посредством функции `scipy.interpolate.interp1d`, что позволяет строить плавные кривые и более точно определять характеристики процесса.

Визуализация осуществляется с помощью библиотеки `matplotlib.pyplot` [5]. На графиках (рис. 1) отображаются экспериментальные точки и аппроксимирующие кривые. Такой подход облегчает интерпретацию данных, позволяет проводить сравнительный анализ различных серий экспериментов и минимизирует влияние субъективного фактора при анализе результатов. Комплексное использование современных библиотек и алгоритмов обеспечивает точность и наглядность анализа экспериментальных данных.

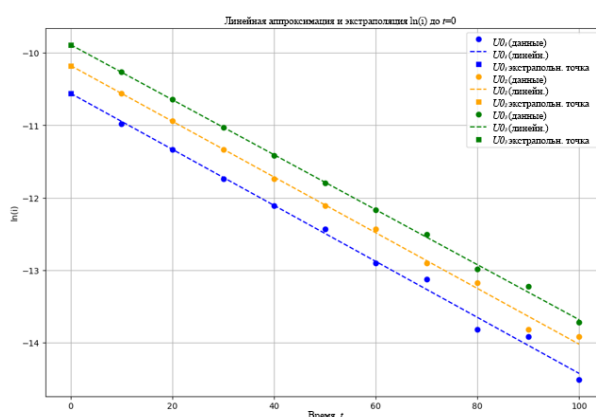


Рис. 1. График зависимости натурального логарифма силы тока от времени

## Преимущества цифрового подхода

Использование современных библиотек и алгоритмов позволяет существенно снизить вероятность ошибок, связанных с ручными вычислениями, учесть как систематические, так и случайные погрешности измерений, а также проводить экстраполяцию для более точного определения параметров источника. Автоматизация обработки данных способствует более глубокому анализу и экономии времени студентов, а интуитивный интерфейс облегчает освоение инструментов.

## Заключение

Разработанная система цифровизации лабораторной работы по исследованию апериодического разряда конденсатора продемонстрировала свою эффективность в учебном процессе. Она позволяет повысить точность и наглядность анализа, облегчить выполнение лабораторных работ студентами и упростить проверку работ преподавателями. Внедрение цифровых технологий способствует развитию у студентов навыков работы с современными инструментами анализа данных и формирует компетенции, востребованные в современной науке и технике.

## Список используемых источников

1. Андреев А. Д., Деткова В. М., Долматова О. А., Передистов Е. Ю., Шарихина Ю. В.. Физика. Электричество. Учебно-методическое пособие по выполнению лабораторных работ СПбГУТ. Санкт-Петербург, 2020.
2. Хан Дж., Пейн Дж. Python для анализа данных: обработка, анализ и визуализация данных с использованием библиотек NumPy, Pandas и Matplotlib. СПб.: Питер. 2018. 464 с.
3. Маккинни У. Python для анализа данных: эффективное использование Pandas, NumPy и IPython. М.: Вильямс, 2017. 450 с.
4. О'Рейли Т. Научные вычисления с Python: использование NumPy, SciPy и Matplotlib. М.: Диалектика, 2015. 350 с.
5. Хан Дж. Визуализация данных с Matplotlib: создание графиков и диаграмм в Python. СПб.: Питер, 2019. 320 с.

*Статья представлена научным руководителем, доцентом кафедры СПбГУТ кандидатом физико-математических наук Детковой В. М.*



УДК 621.372.54

Д. П. Смирнов (магистрант группы РТ-42м, СПбГУТ), [smirnov.dp@sut.ru](mailto:smirnov.dp@sut.ru)**ОБЗОР МЕТОДОВ ВНЕСЕНИЯ ПРЕДЫСКАЖЕНИЯ**

*Данная работа рассматривает различные методы внесения предискажения, применение различных методов, особенности каждого метода, перспективы развития различных методов внесения предискажения, их положительные и отрицательные стороны.*

*цифровое предискажение, линейное предискажение, нелинейное предискажение*

Предискажение (предкоррекция) – это преднамеренное искажение сигнала перед передачей для компенсации известных искажений в тракте передачи или приема. В радиосистемах оно применяется для улучшения отношения сигнал/шум (SNR) за счет подавления высокочастотных шумов, компенсации нелинейностей усилителей мощности (РА), борьбы с межсимвольной интерференцией (ISI) в цифровых системах и оптимизации спектральной эффективности.

Существует 3 метода внесения предискажения (таблица 1):

ТАБЛИЦА 1 Методы внесения предискажения

| Название                 | Способы взаимодействия                                                        |
|--------------------------|-------------------------------------------------------------------------------|
| Линейное предискажение   | сигнал умножается на коэффициент, чтобы компенсировать нелинейность           |
| Нелинейное предискажение | использует сложные функции, чтобы компенсировать нелинейности                 |
| Цифровое предискажение   | использует цифровые алгоритмы для создания и применения функции предискажения |

Целью работы является разбор каждого метода внесения предискажения.

Линейные предискажения применяются для компенсации частотно-зависимых искажений в каналах связи. Их эффективность зависит от типа канала, характеристик сигнала и применяемых методов коррекции.

Они усиливают высокочастотные компоненты сигнала до передачи, чтобы компенсировать их ослабление в канале (например, из-за затухания в кабеле или фильтрации в радиочастотах).



В аналоговые системах (FM-радио, DSL, коаксиальные линии) улучшается отношение сигнал/шум (SNR) на приемной стороне за счет выравнивания спектра, в FM-радио дает до 10–15 дБ улучшения помехоустойчивости на высоких частотах и в DSL (xDSL) компенсирует затухание в витой паре, повышая скорость передачи, но также усиливается высокочастотный шум, в связи с этим требуется точное согласование с декорректирующим фильтром на приемнике.

Линейные предискажения эффективно работают в каналах с четко выраженным частотным затуханием (кабельные линии, FM-радио), в высокоскоростных цифровых интерфейсах с ограниченной полосой и в системах с фиксированными характеристиками канала (DSL, оптика с известной дисперсией) и неэффективны или требуют дополнения в: сильно нелинейных каналах (нужна DPD), быстро меняющихся беспроводных каналах и при очень широкой полосе частот (сложно обеспечить равномерную коррекцию).

ТАБЛИЦА 2 Преимущества и недостатки LPD

|              | Характеристика                           | Пояснение                                                                                                                                       |
|--------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Преимущества | Простота реализации                      | LPD относительно просто реализовать, особенно в сравнении с нелинейными методами предискажения                                                  |
|              | Низкая сложность вычисления              | Для LPD не требуются сложные вычисления, что делает их пригодными для реального времени                                                         |
|              | Низкие затраты на проектирование         | Простые в реализации и не требующие больших вычислительных ресурсов методы LPD могут быть более экономичными, чем нелинейные методы             |
| Недостатки   | Малоэффективен при сильных нелинейностях | LPD не может эффективно компенсировать сильные нелинейные искажения, такие как клиппинг или переходные искажения                                |
|              | Ограниченная точность                    | Линейные модели не могут точно описывать сложные нелинейные характеристики усилителей мощности, что ограничивает точность компенсации искажений |
|              | Ограниченная область применения          | LPD используется исключительно в системах с незначительными нелинейными искажениями, где высокая точность компенсации не является необходимой   |

Нелинейные предискажения (Nonlinear Pre-distortion, NPD) сигнала применяются с использованием более сложных алгоритмов, которые принимают во внимание нелинейные характеристики усилителя мощности. В отличие от линейных предискажений, NPD не просто добавляет линейный сигнал к исходному, а использует нелинейные функции для моделирования и компенсации искажений [1].

Существует 2 метода создания нелинейных предискажений (табл. 2).

ТАБЛИЦА 3 Преимущества и недостатки NPD

| Тип        | Особенности                                                                  | Применение                                                                       |
|------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Аналоговые | Проще в реализации, но менее гибкая                                          | Радиорелейных системах                                                           |
|            | Улучшает ACPР (Adjacent Channel Power Ratio) на 6-12 дБ                      | Аналоговых РЧ трактах                                                            |
|            |                                                                              | Резервных схемах параллельно с DPD                                               |
| Цифровые   | Улучшает ACPР на 15-30 дБ                                                    | В 5G mMIMO DPD обязателен для работы PA с OFDM-сигналами (>100 MHz)              |
|            | Повышает EVM (Error Vector Magnitude) в 2-5 раз                              | В Wi-Fi 6E DPD обеспечивает соответствие спектральным маскам при 160 МГц каналах |
|            | Позволяет усилителям работать ближе к насыщению (увеличивает КПД на 10-20 %) | В спутниковой связи компенсирует нелинейности TWTА усилителей                    |

Нелинейные предискажения показывают наибольшую эффективность в следующих случаях:

1. В мощных РЧ усилителях (РА) с высоким уровнем нелинейности.
2. При работе с широкополосными сигналами (OFDM, широкополосные модуляции).
3. В системах с жесткими требованиями к спектральной чистоте.

Они также избыточны в случае использования узкополосных систем с низким PAPR (например, FM-радио), в низкомощных трактах (до 1 Вт) часто не окупаются и требуют точной калибровки и адаптации.

Наиболее перспективным направлением развития нелинейных предискажений являются гибридные системы (аналоговая предкоррекция +

DPD) в сочетании с машинным обучением для адаптивного управления параметрами.

Цифровое предискажение сигнала (Digital Pre-distortion, DPD) представляет собой метод, применяемый для компенсации нелинейных искажений, возникающих в радиочастотных системах. DPD использует цифровые фильтры для моделирования нелинейных характеристик усилителя и внедрения «обратного искажения» в исходный сигнал. DPD применяет цифровые фильтры для моделирования нелинейности усилителя и добавления «обратного искажения» в исходный сигнал [2].

Основными компонентами DPD является аппаратная платформы реализуемые на FPGA или специализированных DSP (например, TI GC5322) требующих производительность 10-100 GMAC/s для сигналов 5G NR и задержкой обработки  $<1$  мкс в критичных системах, математические модели (Memoryless Polynomial (до 7 порядка), Memory Polynomial (MP), Generalized Memory Polynomial (GMP), Volterra Series (для систем с глубокой памятью)) и адаптивные алгоритмы (LMS/NLMS (до 50 MHz полосы), RLS (для широкополосных систем), субполосная обработка (для сигналов  $>200$  MHz)).

Физическая суть метода основана на обратной математической модели нелинейности РА и адаптивном механизме коррекции [3].

Современные архитектуры реализации DPD делятся на 3 вида (табл. 4).

ТАБЛИЦА 4 Виды реализации DPD

| Вид                                | Особенности                                                          |
|------------------------------------|----------------------------------------------------------------------|
| FPGA-based (Xilinx RFSoc)          | Плюсы: гибкость, параллельная обработка                              |
|                                    | Минусы: высокая мощность ( $>10$ Вт)<br>Частотный диапазон: до 8 GHz |
| Специализированные DSP (TI GC5322) | Плюсы: оптимизированное энергопотребление                            |
|                                    | Минусы: ограниченная полоса ( $\sim 200$ MHz)<br>Задержка: $<500$ ns |
| Гибридные решения                  | Аналоговая предкоррекция + DPD                                       |

Современные системы DPD демонстрируют исключительную эффективность в широкополосных радиосистемах, обеспечивая улучшение линейности на 15-30 dB, повышение энергоэффективности на 10-25 % и снижение общей стоимости системы.

Таким образом можно сделать следующие выводы:

1. Нелинейное предискажение является наиболее эффективным, так как позволяет компенсировать более широкий спектр нелинейных искажений и применим в большинстве сложных систем. Также данный метод является наиболее универсальным, что позволяет применять его в любых условиях и для любой мощности.

2. Линейные предискажения эффективны в простых системах из-за малых затрат на разработку.

3. Цифровые предискажения применяются в мобильных устройствах, где важны малые размеры устройства.

#### **Список используемых источников**

1. Tikhonov V. Yu. Comparison of nonlinear distortion compensation methods in power amplifiers / V. Yu. Tikhonov, A. R. Abdipour // Synchroninfo Journal. 2023. Vol. 9. № 5. PP. 2-8. DOI:10.36724/2664-066x-2023-9-5-2-8. EDN:FLXEDN.

2. Digital predistortion for RF power amplifiers: State of the art and advanced approaches URL: [https://www.researchgate.net/publication/261310345\\_Digital\\_predistortion\\_for\\_RF\\_power\\_amplifiers\\_State\\_of\\_the\\_art\\_and\\_advanced\\_approaches](https://www.researchgate.net/publication/261310345_Digital_predistortion_for_RF_power_amplifiers_State_of_the_art_and_advanced_approaches) (дата обращения 13.11.2024).

3. A Generalized Memory Polynomial Model for Digital Predistortion of RF Power Amplifiers // URL: [https://www.researchgate.net/publication/3319867\\_A\\_Generalized\\_Memory\\_Polynomial\\_Model\\_for\\_Digital\\_Predistortion\\_of\\_RF\\_Power\\_Amplifiers](https://www.researchgate.net/publication/3319867_A_Generalized_Memory_Polynomial_Model_for_Digital_Predistortion_of_RF_Power_Amplifiers) (дата обращения 13.11.2024).

*Статья представлена научным руководителем, доцентом кафедры БТС СПбГУТ, кандидатом технических наук Прасоловым А. А.*

УДК 004.891

**А. С. Чернышов** (аспирант кафедры систем автоматизации и робототехники, СПбГУТ), [chernyshov.as@sut.ru](mailto:chernyshov.as@sut.ru)

## ИССЛЕДОВАНИЕ И РАЗРАБОТКА RAG-СИСТЕМЫ ДЛЯ ИЗВЛЕЧЕНИЯ И АНАЛИЗА ПРОСТРАНСТВЕННОЙ ИНФОРМАЦИИ ИЗ ТЕКСТОВЫХ ДАННЫХ

*Одной из ключевых проблем современных геоинформационных систем (ГИС) является ограниченная возможность извлечения информации о географических объектах на основе анализа текстовых описаний с учетом контекстуальных связей. В данной работе рассматривается разработка системы Retrieval-Augmented Generation (RAG), которая объединяет эффективный поиск по текстовым источникам с использованием векторных баз данных, контекстный анализ на основе больших языковых моделей (LLM) и методы промпт-инжиниринга для генерации релевантной информации пользователю. Предлагаемая архитектура позволяет значительно повысить точность и полноту извлекаемой информации о геообъектах за счет интеграции современных технологий обработки естественного языка и семантического поиска.*

*геосистемы, искусственный интеллект, языковые модели, RAG*

Современные геоинформационные системы сталкиваются с фундаментальной проблемой – невозможностью эффективно извлекать пространственные данные из неструктурированных текстовых источников. Традиционные алгоритмы обработки естественного языка часто оказываются слишком жесткими для работы с контекстуальными связями между географическими объектами, что особенно критично при анализе социально-экономических процессов, городского планирования или экологического мониторинга.

В этом контексте особый интерес представляют гибридные системы Retrieval-Augmented Generation [1], сочетающие семантический поиск по векторным представлениям текста с генеративными возможностями больших языковых моделей [2, 3] (рис. 1.). Такие системы позволяют не только находить релевантные фрагменты в документах, но и интерпретировать их в заданном контексте, формируя осмысленные выводы о пространственных отношениях.

Ключевая ценность предлагаемого подхода заключается в его адаптивности. В отличие от статических ГИС-решений, RAG-архитектура способна

работать с постоянно обновляемыми источниками – законодательными актами, отчетами подрядчиков, новостными лентами и даже пользовательскими заметками в социальных сетях. Это особенно важно для задач оперативного управления территориями, где актуальность данных часто имеет решающее значение.

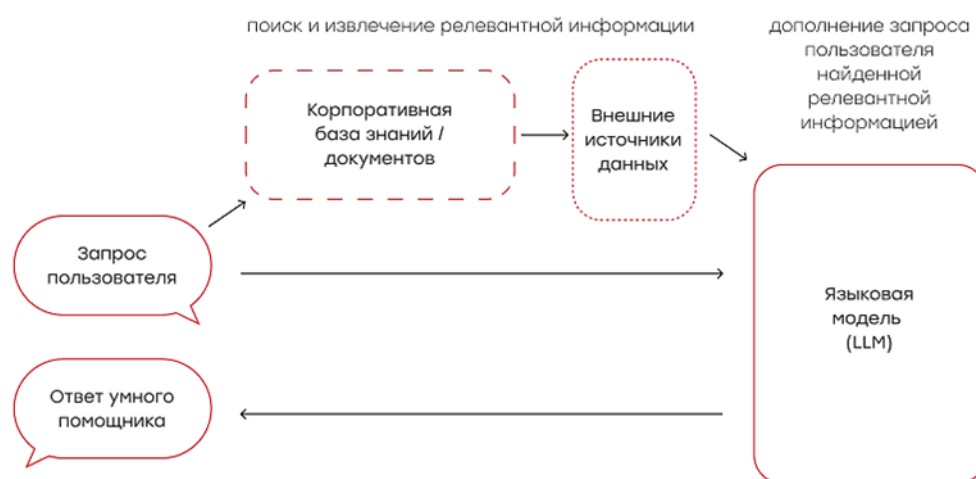


Рис. 1. Схема разработанной Retrieval-Augmented Generation системы

При разработке системы были выявлены следующие проблемы. Во-первых, проблема неоднозначности географических названий требует сложного контекстуального процесса разрешения лексической многозначности – например, различия между «Парком Победы» в Москве и Санкт-Петербурге. Во-вторых, пространственные отношения в текстах часто выражаются имплицитно через грамматические конструкции, что затрудняет их машинный анализ. Наконец, динамический характер многих географических феноменов требует постоянного обновления знаний системы.

Рассмотренный подход к решению этих проблем включает трехэтапную архитектуру. На первом этапе специализированные эмбединговые модели преобразуют как пользовательские запросы, так и корпус документов в векторное пространство. Для этого используются тонко настроенные версии sentence-transformers векторных баз данных, оптимизированные для распознавания географических терминов. Второй этап предполагает гибридный поиск по векторной базе данных с дополнительной фильтрацией по временным меткам и типу источника.

Наиболее сложным оказался этап генерации ответов, где классические LLM часто допускают «галлюцинации» при работе с пространственными

данными. Для минимизации этих ошибок разработана система контекстных промптов [4, 5].

Практическая проверка системы проводилась на задаче анализа административного деления Санкт-Петербурга. В отличие от прямой генерации через LLM, дававшей ошибку в определении количества районов, RAG-система корректно идентифицировала все 18 территориальных единиц [6], дополнив ответ данными об их границах из OpenStreetMap [7] (рис. 2).

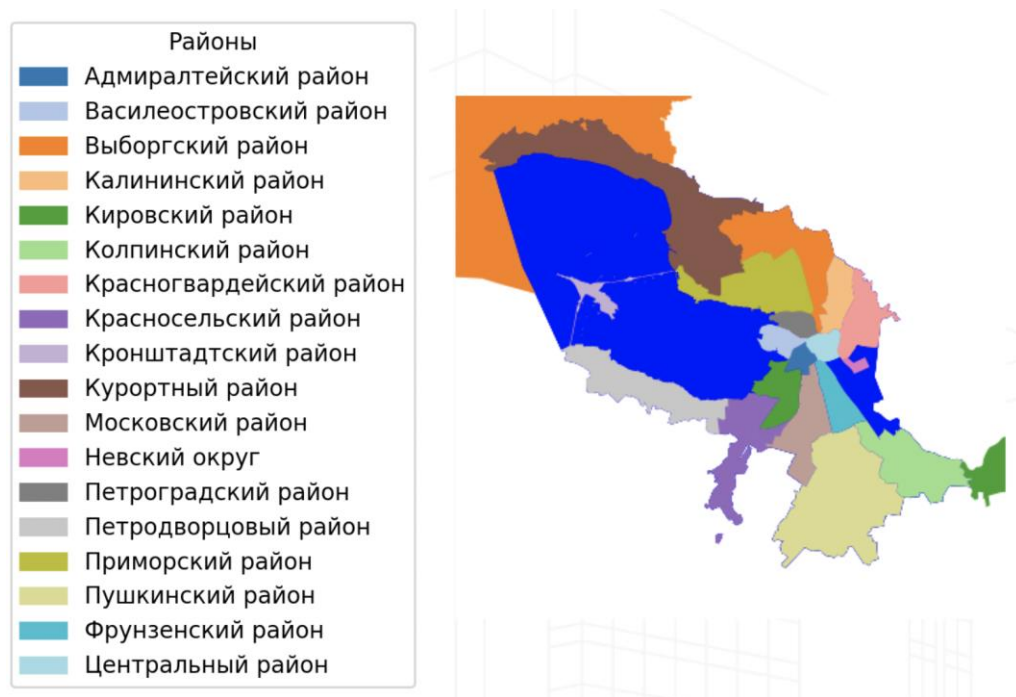


Рис. 2. Результат районирования Санкт-Петербурга основанного на текстовых корпусах

Перспективы развития системы видятся в нескольких направлениях. Интеграция с потоковыми API новостных агрегаторов позволит отслеживать изменения инфраструктуры в режиме, близком к реальному времени. Разработка специализированных онтологий для разных типов пространственных данных (транспортные сети, гидрография, зонирование) повысит точность анализа. Особый интерес представляет адаптация системы для работы с историческими картами и документами, где требуется одновременный учет современных и архаичных топонимов.

Значение этой работы выходит за рамки чисто технической задачи. Создание эффективных инструментов извлечения пространственной информации из текстов открывает новые возможности для междисциплинарных исследований – от цифровой гуманитаристики до урбанистики. В

практическом плане такие системы могут стать основой для следующего поколения интеллектуальных ГИС, способных не только хранить данные, но и активно их пополнять за счет анализа текстовых источников.

Важным направлением дальнейших исследований остается проблема валидации результатов. В отличие от числовых данных, пространственная информация часто допускает множественность интерпретаций. Разработка механизмов оценки достоверности с привлечением экспертных знаний и перекрестных источников представляется ключевой задачей для обеспечения надежности системы в реальных условиях эксплуатации.

### Список используемых источников

1. Dimasklyarov. RAG (Retrieval Augmented Generation) – простое и понятное объяснение // Habr: сайт. 2023. URL: <https://habr.com/ru/articles/779526/> (дата обращения 23.01.2025).
2. IBM. What are large language models (LLMs)? // IBM: сайт. 2023. URL: <https://www.ibm.com/think/topics/large-language-models> (дата обращения 13.01.2025).
3. Sabzalieva E., Valentini A. ChatGPT и искусственный интеллект в высшем образовании. Краткое руководство / Международный институт ЮНЕСКО по высшему образованию в Латинской Америке и Карибском бассейне. UNESCO, 2023. URL: [https://unesdoc.unesco.org/ark:/48223/pf0000385146\\_rus](https://unesdoc.unesco.org/ark:/48223/pf0000385146_rus) (дата обращения 13.01.2025).
4. Яндекс Практикум. Что такое промпт для нейросети и как его составлять // Яндекс Практикум: блог. 2023. URL: <https://practicum.yandex.ru/blog/chto-takoe-prompt-dlya-neyroseti-kak-sozdat/> (дата обращения 17.01.2025).
5. Renze M., Guven E. The Effect of Sampling Temperature on Problem Solving in Large Language Models // arXiv: репозиторий электронных препринтов. 2024. URL: <https://arxiv.org/html/2402.05201v1> (дата обращения 17.01.2025). Лицензия: CC BY 4.0.
6. Закон Санкт-Петербурга от 25 июля 2005 года N 411-68 «О территориальном устройстве Санкт-Петербурга» (с изменениями, внесенными Законом Санкт-Петербурга от 3 апреля 2024 года № 208-50).
7. OpenStreetMap. OpenStreetMap // OpenStreetMap: сайт. 2025. URL: <https://www.openstreetmap.org/> (дата обращения 23.01.2025).

*Статья представлена научным руководителем, профессором кафедры САР СПбГУТ, доктором технических наук Верховой Г. В.*



## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

УДК 004.054

А. Э. Алиев (магистрант группы ИСТ-311м, СПбГУТ), [aliev.ae@sut.ru](mailto:aliev.ae@sut.ru)

### АНАЛИЗ ТРАНСФОРМАЦИИ РЫНКА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ САНКЦИОННОГО ДАВЛЕНИЯ

*В последние годы рынок информационных технологий стал одним из ключевых индикаторов устойчивости и адаптивности национальной экономики в условиях глобальных вызовов. С 2022 года российский ИТ-сектор оказался под мощным давлением внешнеэкономических ограничений, включая масштабные санкции со стороны западных стран. Эти обстоятельства привели к резкому изменению условий функционирования отрасли, вызвали уход иностранных компаний, ограничили доступ к критически важным технологиям и программному обеспечению, а также спровоцировали необходимость в ускоренной трансформации инфраструктуры и бизнес-моделей. В данной статье исследуются вопросы осмысления процессов, происходящих на ИТ-рынке в условиях санкционного давления, а также важность разработки подходов, направленных на обеспечение его устойчивости и развития в новых реалиях.*

*трансформация, ИТ-рынок, анализ, НИОКР, адаптация, превентивные меры*

Трансформация российского рынка информационных технологий (далее ИТ) в последние годы происходит под влиянием совокупности факторов внутреннего и внешнего характера [1]. Главным внешним фактором является санкционное давление, повлекшее ограничение доступа к зарубежным технологиям, финансированию, программному обеспечению и оборудованию. Одновременно усилилось давление со стороны международной конкуренции и глобальной технологической политики.

Среди внутренних факторов можно выделить рост потребности в цифровой независимости, усилия государства по развитию импортонезависимых решений, повышение роли ИТ в обеспечении экономической безопасности, а также ускоренное развитие внутреннего спроса на отечественные продукты в результате ухода зарубежных компаний. Эти процессы обозначают переход от модели потребления внешних решений к модели развития собственных платформ и экосистем, что и определяет вектор трансформации отрасли.

Барьеры развития российского ИТ-рынка включают в себя технологическую зависимость от импорта, нехватку критически важного оборудования, отток кадров, снижение инвестиционной активности и замедление научного обмена с международным сообществом. Также наблюдаются институциональные препятствия: фрагментированность политики цифровизации, недостаточная гибкость регулирования, ограниченный доступ малого и среднего бизнеса к ресурсам [2].

В то же время драйверами развития становятся поддержка со стороны государства, расширение программ импортозамещения, мобилизация внутреннего научного потенциала, развитие образовательных инициатив и резкое повышение спроса на российские ИТ-продукты. Особое значение приобретает активизация внутреннего рынка, развитие открытых решений и формирование новых цифровых коопераций внутри страны.

В условиях нарастания внешнеэкономического давления и необходимости ускоренного развития собственной технологической базы, опыт стран, которые ранее сталкивались с ограничениями на международной арене и при этом сумели выстроить устойчивую, конкурентоспособную ИТ-отрасль, представляет особую ценность [3]. Примеры Китая и Южной Кореи демонстрируют, как при грамотной стратегической политике и долгосрочной ориентации на суверенитет в критических отраслях государство способно трансформировать внешние вызовы в стимул для внутреннего развития.

Китайский опыт можно считать наиболее масштабным примером успешной национальной цифровой трансформации. В течение последних двух десятилетий Китай последовательно реализует стратегию, направленную на достижение технологической независимости и лидерства в цифровом пространстве. Ключевыми направлениями стали локализация программного обеспечения, формирование собственной экосистемы интернет-сервисов и массовая поддержка высокотехнологичных стартапов. В ответ

на ограничения со стороны США в части телекоммуникационного оборудования, мобильных технологий и полупроводников, Китай активизировал инвестиции в национальную микроэлектронику, усилил поддержку НИОКР, начал развивать собственную архитектуру процессоров (например, Loongson и Zhaoxin) и внедрил масштабные государственные программы, такие как «Made in China 2025» и «China Standards 2035». На примере Huawei, Alibaba, Tencent и Baidu можно наблюдать, как компании, ранее зависимые от западных технологий, смогли за сравнительно короткий срок сформировать конкурентоспособные альтернативы. Китайские операционные системы (Kylin OS, HarmonyOS), национальные базы данных, облачные платформы и платежные системы (WeChat Pay, Alipay) активно внедряются в государственный и частный секторы, вытесняя иностранные решения. Также важно отметить, что Китай развивает внутреннюю нормативную и правовую среду, поддерживающую локальных производителей – включая приоритет в госзакупках, специальные налоговые режимы и систему грантов для ИТ-стартапов.

Южная Корея демонстрирует синергетическую модель, сочетающую сильную государственную поддержку, развитие крупного частного сектора и научных учреждений. Ключевым фактором успеха стала высокая концентрация инвестиций в НИОКР, развитие цифровой инфраструктуры и обучение населения цифровым навыкам. Компании, такие как Samsung и LG, являются не только крупнейшими экспортерами электроники, но и разработчиками уникальных технологических решений, в том числе в области микропроцессоров, дисплеев, телекоммуникационного оборудования и мобильных операционных систем.

Южная Корея в числе первых внедрила массовый доступ к широкополосному интернету, продвигая концепцию «умного государства» и интеграцию ИТ-решений в повседневную жизнь граждан. Благодаря тесному взаимодействию между государством, научной средой и индустрией, а также ориенту на экспортноориентированную цифровую экономику, стране удалось достичь одного из самых высоких уровней цифровой зрелости и ИТ-компетентности населения в мире. При этом Корея активно участвует в международных технологических альянсах, сохраняя гибкость и конкурентоспособность на глобальной арене.

Таким образом, опыт Китая и Южной Кореи показывает, что, несмотря на различия в стратегиях, каждая из стран достигла высокого уровня разви-

тия ИТ-отрасли благодаря сочетанию следующих факторов: системный государственный подход, приоритетные национальные программы, долгосрочные инвестиции в НИОКР, поддержка образования и ориентация на внутренний рынок либо экспортные модели. Эти примеры демонстрируют, что внешние ограничения не являются приговором для технологического сектора, а при грамотной политике могут стать толчком к глубокой трансформации и развитию.

В мировой практике существует ряд примеров, где воздействие санкционного давления, недостаточная внутренняя подготовка и слабые институциональные механизмы привели к стагнации или упадку национального ИТ-сектора. Изучение таких кейсов – как негативных моделей развития в условиях международной изоляции – позволяет вычленить системные ошибки и избежать их повторения при построении собственной стратегии технологической трансформации. Наиболее показательные примеры в этом контексте – Венесуэла и Иран.

Случай Венесуэлы иллюстрирует, как политическая нестабильность, гиперинфляция, разрушение рыночных институтов и международная изоляция в совокупности могут парализовать цифровое развитие страны. После введения многолетних санкций со стороны США и ЕС, сопровождающихся внутренними экономическими кризисами, венесуэльский ИТ-рынок оказался в глубоком упадке. Массовый отток специалистов, практически полное отсутствие иностранных инвестиций, устаревшее оборудование и программное обеспечение, невозможность закупки современных технологий – все это сформировало замкнутую, низкоэффективную и фрагментарную ИТ-среду, неспособную к саморазвитию.

Несмотря на попытки внедрения отдельных государственных программ цифровизации, таких как развитие электронного правительства, венесуэльская модель не смогла преодолеть институциональные и экономические барьеры. Отсутствие четкой технологической стратегии, слабая защита прав собственности, дефицит инфраструктуры и непрозрачные условия ведения бизнеса фактически исключили страну из глобальной цифровой экономики. Венесуэла так и не смогла сформировать устойчивую ИТ-экосистему, пригодную для масштабного импортозамещения, не говоря уже о технологической независимости.

Иран – другой яркий пример страны, длительное время находящейся под международными санкциями, но пытающейся реализовать собственную модель развития ИТ-отрасли в условиях внешней изоляции. В отличие

от Венесуэлы, Иран обладает более устойчивой научно-инженерной базой и развитой системой высшего образования. Однако его попытки построения национального цифрового суверенитета натолкнулись на ряд ограничений. Основные сложности касаются хронического дефицита высокотехнологичного оборудования, слабой интеграции с международными технологическими платформами и ограниченного доступа к программному обеспечению критической важности.

Примером является иранская попытка создать «национальный интернет» (или фильтрованный доступ к глобальной сети), которая привела к снижению цифровой открытости, отставанию в развитии онлайн-сервисов и массовому использованию «теневых» технологий, включая VPN, нелегальные копии ПО и серые каналы поставок оборудования. Несмотря на внутренние усилия по развитию локальных мессенджеров, поисковых систем, систем шифрования и блокчейн-приложений, технологическая база Ирана остается частично не самодостаточной. Давление санкций на финансовые институты, ограничения по трансферу технологий, международная изоляция и отсутствие международной сертификации сдерживают полноценное участие страны в глобальных цифровых процессах.

Обобщая негативные примеры, можно выделить несколько общих черт, препятствовавших успешной адаптации: отсутствие четкой и долгосрочной стратегии цифрового развития, недоверие к частной инициативе, нехватка внутренних ресурсов для развития ИТ-инфраструктуры, неэффективная система подготовки кадров, слабая наука и отсутствие кооперации с внешним миром. Санкции в этих случаях не стали стимулом для модернизации, а напротив – закрепили отставание, усилили технологическую зависимость (в том числе от третьих стран) и создали изолированные цифровые экосистемы, не способные к полноценной интеграции.

Для России анализ подобных моделей представляет практическую ценность. Он показывает, что технологический суверенитет невозможен без устойчивых институтов, поддержки внутренней конкуренции, развития образования и научных исследований, а также гибкой адаптации к вызовам, сопровождаемым инвестициями в инфраструктуру, кадры и локализацию. При наличии таких элементов санкционное давление может стать точкой роста, при их отсутствии – фактором деградации.

Анализ международного опыта показал, что успешная адаптация ИТ-рынка в условиях санкционного давления возможна только при наличии системной, долгосрочной стратегии, сочетающей поддержку государства, активное участие частного сектора и развитую научно-образовательную базу.

Китай и Южная Корея демонстрируют эффективность приоритетного инвестирования в НИОКР, локализацию критических технологий, развитие национального ПО и аппаратных решений, а также подготовку кадров. Их стратегии отличает акцент на формирование внутренней экосистемы и создание экспортного потенциала, а не только на импортозамещение.

В противоположность им, примеры Венесуэлы и Ирана показывают, что при отсутствии институциональной устойчивости, финансовых ресурсов и интеграции с глобальной наукой, санкции приводят к технологической деградации. Замкнутость, недостаток частной инициативы, дефицит оборудования и отток специалистов лишают ИТ-сектор шансов на развитие.

Таким образом, для России важно не копировать чужие модели, а адаптировать лучшие практики, уделяя особое внимание целостности цифровой политики, стимулированию разработок, институциональной гибкости и кадровому потенциалу. Устойчивость в условиях санкций требует не столько отказа от внешнего взаимодействия, сколько концентрации усилий на формировании собственной инновационной среды.

#### **Список используемых источников**

1. Горбунова Е. С., Иванов А. А. Влияние санкций на цифровую трансформацию российского ИТ-сектора // Журнал «Экономика и предпринимательство». 2023. С. 45–52.
2. Petrov K., Smirnov D. Sanctions and IT Market Resilience: Case Studies from Russia and Iran // International Journal of Technology Management, 2022. Vol 89. PP. 234–255.
3. Смирнова В. П. Цифровая экономика: вызовы санкций // Изд-во НИУ ВШЭ. 2023. С. 180–183.

*Статья представлена научным руководителем, кандидатом технических наук., доцентом кафедры ИУС СПбГУТ, доцентом Смородиным Г. Н.*

УДК 004.891

**М. М. Байзигитов** (студент группы ИКПИ-13, СПбГУТ),  
[baizigitov.mm@sut.ru](mailto:baizigitov.mm@sut.ru)

**А. В. Пачин** (к.т.н., доцент кафедры ПИВТ, СПбГУТ)

## ПРИМЕНЕНИЕ МЕТОДОВ ОБЪЯСНИМОГО ИИ ДЛЯ МЕДИЦИНСКОЙ ДИАГНОСТИКИ НА ОСНОВЕ ЛАБОРАТОРНЫХ ДАННЫХ

*В условиях ограниченного доступа к полным медицинским данным и роста нагрузки на систему здравоохранения возрастает необходимость в автоматизированных и интерпретируемых решениях, способных оценивать риски заболеваний на ранних стадиях. В данной работе проводится исследование подходов к разработке системы поддержки принятия врачебных решений, использующей данные общего и биохимического анализа крови, липидного профиля, возраста и пола пациента. Особое внимание уделено обеспечению объяснимости результатов с помощью методов LIME и SHAP, что позволяет не только прогнозировать риск, но и интерпретировать вклад каждого параметра. Проведено сравнение нескольких алгоритмов, выбрана оптимальная модель по совокупности метрик качества. В статье также рассматриваются подходы к работе с неполными данными и предлагается стратегия импутации параметров. Полученные результаты демонстрируют потенциал разработки для применения в клинической практике с целью снижения затрат и повышения точности диагностики.*

*интерпретируемая модель, поддержка принятия решений, лабораторные анализы крови, машинное обучение, SHAP, LIME*

Современная медицина сталкивается с необходимостью быстрой и точной предварительной оценки состояния пациентов. Заболевания различной этиологии встречаются очень часто, и любая задержка диагностики или нецелесообразная процедура увеличивают риски для пациента и нагрузку на систему здравоохранения. Длительное ожидание приема у врача и результатов лабораторных анализов заставляет пациентов обращаться к платным услугам (по данным Согаз, средние ежегодные траты россиян на платную медицину превышают 10 тыс. рублей) [1-3]. При этом ошибочный выбор диагностических исследований увеличивает финансовые и временные затраты. В таких условиях важна быстрая и обоснованная первичная оценка: анализ крови – один из наиболее доступных источников информации о состоянии пациента, позволяющий на ранней стадии заподозрить ряд заболеваний.

Развитие методов искусственного интеллекта и машинного обучения позволяет автоматически анализировать медицинские данные, но возникает

проблема доверия к «черному ящику» модели. Непрозрачность алгоритмов затрудняет принятие решений врачами. В данной работе особое внимание уделено объяснимости решений модели: реализованы механизмы интерпретации прогнозов с помощью алгоритмов SHAP и LIME, позволяющие понять, какие параметры крови и насколько влияют на вывод. Это увеличивает прозрачность системы поддержки решений и способствует повышению доверия врачей к ее результатам. Отметим, что разработанное программное обеспечение предназначено для использования квалифицированными медицинскими специалистами и служит вспомогательным инструментом, не заменяя врачебного диагноза.

Использован клинический датасет по диабету II типа из репозитория Сибирского ГМУ. В работе отобраны 23 часто встречающихся параметра анализов: демографические (возраст, пол) и результаты общеклинического и биохимического анализа крови (например, эритроциты, гемоглобин, нейтрофилы, моноциты, эозинофилы, базофилы, общий билирубин, глюкоза, билирубин прямой, общий белок, АЛТ, АСТ, мочевины, креатинин) и показатели липидного профиля (ХС, ЛПНП, ЛПВП, ЛПОНП). Были сформированы две выборки: пациенты с диагнозом СД2 и без него, отбор выполнен с учетом временного окна. Поскольку наборы параметров варьируются по лабораториям, проведена нормализация и фильтрация: выбраны образцы с не менее чем 14 непустыми признаками. Пропущенные значения заменялись медианой соответствующего показателя – такой подход устойчив к выбросам и отражает типичное значение признака. Для устранения дисбаланса классов применен метод случайного андерсемплинга: из числа «здоровых» случайным образом отобрано столько же записей, сколько было «больных».

Для классификации применены ансамблевые алгоритмы машинного обучения, которые хорошо себя зарекомендовали в медицинских задачах: случайный лес, AdaBoost, градиентный бустинг и XGBoost. Модели обучались на указанном наборе данных, и их качество оценивалось с помощью метрик: accuracy, precision, recall, F1-score и ROC AUC. Для анализа результатов работы моделей использованы методы интерпретации: алгоритм SHAP – SHapley Additive exPlanations – позволяет определить глобальную важность признаков на основе их вклада в предсказания; алгоритм LIME дает локальные объяснения отдельного прогноза, подбирая простую модель в окрестности данного примера. Такой комбинированный подход обеспечивает как общее понимание поведения модели, так и объяснение конкретных классификаций.



В таблице 1 приведены результаты сравнения классификаторов по ключевым метрикам. Наилучшие показатели точности и AUC показал алгоритм градиентного бустинга с показателями Accuracy = 0.875, ROC AUC = 0.949. Модель случайного леса продемонстрировала схожий уровень качества с показателями Accuracy = 0.865, ROC AUC = 0.937. XGBoost и AdaBoost показали чуть более низкие результаты, точность около 86 % и AUC  $\approx$  0.935, но также показали высокую эффективность. Все модели обеспечили достаточную точность для первичного скрининга – более 85 % правильно классифицированных случаев – и хорошо различали классы.

ТАБЛИЦА 1. Сравнительная характеристика качества классификаторов по основным метрикам

| Алгоритм          | Accuracy | Precision | Recall | F1-score | ROC AUC |
|-------------------|----------|-----------|--------|----------|---------|
| Random Forest     | 0.865    | 0.862     | 0.879  | 0.871    | 0.937   |
| XGBoost           | 0.858    | 0.849     | 0.882  | 0.865    | 0.935   |
| AdaBoost          | 0.861    | 0.848     | 0.892  | 0.869    | 0.936   |
| Gradient Boosting | 0.875    | 0.867     | 0.895  | 0.881    | 0.949   |

Анализ интерпретируемости моделей с помощью SHAP показал, что самым значимым признаком для прогноза диабета является уровень глюкозы натощак, за ним следуют триглицериды и липопротеины высокой/низкой плотности, а также концентрация калия и возраст пациента.

Эти результаты соответствуют клиническим данным: повышенный уровень глюкозы и аномалии липидного обмена являются известными факторами риска СД2 [4-6]. Например, даже умеренно повышенная гликемия в нормальном диапазоне ассоциируется с возросшим риском развития диабета, а дисбаланс ЛПВП/ЛПНП свидетельствует об инсулинорезистентности [8-10].

Для каждого конкретного пациента система может выдавать локальные объяснения с помощью LIME. Метод LIME визуализирует, какие именно признаки и в какую сторону повлияли на решение модели для данного примера. Так, например, если при анализе отдельного пациента LIME отмечает, что глюкоза существенно выше порога или ЛПВП существенно ниже нормы, это явится весомым аргументом в пользу диагноза СД2. Полученные

веса можно автоматически преобразовывать в понятный текст и генерировать отчет о классификации. Комбинация SHAP и LIME позволяет врачу увидеть общую логику модели и одновременно получить разъяснения конкретного прогноза. Это делает выводы модели более прозрачными и клинически релевантными, что способствует доверию к системе. Разработано программное обеспечение, интегрирующее обученную модель и механизмы интерпретации. Оно позволяет вводить данные анализов пациента и получать вероятностный прогноз риска диабета вместе с объяснением: в интерфейсе отображаются ключевые факторы. Такая система может служить вспомогательным инструментом для врача при первичном скрининге, помогая определить приоритетные направления диагностики и минимизировать ненужные исследования.

Предложенный подход продемонстрировал высокую эффективность в задаче предсказания риска диабета II типа по результатам анализа крови: ансамблевые модели машинного обучения обеспечивают точность около 86–87 % при достаточной объяснимости решений. Разработанная система имеет технический потенциал для практического применения и может стать доступной альтернативой дорогостоящим коммерческим решениям с аналогичной функцией. Важным преимуществом является прозрачность: сочетание методов SHAP и LIME позволяет формализовать глобальные зависимости и одновременно предоставлять локальные объяснения для каждого пациента. Это способствует доверию как со стороны врачей, так и со стороны разработчиков ИИ, поскольку обоснованность вывода становится понятной. Вместе с тем реальная польза модели ограничена качеством исходных данных: требуется большой репрезентативный клинический датасет для обучения. В российских условиях доступ к крупным размеченным медицинским данным по-прежнему ограничен, что ставит задачу сбора и обогащения локальных баз. Перспективным направлением является использование данных анамнеза и медицинских историй (например, с помощью NLP-методов) для расширения признакового пространства модели. Также актуально исследовать дополнительные методы обработки пропусков и улучшения качества данных. Таким образом, создание интерпретируемой системы поддержки врачебных решений на основе анализа крови позволяет повысить информированность врача при постановке диагноза. Разработанная модель не заменяет медицинский вывод, а служит инструментом поддержки, упрощая предварительную оценку состояния пациента и выделяя

возможные факторы риска. Последующие работы будут направлены на интеграцию дополнительных источников данных и автоматизацию процесса формирования развернутых медицинских отчетов с объяснениями на естественном языке.

### Список используемых источников

1. Пресс-центр «Согаз». Москва, 2023. URL: <https://www.sogaz.ru/sogaz/pressroom/aboutus/852998/> (дата обращения 10.04.2025).
2. Alsheref F., Gooma W. Blood Diseases Detection using Classical Machine Learning Algorithms // Int. J. of Adv. Comp. Sci. and Appl., 2019. Vol. 10. № 7. PP. 2–5.
3. Гусев А. В., Гавриленко Г. Г., Гаврилов Д. В. Разработка модели машинного обучения для интерпретации результатов лабораторной диагностики с целью выявления подозрений на заболевания // Лабораторная служба, 2022, № 2. С. 9–17.
4. Кротова О. С., Хворова Л. А., Пиянзин А. И. Математические модели и алгоритмы машинного обучения в диагностике осложнений сахарного диабета первого типа // Известия Алт. гос. ун-та, 2021. № 1(117). С. 97–101. DOI:10.14258/izvasu(2021)1-16.
5. Gordon J., Lerner B. Insights into Amyotrophic Lateral Sclerosis from a Machine Learning Perspective // J. Clin. Med., 2019. Vol. 8, № 10:1578. DOI:10.3390/jcm8101578.
6. Abdul-Ghani M. A., DeFronzo R. A. Plasma glucose concentration and prediction of future risk of type 2 diabetes // Diabetes Care., 2009. Vol. 32. Suppl 2. S194–S198. DOI:10.2337/dc09-S309.
7. Tirosh A., Shai I. et al. Changes in triglyceride levels over time and risk of type 2 diabetes in young men // Diabetes Care., 2008. Vol. 31. № 10. PP. 2032–2037. DOI:10.2337/dc08-0825.
8. Huang J., Lin H. et al. Association between serum LDL-C concentrations and risk of diabetes: A prospective cohort study // J. Diabetes, 2023. Vol. 15. № 10. PP. 881–889. DOI:10.1111/1753-0407.13440.
9. Haase C. L., Nordestgaard B. G. et al. HDL Cholesterol and Risk of Type 2 Diabetes: A Mendelian Randomization Study // Diabetes, 2015. Vol. 64. № 9. PP. 3328–3333. DOI:10.2337/db14-1603.
10. Chatterjee R., Yeh H.C. et al. Serum and dietary potassium and risk of incident type 2 diabetes mellitus: the ARIC study // Arch. Intern. Med., 2010. Vol. 170. № 19. PP. 1745–1751. DOI:10.1001/archinternmed.2010.362.

УДК 004.41

**С. Н. Баранов** (студент группы ИКПИ-11, СПбГУТ), [baranov.sn@sut.ru](mailto:baranov.sn@sut.ru)

**Е. В. Краева** (старший преподаватель кафедры ПИиВТ, СПбГУТ)

**Д. В. Тарасова** (студент группы ИКПИ-11, СПбГУТ)

## **АВТОМАТИЗАЦИЯ МЕДИЦИНСКИХ ПРОЦЕССОВ В СТОМАТОЛОГИИ: ФУНКЦИОНАЛЬНЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

*Статья посвящена вопросу автоматизации бизнес-процессов в частной стоматологической клинике на основе функционального подхода к проектированию программного обеспечения. Представлено обоснование выбора микросервисной архитектуры. Описана структура информационной системы, включающая модули для трех ключевых ролей: пациента, врача и администратора с разграничением прав доступа и функциональной специализацией. Выполнена оценка предполагаемой эффективности внедрения с использованием метода GOMS.*

*разработка ПО, цифровизация медицины, автоматизация процессов, стоматология, функциональное проектирование, микросервисная архитектура, информационные системы, ролевая модель*

Цифровизация здравоохранения является приоритетным направлением развития информационных технологий. Медицинские учреждения, включая частные стоматологические клиники, сталкиваются с необходимостью повышения эффективности администрирования и обслуживания пациентов [1]. При этом, как правило, существует ряд организационно-технических задач: необходимость централизованного учета записей пациентов, управления расписанием врачей, ведения медицинской документации и контроля расходных материалов. Многие из этих процессов до сих пор выполняются вручную, что снижает общую производительность и увеличивает вероятность ошибок. Одним из способов решения перечисленных задач является внедрение специализированных информационных систем, автоматизирующих основные бизнес-процессы клиники. Целью данной статьи является описание функционального подхода к проектированию программного обеспечения, предназначенного для автоматизации деятельности стоматологической клиники.

Объектом автоматизации выступает частная стоматологическая клиника, в которой необходимо организовать системное взаимодействие между пациентами, врачами и администраторами. Требования к программному обеспечению включают обеспечение непрерывной работы, надежность хра-

нения данных, защиту информации, а также эргономичный пользовательский интерфейс. Система должна обеспечивать регистрацию пользователей, управление расписанием, ведение электронной медицинской документации и формирование аналитической отчетности.

В качестве концептуальной основы проектирования был выбран функциональный подход, ориентированный на разбиение системы на отдельные модули, каждый из которых выполняет конкретные задачи, соответствующие бизнес-требованиям и пользовательским ролям. ПО реализовано в виде клиент-серверного веб-приложения с микросервисной архитектурой [2].

Выбор данной архитектуры обусловлен рядом факторов, соответствующих требованиям надежности, масштабируемости и гибкости в условиях эксплуатации информационной системы медицинского назначения.

Во-первых, микросервисная архитектура обеспечивает разделение бизнес-логики по функциональным областям: отдельные сервисы отвечают за регистрацию и авторизацию, управление расписанием, обработку приемов, учет расходных материалов и формирование аналитики. Данный подход способствует улучшению структурной ясности системы, а также упрощает процессы тестирования и поэтапного развития отдельных компонентов.

Во-вторых, масштабируемость системы достигается за счет возможности независимого масштабирования наиболее нагруженных модулей, что является особенно важным в условиях роста числа пользователей и объема обрабатываемых данных.

В-третьих, отказоустойчивость микросервисной архитектуры позволяет избежать полной недоступности системы при сбое одного из компонентов: каждый сервис является изолированным, и его сбой не вызывает отказ всей системы.

Кроме того, микросервисная архитектура обеспечивает высокую адаптивность при развертывании и сопровождении, позволяя интегрировать дополнительные модули без нарушения целостности существующей архитектуры.

Таким образом, выбор микросервисной архитектуры обусловлен требованиями к отказоустойчивости, масштабируемости и технологической независимости модулей, что является актуальным в условиях динамично изменяющихся требований медицинских учреждений.

В системе реализована ролевая модель, предполагающая разграничение прав доступа между пользователями. Данная модель предусматривает следующие роли: пациент, врач, администратор. Для каждой роли в системе выделяются соответствующие логические модули, состоящие из нескольких сервисов. В зависимости от роли предоставляется доступ к различным функциональным возможностям.

Так, модуль администратора обеспечивает централизованное управление основными процессами клиники. Он включает в себя регистрацию и администрирование учетных записей пользователей, планирование и координацию графиков работы врачей, управление расписанием приемов пациентов, а также ведение учета расходных медицинских материалов. Дополнительно модуль предоставляет средства анализа деятельности клиники, включая оценку эффективности работы медицинского персонала и динамику посещаемости.

Модуль врача предназначен для ведения клинического приема и медицинской документации. Он позволяет врачу фиксировать жалобы пациента, выставлять диагнозы и формировать рекомендации. Также врач получает доступ к электронной медицинской карте пациента, может записывать пациентов на повторный прием.

Модуль пациента ориентирован на создание эргономичного пользовательского интерфейса для записи на прием и взаимодействия с клиникой. Пользователь может создать аккаунт в системе, записаться, перенести или отменить прием, а также просматривать информацию о прошедших и предстоящих визитах. Дополнительно реализована возможность загрузки внешних медицинских документов.

Для более наглядного представления механизма взаимодействия между сервисами системы в рамках одного из ключевых бизнес-процессов – записи пациента на прием – была разработана диаграмма последовательности (рис. 1). Она демонстрирует последовательность вызова сервисов и обмена сообщениями.

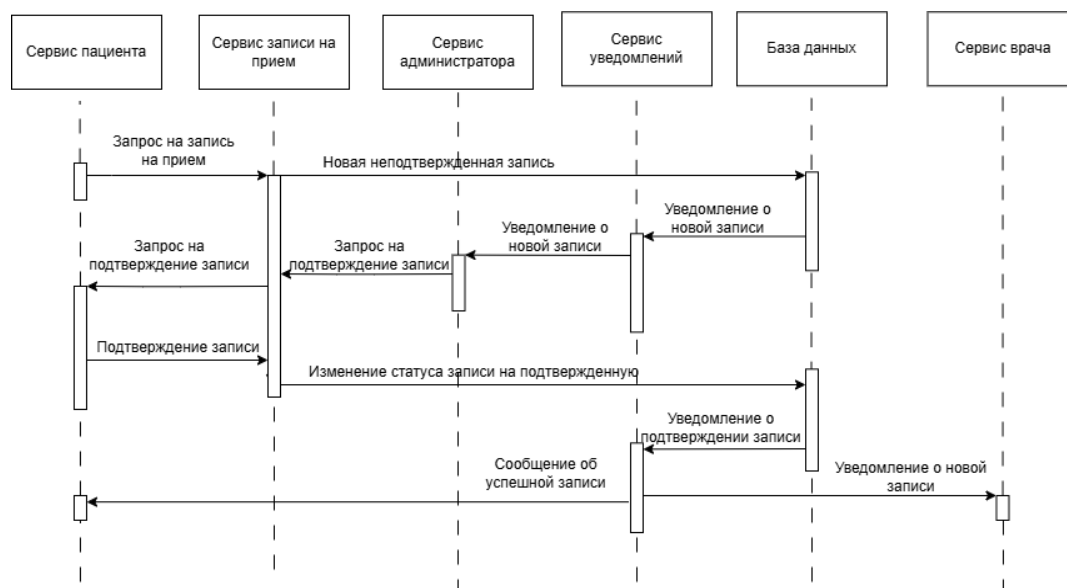


Рис. 1. Диаграмма последовательности записи пациента на прием

В результате внедрения разработанного программного обеспечения в стоматологической клинике ожидаются следующие показатели эффективности:

1. Сокращение времени записи на прием: для оценки ожидаемого сокращения времени записи был проведен анализ по методу GOMS [3]. Данный метод позволил детально рассчитать временные затраты на оформление записи с использованием системы. На рисунках 2-3 представлена форма записи через программное обеспечение.

Запись на приём

Выберите специализацию врача

Терапевт ▼

Выберите врача

Иванов Д.В. ▼

Выберите удобное время

| вт, 22 апр. | ср, 23 апр. |
|-------------|-------------|
| 10:00       | 09:00       |
| 11:00       | 11:00       |
| 12:00       |             |

Рис. 2. Форма записи пациента на прием: выбор специализации, врача, даты и времени

← Назад

**Вы записываетесь на приём:**

**Специализация:** Терапевт  
**Врач:** Иванов Д.В.  
**Дата:** 22.04.2025  
**Время:** 10:00

Фамилия

Имя

Отчество

Дата рождения

Пол  
☐ Мужской ☐ Женский

Номер телефона

☐ Я согласен на обработку персональных данных

**Записаться**

Рис. 3. Форма записи пациента на прием: ввод личных данных

Расчет времени выполнения задачи осуществлялся по формуле:

$$T = \sum_{i=1}^n t_i, \quad (1)$$

где  $T$  – общее время выполнения задачи,  $t_i$  – время выполнения отдельного оператора (действия),  $n$  – количество операторов.

Операторы, используемые для вычисления, приведены в таблице 1.

ТАБЛИЦА 1. Операторы GOMS

| Оператор | Описание                                      | Среднее время выполнения, с |
|----------|-----------------------------------------------|-----------------------------|
| К        | Нажатие клавиши                               | 0,28                        |
| Р        | Перемещение указателя мыши на цель на дисплее | 1,1                         |
| В        | Нажатие кнопки мыши                           | 0,1                         |
| Н        | Перемещение руки на мышь/клавиатуру           | 0,4                         |
| М        | Ментальный акт рутинного мышления/восприятия  | 1,2                         |

В результате расчета время, затрачиваемое на запись на прием, составило 46,24 секунды, в то время как ручная запись на прием составляет около 3 минут. Таким образом, внедрение системы ускорит процесс записи практически в 4 раза;

2. Повышение точности ведения медицинской документации: использование электронных форм и обязательных полей снизит частоту ошибок и исключит случаи дублирования данных;

3. Аналитика для принятия решений: встроенные отчеты позволят анализировать эффективность врачей, количество отмен визитов, источники записей на прием, что обеспечивает информационную базу для принятия обоснованных управленческих решений.

Программное обеспечение для автоматизации стоматологической клиники, разработанное с использованием функционального подхода и микросервисной архитектуры, отвечает требованиям современной медицинской практики. Его внедрение позволяет повысить контролируемость и эффективность внутренних процессов работы клиники, а также создать клиентоориентированную цифровую среду, улучшающую пользовательский опыт взаимодействия с клиникой. Перспективы дальнейшего развития включают реализацию мобильного приложения и интеграцию с государственными информационными системами.



**Список используемых источников**

1. Баланов А. Н. Цифровизация в здравоохранении. Разработка, интеграция и внедрение современных систем: учебное пособие для вузов / А. Н. Баланов. Санкт-Петербург: Лань, 2024. С. 9–18.
2. Кравченко Д. А. Микросервисная архитектура // Интерактивная наука. 2022. № 4 (69). С. 43-44. URL: <https://cyberleninka.ru/article/n/mikroservisnaya-arhitektura> (дата обращения 23.04.2025).
3. Kieras D. Using the Keystroke-Level Model to Estimate Execution Times // University of Michigan. 1993. С. 2–10. URL: <https://www.cs.umd.edu/~golbeck/INST631/KSM.pdf> (дата обращения 26.04.2025).

*Статья представлена научным руководителем, старшим преподавателем кафедры ПИиВТ СПбГУТ Краевой Е. В.*

УДК 004.932:78

Д. Р. Бариев (студент группы ИСТ-212, СПбГУТ), [bariev.dr@sut.ru](mailto:bariev.dr@sut.ru)

## ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ АВТОМАТИЧЕСКОГО ПОДБОРА МУЗЫКАЛЬНЫХ КОМПОЗИЦИЙ НА ОСНОВЕ АНАЛИЗА ВИЗУАЛЬНЫХ ХАРАКТЕРИСТИК ИЗОБРАЖЕНИЯ

*Актуализируется разработка комплексного решения для автоматического подбора готовых музыкальных композиций на основе глубокого анализа визуальных характеристик изображения. Проведен анализ существующих сервисов, специализирующихся на анализе изображений, музыкальных рекомендациях и генерации музыки, выявлены их ключевые недостатки. Описана модульная архитектура системы, демонстрирующая взаимодействие ключевых компонентов: модулей анализа изображений, подбора музыки и интеграции со стриминговыми сервисами. Функционал системы проиллюстрирован с помощью диаграммы вариантов использования, отражающей основные возможности для ключевых пользователей сервиса. Определены перспективы развития информационной системы для автоматического подбора музыкальных композиций на основе визуального анализа изображений.*

*информационная система, объектно-ориентированное моделирование, анализ изображений, подбор музыки, визуальные характеристики, UML*

В мире, насыщенном визуальным контентом, потребность в адекватном музыкальном сопровождении постоянно растет. Однако создание гармоничных аудиовизуальных продуктов часто требует значительных временных и творческих затрат. Существующие инструменты либо генерируют новую музыку, либо рекомендуют ее без учета визуального ряда, либо анализируют изображения без подбора существующих композиций. Подобное говорит о нехватке на рынке комплексных решений, способных автоматически подбирать готовые музыкальные композиции [1], основываясь на глубоком анализе визуальных данных изображения, таких как цветовая палитра, стиль и эмоциональный настрой [2].

Актуальность задачи обусловлена ростом спроса на персонализированный контент, тенденцией к автоматизации его создания и востребованностью подобных систем в маркетинге, развлекательной индустрии и арт-проектах. Целью данной работы является проектирование информационной системы (далее – ИС), способной решить эту проблему путем автоматизации подбора музыки на основе анализа изображений.

Для определения ниши проектируемой системы проведен анализ существующих решений на рынке и в академической среде. Выявлено, что прямых аналогов, полностью реализующих задуманный функционал, нет. Существующие системы можно разделить на несколько групп:

- системы генерации музыки по тексту (например, Suno, Udio), которые создают новые композиции по описанию, но не работают с изображениями и существующей музыкой;

- музыкальные рекомендательные системы (например, Yandex Музыка, Spotify), которые анализируют аудиоданные и предпочтения пользователей, но не учитывают визуальный контекст [1];

- системы анализа и генерации изображений (например, DeepAI, ChatGPT), которые фокусируются на визуальных данных и не занимаются подбором музыки;

- нейросети для анализа эмоций (например, Emotion AI), которые распознают эмоции, но не предлагают комплексного решения для подбора контента на основе связи изображения и звука [3];

- сервисы генерации музыки по изображениям (например, Melobytes), которые создают новую музыку на основе изображений, но не подбирают существующие композиции.

Основной недостаток всех этих систем – отсутствие интеграции глубокого визуального анализа с возможностью подбора готовых музыкальных композиций из существующих баз данных. Проектируемая ИС призвана заполнить эту нишу путем предоставления автоматизированного инструмента для анализа изображений и подбора к ним музыки из доступных композиций, что позволит избавить пользователя от ручного сопоставления.

Проектирование осуществлялось с использованием объектно-ориентированной методологии и языка UML (Unified Modeling Language), что позволило структурировано описать статическую и динамическую структуры системы.

Для решения поставленной задачи предлагается ИС с модульной архитектурой, обеспечивающей гибкость и масштабируемость. Ключевые компоненты системы и их взаимодействие показаны на рис. 1.



Рис. 1. Схема взаимодействия модулей ИС

Архитектура системы состоит из ряда функциональных модулей, каждый из которых выполняет специфические задачи и взаимодействует с остальными для обеспечения комплексной работы. Модуль веб-сервера предоставляет пользовательский интерфейс и координирует работу. Модуль загрузки и обработки изображений принимает и предобрабатывает изображения. Модуль анализа визуальных характеристик выполняет основной анализ изображения, определяя цветовую палитру, стиль (CNN) и эмоциональный настрой (ML-модели) [2, 3]. Модуль подбора музыкальных композиций на основе этих данных и заданных критериев ищет и ранжирует подходящие композиции [1]. Модуль интеграции со стриминговыми сервисами взаимодействует с внешними API (например, Spotify, Yandex Music) для поиска и экспорта музыки. Модуль данных отвечает за хранение всей информации (композиций, пользователей, истории, статистики). Дополнительно предусмотрены модули администрирования, статистики и техподдержки для управления системой и поддержки пользователей.

Взаимодействие акторов с системой и их основные функции наглядно демонстрирует диаграмма вариантов использования [4], представленная на рис. 2.

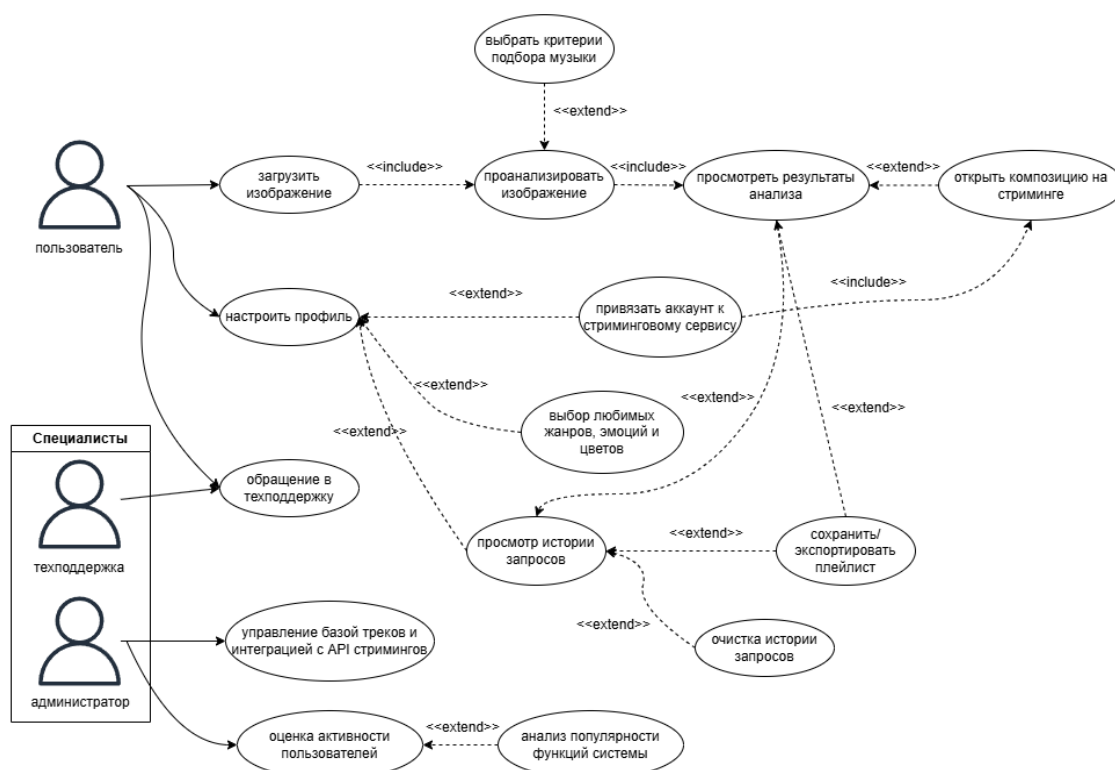


Рис. 2. Общая диаграмма прецедентов для ИС

Взаимодействие с системой осуществляется несколькими ключевыми акторами. Пользователь загружает изображения, получает и экспортирует музыкальные рекомендации, а также управляет своим профилем и обращается в техподдержку. Администратор управляет базой данных музыки, модерацией контента, пользователями и системными настройками. Техническая поддержка осуществляет мониторинг системы, устранение неполадок и поддержку пользователей.

Основными прецедентами являются загрузка изображений, анализ изображений, экспорт плейлиста, настройка профиля и обращение в техническую поддержку. Данные сценарии охватывают весь основной цикл работы пользователя с системой: от загрузки исходного материала до получения конечного результата в виде плейлиста.

Логику работы системы детализируют диаграммы деятельности [4]. Например, диаграмма деятельности для прецедента «Проанализировать изображение» на рис. 3 показывает шаги от инициации анализа пользователем до вывода списка рекомендованных композиций, включая этапы анализа цвета, стиля, эмоций, фильтрации и ранжирования музыки [1].

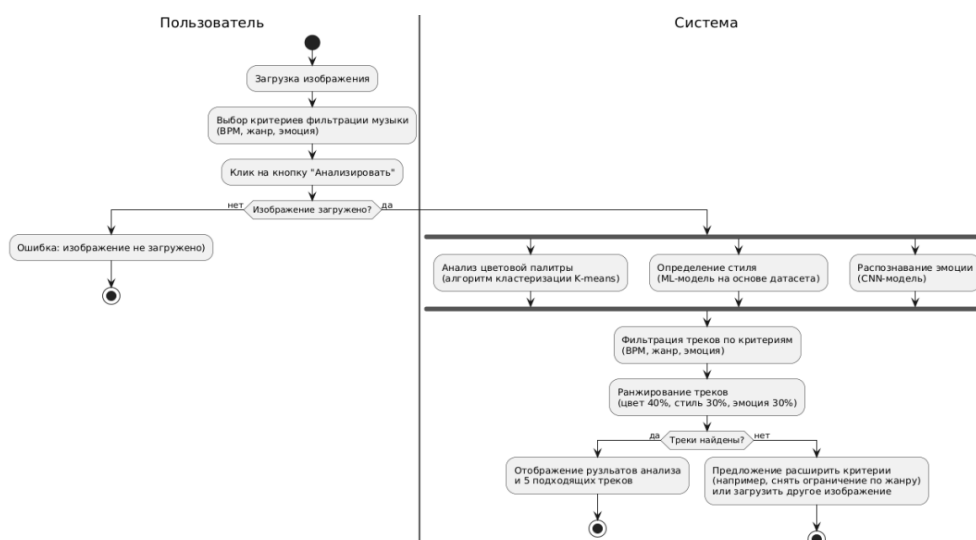


Рис. 3. Диаграмма деятельности для прецедента «Проанализировать изображение»

В работе сформулированы требования, определены актеры и сценарии использования, а также разработаны модульная архитектура и UML-диаграммы прецедентов и деятельности.

Проектируемая система решает актуальную задачу интеграции визуальных и аудиоданных, предлагая уникальный функционал по подбору готовых музыкальных композиций, что отличает ее от существующих решений. Полученные в ходе проектирования модели и диаграммы служат прочной основой для дальнейшей практической реализации инструментального средства.

Перспективы развития системы включают внедрение более совершенных алгоритмов машинного обучения и нейронных сетей (например, Vision Transformers) для анализа изображений и многомодального обучения для выявления более глубоких связей между визуальными и аудио характеристиками [2, 3]. Также планируется интеграция механизмов обратной связи и рекомендательных систем для повышения персонализации и точности подбора музыки.

#### Список используемых источников

1. Менькин А. В. Разработка музыкальной рекомендательной системы на основе обработки метаданных контента // Вестник НГУ. Серия: Информационные технологии. 2019. № 3.
2. Селянкин В. В. Компьютерное зрение. Анализ и обработка изображений / В. В. Селянкин. 3-е изд., стер. Санкт-Петербург: Лань, 2023. 152 с.
3. Филиппов Ф. В. Нейросетевые технологии: учебное пособие / Ф. В. Филиппов. Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2020. 129 с.
4. Котлова М. В., Давыдова Е. В. Методы и средства проектирования информационных систем и технологий: учебное пособие. СПб.: СПбГУТ, 2015. 62 с.

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.422.8:378.1

**Г. В. Большаков** (студент группы ИСТ-111, СПбГУТ),  
[bolshakov1.gv@sut.ru](mailto:bolshakov1.gv@sut.ru)

**П. И. Козлов** (студент группы ИСТ-111, СПбГУТ), [kozlov.pi@sut.ru](mailto:kozlov.pi@sut.ru)

## **ФОРМИРОВАНИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПОДДЕРЖКИ СТУДЕНЧЕСКИХ СТАРТАПОВ**

*Проведен анализ современных тенденций студенческого предпринимательства в России и выявлены ключевые проблемы, связанные с отсутствием единой цифровой платформы. Определены требования к системе, интегрирующей процессы проектной деятельности от создания команд до участия в мероприятиях. Сформирована схема взаимодействия модулей, описывающая ключевые компоненты системы и их функциональные возможности. Построена диаграмма прецедентов для ключевых пользовательских ролей и спроектированы основные экранные формы интерфейса. Представленная модель может быть адаптирована для внедрения в инфраструктуру различных учебных заведений в качестве компонента университетской цифровой экосистемы, способствующей поддержке студенческих инициатив.*

*студенческое предпринимательство, информационная система, проектная деятельность, университетская экосистема, UML, поддержка стартапов*

В российских вузах все больше студентов увлекаются технологическим предпринимательством. Благодаря совместным усилиям государства, университетов и бизнеса идеи, которые рождаются в аудиториях, имеют все шансы на реализацию. Исследования показывают, что для устойчивого роста стартап-активности необходима сбалансированная комбинация трех факторов: мотивации, навыков и инфраструктуры [1, 2]. В ответ на растущий интерес к предпринимательству государство активно развивает нормативно-правовую базу и создает цифровые экосистемы. Университеты создают стартап-студии и включают стартап-проекты в учебный план. Корпорации предлагают отраслевые акселераторы и пилотные площадки. Все эти меры направлены на то, чтобы каждая команда могла пройти путь от идеи до рынка в кратчайшие сроки.

В рамках национального отчета GUESSS (Global University Entrepreneurial Spirit Students' Survey), проведенного в России в 2023 г., приняли участие более 4600 студентов из вузов России. Результаты исследования показали, что 41,5 % респондентов намерены основать собственный бизнес в течение пяти лет после окончания учебы. Более того, 20 % студен-

тов уже активно участвуют в разработке стартап-проектов в процессе обучения, что на 11,5 % превышает средний мировой уровень и свидетельствуют о том, что среди молодого поколения формируется новое видение предпринимательства как реального пути к успеху [1].

Несмотря на высокий интерес к предпринимательству, 66,1 % опрошенных студентов не имели возможности пройти ни одного формального курса по этому направлению в своих вузах. Из-за этого многие вынуждены изучать основы финансового моделирования, клиентского развития и навыки презентации инвесторам через внешние интенсивы, платные программы и хакатоны, что создает дополнительную финансовую нагрузку и не всегда гарантирует высокое качество обучения [1].

Правительство Российской Федерации издало Распоряжение № 2894-р от 18 октября 2023 года, в котором обозначило стратегические направления в области цифровой трансформации образования. Основная цель документа – обеспечить доступ к инновационным ресурсам не менее 60 % студентов к 2026 году. Планируется внедрение коллективных платформ для проектирования и автоматизированных систем оценки достижений [3].

В рамках федеральных проектов и цифровых студий достигнуты успехи, однако остаются некоторые важные вызовы:

- уровень цифровой зрелости российских вузов различается, лишь немногим более 40 % учебных заведений располагают полноценной системой управления обучением (LMS), в которой есть модули для управления стартапами;
- кроме того, существует проблема нехватки менторов, в студенческих студиях соотношение между наставником и командой составляет 1:15, в то время как оптимальным считается 1:5;
- еще один важный аспект – недостаток междисциплинарности, лишь 22 % программ предполагают совместную работу студентов из разных областей, таких как информационные технологии (ИТ), экономика и дизайн.

Тем не менее сегодня благодаря масштабным исследованиям мотивации студентов, скоординированным государственным стратегиям и развитой сети акселераторов закладывается прочный фундамент для создания новой волны высокотехнологичных стартапов. Каждый студент получает не только теоретические знания, но и реальные инструменты для их реализации.



На основании проведенного анализа сформированы основные функциональные требования к системе. Для студентов система должна обеспечивать: формирование и вступление в команды; создание и редактирование проектов; подачу заявок на участие в мероприятиях. Для представителей администрации вузов необходимо предоставлять функции: формирование списка событий; создание, изменение и одобрение проектов и команд.

Правильное выделение модулей в информационной системе позволяет добиться гибкости, масштабируемости и простоты технической поддержки. В основе проектируемого решения лежит принцип разделения ответственности: каждый модуль отвечает за свою предметную область, взаимодействуя с остальными по четко определенным интерфейсам. Такая архитектура, представленная на рис. 1, облегчает параллельную разработку, тестирование и модернизацию системы, не создавая опасности повредить связанные элементы при внесении изменений.



Рис. 1. Модульная схема информационной системы

При разработке информационной системы важно не только определить ее модульную структуру, но и четко формализовать поведение компонентов в ответ на действия пользователя. Поведенческая модель отражает, как элементы системы взаимодействуют между собой во времени при выполнении пользовательских сценариев. Для описания таких взаимодействий используется диаграмма прецедентов, которая позволяет задать внешнее поведение системы.

Диаграмма прецедентов (Use Case) на рис. 2 демонстрирует все основные взаимодействия между двумя важными участниками проектной деятельности в вузе: Студентом (пользователем системы) и Администратором (проектным офисом).

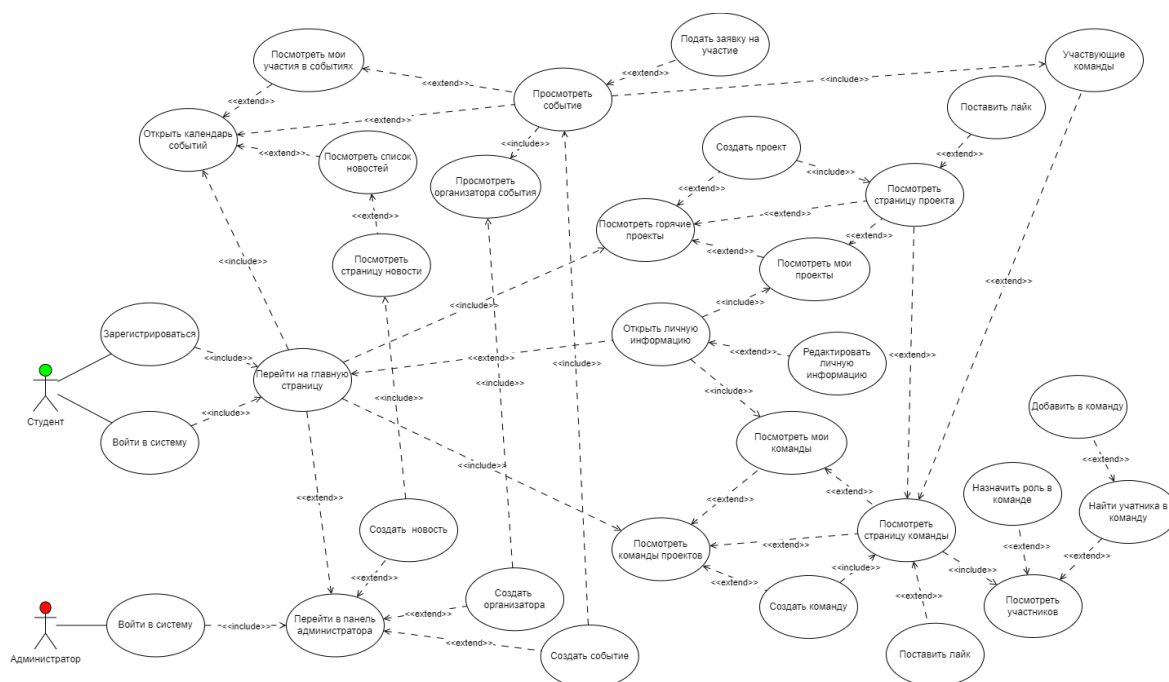


Рис. 1. Диаграмма прецедентов информационной системы

Студент осуществляет множество действий, начиная с регистрации в системе и заканчивая активным участием в проектах и мероприятиях. Основные действия включают в себя: регистрацию и вход в систему, просмотр новостей и событий, подачу заявки на участие в мероприятии, создание и редактирование проектов, формирование и добавление в команды и заполнение личной информации и ее изменение.

Получается, что студент не только наблюдает за развитием экосистемы стартапов в университете, но и активно участвует в ее формировании.

Актор «Администратор» имеет доступ к административной панели и дополнительным функциям: создание, изменение и одобрение проектов или отправка на доработку; управление новостями и событиями; формирование команд; настройка доступа, ролей и контроля прав пользователей.

Диаграмма демонстрирует, что интерфейс и набор действий для администратора отличается от студенческого, что позволяет разграничить права доступа и сделать систему более безопасной и управляемой.

Рассматриваемая информационная система ориентирована на студентов и администраторов университетской стартап-деятельности. В основе ее пользовательского интерфейса лежит принцип функционального минимализма, который гармонично сочетается с корпоративным стилем визуального оформления. Цветовая палитра системы выдержана в строгих тонах, а типографика ясна и структурирована, что позволяет легко ориентироваться

в интерфейсе и соответствовать эстетическим ожиданиям молодых пользователей, не перегружая экран лишними элементами.

Впервые попадая в систему, пользователь оказывается на главной странице, которая выполняет две функции: служит информационной витриной и является точкой входа в систему. На главной странице представлены основные разделы: лента новостей, календарь событий, горячие проекты и команды проектов, а через верхнюю панель можно попасть в раздел личная информация. Страница построена на блочной логике с использованием интерактивных визуальных карточек, каждая из которых ведет к соответствующему разделу.

Рассмотрим страницы «Календарь событий» и «Личная информация» на рис. 3 и 4 соответственно.

### КАЛЕНДАРЬ СОБЫТИЙ

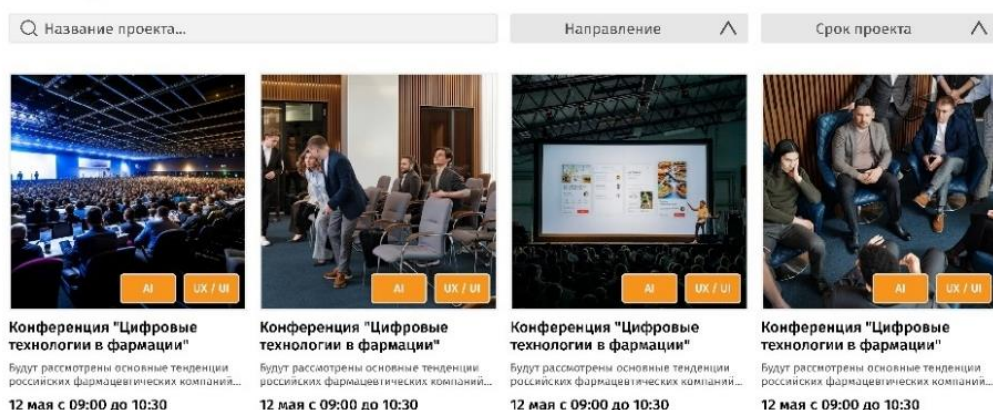


Рис. 3. Страница «Календарь событий»

### ЛИЧНАЯ ИНФОРМАЦИЯ

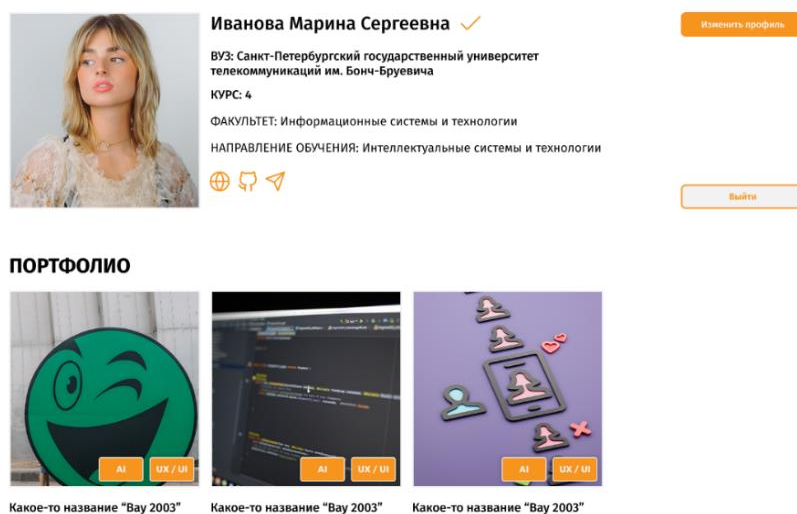


Рис. 4. Страница «Личная информация»

Предложенное решение не только соответствует актуальным требованиям современного образования, но и предоставляет эффективный инструмент для формирования новой предпринимательской культуры в университетской среде. В перспективе оно может стать частью национальной цифровой платформы поддержки молодежных инициатив, объединяя студентов, преподавателей, инвесторов и промышленных партнеров в единую информационную экосистему.

#### Список используемых источников

1. GUESS Russia 2023. Национальный отчет // Национальный исследовательский университет «Высшая школа экономики». URL: [https://spb.hse.ru/data/2024/06/04/2130333367/GUESSS %20Russia %202023\\_Rus.pdf](https://spb.hse.ru/data/2024/06/04/2130333367/GUESSS%20Russia%202023_Rus.pdf) (дата обращения 28.04.2025).
2. OECD. Education at a Glance 2023. OECD Indicators. URL: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/education-at-a-glance-2023\\_581c9602/e13bef63-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/education-at-a-glance-2023_581c9602/e13bef63-en.pdf) (дата обращения 28.04.2025).
3. Распоряжение Правительства РФ от 18.10.2023 № 2894-р «Об утверждении стратегического направления цифровой трансформации образования» // Официальный интернет-портал правовой информации. URL: <https://legalacts.ru/doc/rasporjazhenie-pravitelstva-rf-ot-18102023-n-2894-r-ob-utverzhdanii/> (дата обращения 28.04.2025).

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 557.575

**А. П. Бура** (студент группы ИКПИ-34, СПбГУТ)**М. А. Жуков** (студент группы ИКПИ-34, СПбГУТ)**И. М. Колганов** (студент группы ИКПИ-34, СПбГУТ)**Д. И. Кураш** (студент группы ИКПИ-34, СПбГУТ)**К. А. Орлова** (студент группы ИКПИ-34, СПбГУТ), [orlova.ka@sut.ru](mailto:orlova.ka@sut.ru)**ТЕОРИЯ ГРАФОВ В ПРОДОЛЖЕНИИ РОДА С ПРОГНОЗОМ**

*Теория графов является важной областью математики и информатики, находящей применение в различных сферах: от социального анализа и биоинформатики до оптимизации логистических процессов и разработки алгоритмов для компьютерных сетей. С увеличением объемов данных и усложнением систем, использование графов как модели для анализа и визуализации взаимосвязей становится все более актуальным. В современных условиях, когда прогнозирование событий на основе сложных взаимосвязей становится критически важным, применение теории графов для этой цели предлагает новые подходы и инструменты.*

*теория графов, прогнозирование событий, продолжение рода, моделирование генеалогических структур*

Резус-конфликт остается одной из ключевых проблем в акушерстве и репродуктивной медицине, несмотря на существующие методы профилактики. Это иммунологическое осложнение возникает при беременности, когда у резус-отрицательной матери (Rh-) развивается резус-положительный плод (Rh+), унаследовавший антиген от отца. Иммунная система матери воспринимает эритроциты ребенка как чужеродные и начинает вырабатывать антитела, что может привести к гемолитической болезни новорожденных (ГБН), тяжелой анемии, желтухе и даже внутриутробной гибели плода.

Масштаб проблемы:

- ~15 % женщин в мире имеют резус-отрицательную кровь (частота варьируется в зависимости от этнической группы: у европейцев – около 15 %, у африканцев – 5 %, у азиатов – менее 1 %);
- в 10-15 % случаев браков резус-отрицательная женщина беременеет от резус-положительного мужчины, что создает риск резус-конфликта;
- без профилактики анти-RhD иммуноглобулином сенсibilизация (выработка антител) происходит в ~1-2 % первых беременностей и до 15 % при повторных;
- в странах с низким уровнем медицинского контроля ГБН развивается у 0,6 % всех новорожденных, приводя к тяжелым последствиям в 0,1 % случаев.

Многие пары не знают о потенциальной опасности резус-конфликта до наступления беременности. По данным опросов:

- >40 % женщин репродуктивного возраста не знают свой резус-фактор;

- ~30 % пар не проверяют совместимость крови перед зачатием;

В развивающихся странах до 60 % случаев ГБН диагностируются слишком поздно из-за отсутствия скрининга.

Поэтому, резус-конфликт – предотвратимое осложнение, однако его последствия остаются значимыми из-за недостаточной информированности пар и пробелов в медицинском сопровождении. Теория графов может помочь в прогнозировании рисков, автоматизации анализа родственных связей и разработке персонализированных рекомендаций для пар с резус-несовместимостью.

Теория графов предоставляет мощные инструменты для моделирования и анализа сложных систем, включая генетические связи, наследование признаков и прогнозирование репродуктивных рисков. В контексте продолжения рода графы помогают:

1. Визуализировать родственные связи – строить генеалогические деревья, выявлять наследственные заболевания.

2. Прогнозировать генетические риски – определять вероятность передачи мутаций и болезней потомкам.

3. Оптимизировать подбор партнеров – анализировать совместимость по группе крови и резус-фактору для минимизации рисков при зачатии.

4. Моделировать демографические сценарии – предсказывать численность потомков и их генетическое разнообразие.

Анализ таблицы 1 подтверждает, что присутствуют немало рисков, которые могут привести к резус-конфликту.

ТАБЛИЦА 1. Таблица совместимости групп крови и резус-факторов при зачатии

| Группа крови матери | Группа крови отца | Резус-фактор матери | Резус-фактор отца | Риски                          | Рекомендации                     |
|---------------------|-------------------|---------------------|-------------------|--------------------------------|----------------------------------|
| О (I)               | О (I)             | Rh+                 | Rh+               | Нет                            | Безопасно                        |
| О (I)               | А (II)            | Rh-                 | Rh+               | Резус-конфликт (если плод Rh+) | Контроль антител, иммуноглобулин |
| А (II)              | В (III)           | Rh+                 | Rh+               | Нет                            | Безопасно                        |

| Группа крови матери | Группа крови отца | Резус-фактор матери | Резус-фактор отца | Риски                                        | Рекомендации       |
|---------------------|-------------------|---------------------|-------------------|----------------------------------------------|--------------------|
| В (III)             | АВ (IV)           | Rh-                 | Rh+               | Резус-конфликт (если плод Rh+)               | Контроль антител   |
| АВ (IV)             | АВ (IV)           | Rh+                 | Rh-               | Нет                                          | Безопасно          |
| Любая               | Любая             | Rh-                 | Rh+               | Резус-конфликт (если плод Rh+)               | Иммунопрофилактика |
| О (I)               | АВ (IV)           | Rh+                 | Rh+               | Гемолитическая болезнь (если у ребенка не О) | Наблюдение у врача |

Ключевые риски:

- Резус-конфликт – возникает, если у матери Rh-, а у плода Rh+ (возможна анемия, желтуха у новорожденного).
- Несовместимость по группе крови – если у матери О (I), а у ребенка А/В/АВ, возможна легкая гемолитическая болезнь.

На рисунке 1 приведен пример работы нашего алгоритма.

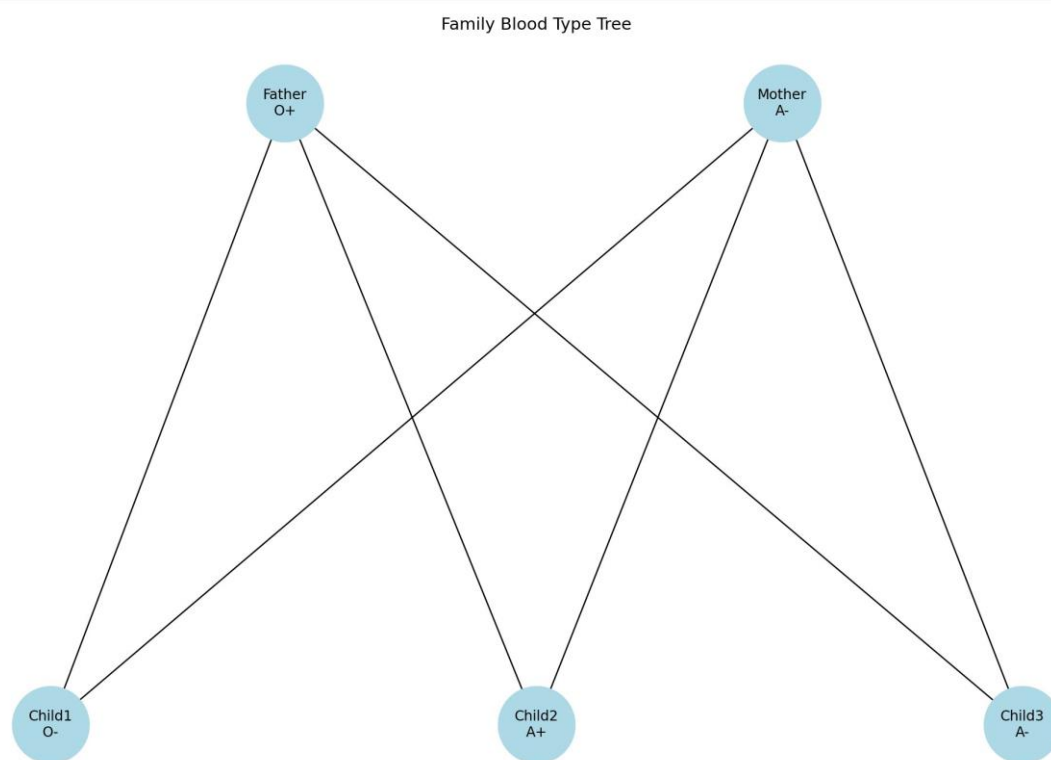


Рис 1. Моделирование групп крови для трех детей с использованием графов

**Список используемых источников**

1. Bondy J. A., Murty U. S. R. Graph Theory. Springer, 2008. 651 p. ISBN 978-1-84628-969-9.
2. Dean L. Blood Groups and Red Cell Antigens. NCBI, 2005. 212 p. URL: <https://www.ncbi.nlm.nih.gov/books/NBK2261/> (дата обращения 10.04.2025).
3. Moise K. J. Management of rhesus alloimmunization in pregnancy // Obstetrics & Gynecology. 2008. Vol. 112. № 1. PP. 164-176. DOI: 10.1097/AOG.0b013e31817d453c.
4. Urbaniak S. J., Greiss M. A. RhD haemolytic disease of the fetus and the newborn // Blood Reviews. 2000. Vol. 14. № 1. PP. 44-61. DOI:10.1054/blre.1999.0123.
5. ВОЗ. Руководство по применению анти-D иммуноглобулина в акушерской практике. Женева: Всемирная организация здравоохранения, 2021. 48 с. ISBN 978-92-4-002265-6.
6. Koller D., Friedman N. Probabilistic Graphical Models: Principles and Techniques. MIT Press, 2009. 1231 p. ISBN 978-0-262-01319-2.
7. Reid M. E., Lomas-Francis C. The Blood Group Antigen FactsBook. 2nd ed. Academic Press, 2004. 576 p. ISBN 978-0-12-586585-2.
8. Zipursky A., Paul V. K. The global burden of Rh disease: a systematic review // The Lancet Haematology. 2019. Vol. 6. № 3. PP. e156-e166. DOI: 10.1016/S2352-3026(19)30018-1.

*Статья представлена научным руководителем, кандидатом физико-математических наук, заведующим кафедрой ВМ СПбГУТ, доцентом Плотниковым П. В.*



УДК 004.4

Д. В. Вайтович (студент группы ИСТ-211, СПбГУТ), [vaitovich.dv@sut.ru](mailto:vaitovich.dv@sut.ru)

## ПРОЕКТИРОВАНИЕ ГИБКОЙ ОБУЧАЮЩЕЙ ПЛАТФОРМЫ ДЛЯ РАБОТЫ С API

*В статье представлено проектирование адаптивной информационной системы, предназначенной для обучения пользователей работе с API. Актуальность работы обусловлена сложностью освоения API начинающими специалистами из-за необходимости глубокого понимания технической документации. Предлагаемое решение включает графический интерфейс, который позволяет изучать структуру API-запросов без написания кода, что минимизирует сложность обучения, упрощает практическое освоение инструментов и их применение в профессиональной деятельности. Реализована возможность работы с шаблонным API, отображения ответов сервера в наглядном формате, а также детального анализа ошибок. Особое внимание уделено адаптивности сервиса: начинающим пользователям доступен упрощенный интерфейс с базовым функционалом, а опытным специалистам – расширенные возможности, включающие загрузку и тестирование собственных API.*

*API, RESTful интерфейсы, конструктор запросов, валидация API, адаптивная система, пользовательские API, интеграция систем*

В эпоху активно развивающихся современных цифровых технологий API (Application Programming Interface) [1] играют ключевую роль в интеграции различных сервисов и приложений. Однако освоение работы с API часто вызывает трудности у начинающих разработчиков из-за сложности инструментов и необходимости глубокого понимания технической документации.

API – это общий термин, который применяется в контексте совершенно разных систем. REST API – это конкретный архитектурный стиль API, который используется для обмена данными между клиентами и серверами.

Часть работы с REST API – это создание описаний работы API: информации о ресурсах, параметрах запросов, возвращаемых данных, конечных точках и других важных вещах. Чтобы автоматизировать это описание, сделать его структурированным и прозрачным, разработчики используют специализированное программное обеспечение.

С развитием цифровых технологий растет потребность в обучающих платформах для освоения работы с API. Самостоятельное изучение теории часто оказывается недостаточным: новичкам трудно перейти от теории к

практике и понять, как строится взаимодействие между клиентом и сервером. Хотя современные инструменты, такие как Postman, SoapUI, Insomnia и Swagger [2, 3], эффективны, но они ориентированы на опытных разработчиков. Новичкам сложно использовать их без предварительных знаний – требуется разбираться в запросах, заголовках и структуре данных.

Необходима обучающая платформа с интуитивным интерфейсом, пошаговым обучением, встроенными подсказками и адаптацией под уровень пользователя. Подобная система упростит освоение API и повысит вовлеченность. В качестве решения предлагается модульная архитектура, обеспечивающая гибкость, масштабируемость и удобное расширение функций для работы с API.

Основные функциональные блоки системы включают:

- конструктор запросов – позволяет формировать HTTP-запросы через визуальный интерфейс без необходимости программирования, с выбором метода, заголовков и параметров;
- валидация и обработка ошибок – автоматически анализирует ответы сервера и предоставляет пояснения по возникающим ошибкам;
- история действий пользователя – сохраняет отправленные запросы и ответы для анализа прогресса и возврата к выполненным заданиям;
- загрузка и тестирование пользовательских API – обеспечивает работу с собственными спецификациями API, отправку тестовых запросов и анализ результатов;
- адаптивный интерфейс – изменяет уровень сложности и функциональность системы в зависимости от подготовки пользователя.

На начальном этапе пользователь определяет тип работы – взаимодействие с шаблонным API, загрузка и тестирование собственного API либо настройка уровня подготовки. При выборе работы с шаблонным API осуществляется формирование запроса через визуальный конструктор, отправка его на сервер и анализ ответа. В случае работы с пользовательским API пользователь загружает собственную спецификацию, после чего система проводит валидацию API, позволяет настроить параметры запросов и выполнить тестирование. В любом случае предусмотрена обработка ошибок и предоставление рекомендаций пользователю.

Диаграмма прецедентов отображает зависимости между действиями пользователя и модулями системы для работы с API (рис. 1).



Рис. 1. Диаграмма прецедентов гибкой обучающей платформы для работы с API

На рис. 2 представлены принципы работы с конструктором запроса, где пользователь выбирает, какой запрос будет сформирован без написания кода, а система проводит валидацию запроса.

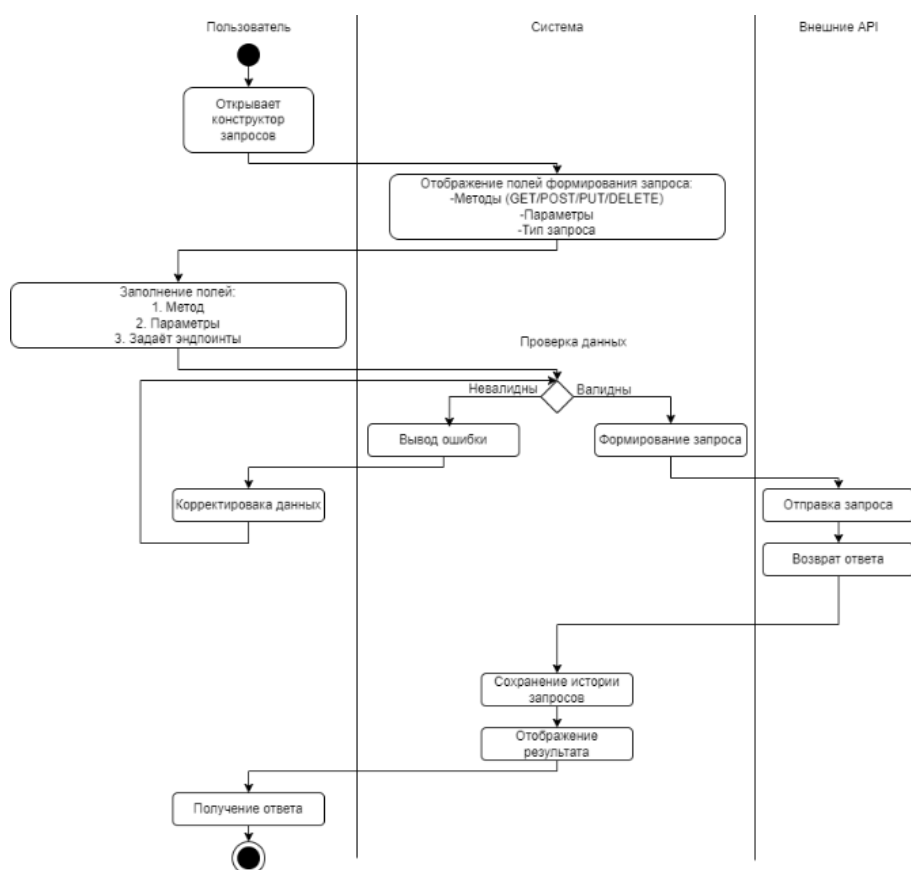


Рис. 2. Диаграмма деятельности «Формирование запроса через конструктор запросов»

На рис. 3 представлены принципы загрузки спецификации API для его дальнейшего тестирования, в рамках чего система проверяет его состояние и определяет, возможно ли продолжить работу с ним.

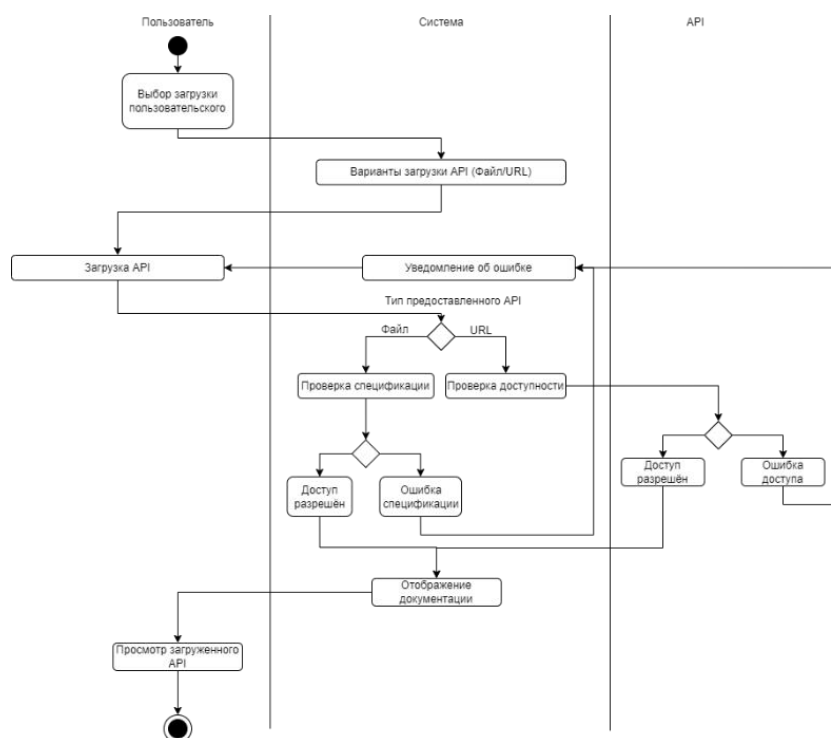


Рис. 3. Диаграмма деятельности «Загрузка пользовательского API»

Пользователь выбирает уровень подготовки для адаптации системы под свои навыки (рис. 4).

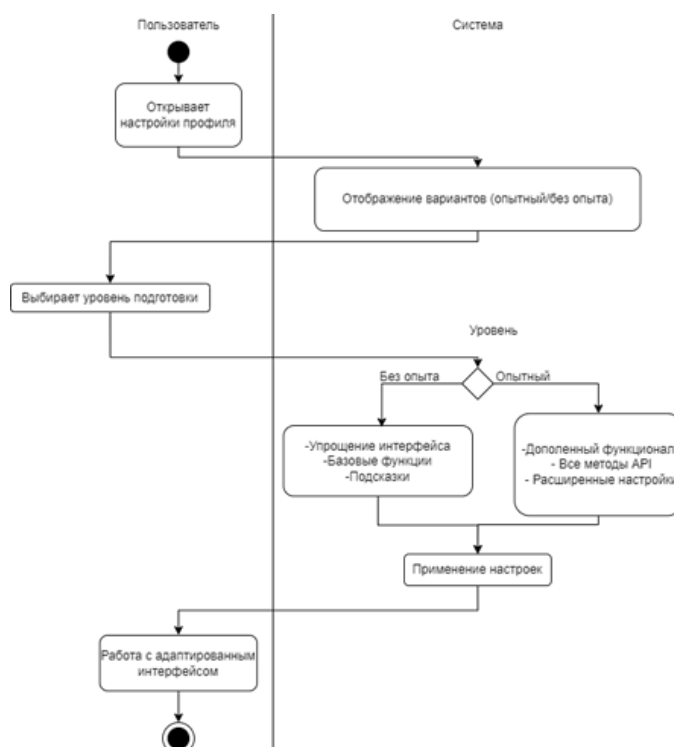


Рис. 4. Диаграмма деятельности «Выбор уровня подготовки пользователя»

Система обеспечивает адаптацию интерфейса в зависимости от выбранного уровня специалиста, что способствует ускорению и упрощению

обучения [4]. Начинающие специалисты быстрее осваивают базовые принципы построения и отправки API-запросов без необходимости изучения сложной технической документации. Опытные пользователи имеют возможность загружать собственные файлы или URL API для углубленного тестирования API.

Данная гибкая информационная система позволяет:

- повысить формирование базовых навыков работы с API;
- снизить порог вхождения в IT-сферу;
- повысить качество профессиональной подготовки.

Рассмотренная система дает возможность развить практические навыки работы с API, формирует у специалистов правильные подходы обращения с API. Адаптация интерфейса и интеграция собственного API делают обучение персонализированным.

В дальнейшем планируется расширение функциональности системы за счет внедрения поддержки новых технологий взаимодействия, таких как GraphQL и gRPC, а также рассматривается возможность внедрения искусственного интеллекта и языковой модели для дальнейшего развития проекта в гибкую самоадаптирующуюся систему (SAAPI – Self-adaptive API).

#### Список используемых источников

1. REST API: основы и принципы работы // Хабр. URL: <https://habr.com/ru/articles/483204/> (дата обращения 02.05.2025).
2. Postman: документация для разработчиков // Postman Learning Center. URL: <https://learning.postman.com/docs/getting-started/introduction/> (дата обращения 02.05.2025).
3. Swagger: инструменты для работы с API // Swagger.io. URL: <https://swagger.io/docs/> (дата обращения 02.05.2025).
4. Гибкие (адаптивные) системы обучения // EdTech Magazine. URL: <https://edtechmagazine.com/higher/article/2023/03/adaptive-learning-systems> (дата обращения 02.05.2025).

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.42

А. А. Васильков (студент группы ИКПИ-23, СПбГУТ)

Д. А. Даненко (студент группы ИКПИ-23, СПбГУТ)

А. А. Харлова (студент группы ИКПИ-23, СПбГУТ), [kharlova.aa@sut.ru](mailto:kharlova.aa@sut.ru)

## ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ МЕЖДУ КОРРЕКТНОСТЬЮ ПРОГРАММ И СТИЛЕМ ПРОГРАММИРОВАНИЯ

*В работе представлены результаты комплексного анализа компьютерных программ, написанных студентами «Школы 21» во время осеннего интенсива в 2024 году. Исследование охватывает лексический, синтаксический и структурный анализ исходного кода на языке программирования C, выполненный с применением современных методов статического анализа. Выявлена определенная зависимость между корректностью программ и использованием некоторых конструкций программирования. Исследование позволяет сформулировать практические рекомендации по совершенствованию образовательных методик, направленные на формирование у начинающих разработчиков устойчивых навыков создания качественного программного обеспечения. Выявленные закономерности подчеркивают важность системного подхода к обучению основам программирования, сочетающего освоение языковых конструкций с развитием культуры написания кода.*

*стиль программирования, качество кода, статический анализ, язык C, коэффициент корреляции, педагогика программирования*

Стиль программирования оказывает существенное влияние на корректность и работоспособность программного обеспечения. Количественная оценка этого влияния остается сложной задачей из-за отсутствия формализованных метрик и большого количества критериев оценки качества кода. Настоящее исследование направлено на устранение этого пробела путем эмпирического анализа взаимосвязи между стилевыми характеристиками и функциональной корректностью программ, написанных начинающими разработчиками.

Цель работы. Выявление количественных зависимостей между стилевыми характеристиками программ на языке программирования C и их функциональной корректностью.

Объект исследования. В ходе исследования проанализировано 72 программы, отобранные из GitLab-репозитория 24 участников осеннего образовательного интенсива «Школа 21». Для каждого участника рассматривались три различных задания, решенные в индивидуальном стиле. Все испытуемые продемонстрировали разный уровень успешности при прохождении тестирования, что позволило провести сравнительный анализ стилей программирования в зависимости от результатов обучения.

Экспериментальная база. Исследование проводилось на базе образовательного интенсива «Школа 21» (г. Великий Новгород) в период с 30 сентября по 26 октября 2024 года. В интенсиве приняло участие 184 студента начального уровня подготовки, однако исходные коды программ предоставили только 24 человека. Отсутствие данных по остальным участникам не привело к статистически значимым искажениям результатов исследования.

Методология оценки. Функциональная состоятельность программных решений оценивалась автоматизированной системой верификации «Школы 21». Корректность каждого решения определялась процентным соотношением успешно пройденных тестов из общего числа, предусмотренных заданием.

В рамках исследования была разработана и применена комплексная система оценки стиля программирования, включающая 15 формализованных метрик (1-5). Описание метрик приведено в Таблице 1. Для обеспечения полноты и достоверности анализа каждая метрика охарактеризована методом вычисления – алгоритмом количественной оценки; типом шкалы измерения.

ТАБЛИЦА 1. Система метрик оценки стиля программирования

| № п/п | Метрика                        | Метод вычисления                                        | Тип шкалы            |
|-------|--------------------------------|---------------------------------------------------------|----------------------|
| 1     | Длина идентификаторов          | Подсчет количества символов в именах переменных/функций | Абсолютная (символы) |
| 2     | Стиль именования               | Анализ паттернов camelCase/snake_case                   | Номинальная          |
| 3     | Частота «неинформативных» имен | Подсчет вхождений шаблонов (tmp, data и т.д.)           | Относительная (%)    |
| 4     | Плотность комментариев         | Отношение строк комментариев к общему LOC               | Процентная (%)       |
| 5     | Наличие мертвого кода          | Поиск закомментированных блоков длиннее 5 строк         | Бинарная (да/нет)    |
| 6     | Единообразие отступов          | Анализ согласованности пробелов/табуляций               | Индекс (0–100 %)     |
| 7     | Длина строки                   | Подсчет строк, превышающих 120 символов                 | Относительная (%)    |

| №<br>п/п | Метрика                       | Метод вычисления                                                 | Тип шкалы               |
|----------|-------------------------------|------------------------------------------------------------------|-------------------------|
| 8        | Глубина вложенности           | Определение максимального уровня вложенности конструкций         | Абсолютная (уровни)     |
| 9        | Соотношение switch/if-else    | Подсчет количества switch относительно всех условных конструкций | Процентная (%)          |
| 10       | Длина функции                 | Подсчет строк кода в теле функции                                | Абсолютная (строки)     |
| 11       | Неявные приведения типов      | Выявление опасных автоматических преобразований                  | Абсолютная (количество) |
| 12       | Динамическое выделение памяти | Количество вызовов malloc/calloc                                 | Абсолютная (количество) |
| 13       | Объем кода (LOC)              | Подсчет значимых строк (исключая пустые и комментарии)           | Абсолютная (строки)     |
| 14       | Соотношение код/комментарии   | Отношение LOC к строкам комментариев                             | Процентная (%)          |
| 15       | Коэффициент повторения        | Анализ дублированных фрагментов кода                             | Процентная (%)          |

Анализ стилевых метрик. Для установления взаимосвязи между стилевыми характеристиками кода и его функциональной корректностью был проведен комплексный статистический анализ, включающий три последовательных этапа исследования. Первоначально для каждой из 15 рассматриваемых стилевых метрик рассчитывался коэффициент линейной корреляции Пирсона. Этот показатель количественно оценивал степень и направление статистической зависимости между конкретной стилевой характеристикой и уровнем корректности программы, определяемым как процент успешно пройденных автоматизированных тестов.

Полученные коэффициенты корреляции подвергались проверке на статистическую значимость с использованием t-критерия Стьюдента. Данная процедура позволяла определить, являются ли выявленные взаимосвязи достоверными или могут быть объяснены случайными колебаниями в выборке. Для расчетов использовалась стандартная формула t-статистики, учитывающая как величину коэффициента корреляции, так и объем исследуемой выборки.



Все корреляции, признанные статистически значимыми на заданном уровне доверия ( $p < 0.05$ ), дополнительно анализировались с точки зрения практической значимости через расчет показателя силы эффекта. Этот показатель, вычисляемый как стандартизированная разность средних значений корректности для групп с «хорошими» и «плохими» значениями стилевой метрики, позволял оценить реальное влияние конкретной характеристики стиля на работоспособность программы. Особое внимание уделялось метрикам, демонстрирующим сильный эффект ( $d > 0.5$  по шкале Коэна), так как их оптимизация могла привести к наиболее заметному улучшению качества кода.

Результаты анализа. В ходе исследования было проанализировано 15 формализованных стилевых метрик программного кода и их влияние на функциональную корректность программ.

Приведенные в Таблице 2 стилевые параметры демонстрируют выраженную зависимость с функциональной корректностью программ. Данные метрики обладают свойством высокой чувствительности – даже незначительные изменения их значений приводят к существенному изменению результата выполнения программы начинающих разработчиков.

ТАБЛИЦА 2. Влияние ключевых метрик на корректность программ

| Параметр программы            | Высокая корректность ( $X > 90\%$ ) | Средняя корректность ( $90\% < X < 60\%$ ) | Низкая корректность ( $60\% < X < 30\%$ ) | Критический уровень ( $X < 30\%$ ) |
|-------------------------------|-------------------------------------|--------------------------------------------|-------------------------------------------|------------------------------------|
| Глубина вложенности           | $1.2 \pm 0.5$ уровня                | $2.1 \pm 0.7$ уровня                       | $3.5 \pm 0.9$ уровня                      | $4.8 \pm 1.1$ уровня               |
| Длина функции                 | $28 \pm 6$ строк                    | $42 \pm 10$ строк                          | $65 \pm 15$ строк                         | $89 \pm 20$ строк                  |
| Единообразие отступов         | $95 \pm 3\%$                        | $82 \pm 5\%$                               | $68 \pm 7\%$                              | $54 \pm 9\%$                       |
| Коэффициент повторения        | $3.5 \pm 1.5\%$                     | $8.2 \pm 2.8\%$                            | $16.4 \pm 4.2\%$                          | $25.7 \pm 5.5\%$                   |
| Динамическое выделение памяти | $2.3 \pm 1.1$<br>вызовов            | $5.1 \pm 2.3$<br>вызовов                   | $9.8 \pm 3.5$<br>вызовов                  | $14.6 \pm 4.7$<br>вызовов          |

Глубина вложенности управляющих конструкций демонстрирует выраженную экспоненциальную зависимость – увеличение с 1.2 до 4.8 уровней сопровождается ростом количества ошибок в 2.5-3 раза, причем критический порог наблюдается при превышении 3 уровней вложенности. Аналогично значимой оказалась зависимость для длины функций, где превышение 60 строк кода приводит к резкому ухудшению качества с возрастанием ошибок на 45-50 %, в то время как оптимальный диапазон 20-40 строк соответствует максимальным показателям корректности.

Анализ единообразия форматирования выявил линейную зависимость – снижение согласованности отступов с 95 % до 54 % последовательно увеличивает количество синтаксических ошибок на 25-30 %. Коэффициент дублирования кода показывает логарифмическую зависимость с критическим порогом в 15 %, после которого наблюдается 35-40 % рост ошибок сопровождения. Динамическое выделение памяти характеризуется степенной зависимостью, где увеличение количества вызовов функций выделения с 2-3 до 10-15 на функцию приводит к 50-60 % росту критических ошибок управления памятью.

**Интерпретация результатов.** Анализ выявил существенные различия в стилевых характеристиках программ начинающих разработчиков. Успешные решения отличаются строгим соблюдением принципов структурного программирования и вниманием к читаемости кода. Ключевое отличие проявляется в организации кода – качественные работы демонстрируют плоскую иерархию с умеренными размерами функциональных блоков, избеганием глубокой вложенности, характерной для проблемных решений.

Важным отличительным фактором выступает осознанный подход к именованию переменных. Успешные программы используют информативные идентификаторы, отражающие семантику элементов, в отличие от абстрактных наименований в слабых решениях. Это особенно значимо для начинающих разработчиков, облегчая процесс отладки и анализа кода.

Качественные решения также отличаются аккуратным управлением ресурсами и строгим соблюдением стилевого единообразия. Поддержание согласованного форматирования облегчает работу с кодом, что критично на начальных этапах обучения. Баланс между кодом и комментариями в успешных программах выдерживается более осознанно – пояснения затрагивают ключевые алгоритмы без избыточного дублирования очевидной информации.

**Заключение.** Проведенное исследование достигло поставленной цели, выявив количественные зависимости между стилевыми характеристиками

программ на языке С и их функциональной корректностью. Полученные результаты демонстрируют, что соблюдение определенных стилевых норм существенно влияет на качество программного кода у начинающих разработчиков.

Выявленные количественные закономерности позволяют сформулировать конкретные рекомендации по оптимизации процесса обучения программированию на языке С. Акцент на формирование правильных стилевых привычек, включая осознанное именование переменных, соблюдение принципов модульности и единообразия форматирования, может значительно повысить качество создаваемых программных решений. Полученные результаты имеют практическую ценность для совершенствования методик преподавания основ программирования.

*Примечание.* Для сохранения конфиденциальности ссылки на репозитории участников не приводятся. Тексты программ собраны в GitHub репозитории авторов, доступном по ссылке: <https://github.com/ekkimukk/prok>.

#### Список используемых источников

1. Grigas G. Investigation of the relationship between program correctness and programming style. *Informatica*. 1995;6(3):265-276. DOI:1.10.3233/INF-1995-6302.
2. Kozlowski S. W. J., & Ilgen D. R. (2006). Enhancing the Effectiveness of Work Groups and Teams. *Psychological Science in the Public Interest*, 7(3), 77-124. <https://doi.org/10.1111/j.1529-1006.2006.00030.x> (Original work published 2006) (дата обращения 10.04.2025).
3. Pashler H., McDaniel M., Rohrer D., & Bjork R. (2009). Learning Styles: Concepts and Evidence. *Psychological Science in the Public Interest*, 9(3), 105-119. <https://doi.org/10.1111/j.1539-6053.2009.01038.x> (Original work published 2008) (дата обращения 10.04.2025).
4. Huang S.-B., Jeng Y.-L., & Lai C.-F. (2021). Note-Taking Learning System: The Use of the Learning Style Theory and the Peer Learning Method on Computer Programming Course. *Journal of Educational Computing Research*, 59(5), 870-895. <https://doi.org/10.1177/0735633120985235> (Original work published 2021) (дата обращения 10.04.2025).
5. Karnes, F. A., McCallum, R. S., & Oehler, J. J. (1985). The Relationship Between Learning Style Preference and Personality Variables: An Exploratory Investigation with Gifted Students. *Gifted Child Quarterly*, 29(4), 172-174. <https://doi.org/10.1177/001698628502900407> (Original work published 1985) (дата обращения 10.04.2025).

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Вивчарем Р. М.*

УДК 004.422.8:371.2

**Р. А. Верещагин** (студент группы ИСТ-112, СПбГУТ),  
[vereshagin.ra@sut.ru](mailto:vereshagin.ra@sut.ru)

## **РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ УЧЕБНЫМ ВЗАИМОДЕЙСТВИЕМ МЕЖДУ ПРЕПОДАВАТЕЛЯМИ И СТУДЕНТАМИ**

*Обоснована актуальность разработки информационной системы управления учебным взаимодействием между преподавателями и студентами. Проведен анализ существующих цифровых инструментов сопровождения образовательной деятельности и выявлены их ключевые ограничения. Изучены особенности цифрового взаимодействия участников образовательного процесса. Сформулированы функциональные требования к системе. Описан жизненный цикл задания, включающий процессы выполнения, проверки и выставления оценки. Реализованы основные компоненты и алгоритмы взаимодействия между преподавателями и студентами для организации учебного процесса. Определены перспективы интеграции системы в инфраструктуру учебного заведения и ее дальнейшего развития.*

*информационная система, цифровые инструменты, управление курсами, архитектура системы, компоненты ПО, организация учебного процесса, электронное обучение, взаимодействие преподаватель-студент, образовательная деятельность*

В условиях активной цифровизации образования становится все более актуальной задача разработки новых инструментов, способных упростить и структурировать взаимодействие преподавателей и студентов. Существующие LMS-системы, такие как Moodle, Google Classroom или Canvas, хотя и предоставляют широкий функционал, но зачастую оказываются избыточными, плохо адаптированными под конкретные образовательные практики и не учитывают реальные потребности преподавателей и обучающихся [1]. Это выражается в сложности интерфейсов, отсутствии гибкой обратной связи, перегрузке лишними функциями, а также в необходимости применения сторонних сервисов – от мессенджеров до облачных хранилищ. Все это снижает прозрачность учебного процесса и усложняет контроль за выполнением заданий [2]. В этой связи возникла необходимость разработки информационной системы, ориентированной на специфические задачи управления курсами и взаимодействия между участниками образовательного процесса в условиях университета.

В рамках исследования проведен анализ существующих цифровых инструментов и выделены их ключевые ограничения. Наиболее часто встречающиеся проблемы – сложность освоения, устаревшие интерфейсные решения и неинтуитивная навигация [3]. Подобное приводит к тому, что преподаватели вынуждены использовать разные платформы одновременно, а студенты теряют важную информацию из-за отсутствия централизованного канала связи.

В связи с выявленными ограничениями обоснована необходимость разработки системы, обеспечивающей централизованное управление заданиями, стабильную коммуникацию между участниками учебного процесса, поддержку хранения и оценивания студенческих работ, а также интегрированный механизм обратной связи, исключающий применение сторонних сервисов.

Изучив современные подходы к цифровому обучению, определены ключевые требования к функциональности системы [4, 5]. Она должна поддерживать создание курсов и заданий, прием и хранение работ студентов, выставление оценок с возможностью добавления комментариев, а также рассылку уведомлений о новых материалах и дедлайнах. Для преподавателя предусмотрен доступ к статистике по успеваемости и инструмент проверки уникальности текстов. Для студента – личный кабинет с актуальными заданиями, оценками и полученными замечаниями.

Для реализации системы разработаны ключевые компоненты, обеспечивающие эффективное взаимодействие между преподавателями и студентами. Преподаватель имеет возможность создавать задания, просматривать и оценивать загруженные студентами работы, оставлять комментарии и формировать объявления для группы. Студент, в свою очередь, получает доступ к личному кабинету, где отображаются активные задания, результаты проверки, замечания преподавателя и системные уведомления. Интегрирован алгоритм сравнения текстовых документов, позволяющий автоматически выявлять заимствования. В результате достигается прозрачность взаимодействия и минимизируется необходимость в сторонних инструментах.

Центральное место в системе занимает жизненный цикл задания, включающий этапы публикации, выполнения, проверки и оценки. Преподаватель формирует задание, студент загружает решение, после чего преподаватель проверяет его и выставляет оценку с комментарием.

При этом реализован механизм сравнения документов, выявляющий совпадения между текстами и помогающий преподавателю объективно оценивать работы. Визуализация найденных совпадений обеспечивается с помощью подсветки в HTML-отчете. Такая схема повышает прозрачность учебного взаимодействия, минимизируя необходимость в сторонних инструментах, и позволяет оперативно выявлять случаи недобросовестного заимствования.

На рис. 1 представлена диаграмма прецедентов, иллюстрирующая действия преподавателя при работе с системой: от публикации задания до оценки результатов.

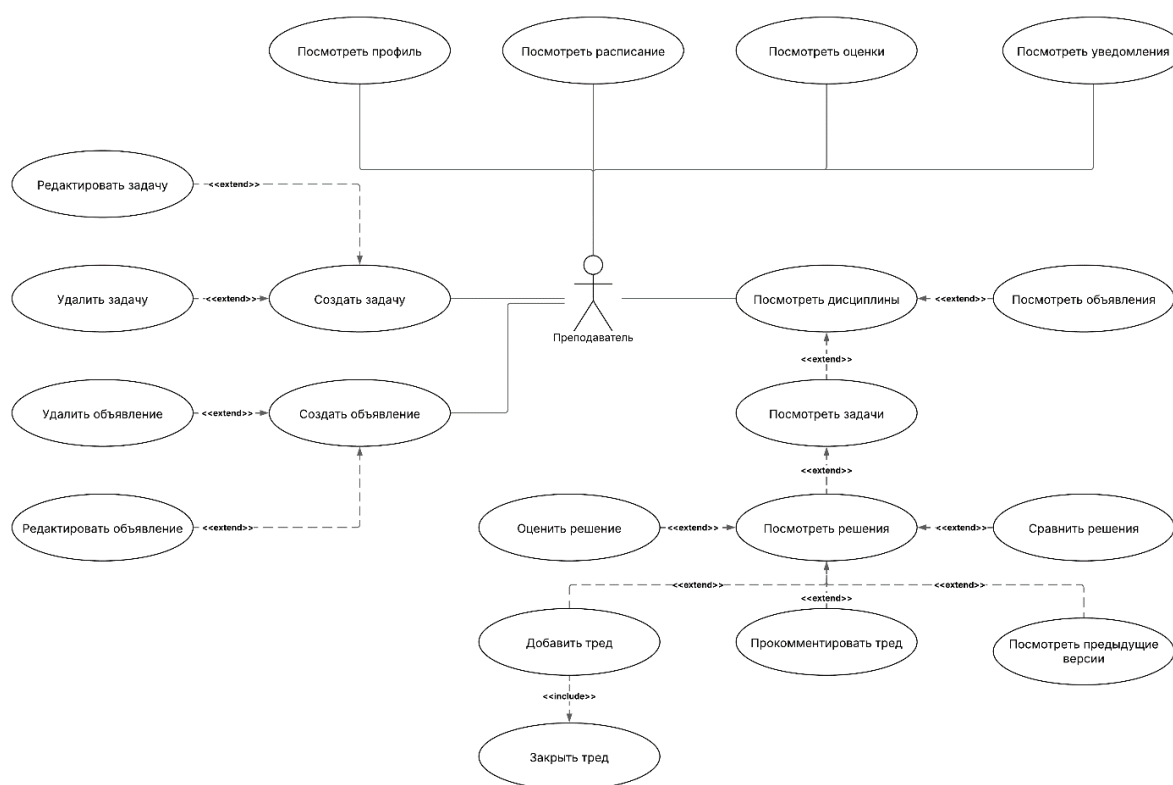


Рис. 1. Диаграмма прецедентов для роли «Преподаватель»

Архитектура системы построена на принципах разделения ответственности. Взаимодействие между компонентами организовано по модели «клиент–сервер»: пользовательский интерфейс работает с сервером через API, бизнес-логика взаимодействует с базой данных и файловым хранилищем. Такое решение позволяет масштабировать систему и при необходимости добавлять новые функции без переработки всей архитектуры.

Рисунки 2-4 демонстрируют пользовательские интерфейсы основных этапов взаимодействия: форму загрузки работы студентом (рис. 2), окно оценки и комментирования (рис. 3), результат автоматического сравнения

документов (рис. 4). Данные компоненты подтверждают практическую реализацию функциональных требований и ориентированность системы на реальные сценарии образовательного процесса.

Рис. 2. Форма загрузки решения

Рис. 3. Форма выставления оценки и комментария преподавателем

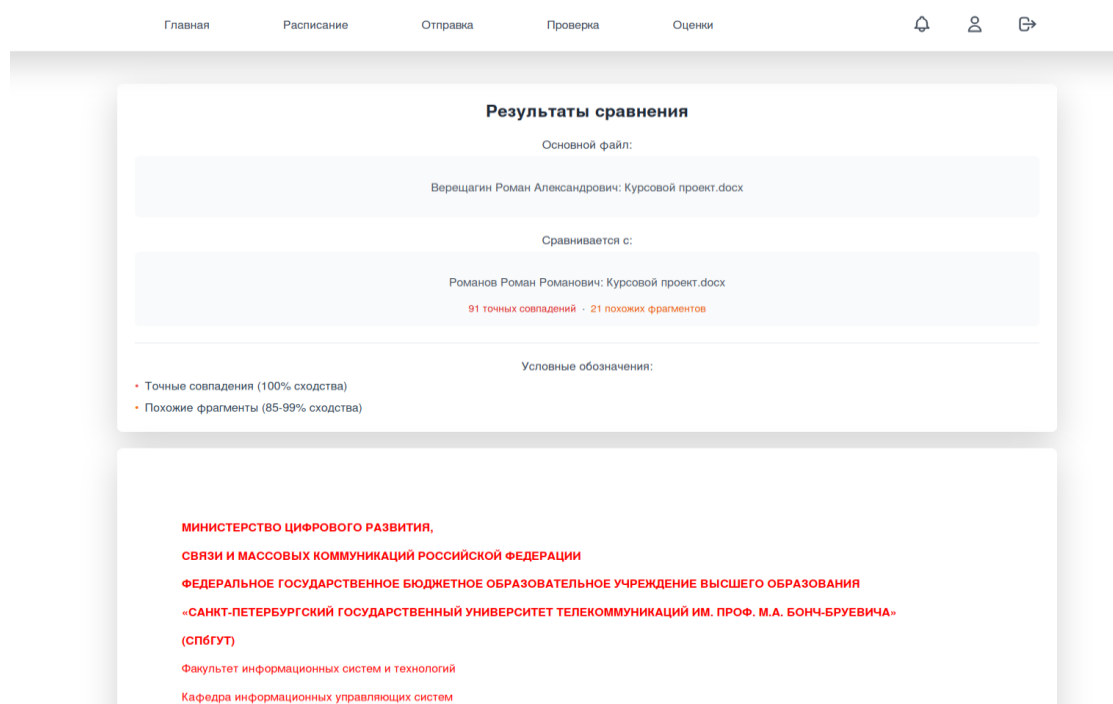


Рис. 4. Результат сравнения студенческих работ

Разработка данной информационной системы позволяет решить ряд практических задач, связанных с организацией цифрового взаимодействия в учебном процессе. На основе архитектуры и функциональных возможностей определены перспективы интеграции системы в цифровую инфраструктуру вуза – в том числе с платформами управления учебным расписанием, корпоративными учетными записями и системами отслеживания посещаемости (например, электронными пропусками). Предлагаемая система позволит унифицировать потоки данных, снизить дублирование информации и повысить прозрачность образовательного процесса. Также в дальнейшем возможно развитие системы за счет расширения функционала аналитики и добавления панели администратора.

#### Список используемых источников

1. Исаева Е. С. Современные LMS платформы дистанционного обучения: анализ и сравнение // Педагогика. Вопросы теории и практики. 2021. №6. URL: <https://cyberleninka.ru/article/n/sovremennyye-lms-platformy-distantsionnogo-obucheniya-analiz-i-sravnenie> (дата обращения 10.05.2025).

2. Нанай Ф. А. Цифровые технологии в контексте дистанционного обучения: вызовы, возможности и проблемы (на примере использования платформы Zoom и СДО Moodle) / Ф. А. Нанай, Л. А. Ростомян // Муниципальное образование: инновации и эксперимент. 2021. № 2(77).



3. Кобелева Н. Ф. Обзор некоторых инструментов СДО MOODLE и возникающих при их использовании вопросов и проблем / Н. Ф. Кобелева // Актуальные вопросы образования. 2023. № 3.

4. Карпачева И. А. Управление процессом обучения: от традиционных моделей к интеллектуальному управлению / И. А. Карпачева, В. С. Меренкова, С. Н. Дворяткина // Психология образования в поликультурном пространстве. 2020. № 3(51).

5. Григорьева И. В. Инновационные образовательные технологии и интерактивные методы обучения / И. В. Григорьева // Вестник Университета Российской академии образования. 2020. № 4.

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.021

**Р. А. Верещагин** (студент группы ИСТ-112, СПбГУТ),  
[vereshagin.ra@sut.ru](mailto:vereshagin.ra@sut.ru)

**А. О. Жаранова** (старший преподаватель кафедры ИУС, СПбГУТ),  
[zharanova.ao@sut.ru](mailto:zharanova.ao@sut.ru)

## РАЗРАБОТКА АЛГОРИТМА СРАВНЕНИЯ ДОКУМЕНТОВ НА ОСНОВЕ ЛЕММАТИЗАЦИИ И НОРМАЛИЗОВАННОГО РЕДАКЦИОННОГО СХОДСТВА

*Предложен алгоритм автоматизированного сравнения текстовых фрагментов, основанный на лемматизации, алфавитной сортировке токенов и вычислении нормализованного редакционного расстояния Левенштейна. Описана методика сегментации текста на предложения, их лингвистической нормализации и приведения слов к базовым формам. Представлен математический аппарат на основе динамического программирования для расчета сходства строк. Установлены пороговые значения, позволяющие классифицировать фрагменты как точные совпадения либо как близкие по смыслу. Рассмотрены перспективы внедрения алгоритма в системы контроля академической добросовестности.*

*лемматизация, токенизация, нормализованное редакционное сходство, алгоритм Левенштейна, динамическое программирование, сегментация текста, нормализация слов, классификация совпадений, академическая добросовестность, семантическое сходство*

Задача автоматизированного выявления текстовых совпадений приобретает все большую значимость в условиях цифровизации образования и роста требований к академической добросовестности. Современные методы анализа текстов должны учитывать как лексическое, так и структурное разнообразие естественного языка, включая перестановку слов, изменение грамматических форм и использование синонимов. В рамках данной работы предложен алгоритм, обеспечивающий высокоточную идентификацию совпадений на уровне предложений [1]. Основу алгоритма составляет сочетание лингвистической предобработки и редакционного сравнения нормализованных текстовых фрагментов.

На первом этапе алгоритм извлекает текстовое содержимое из DOCX-документов. Для этого производится обход структурных блоков файла – таких как абзацы, таблицы и другие текстовые элементы. Извлеченный текст очищается от лишних символов, пробелов и форматирования, а также преобразуется к нижнему регистру. Это позволяет унифицировать данные и подготовить их к последующим операциям.

Далее происходит разбиение текста на предложения. Этот шаг необходим, чтобы сравнивать не весь документ целиком, а более мелкие смысловые единицы. Для разметки используется токенизатор из библиотеки `nltk`, адаптированный под особенности русского языка.

После сегментации каждое предложение подвергается лемматизации: слова приводятся к словарным формам, что особенно важно для работы с русскоязычными текстами, где одно и то же слово может иметь множество морфологических вариантов.

После предварительной обработки текстов происходит основной этап – математическое сравнение предложений на основе вычисления меры их сходства. Для этих целей используется метрика сходства строк `token_sort_ratio`, реализованная в библиотеке `RapidFuzz`. Математическая модель, лежащая в основе данной метрики, основана на сравнении двух текстовых строк путем анализа множества содержащихся в них слов (токенов).

Для каждой пары предложений  $S_1$  и  $S_2$  всех сравниваемых документов алгоритм формирует две строки  $A$  и  $B$ . Сначала токены каждого предложения сортируются в алфавитном порядке, после чего объединяются в одну строку через пробел. Такой прием гарантирует независимость результата от порядка слов в исходном предложении и позволяет выявлять сходные по составу фразы, даже если их синтаксис был перестроен [2].

Основной метрикой сходства является нормализованное редакционное расстояние Левенштейна, задающееся через функцию  $d_{i,j}$  для строк длины  $i$  и  $j$ :

$$d_{i,j} = \begin{cases} i, j = 0 \\ j, i = 0 \\ \min(d_{i-1,j} + 1, d_{i,j-1} + 1, d_{i-1,j-1} + \delta(a_i, b_j)), i > 0, j > 0, \end{cases}$$

где  $a_i$  и  $b_j$  –  $i$ -й и  $j$ -й символ строк  $A$  и  $B$ , а  $\delta(a_i, b_j)$  равна 0 при  $a_i = b_j$  и 1 в противном случае [3].

Итоговое расстояние равно  $d_{m,n}$ , где  $m = |A|$  и  $n = |B|$  ( $|A|$  и  $|B|$  – длины строк  $A$  и  $B$  соответственно). Для перевода расстояния в процент сходства (Similarity) используется нормировка по максимальной длине строк:

$$\text{Similarity}(S_1, S_2) = 100 \times \left(1 - \frac{d_{m,n}}{\max(|A|, |B|)}\right) \%.$$

Далее результаты математического сравнения классифицируются на две основные группы в зависимости от степени сходства. В первую категорию попадают «точные совпадения» – предложения, степень сходства которых равна 100 %. Ко второй группе относятся «похожие совпадения», степень сходства которых превышает заданный пороговый уровень, чаще всего принимаемый на уровне 85 %. Указанный порог является регулируемым параметром и может быть настроен согласно требованиям преподавательского состава или внутренним стандартам образовательного учреждения.

Внедрение данного алгоритма в автоматизированные системы контроля академической добросовестности открывает широкие перспективы для повышения объективности и прозрачности оценки студенческих работ. За счет адаптивности порогов схожести и устойчивости к перестановке слов и грамматическим трансформациям алгоритм может эффективно использоваться как в локальных системах антиплагиата образовательных учреждений, так и в масштабируемых облачных решениях. Интеграция с платформами дистанционного обучения, цифровыми библиотеками и системами хранения работ позволит сформировать единую среду мониторинга оригинальности, обеспечивая профилактику недобросовестных практик и содействуя формированию академической культуры.

#### **Список используемых источников**

1. Алгоритмические способы решения задачи нечеткого сравнения строк / Д. Г. Галимуллин, И. Е. Гусев, М. С. Новиков [и др.] // Завалишинские чтения'24: Сборник докладов XIX Международной конференции по электромеханике и робототехнике, Санкт-Петербург, 16–17 апреля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2024.
2. Ефремова А. Н. Сравнительный анализ алгоритмов нечеткого сравнения строк / А. Н. Ефремова // Труды Братского государственного университета. Серия: Естественные и инженерные науки. 2023.
3. Свищева И. В. Расстояние Левенштейна / И. В. Свищева, И. В. Беликов // Моя профессиональная карьера. 2022.

## УДК 519.2

**Р. М. Вивчарь** (к.т.н., доцент, доцент кафедры ПИиВТ, СПбГУТ),  
[vivchar.rm@sut.ru](mailto:vivchar.rm@sut.ru)

**В. А. Гончаров** (магистрант группы ИКПИ-492м, СПбГУТ),  
[goncharov.va@sut.ru](mailto:goncharov.va@sut.ru)

## МЕТОДИКА ПОИСКА КОРНЕВЫХ ПРИЧИН НАРУШЕНИЙ НОРМАЛЬНОГО ФУНКЦИОНИРОВАНИЯ ГИБРИДНОЙ СЕТИ

*Гибридные сети, объединяющие как традиционные проводные, так и современные беспроводные технологии, обеспечивают повышенную гибкость и надежность передачи данных. Однако их сложная архитектура также создает множество проблем, особенно в вопросах поддержки эксплуатационной эффективности и надежности. Для решения таких проблем использовалась методология анализа корневых причин проблемы. Дополнив методами из раздела «Теория вероятностей и математическая статистика», был разработан экспертно-статистический метод моделирования и анализа причин нарушений нормального функционирования гибридной сети на основе применения Байесовой сети с использованием типовых шаблонов причинно-следственных связей, позволяющий проводить автоматизированный анализ, диагностику и прогнозирование причин нарушений.*

*гибридные сети, Байесовы сети, анализ корневых причин, АКП*

В эпоху, характеризующуюся быстрым развитием технологий и растущей зависимостью от взаимосвязанных систем, гибридные сети стали основными инфраструктурами, лежащими в основе связи и обмена данными в различных областях. Эти сети, объединяющие как традиционные проводные, так и современные беспроводные технологии, обеспечивают повышенную гибкость и надежность передачи данных. Однако их сложная архитектура также создает множество проблем, особенно в вопросах поддержки эксплуатационной эффективности и надежности. Нарушения в их нормальном функционировании могут привести к значительным сбоям, влияющим на все: от индивидуального опыта пользователя до критически важных бизнес-операций. Поэтому понимание корней этих нарушений имеет важное значение для обеспечения устойчивости и долговечности гибридных систем связи.

В современном менеджменте качества для обозначения процесса решения проблем на основе поиска и устранения ее корневых причин используется термин анализ корневых причин (root cause analysis, RCA) [1, 2]. Анализ корневых причин (АКП) – это структурированное исследование, целью которого является идентификация истинных причин проблемы и принятие действий, необходимых для устранения этих причин. Поскольку в основе любой проблемы лежат

причины этой проблемы, то для ее решения необходимо вначале идентифицировать причину, а затем выработать и предпринять корректирующее воздействие для устранения этой причины, что в конечном итоге приведет к разрешению проблемы, при этом эффективное решение проблемы невозможно без поиска и устранения ее корневой (системной) причины (root cause) [2].



Рис. 1. Диаграмма Исикавы

На рис. 1 представлена диаграмма Исикавы – графический способ исследования и определения наиболее существенных причинно-следственных взаимосвязей между факторами и последствиями, которые ведут к нарушению нормального функционирования гибридной сети.

Зная причины и последствия, можно построить граф, каждую вершину описать в виде дискретной случайной величины и задать множество ее значений с помощью метода Байеса.

Метод Байеса относится к классу статистических методов распознавания причин надежности и является наиболее эффективным [3, с. 11-18]. Он основан на теореме Байеса, которая позволяет рассчитать апостериорную вероятность гипотезы при условии наступления свидетельства; также возможно, как прогнозирование, так и диагностирование дефектов. Данный метод нашел применение и при анализе и диагностике причин несоответствий в области качества [4].

Байесовы сети (БС) – это разновидность графовых моделей, отражающие вероятностные связи между событиями предметной области.

По сравнению с методами анализа корневых причин, обладающими высокой долей субъективизма, в основе БС лежит строгий аппарат теории ве-

роятностей, статистики и теории графов. Следовательно, выводы, получаемые на основе БС, можно считать объективными при условии объективности входных данных.

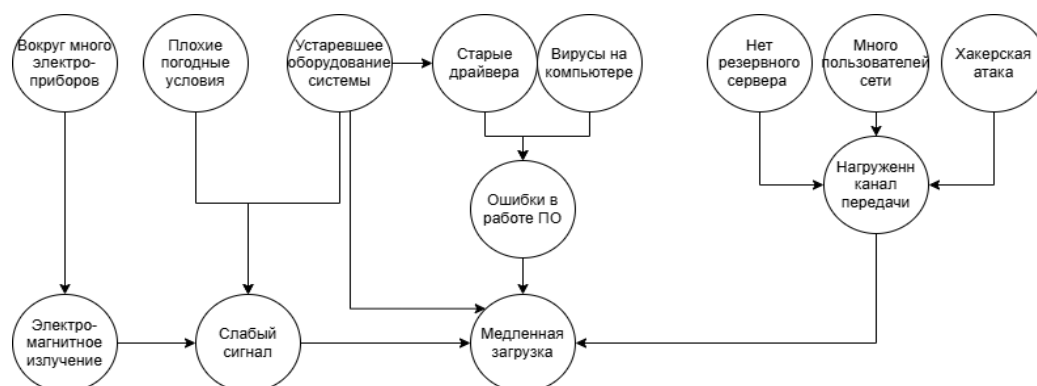


Рис. 2. Байесова сеть

На рис. 2 изображена Байесова сеть, описывающая причинно-следственные связи (события), приводящие к возникновению медленной загрузки данных в гибридной сети связи.

Согласно Байесовскому подходу [5, 6], под вероятностью понимается степень доверия гипотезам, связанным с событиями реального мира. Обычно степень доверия к пропозиции  $A$ , полученной на основе совокупности знаний  $K$  субъекта, обозначают  $P(A | K)$ . При проведении расчетов символ  $K$  опускают и записывают  $P(A)$ .

При расчетах имеется возможность совместного использования степеней доверия и вероятностей в классической (частотной) трактовке, что является важным преимуществом БС. В частности, это позволяет в единой модели учесть как знания экспертов (субъективную информацию), так и вероятностные распределения (объективную информацию), которые могут быть получены на основе статистических данных либо иных сведений о моделируемой системе:

$$P(A) = \sum_i P(A, B_i),$$

$$P(A, B) = P(B) * P(A|B) \quad (1)$$

Вероятность любого события  $A$  может быть вычислена путем обуславливания на множестве несовместных событий  $B_i$ ,  $i = 1, 2, \dots, n$ , образующих полную группу и последующего суммирования:

$$P(A) = \sum_i P(A|B_i)P(B_i) \quad (2)$$

Декомпозиция (2) представляет собой базу для проведения гипотетических рассуждений. Это означает, что степень доверия к любому событию  $A$

представляет собой взвешенную сумму степеней доверия к этому событию во всех случаях, когда осуществление  $A$  возможно.

В результате на рис. 3 предложена методика, которая позволяет построить причинную Байесову сеть для анализа и моделирования несоответствий, при этом использование формул и Байесовского подхода позволяет в единой модели учитывать как статистическую информацию о нарушениях, так и знания экспертов, формально представленные в виде графа и субъективных вероятностей.

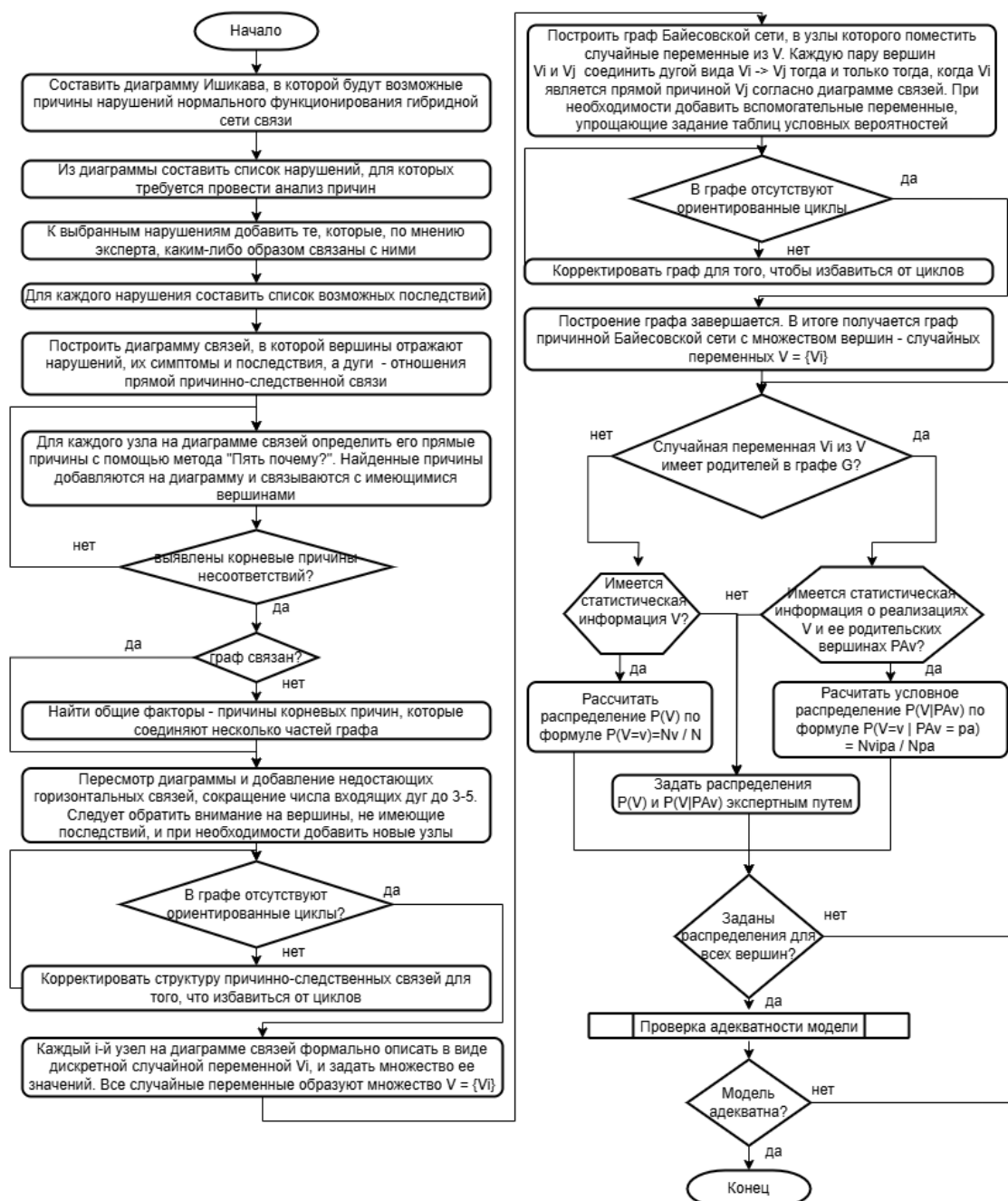


Рис. 3. Схема экспертно-статистического метода моделирования и анализа причин нарушений нормального функционирования гибридной сети



**Список используемых источников**

1. Савинкина В. А. Анализ корневых причин / по материалам статьи Root Cause Analysis vs. Shallow Cause Analysis by Robert J. Latino, опубликованной на сайте [www.reliability.com](http://www.reliability.com) подготовила В.А. Савинкина; Robert J. Latino // Методы менеджмента качества. 2008. № 8. С. 51-53.
2. Andersen B. Root cause analysis: simplified tools and techniques / B. Andersen, T. Fagerhaug. American Society for Quality, Quality Press, 2006. 240 p.
3. Биргер И. А. Техническая диагностика / И. А. Биргер. М.: Машиностроение, 1978. 240 с.
4. Червяков И. В. Использование методов технической диагностики для поиска причин несоответствий / И. В. Червяков // Методы менеджмента качества. 2009. № 4. С. 40-43.
5. Pearl J. Probabilistic Reasoning in Intelligent Systems / J. Pearl. San Francisco: Morgan Kaufmann, 1988. 520 p.
6. Pearl, J. Causality: Models, Reasoning and Inference / J. Pearl. Cambridge University Press. 2-nd edition, 2009. 464 p.

УДК 004.42

Д. В. Винокурова (аспирант кафедры ИС, РГПУ им. А. И. Герцена),  
[d.v.vinokurova@gmail.com](mailto:d.v.vinokurova@gmail.com)

## ПРОГРАММНЫЙ ПОДХОД К ВЫБОРУ НАЧАЛЬНЫХ ПРИБЛИЖЕНИЙ ДЛЯ РЕШЕНИЯ НЕЛИНЕЙНЫХ УРАВНЕНИЙ ЧИСЛЕННЫМИ МЕТОДАМИ

*Сходимость численных методов, применяемых для поиска корней нелинейных уравнений, зависит от правильного выбора начальных приближений. В учебных целях при ручной отработке навыков решения задач подобного типа важно прийти к решению за конкретное количество итераций. Неудачный выбор начальных приближений может привести к увеличению количества итераций и отсутствию сходимости численного метода. Для исключения подобных ситуаций при поиске начальных приближений, необходимых для решения нелинейных уравнений численными методами, предлагается подход, основанный на программной реализации с использованием языка Python, который обеспечивает сходимость методов за определенное число шагов. Приводится сравнительный анализ количества итераций необходимых для поиска корней с применением алгоритма поиска начальных приближений и ручного метода подбора интервалов локализации корня на семи типах уравнений. Программная реализация показала свою успешность на 520 различных нелинейных уравнениях и может применяться в учебном процессе.*

*вычислительная математика, нелинейные уравнения, автоматизация, Python, численные метод, начальные приближения*

Для решения нелинейных уравнений применяют известные численные методы, такие как метод половинного деления, метод простой итерации, метод Ньютона, метод хорд и многие другие. Сходимость некоторых методов напрямую зависит от правильного выбора начальной точки или интервала. Как правило, в литературе [1-4] не делается акцент на том, каким образом получают начальные приближения для различных численных методов, а приводимые примеры ограничиваются функциями, которые не содержат асимптоты и существенные ограничения на область допустимых значений [2, 4].

В учебных целях преподавателю часто необходимо предоставлять обучающимся комплект различных типовых вариантов задач по нелинейным уравнениям для их решения определенным методом. С целью получения навыков использования численных методов для решения такого рода задач, обучающиеся должны осуществлять итерации вручную. Если начальные

приближения будут выбраны неудачно, то потребуется большое количество шагов и в худшем случае метод может не сойтись.

Цель исследования: программная реализация алгоритмического подхода к выбору начальных приближений для решения нелинейных уравнений численными методами.

Для достижения поставленной цели предлагается решение в виде алгоритма на языке программирования Python, который осуществляет поиск начальных приближений на заданном интервале. Алгоритм основывается на фундаментальной теореме Больцано-Коши о нуле непрерывной функции [5, с. 128], которая применима только если функция на отрезке  $[a, b]$  является непрерывной. Выполнение данного условия в программе обеспечивается определением непрерывных областей функции. Код предлагаемого алгоритма доступен в Zenodo [6]. Модуль *roots\_nonlinear\_eq* содержит функцию для поиска начальных приближений *find\_initial\_approximations*, которая содержит один обязательный параметр *equation* – текущее уравнение и четыре дополнительных параметра: *initial\_range* – интервал для поиска начальных приближений, который задается в виде кортежа  $(x_{min}, x_{max})$ , *f\_interval* – флаг наличия интервалов или отсутствия (для некоторых методов начальные приближения могут задаваться в виде одной точки либо в виде интервала), *num\_points* – количество точек для построения сетки, *ndigit* – количество знаков после запятой.

В зависимости от типа уравнения, вычисляются значения  $x$ , которые сохраняются в переменной *x\_values* в пределах заданного диапазона  $x_{min}$  и  $x_{max}$ . Если функция является нетригонометрической и не принадлежит к классу дробно-рациональных функций и комбинированных функций, содержащих дробно-рациональные функции с другими типами функций, а также непрерывная область не содержит всю область действительных чисел, то значения переменной *x\_values* формируются при помощи функции *create\_cont\_domain\_values*. В противном случае, *x\_values* заполняется значениями, с использованием функции *linspace* из библиотеки Numpy, которая позволяет равномерно распределять числа. В цикле выполняется поиск начальных приближений, концы отрезка оцениваются на наличие различных знаков. Если условие истинно, значит в данном интервале имеется корень. Затем осуществляется проверка выполнения условий для различных типов уравнений. В первом условии проверяется содержит ли данное уравнение особые типы функций и не включает ли непрерывная область всю об-

ласть действительных чисел, во втором проверяется не относится ли функция к классу тригонометрических, третье условие выполняется в случае невыполнения первых двух. После проверки условий формируются начальные приближения.

Функция *create\_cont\_domain\_values* используется не для всех типов функций:

тригонометрические функции являются периодическими и в библиотеке SymPy их непрерывные области записываются через лямбда-функции. При наличии сложных функций внутри аргумента усложняется запись непрерывных интервалов и их необходимо раскрывать по определенным алгоритмам. Существует риск пропуска особенностей поведения функции, поэтому проводится проверка на наличие асимптот;

в дробно-рациональных уравнениях и комбинированных уравнениях, включающих комбинацию дробно-рациональных функций с другими типами функций при таком способе формирования значений, могут получаться лишние корни, из-за слишком близких значений вблизи асимптот.

В модуле *roots\_nonlinear\_eq* для вызова численных методов с определенными параметрами были добавлены функции *find\_roots\_with\_user\_functions* и *find\_roots\_with\_root\_scalar*. В функции *find\_roots\_with\_user\_functions* можно осуществлять поиск корней, опираясь на собственную реализацию алгоритмов численных методов (рис. 1).

Функция *find\_roots\_with\_root\_scalar* основывается на методологии функции *root\_scalar* из модуля SciPy. В модуле *examples* приведены примеры вызова различных типов функций с использованием двенадцати методов (восьми методов, реализованных в *root\_scalar* и четырех методов, реализованных автором статьи) из модуля *roots\_nonlinear\_eq*.

Сравнительный анализ количества итераций, необходимых для нахождения корней с применением алгоритма поиска начальных приближений и ручного метода подбора интервалов локализации корня на семи типах уравнений (логарифмических, показательных, тригонометрических, дробно-рациональных, иррациональных, полиномиальных и комбинированных), показал эффективность предлагаемого алгоритма и позволил найти приближения, которые привели к сходимости численных методов (рис. 2, 3).

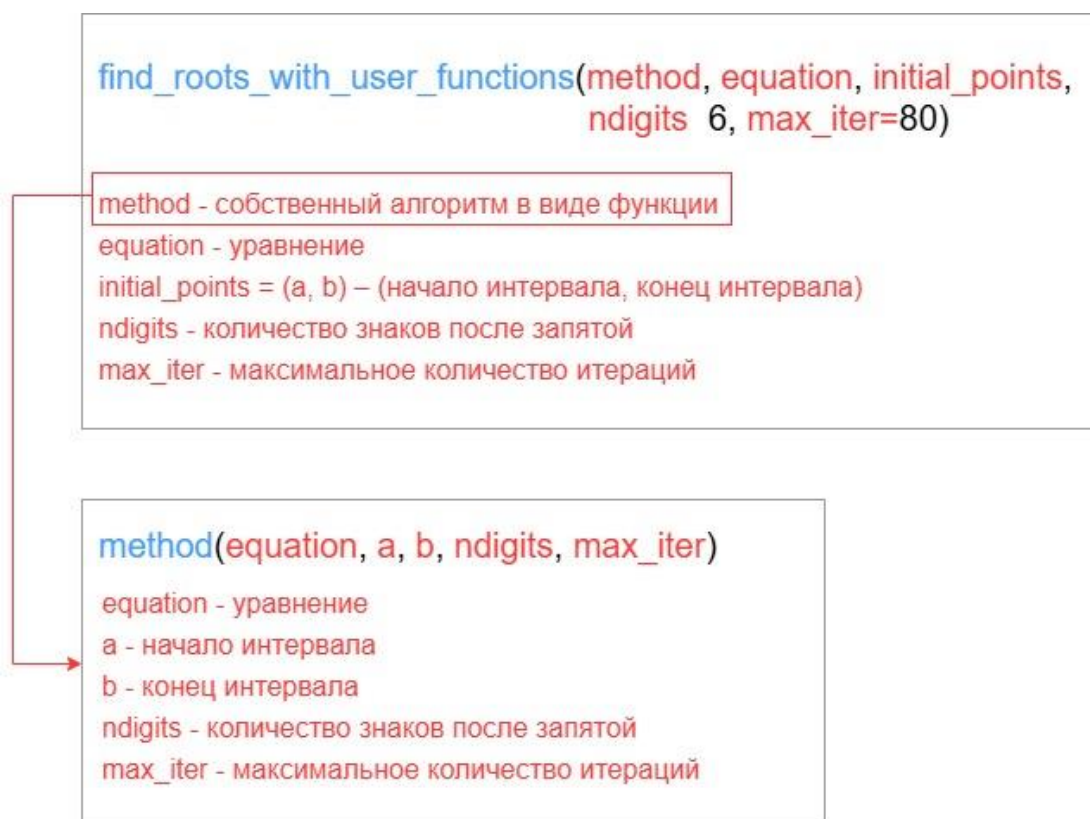


Рис. 1. Параметры функции, вызывающей собственные алгоритмы

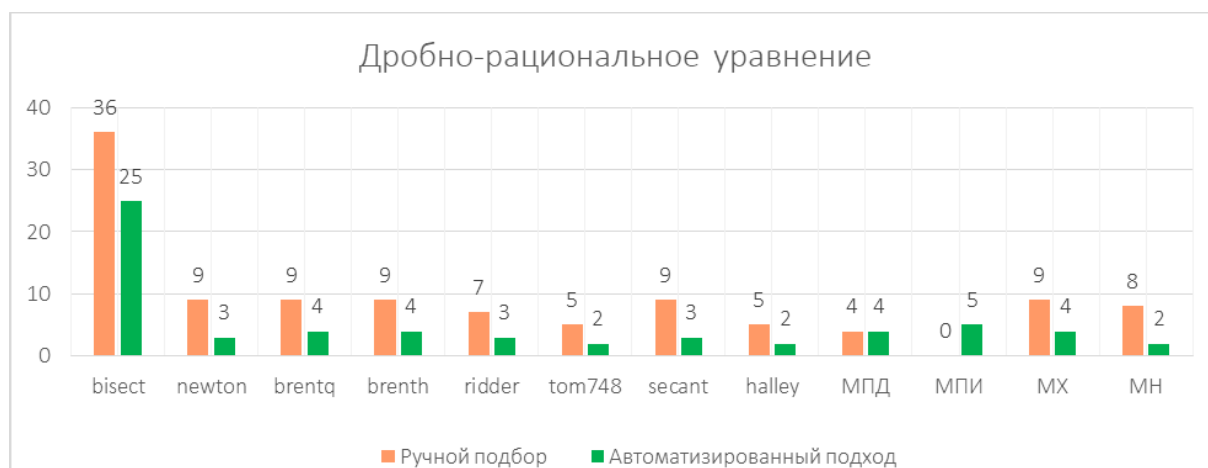


Рис. 2. Сравнительная гистограмма необходимого количества итераций для решения дробно-рационального уравнения различными методами

Отметим, что на гистограммах максимальное количество итераций ограничено значением 50, которое фактически могло иметь большее значение. Результаты анализа для других функций доступны в Zenodo в файле Excel [6].

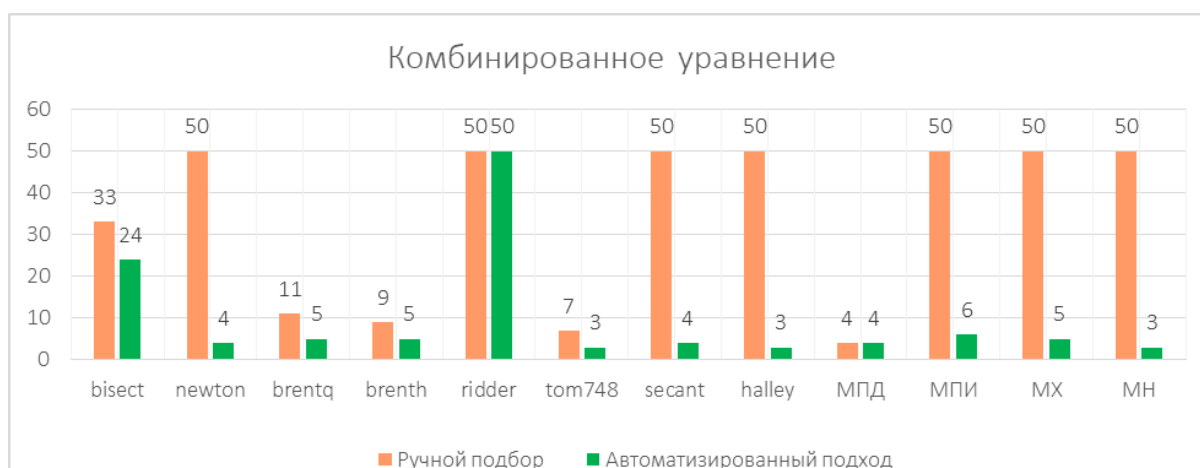


Рис. 3. Сравнительная гистограмма необходимого количества итераций для решения комбинированного уравнения различными методами

Реализованный подход был протестирован на 520 различных нелинейных уравнениях [6]:

- 40 логарифмических уравнениях;
- 40 показательных уравнениях;
- 120 тригонометрических уравнениях;
- 30 дробно-рациональных уравнениях;
- 20 иррациональных уравнениях;
- 50 полиномиальных уравнениях;
- 220 комбинированных уравнениях.

Полученные корни уравнений сравнивались с эталонными результатами, вычисленными в системе Wolfram Mathematica. Результаты тестирования показали успешность применения данного алгоритма. Для поиска множества корней в диапазоне, при их большом количестве, в некоторых случаях необходимо увеличивать количество точек в *num\_points*.

Представленный алгоритм был внедрен в один из разделов создаваемой системы генерации задач по вычислительной математике и будет использован в учебном процессе для генерации различных вариантов задач по нелинейным уравнениям. Алгоритм программы доступен в репозитории Zenodo [6] и может использоваться широким кругом разработчиков генерируемых учебных материалов и преподавателями.

#### Список используемых источников

1. Зенков А. В. Вычислительная математика для IT-специальностей. М; Вологда: Инфра-Инженерия, 2022. 128 с. ISBN 978-5-9729-0883-7.
2. Мицель А. А. Вычислительные методы. Томск: Эль Контент, 2013. 198 с. ISBN 978-5-4332-0121-7.

3. Агапова Е. Г. Вычислительная математика. Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2017. 92 с. ISBN 978-5-7389-2354-8.

4. Коледин В. В. Вычислительная математика: учебное пособие. Нижневартовск: [б.и.], 2023. 100 с.

5. Фихтенгольц Г. М. Основы математического анализа. Ч. 1. СПб.: Лань, 2024. 448 с. ISBN 978-5-507-47695-4.

6. Винокурова Д. В. Программная реализация алгоритма поиска начальных приближений для решения нелинейных уравнений и анализ результатов, 2024. URL: <https://doi.org/10.5281/zenodo.15540249> (дата обращения 29.05.25)

*Статья представлена научным руководителем,  
доктором физико-математических наук, профессором Флегонтовым А. В.*

УДК 004.7

М. А. Волков (студент группы ИКПИ-11, СПбГУТ), [volkov1.ma@sut.ru](mailto:volkov1.ma@sut.ru)

## АВТОМАТИЗАЦИЯ УЧЕТА РЕСУРСОВ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА SNMP

*Современные телекоммуникационные сети становятся все более сложными, что требует эффективных методов мониторинга и управления. Одним из таких методов является использование протокола SNMP, который обеспечивает централизованный сбор данных о состоянии сетевого оборудования. Точность и полнота получаемой информации напрямую влияют на возможность оперативного реагирования на неисправности и оптимизацию работы сети. Это делает актуальной задачу разработки программного обеспечения для автоматизированного сбора, обработки и анализа данных о состоянии телекоммуникационного оборудования. В рамках данной работы рассматривается реализация такой системы на основе протокола SNMP с использованием языка программирования PHP.*

*автоматизация, SNMP, телекоммуникационное оборудование, сеть доступа, база данных*

Сеть доступа – это часть телекоммуникационной инфраструктуры, которая соединяет оборудование конечных пользователей с магистральной сетью оператора связи. Основными компонентами сети доступа являются абонентские линии, соединяющие пользовательские устройства с ближайшими узлами связи, и оборудование, обеспечивающее передачу и маршрутизацию данных. В зависимости от используемых технологий, сети доступа могут быть построены на основе медных кабелей, оптоволоконных линий или их комбинаций. Сеть доступа может быть организована при помощи таких технологий как ADSL, PON и Ethernet, каждая из которых обладает своими преимуществами и областями применения [1]:

- ADSL (Asymmetric Digital Subscriber Line) – асимметричная цифровая абонентская линия, позволяет передавать данные по медным телефонным линиям, обеспечивая асимметричный доступ в интернет, где скорость загрузки данных превышает скорость выгрузки. Основной принцип работы ADSL заключается в разделении полосы пропускания телефонного кабеля на несколько частотных диапазонов, что позволяет одновременно передавать голосовые и цифровые сигналы (рис. 1). Это достигается с помощью технологии мультиплексирования с разделением по частоте (FDM). Это



удобно для большинства пользователей, но ограничено качеством и протяженностью медных линий.



Рис. 1. ADSL сеть

- PON (Passive Optical Network) – пассивная оптическая сеть, использующая одну волоконно-оптическую линию для обслуживания нескольких конечных точек (рис. 2). Это достигается за счет применения пассивных оптических разветвителей (сплиттеров), которые делят оптический сигнал на несколько выходов, позволяя ему достигать множества абонентов. Это обеспечивает высокую скорость передачи данных и минимальные затраты на обслуживание, что делает PON хорошим решением для широкополосного доступа.

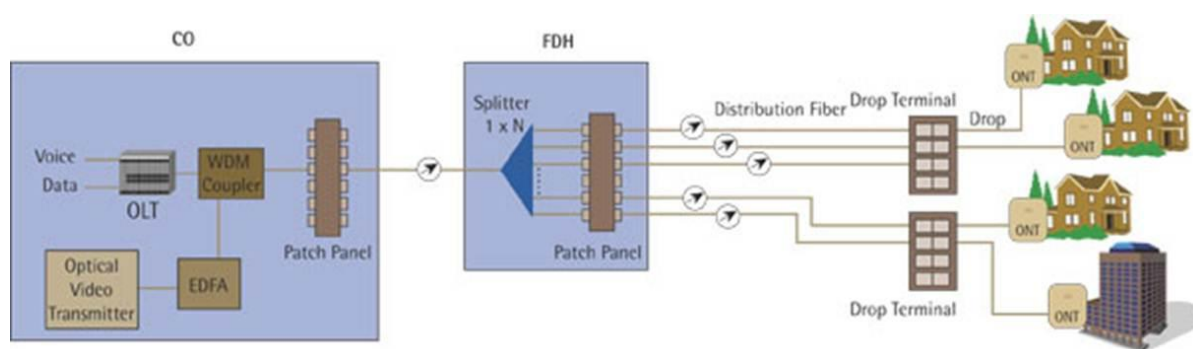


Рис. 2. Пассивная оптическая сеть

- Ethernet – доминирующая технология, используемая в проводных локальных сетях (LAN), обеспечивающая высокоскоростную и надежную передачу данных между устройствами. Ethernet работает на канальном и физическом уровнях модели OSI. На физическом уровне стандарты Ethernet определяют проводные соединения и электрические сигналы, а на канальном уровне – формат кадров и протоколы управления доступом к среде. Ос-

новые компоненты Ethernet-сети: сетевые адаптеры, коммутаторы и кабельная инфраструктура. Устройство, желающее отправить данные, формирует кадр, который затем передается по кабелю к коммутатору или маршрутизатору, обеспечивая связь между устройствами в локальной сети. Благодаря высокой скорости и надежности Ethernet широко применяется как в локальных сетях (LAN), так и в инфраструктуре операторов связи.

Для эффективного управления и мониторинга сетевого оборудования в современных телекоммуникационных системах применяется протокол SNMP (Simple Network Management Protocol). Он позволяет собирать информацию о состоянии устройств, контролировать их работу и управлять настройками удаленно (рис. 3). Работа SNMP основана на клиент-серверной модели, где менеджер (NMS – Network Management System) отправляет запросы агентам, установленным на сетевых устройствах. Агент обрабатывает запрос и предоставляет информацию в виде объектов данных, организованных в иерархической структуре, называемой MIB (Management Information Base). Основные операции SNMP включают получение данных (GET), изменение параметров устройства (SET) и отправку уведомлений о событиях (TRAP). Использование SNMP обеспечивает централизованный мониторинг и помогает оперативно реагировать на неисправности, снижая затраты на обслуживание сети [2].

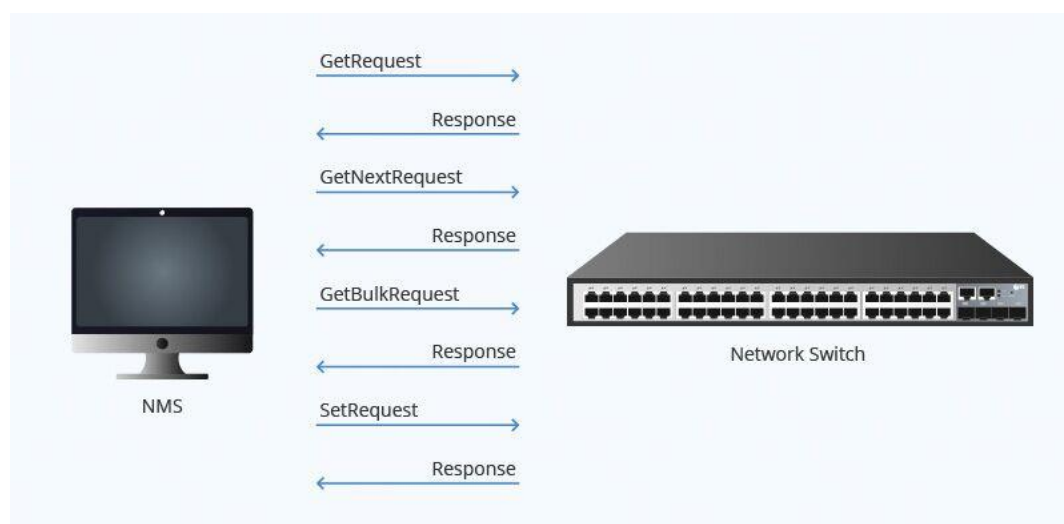


Рис. 3. Процесс Get/GetNext/GetBulk/Set приложения SNMPv2c

В данной работе рассматривается разработка системы сбора информации о состоянии оборудования сети доступа на основе SNMP. С использованием языка программирования PHP был разработан скрипт, который выполняет автоматизированный опрос сетевых устройств, обрабатывает полученные данные и сохраняет их в базу данных. Цель системы – создать

удобный и эффективный механизм контроля за состоянием сетевой инфраструктуры, что позволит операторам связи оптимизировать процессы управления и повысить надежность предоставляемых услуг.

Проектируемая система опирается на принципы системного анализа, позволяющие эффективно организовать процессы сбора и обработки информации (рис. 4). В основе системы лежит концепция управления, включающая три ключевые подсистемы: управляющую систему (УС), объект управления (ОУ) и систему связи (СС) [3].

- Управляющая система (УС) отвечает за принятие решений на основе анализа собранных данных. В данном случае роль УС выполняет разработанный PHP-скрипт, обрабатывающий информацию, полученную через SNMP.

- Объект управления (ОУ) – это устройства сети доступа (ADSL, PON, Ethernet), которые предоставляют информацию о своем состоянии.

- Система связи (СС) обеспечивает передачу данных между УС и ОУ, в данном случае используя протокол SNMP.

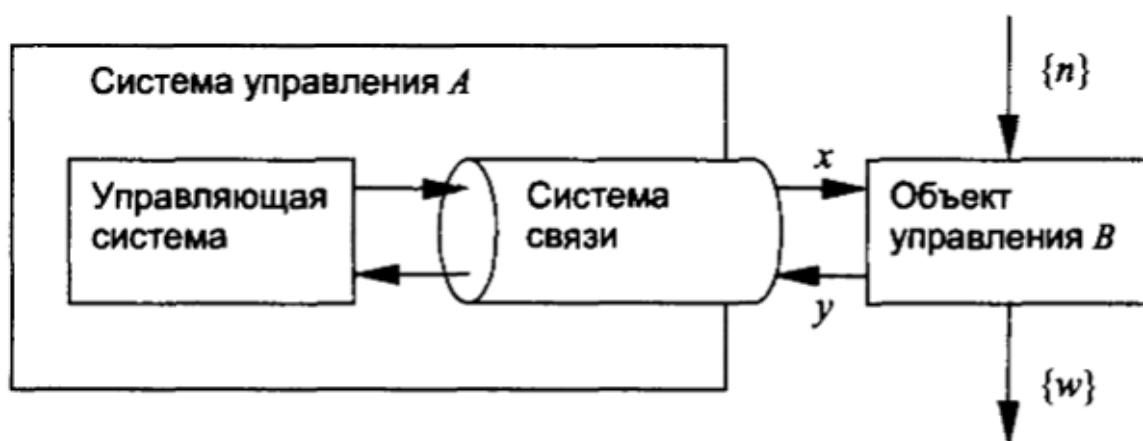


Рис. 4. Система с управлением

Такое построение системы позволяет организовать полноценный цикл управления, включающий сбор информации, ее анализ и корректировку состояния оборудования на основе принятых решений.

Для реализации системы был использован язык программирования PHP [4]. Данный выбор обусловлен рядом факторов:

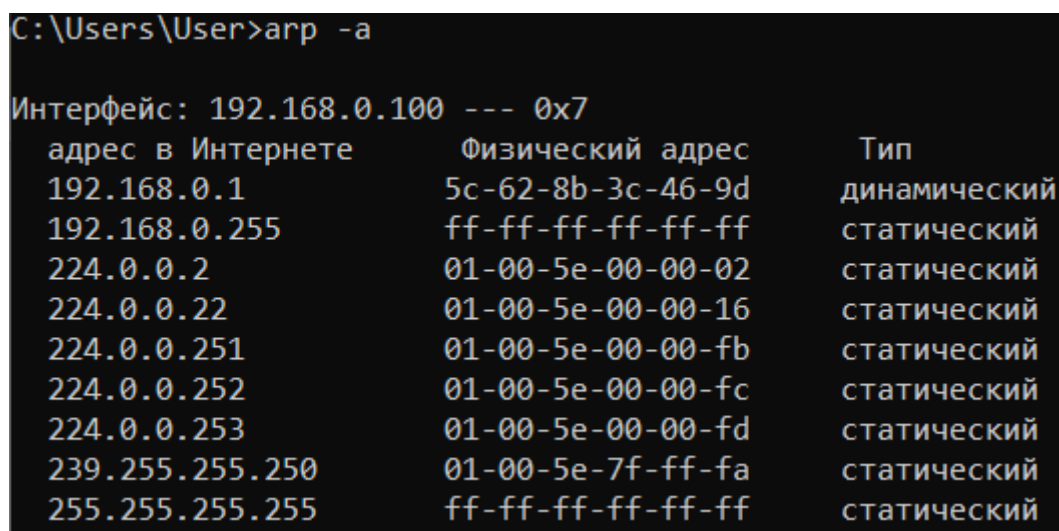
1. Гибкость – PHP позволяет легко интегрировать различные библиотеки и работать с сетевыми протоколами, в том числе и с протоколом SNMP.
2. Простота и доступность – PHP широко используется в разработке веб-приложений, что упрощает визуализацию собранных данных.

3. Наличие встроенных функций работы с SNMP – RNP предоставляет стандартные функции `snmpwalk()` и `snmpget()`, что значительно упрощает процесс получения данных.

Основные этапы работы скрипта:

1. Определение параметров локальной сети – функция `get_local_network()` анализирует сетевые настройки текущего устройства, получая его IP-адрес и маску подсети. На основе этих данных формируется адресная зона поиска, что позволяет ограничить область сканирования только необходимым диапазоном.

2. Получение списка активных устройств – функция `get_ip_addresses()` использует команду `arp -a` для сбора списка IP-адресов устройств, присутствующих в локальной сети (рис. 5). Полученный список проходит фильтрацию, основанную на маске подсети, чтобы исключить ненужные записи.



```
C:\Users\User>arp -a
```

| Интерфейс:        | 192.168.0.100     | ---          | 0x7 |
|-------------------|-------------------|--------------|-----|
| адрес в Интернете | Физический адрес  | Тип          |     |
| 192.168.0.1       | 5c-62-8b-3c-46-9d | динамический |     |
| 192.168.0.255     | ff-ff-ff-ff-ff-ff | статический  |     |
| 224.0.0.2         | 01-00-5e-00-00-02 | статический  |     |
| 224.0.0.22        | 01-00-5e-00-00-16 | статический  |     |
| 224.0.0.251       | 01-00-5e-00-00-fb | статический  |     |
| 224.0.0.252       | 01-00-5e-00-00-fc | статический  |     |
| 224.0.0.253       | 01-00-5e-00-00-fd | статический  |     |
| 239.255.255.250   | 01-00-5e-7f-ff-fa | статический  |     |
| 255.255.255.255   | ff-ff-ff-ff-ff-ff | статический  |     |

Рис. 5. Пример работы команды `arp -a`

3. Опрос устройств через SNMP – функция `get_device_info()` выполняет запросы к сетевым устройствам по протоколу SNMP, используя команды `snmpwalk`. Она получает данные по заданным OID (объектным идентификаторам), обрабатывает их и формирует массив для дальнейшего анализа.

4. Сбор информации о трафике интерфейсов – для мониторинга нагрузки на сетевых интерфейсах устройства применяется `get_interface_traffic()`. В данном процессе используются MIB-объекты IF-MIB, которые предоставляют сведения о количестве обработанных пакетов и активности интерфейсов.

5. Мониторинг ресурсов устройства – функция `get_device_resources()` собирает данные о загрузке процессора, использовании оперативной памяти

и дискового пространства, обращаясь к HOST-RESOURCES-MIB. Полученные данные конвертируются в удобочитаемый формат.

6. Формирование и представление данных – результаты работы скрипта оформляются в виде HTML-страницы с таблицами, содержащими информацию о сетевых устройствах (рис. 6, 7, 8).

| ID | Имя устройства  | IP-адрес    | Маска подсети   | Логин | Пароль | Passwd enabled | Действия                                           |
|----|-----------------|-------------|-----------------|-------|--------|----------------|----------------------------------------------------|
| 1  | LAPTOP-539V7OBN | 172.20.10.4 | 255.255.255.240 | -     | -      | false          | <a href="#">Интерфейсы</a> <a href="#">Ресурсы</a> |
| 2  | LAPTOP-5I3KCVV7 | 172.20.10.3 | 255.255.255.240 | -     | -      | false          | <a href="#">Интерфейсы</a> <a href="#">Ресурсы</a> |

Рис. 6. Пример автоматически заполненной таблицы

| Интерфейс                                  | In Unicast<br>(пакеты) | Out Unicast<br>(пакеты) | In Multicast<br>(пакеты) | Out Multicast<br>(пакеты) |
|--------------------------------------------|------------------------|-------------------------|--------------------------|---------------------------|
| Software Loopback Interface 1.             | 0                      | 0                       | 0                        | 0                         |
| Bluetooth Device (Personal Area Network).  | 0                      | 0                       | 0                        | 0                         |
| Microsoft 6to4 Adapter.                    | 0                      | 0                       | 0                        | 0                         |
| WAN Miniport (IP).                         | 0                      | 0                       | 0                        | 0                         |
| WAN Miniport (Network Monitor).            | 0                      | 0                       | 0                        | 0                         |
| Microsoft Wi-Fi Direct Virtual Adapter #2. | 0                      | 0                       | 0                        | 0                         |
| Intel(R) Wi-Fi 6 AX200 160MHz.             | 13734                  | 7370                    | 59                       | 387                       |

Рис. 7. Пример таблицы с информацией о сетевых интерфейсах

| CPU Загрузка | Диски                                                                                                                                  | Оперативная память          |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 2.42 %       | C: 0.0528 ГБ / 0.0579 ГБ<br>D: 0.051 ГБ / 0.2329 ГБ<br>Virtual Memory: 0.0002 ГБ / 0.0006 ГБ<br>Physical Memory: 0.0001 ГБ / 0.0001 ГБ | <Неизвестно> ГБ / 7.3724 ГБ |

Рис. 8. Пример таблицы с информацией о ресурсах оборудования

Для хранения собранных данных предлагается структура базы данных, включающая следующие таблицы (рис. 9):

1. `devices` – содержит информацию об устройствах (ID, имя устройства, IP-адрес, маска подсети, учетные данные).
2. `interface_traffic` – хранит статистику по интерфейсам (ID устройства, название интерфейса, входящие и исходящие пакеты).
3. `device_resources` – содержит данные о загрузке процессора и использовании оперативной памяти.
4. `disks` – содержит данные об использовании дисковой памяти.

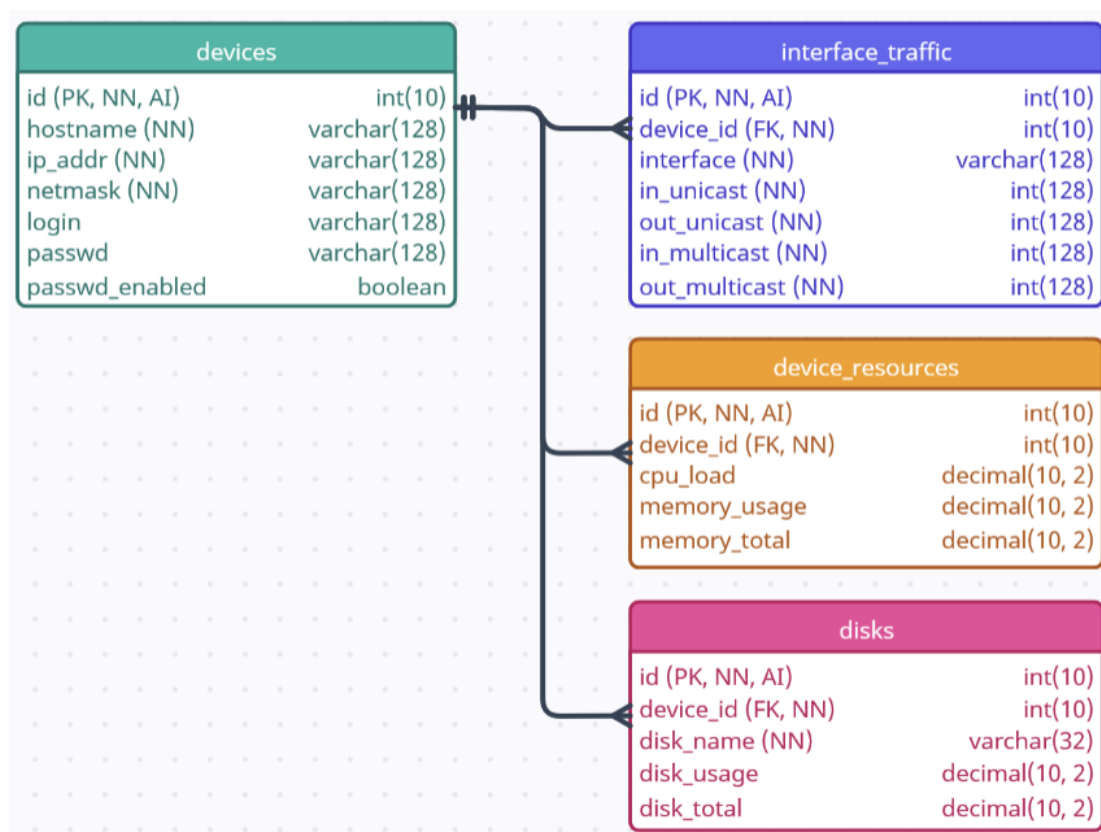


Рис. 9. EDR-диаграмма базы данных

Реализованная в рамках статьи система позволяет автоматизировать мониторинг оборудования сети доступа, обеспечивая следующие аспекты:

- быстрое обнаружение сетевых устройств;
- анализ объемов трафика и выявление перегруженных каналов;
- контролируемый сбор данных о ресурсах оборудования и оценка производительности сетевых устройств;
- представление результатов мониторинга пользователю в наглядном формате.

Система учета ресурсов оборудования сети доступа, разработанная с использованием языка программирования PHP и протокола SNMP, позволяет снизить временные и финансовые затраты на обнаружение и устранение неполадок в инфраструктуре сети. Гибкость и масштабируемость системы позволяют рекомендовать ее для использования в малых и средних организациях связи с целью повышения надежности и эффективности управления сетевым оборудованием.

#### Список используемых источников

1. Архитектура сети доступа. Распространенные и перспективные технологии. URL: [https://fibertop.ru/architecture\\_last\\_mile.htm/](https://fibertop.ru/architecture_last_mile.htm/) (дата обращения 27.02.2025).

2. Что такое SNMP и как он работает? URL: <https://community.fs.com/ru/article/understanding-snmp.html> (дата обращения 27.02.2025).

3. Анфилатов В. С., Емельянов А. А., Кукушкин А. А. Системный анализ в управлении. Учебное пособие / Под ред. Емельянова А. А. М.: Финансы и статистика, 2002. гл. 4.

4. Руководство по PHP. URL: <https://www.php.net/manual/ru/index.php> (дата обращения 27.02.2025).

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Журавелем Е. П.*



**УДК 004.041****Д. И. Восьмаков** (студент группы ИКПИ-14, СПбГУТ), [vosmakov.di@sut.ru](mailto:vosmakov.di@sut.ru)

## **РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ СТУДЕНТОВ И ПРЕПОДАВАТЕЛЕЙ УНИВЕРСИТЕТА**

*В настоящей работе рассматривается вопрос применения информационных систем в ходе образовательной деятельности высших учебных заведений. Предлагается на рассмотрение концепция информационной системы для упрощения взаимодействия между участниками образовательного процесса, учитывающая особенности процессов ввода данных о рабочих программах дисциплин и составления расписания. Рассматривается возможный вариант проектирования архитектуры разрабатываемой системы. Описываются перспективы развития информационной системы, построенной по данной концепции.*

*университет, автоматизация, информационная система, учебный план*

### **Введение**

Деятельность высших учебных заведений, как и многие другие отрасли, в настоящее время претерпевает изменения, связанные с цифровой трансформацией и информатизацией рабочих процессов. Все чаще учебные заведения начинают использовать информационные сервисы, позволяющие упростить обмен информацией между субъектами образовательной деятельности: студентами, преподавателями, абитуриентами и руководством университета. Тенденции к цифровизации и автоматизации процессов в высших учебных заведениях привели к возникновению отдельных классов информационных систем – систем управления университетом (англ. University Management System) и систем информирования студентов (англ. Student Information System).

Как правило, типовая информационная система для университетов включает в себя функционал для просмотра и формирования расписания, ввода и изменения учебного плана, функционал для проведения занятий, хранения данных зачетных книжек и экзаменационных ведомостей, подсистему обмена сообщениями. Использование информационной системы позволяет снизить трудозатраты на обработку информации (в среднем 40 % предприятий оценивают эффект внедрения как положительный согласно [1]), упростить процесс получения актуальной информации об учебном процессе. Таким образом, практика показывает, что внедрение информационной системы в деятельность высшего учебного заведения имеет положительный эффект для достижения целей функционирования университета.



По данным исследований [2], в 2023 г. в деятельности 25 % высших учебных заведений Российской Федерации использовались системы управления обучением, в 51 % выполнена цифровизация административных подразделений. Достижение полной цифровизации отрасли высшего образования в Российской Федерации планируется к 2030 г. [3]. Стоит отметить также сложившуюся тенденцию к импортозамещению программного обеспечения в связи с повышением требований к информационной безопасности, сравнительно небольшим количеством отечественных решений подобного класса (в 2024 г. всего 20 % вузов пользовались отечественным ПО, входящим в состав проекта «Цифровой университет») [3], потребностью пользователей в предоставлении своевременной квалифицированной технической поддержки без языкового барьера. Таким образом, в ближайшие годы потребность в информационных системах для университетов Российской Федерации будет возрастать.

### Преимущества и недостатки существующих систем

Сравнительный анализ прямых конкурентов с системой «Университет» приведен в таблице 1.

ТАБЛИЦА 1. Сравнение функционала системы «Университет» и конкурентов

| Функционал                                            | Система               |               |                          |                       |
|-------------------------------------------------------|-----------------------|---------------|--------------------------|-----------------------|
|                                                       | «Университет»         | Campus        | 1С: Университет          | Личный кабинет СПбГУТ |
| Вид ПО                                                | Открытый исходный код | Проприетарное | Проприетарное            | Проприетарное         |
| Возможность отправлять сообщения                      | +                     | -             | -                        | +                     |
| Отображение расписания студенту                       | +                     | +             | В виде отдельного модуля | +                     |
| Работа с РПД                                          | +                     | +             | +                        | +                     |
| Электронный журнал                                    | +                     | +             | -                        | +                     |
| Формирование расписания на основе тематических планов | +                     | -             | -                        | -                     |

Ключевой особенностью системы «Университет» по сравнению с вышеперечисленными конкурентами предполагается реализовать возможность формирования расписания на основе рабочих программ дисциплин. Данная особенность позволит решить следующие проблемы в организации учебного процесса:

- Необходимость вручную указывать темы занятий после их проведения, что повышает нагрузку на преподавателей.
- Формирование расписания без учета порядка проведения занятий. Например, первая практическая работа по дисциплине ставится перед лекцией. Данные ситуации негативно влияют на учебный процесс, заставляя преподавателей менять порядок изложения материала.

### Проектирование информационной системы

В большинстве современных веб-приложений применяется трехзвенная архитектура, включающая в себя клиентскую часть, серверную часть и базу данных (рисунок 1).

Слой клиента – отвечает за представление информации из приложения в удобном для пользователя виде, а также за считывание данных, полученных из ввода пользователя в формы.

Слой логики – отвечает за выполнение операций по обработке информации, определенных бизнес-требованиями и бизнес-правилами. В слое логики также размещается объектная модель приложения.

Слой данных – отвечает за сохранение и получение информации из базы данных.

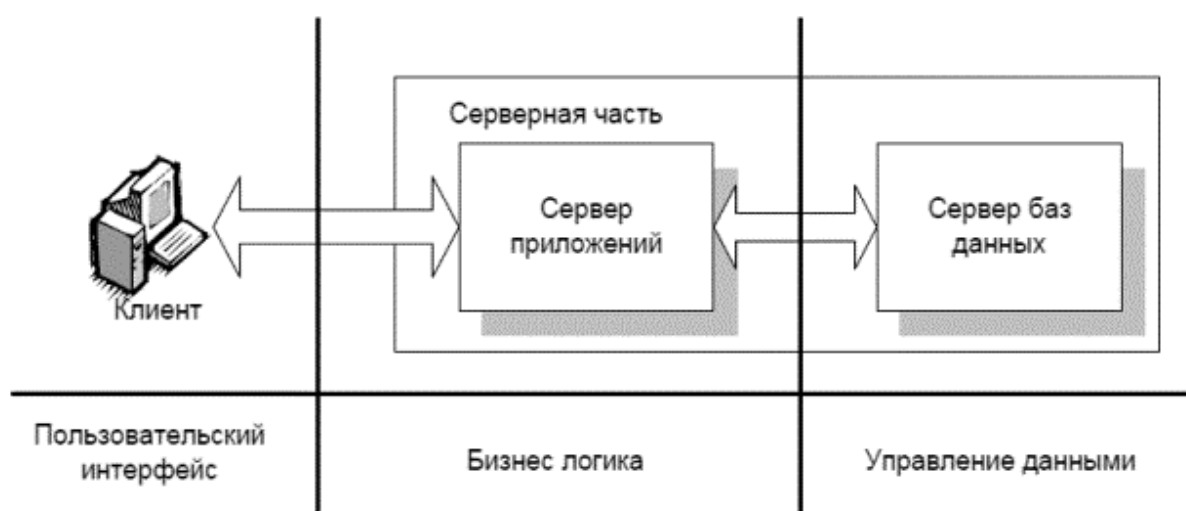


Рис. 2. Классическая трехзвенная архитектура веб-приложений

Предполагается использование аналогичного подхода в системе «Университет» в связи с тем, что данный подход четко устанавливает границы ответственности компонентов системы, способствует написанию более поддерживаемого кода за счет снижения зависимости различных частей приложения между собой, а также облегчает тестирование за счет возможности тестировать каждый слой приложения по отдельности.

Детализированная архитектура проекта представлена на диаграмме компонентов на рисунке 2.

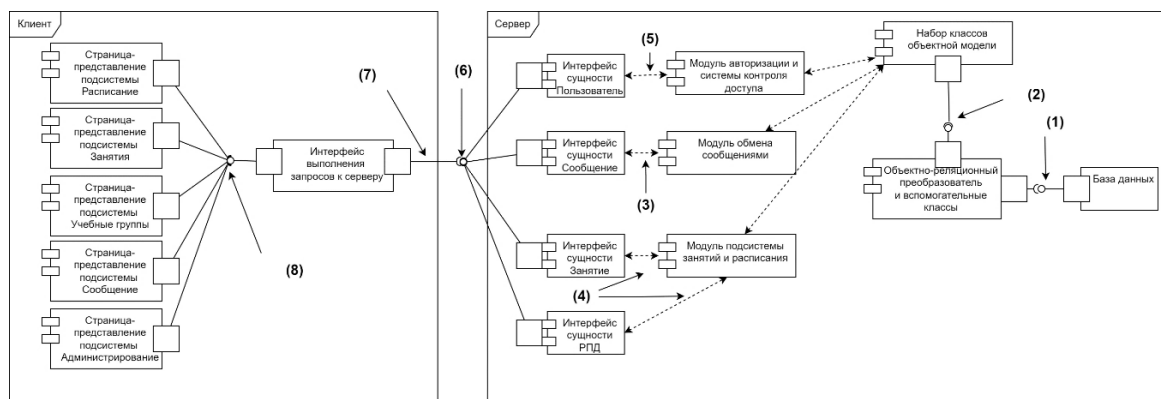


Рис. 2. Представление архитектуры информационной системы «Университет» в виде диаграммы компонентов

На схеме цифрами обозначены связи между компонентами. В каждой связи используется определенный тип данных. Так, для данной схемы:

1. SQL-запросы.
2. Вызовы функций интерфейса.
3. Данные сообщений пользователей.
4. Данные занятий и РПД.
5. Данные пользователей.
6. HTTP-запросы.
7. JSON с данными сущностей (промежуточный формат).
8. Объектные данные сущностей.

Подсистема управления учетными записями должна обеспечивать аутентификацию и авторизацию пользователей, а также возможности по управлению личными данными пользователей в системе.

Подсистема «Расписание» должна обеспечивать функционал по отображению расписания занятий различным типам пользователей в различных форматах, а также предусматривать операции по поиску занятия по указанным пользователем критериям.

Подсистема «Занятие» в составе приложения предусматривает возможность хранения следующей информации об учебном процессе:

- дисциплины;
- рабочие программы дисциплин;
- направления подготовки.

Кроме того, в состав подсистемы входит экранная форма и функционал для проведения занятия, доступный для пользователя с ролью «Преподаватель» при нажатии на карточку занятия в расписании.

Подсистема «Сообщения» предназначена для организации обмена информацией в системе. Предусматриваются следующие варианты работы:

- отправка сообщений пользователям или учебным группам со страницы подсистемы «Сообщения»;
- отправка сообщений студентам учебной группы с привязкой к определенному занятию.

Подсистема «Учебные группы» предназначена для хранения и обработки данных о контингенте студентов и предусматривает следующие функции:

- формирование и расформирование учебных групп;
- перевод студентов из одной группы в другую, редактирование состава учебных групп;
- использование данных об учебных группах в других частях приложения.

Подсистема «Администрирование» предназначена для поддержки и обслуживания системы. В функции подсистемы входит:

- возможность просмотра, утверждение и отклонение заявок на регистрацию пользователей;
- возможность изменения прав пользователей.

Защита информации от несанкционированного доступа в системе «Университет» должна основываться на следующих принципах и подходах:

- проектирование и реализация системы с учетом требований Федерального закона №152-ФЗ «О персональных данных» [0];
- использование алгоритма хэширования SHA-256 [0] при обработке данных (паролей). Передача паролей и токенов доступа только в зашифрованном виде;
- использование механизма аутентификации и авторизации пользователя на основе технологии JWT;
- разграничение доступа к функционалу системы и данным в зависимости от роли пользователя;

- ведение журнала действий пользователей и администраторов системы;
- проверка корректности данных, вводимых пользователем в формы, для предотвращения атак вида SQL-инъекции и XSS, а также предотвращения заполнения базы данных некорректной информацией.

## Вывод

Таким образом, для повышения эффективности образовательного процесса и обеспечения студентов университета информацией может быть предложено создание и внедрение информационной системы, охватывающей основные процессы во взаимодействии студентов и преподавателей. Аспекты проектирования прототипа подобной системы были описаны в настоящей работе.

## Список используемых источников

1. Хлебенских Л. В., Лазарева А. Ю. Оценка эффективности внедрения информационных технологий на российских предприятиях // Вестник Алтайской академии экономики и права. 2022. № 7-2. С. 313-318; URL: <https://vaael.ru/ru/article/view?id=2337> (дата обращения 29.04.2025).
2. Что такое цифровой вуз для ректора, студента и государства / блог компании РСХБ // Хабр. URL: <https://habr.com/ru/companies/rshb/articles/808707/> (дата обращения 06.05.2025).
3. Цифровизация образования в России выходит на новый уровень / Российская газета. 13.02.2023. URL: <https://rg.ru/2023/02/13/cifrovizaciia-obrazovaniia-v-rossii-vykhodit-na-novuj-uroven.html> (дата обращения 06.05.2025).
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. 31 (ч. 1). Ст. 3441. С изменениями и дополнениями.
5. Реализация алгоритма SHA-256 // Хабр. URL: <https://habr.com/ru/articles/729260/> (дата обращения 26.05.2025).

*Статья представлена научным руководителем, исполняющим обязанности заведующего кафедрой ПИИВТ Краевой Е. В.*

УДК 004

**М. В. Герасимова** (студент группы ИСТ-233, СПбГУТ),

[gerasimova.mv@sut.ru](mailto:gerasimova.mv@sut.ru)

**С. С. Калинина** (студент группы ИСТ-233, СПбГУТ), [kalinina.ss@sut.ru](mailto:kalinina.ss@sut.ru)

## **ИНТЕГРАЦИЯ СИСТЕМНОГО АНАЛИЗА И ВЕБ-ДИЗАЙНА В ПРОЦЕССЕ РАЗРАБОТКИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**

*Рассмотрена проблема усложнения цифровых продуктов и возрастания ожиданий пользователей, что требует новых подходов к проектированию интерфейсов. Проведен анализ существующих методов веб-дизайна и системного анализа с точки зрения возможностей их интеграции. Предложена концепция, сочетающая структурный системный анализ с креативными инструментами веб-дизайна для повышения эффективности разработки современных цифровых продуктов. Разработан циклический подход, включающий этапы анализа, проектирования, реализации и оценки. Основное внимание уделено созданию единой системы метрик и использованию сквозных артефактов в контексте гибких методологий. Предложены практические рекомендации по декомпозиции задач, моделированию процессов, визуальному анализу конкурентов и созданию дизайн-систем.*

*системный анализ, веб-дизайн, гибкие подходы, цифровые продукты, единая система метрик*

Современные цифровые продукты становятся все сложнее, а ожидания пользователей в отношении удобства, скорости и эстетики интерфейсов стремительно растут. Согласно статистике, 88 % пользователей не возвращаются на сайт после негативного опыта взаимодействия, а 70 % проектов терпят неудачи из-за плохой UX/UI-проработки [1]. Для устранения данных проблем необходимы новые подходы, сочетающие системный анализ и веб-дизайн для создания эффективных интерфейсов.

Традиционные подходы к проектированию интерфейсов часто оказываются недостаточно эффективными [2]. Системный анализ использует IDEF0 или BPMN для моделирования бизнес-процессов, а также Use Case и User Stories для описания функциональных требований, чем обеспечивает структурированность, но может упускать креативную составляющую. Веб-дизайн же в свою очередь фокусируется на визуальной привлекательности с помощью Customer Journey Mapping, Moodboard и дизайн-систем, но не всегда учитывает системные взаимосвязи. Подобное приводит к разрыву между технической и дизайн-составляющими, что снижает качество итогового продукта [3].

В связи с этим актуализируется вопрос разработки интегрированной методологии, объединяющей принципы системного анализа и инструменты веб-дизайна для создания эффективных пользовательских интерфейсов в условиях роста сложности цифровых продуктов.

Современная разработка цифровых продуктов требует структурированного подхода системного анализа и креативных методов веб-дизайна. Для этого предлагается использовать циклическую модель, состоящую из четырех взаимосвязанных этапов.

Первый этап – анализ, который начинается с системного исследования требований к продукту. Аналитики применяют формализованные методы, такие как построение диаграмм IDEF0 для функционального моделирования или BPMN для описания бизнес-процессов [4]. Параллельно дизайнеры проводят качественные исследования пользовательской аудитории, используя методы Customer Journey Mapping и сравнительный визуальный анализ конкурентов через создание Moodboard [5]. Ключевым связующим звеном на этом этапе становится система единых метрик, где технические параметры сопоставляются с пользовательскими показателями.

На следующем этапе проектирования системные аналитики переводят полученные данные в логические модели, разрабатывая детальные User Flow и Use Case-сценарии. Дизайнеры, опираясь на эти структуры, создают интерактивные прототипы, одновременно формируя дизайн-систему для обеспечения визуальной согласованности. Здесь критически важным становится использование сквозных артефактов.

Третий этап – реализация, которая объединяет усилия разработчиков, работающих по утвержденным моделям процессов и дизайн-макетам. Особое внимание уделяется микроинтеракциям, которые, будучи изначально задуманы дизайнерами, требуют точной технической реализации, контролируемой аналитиками.

Завершающий этап оценки включает А/В-тестирование интерфейсных решений и анализ отклонений от запланированных метрик. Проводятся совместные ретроспективы с участием аналитиков и дизайнеров, где обсуждаются не только количественные показатели, но и качественные аспекты пользовательского опыта.

Для обеспечения эффективного взаимодействия между системным анализом и веб-дизайном предлагается три фундаментальных механизма интеграции.

Первое – единая система метрик: система согласованных количественных и качественных показателей, которая позволяет оценивать продукт как с технической, так и с пользовательской стороны.

Второе – сквозные артефакты: документы и модели, которые эволюционируют на протяжении всего жизненного цикла разработки, сохраняя связь между первоначальными требованиями и конечной реализацией.

И третье – применение Agile – итеративной философии разработки, при которой проект разбивается на короткие циклы (спринты), а требования постепенно уточняются и адаптируются через постоянную обратную связь.

Представленные инструменты естественным образом вписываются в двойную diamond-модель. В первом алмазе (исследование-синтез) ключевую роль играют единые метрики, как основа для принятия решений, и первичные артефакты. Во втором алмазе акцент смещается на детализированные артефакты и Agile-процессы для быстрой итерации. Такой подход создает целостную систему, где формализованные методы системного анализа и творческие подходы веб-дизайна не противоречат, а взаимно усиливают друг друга на каждом этапе разработки.

После адаптации двойной diamond-модели под задачи интеграции системного анализа и веб-дизайна можно определить два последовательных цикла: «Исследование-Синтез» и «Проектирование-Реализация» (рис. 1). Каждый цикл содержит фазы дивергенции и конвергенции, что обеспечивает баланс между глубиной анализа и креативностью подходов.



Рис. 1. Адаптированная двойная diamond-модель

Первый алмаз – фаза исследования и синтеза требований. В фазе дивергенции происходит параллельная работа двух специализаций – системного



анализа и веб-дизайна. Системные аналитики проводят всесторонний анализ проблемного поля, выявляют технические ограничения, архитектурные требования и потенциальные узкие места системы. Веб-дизайнеры в это же время реализуют качественные исследования пользовательского опыта, в рамках которых особое внимание уделяется эмоциональным реакциям пользователей и визуальным трендам. Обе команды работают независимо, но регулярно обмениваются промежуточными результатами на кросс-функциональных воркшопах.

В фазе конвергенции наступает период структурирования полученных данных. Создается единый источник истины – документ с приоритизированными требованиями, который включает как функциональные спецификации, так и принципы UX/UI. Проводится валидация требований через прототипирование ключевых сценариев, что позволяет выявить и устранить противоречия между системными возможностями и дизайн-решениями на ранней стадии.

Второй алмаз – фаза проектирования и реализации. В фазе дивергенции команда переходит в режим творческого поиска. Аналитики разрабатывают различные варианты архитектурных решений и логики работы системы, оценивая каждый по критериям масштабируемости и производительности. Дизайнеры создают множество концепций интерфейсов. Важным аспектом является синхронизация творческих процессов.

В фазе конвергенции происходит фокусировка на наиболее жизнеспособных вариантах. Проводится серия оценочных сессий. Создается финальный дизайн-документ, интегрирующий технические спецификации, детализированные UI-киты с интерактивными прототипами и план внедрения с учетом итеративности Agile-подхода, а также утверждается система метрик успеха, которая будет использоваться на этапе тестирования.

Двойная diamond-модель предусматривает нелинейность процесса [5]. На этапе реализации продукта постоянно поступают данные тестирования, которые могут помочь вернуться в фазу исследования. Это улучшает процесс работы и взаимодействие между аналитиками и дизайнерами.

Интеграция системного анализа и веб-дизайна устраняет ключевые проблемы, возникающие во время разработки цифровых продуктов. Предложенная циклическая модель делает каждый этап точкой синхронизации подходов дизайнеров и аналитиков. Главное преимущество – постоянная обратная связь через единые метрики, благодаря которым технические параметры и UX-показатели оцениваются в едином контексте, что позволяет

сразу выявить и устранить возникающие между логикой системы и восприятием интерфейса противоречия.

Двойная diamond-модель создает пространство для параллельного исследования и синтеза идей. Благодаря гибкости этой модели можно возвращаться к уточнению данных на любом этапе. Это помогает балансировать между глубиной анализа и креативностью.

Объединение структурированных методов системного анализа с креативными подходами дизайна помогает создать базу для будущей разработки интерфейса, эффективного как с технической, так с визуальной точки зрения. Предложенная методология способствует созданию современных цифровых продуктов, сочетающих в себе системную надежность и пользовательский опыт. Это особенно актуально в условиях растущей сложности ИТ-решений и повышающихся ожиданий пользователей.

#### **Список используемых источников**

1. Купер А., Рейнманн Р., Кронин Д. About Face 4: Основы взаимодействия человека с компьютером. М.: Диалектика, 2020. 720 с.
2. Спицина И. А., Аксенов К. А. Применение системного анализа при разработке пользовательского интерфейса информационных систем. М.: Издательство Уральского университета. 100 с.
3. Тидвелл Д. Разработка пользовательских интерфейсов. М.: ДМК Пресс, 2019. 520 с.
4. Сазерленд Д. Scrum: Революционный метод управления проектами. М.: Манн, Иванов и Фербер, 2020. 288 с.
5. Богданов С. В., Исаева А. Э., Козлова Е. В., Муртузалиева Т. В., Пурлик В. М. Дизайн-Мышление как подход к разработке инновационных решений, ориентированных на человека. Вестник Московского университета. Серия 21. Управление (государство и общество). С. 3-22.

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.032.26

## ТРАНСФОРМЕРНЫЕ АРХИТЕКТУРЫ И FEW-SHOT LEARNING: НОВАЯ ПАРАДИГМА В МАШИННОМ ОБУЧЕНИИ ДЛЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Д. А. Голактионов (студент группы ИСМ-31з, СПбГУТ)  
О. В. Раковский (к.т.н., доцент кафедры ИУС, СПбГУТ),  
[rakovskii.ov@sut.ru](mailto:rakovskii.ov@sut.ru)

*Современные информационные системы все чаще используют трансформерные архитектуры и методы Few-Shot Learning благодаря их способности эффективно работать с ограниченными объемами данных и автоматически выявлять сложные закономерности без трудоемкого проектирования признаков. Эти технологии открывают новые возможности для машинного обучения, позволяя создавать адаптивные системы, которые быстро реагируют на изменения в данных и не требуют миллионов размеченных примеров для обучения.*

*трансформеры, Few-Shot Learning, машинное обучение, self-attention, адаптивные системы*

Современные информационные системы сталкиваются с серьезными вызовами, связанными с необходимостью обработки сложных, динамично изменяющихся данных в условиях дефицита размеченной информации. Традиционные подходы машинного обучения, основанные на статических моделях, требующие значительных объемов обучающих данных, представляют снижение эффективности в этих условиях. Особенно актуально эта проблема проявляется в таких критически важных областях, как обнаружение финансового мошенничества, медицинская диагностика и кибербезопасность, в которых требования к скорости адаптации и точности анализа постоянно возрастают.

Основная проблема классических подходов заключается в их зависимости от больших объемов размеченных данных. Для достижения оптимальной точности нередко требуются десятки или сотни тысяч примеров. Более того, эти подходы требуют трудоемкого процесса проектирования признаков (feature engineering), что значительно замедляет внедрение и разработку систем.

Главным препятствием для всеобщего применения классических алгоритмов машинного обучения в нынешних условиях стала их потребность в данных. Большинство ML-моделей (Machine Learning) требуют тысяч или

даже миллионов примеров для достижения удовлетворительного уровня точности. Одним из примеров является задача распознавания поддельных документов – для обучения даже относительно простой нейронной сети необходимо собрать и разметить десятки тысяч образцов документов. На практике такие объемы качественно размеченных данных доступны лишь крупнейшим корпорациям и государственным структурам.

Яркой иллюстрацией этой проблемы может служить реальный случай из практики одного из европейских банков. После успешного внедрения модели для выявления мошенничества с кредитными заявками, система стабильно работала в течение нескольких месяцев, эффективно выявляя попытки использования поддельных паспортов. Однако, когда мошенники изменили свою схему и перешли на использование украденных биометрических данных, система оказалась совершенно беспомощной – новая атака не была представлена в обучающей выборке, и модель не смогла ее распознать. Полный цикл переобучения системы на новых данных занял более трех месяцев, в течение которых банк нес существенные потери.

Не менее серьезной проблемой является необходимость ручного проектирования признаков для традиционных алгоритмов. Методы типа SVM (Support Vector Machine) или логистической регрессии не способны автоматически извлекать значимые признаки из сырых данных [1]. Аналитикам приходится вручную создавать и тестировать сотни параметров, таких как "средняя сумма транзакции за месяц" или "количество ночных входов в систему". Этот процесс не только требует значительных временных затрат, но и создает проблему хрупкости системы – при любом изменении бизнес-процессов всю систему признаков приходится пересматривать и перенастраивать.

Трансформерные архитектуры, первоначально разработанные для решения задач и обработки языковых данных (NLP), предлагают принципиально новый подход к анализу данных. Их ключевое преимущество заключается в механизме self-attention, который может быть формально описан следующим образом:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right) V$$

где  $Q, K, V$  – матрицы запросов, ключей и значений,  $d_k$  – размерность ключей. Этот механизм позволяет модели автоматически определять и учиты-

вать наиболее релевантные взаимосвязи во входных данных без явного указания признаков, что особенно ценно при работе с неструктурированной информацией.

Практическое применение трансформеров демонстрирует их универсальность и эффективность. В медицинской диагностике, например, системы на основе BERT (Bidirectional Encoder Representations from Transformers) или GPT (Generative Pre-trained Transformer) способны анализировать текстовые описания симптомов и выделять ключевые клинические признаки без предварительного ручного кодирования правил [2]. Врач может ввести запрос типа: "Пациент, 45 лет, жалуется на боль в груди, иррадиирующую в левую руку", и модель не только корректно интерпретирует эту информацию, но и выявляет сложные взаимосвязи между симптомами, предлагая дифференциальный диагноз.

Схема архитектуры Transformer представлена на рис. 1.

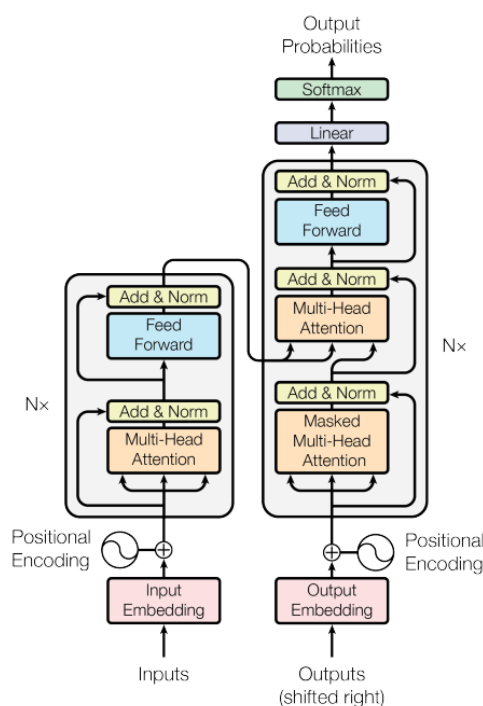


Рис. 1. Модель архитектуры Transformer

Особый прорыв в области машинного обучения связан с развитием методов Few-Shot Learning (FSL), которые позволяют моделям адаптироваться к новым задачам, используя всего несколько примеров [3]. Математически этот процесс может быть описан через байесовский вывод:

$$P(y|x, D) = \frac{P(D|y, x)P(y|x)}{P(D|x)}$$

где  $D$  – набор примеров few-shot (обычно от 1 до 5);

$x$  – входной текст;

$y$  – ожидаемый ответ;

$P(D|y, x)$  – насколько данные соответствуют известным примерам;

$P(y|x)$  – базовая вероятность ответа без примеров (zero-shot);

$P(D|x)$  – нормализующий член.

Такой подход радикально сокращает потребность в размеченных данных и ускоряет процесс адаптации моделей таблицы 1 к новым условиям.

ТАБЛИЦА 1. Сравнение характеристик разных подходов в машинном обучении

| Характеристика            | Традиционное ML | Few-Shot Learning | Zero-Shot Learning |
|---------------------------|-----------------|-------------------|--------------------|
| Требуемые примеры         | $10^3$ - $10^6$ | 1-5               | 0                  |
| Время адаптации           | Часы-дни        | Минуты            | Мгновенно          |
| Вычислительная сложность  | Высокая         | Средняя           | Низкая             |
| Точность в новых условиях | Низкая          | Высокая           | Средняя            |

Финансовый сектор представляет собой одну из наиболее показательных областей применения новых технологий. Современные системы обнаружения мошенничества на основе трансформеров демонстрируют впечатляющие результаты по сравнению с традиционными подходами. Если раньше системы работали на основе жестких правил, типа "если сумма перевода превышает  $\text{R}100,000$  – проверить", то современные решения анализируют взаимосвязанные параметры операционного процесса: географию платежа, историю поведения пользователя, временные паттерны и множество других параметров. Результаты внедрения таких систем показывают снижение уровня ложных срабатываний на 30 % при одновременном повышении точности обнаружения более новых видов мошенничества.

В медицинской диагностике системы типа Med-PaLM от Google демонстрируют точность дифференциальной диагностики, сопоставимую с врачами-экспертами, используя только лишь краткое текстовое описание симптомов и несколько референсных примеров. Важнейшим преимуществом такого подхода является возможность работать в условиях ограниченных

медицинских данных, что очень актуально для редких заболеваний или специализированных клиник.

Успешное внедрение трансформерных архитектур и методов Few-Shot Learning требует создания соответствующей технологической и кадровой базы. С технической точки зрения существует потребность в необходимых специализированных библиотеках типа Hugging Face, содержащих предобученные модели (BERT, GPT и др.), фреймворки для быстрого прототипирования (PyTorch Lightning), а также модели для работы с гетерогенными данными (Google T5).

Вычислительная инфраструктура должна включать мощные GPU/TPU для обучения моделей [4]. Для организаций, не обладающих своими собственными вычислительными ресурсами, самым оптимальным решением может стать использование облачных платформ для ML-разработки типа AWS SageMaker или Google Vertex AI.

Кадровое обеспечение требует наличия в команде квалифицированных Data Scientists для настройки моделей и ML Engineers для их интеграции в существующие информационные системы. При этом важно отметить, что работа с трансформерами и FSL требует несколько иных компетенций, чем традиционное машинное обучение, что особо важно при подготовке и найме специалистов.

Будущее развитие трансформерных архитектур и методов маломасштабного обучения связано с несколькими ключевыми направлениями. Наиболее перспективным представляется создание мультимодальных трансформеров, способных одновременно обрабатывать текст, изображения и табличные данные [5]. Формально это можно представить как:

$$h_{fusion} = \phi([h_{text}; h_{image}; h_{tabular}])$$

где  $\phi$  – функция объединения представлений разных модальностей.

Другим важным направлением является разработка методов автоматического Few-Shot Learning, где модель сама определяет оптимальную архитектуру для новой задачи, основываясь на предоставленные примеры. Это позволяет еще больше снижать барьеры для внедрения машинного обучения в областях с ограниченными наборами данных.

Отдельного внимания заслуживает направление генерации синтетических данных для обучения моделей. Современные генеративные модели

позволяют создавать качественные synthetic data, которые могут значительно расширять возможности обучения в условиях ограниченных реальных данных.

Трансформерные архитектуры и Few-Shot Learning представляют собой не просто новые инструменты в арсенале машинного обучения, а принципиально новую парадигму построения информационных систем. Они позволяют преодолевать ключевые ограничения стандартных подходов: зависимость от больших объемов данных, необходимость ручного проектирования признаков и медленную адаптацию к изменениям.

Уже сегодня эти технологии готовы к промышленному внедрению в таких областях, как:

- финансовый мониторинг и обнаружение мошенничества;
- медицинская диагностика и анализ медицинских изображений;
- обработка естественного языка и семантический анализ;
- кибербезопасность и обнаружение аномалий.

Организациям, сталкивающимся с проблемами быстро меняющейся среды, нехваткой размеченных данных или необходимостью анализа сложных неструктурированных данных, рекомендуется рассмотреть внедрение этих технологий в ближайшей перспективе. Как показывает практика, преимущества такого перехода многократно окупают связанные с ним затраты.

#### Список используемых источников

1. Татарникова Т. М. Методы машинного обучения: учебное пособие / Т. М. Татарникова, В. В. Боженко. Санкт-Петербург: ГУАП, 2023. 100 с. ISBN 978-5-8088-1885-9. URL: <https://e.lanbook.com/book/461489> (дата обращения 20.04.2025).
2. Калгина, И. С. Интеллектуальные информационные системы: учебное пособие / И. С. Калгина. Чита: ЗабГУ, 2023. 123 с. ISBN 978-5-9293-3270-8. URL: <https://e.lanbook.com/book/438236> (дата обращения 21.04.2025).
3. Баланов А. Н. Искусственный интеллект. Понимание, применение и перспективы: учебник для вузов / А. Н. Баланов. 2-е изд., стер. Санкт-Петербург: Лань, 2025. 312 с. URL: <https://e.lanbook.com/book/448697> (дата обращения 22.04.2025).
4. Баланов А. Н. Комплексное руководство по разработке: от мобильных приложений до веб-технологий: учебное пособие для вузов / А. Н. Баланов. 2-е изд., стер. СПб.: Лань, 2025. 412 с. ISBN 978-5-507-53193-6. URL: <https://e.lanbook.com/book/478178> (дата обращения 23.04.2025).
5. Михненко П. А. Анализ мультимодальных данных в управлении проектами: перспективы использования машинного обучения // Управленческие науки. 2023. № 4. URL: <https://cyberleninka.ru/article/n/analiz-multimodalnyh-dannyh-v-upravlenii-proektami-perspektivy-ispolzovaniya-mashinnogo-obucheniya> (дата обращения 24.04.2025).

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ИУС СПбГУТ Раковским О. В.*



УДК 004.422.8:52

А. С. Голощанов (студент группы ИСТ-211, СПбГУТ),

[goloshapov.as@sut.ru](mailto:goloshapov.as@sut.ru)

М. В. Мерзляков (студент группы ИСТ-211, СПбГУТ), [filippova.ev@sut.ru](mailto:filippova.ev@sut.ru)

Е. В. Филиппова (студент группы ИСТ-211, СПбГУТ),

[merzliakov.mv@sut.ru](mailto:merzliakov.mv@sut.ru)

## ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ МОНИТОРИНГА СЕВЕРНОГО СИЯНИЯ И ДРУГИХ АСТРОНОМИЧЕСКИХ ЯВЛЕНИЙ

*В данной статье представлен проект информационной системы для мониторинга астрономических явлений. Проведен анализ конкурентоспособных систем, на основе которого определены функциональные требования и структура модулей проектируемого сервиса. Построена карта пользовательских сценариев, позволяющая актуализировать необходимые возможности сервиса. Сформирована диаграмма вариантов использования, отражающая основные сценарии взаимодействия с системой и роли ключевых пользователей. Предлагаемая система объединяет все необходимые инструменты для отслеживания астрономических явлений в рамках единой платформы, упрощая организацию наблюдений и способствуя популяризации астрономии среди широкой аудитории пользователей.*

*проектирование, Telegram-бот, UML, астрономические явления, Северное сияние, астрономия, погода*

Популяризация астрономии требует современных средств наблюдения и информирования пользователей об астрономических событиях. Проектируемая информационная система (далее – ИС) направлена на формирование единой платформы для мониторинга таких явлений, как Северное сияние, метеорные потоки и другие космические события. Основное внимание уделено удобству использования и интеграции с актуальными источниками данных.

В рамках анализа изучены популярные Telegram-боты и сервисы: Animated Weather, GoAurora, SWeather.Bot и NOAA Solar Bot. Основными недостатками выявлены: перегруженность интерфейса, отсутствие поддержки русского языка, отсутствие модулей просмотра погоды и фотогалерей, ориентированность на профессиональных пользователей. Данный анализ послужил основанием для разработки нового решения.

Проектируемая система должна включать следующие компоненты:

- регистрация и приветствие;

- просмотр параметров Северного сияния;
- прогноз погоды с учетом геопозиции;
- список ближайших астрономических явлений;
- выбор локации для наблюдений;
- просмотр и загрузка пользовательских фотографий.

Исходя из вышеописанных требований, сервис включает модули «Регистрация», «Главное меню», «Параметры», «Места», «Галерея», «Погода» и «Список астрономических явлений».

На представленной схеме (рис. 1) также указаны компоненты, которые входят в состав каждого модуля, и связи между модулями. Рассмотрим их подробнее.

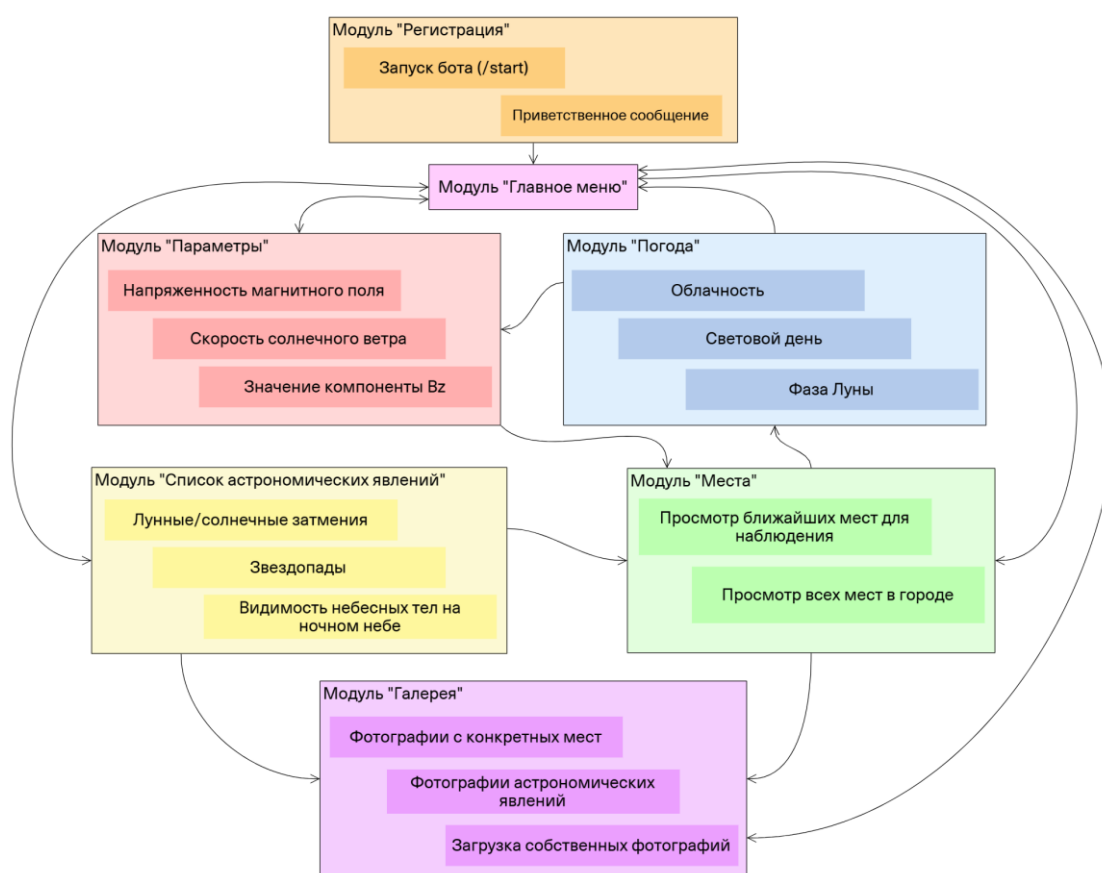


Рис. 1. Схема взаимодействия модулей ИС

В результате построения схемы модулей выявлены пользовательские сценарии, отражающие весь возможный функционал сервиса. Помимо этого, карта пользовательских сценариев (рис. 2) позволила выделить релизы, определив, какие функции необходимо разработать в первую очередь [1].

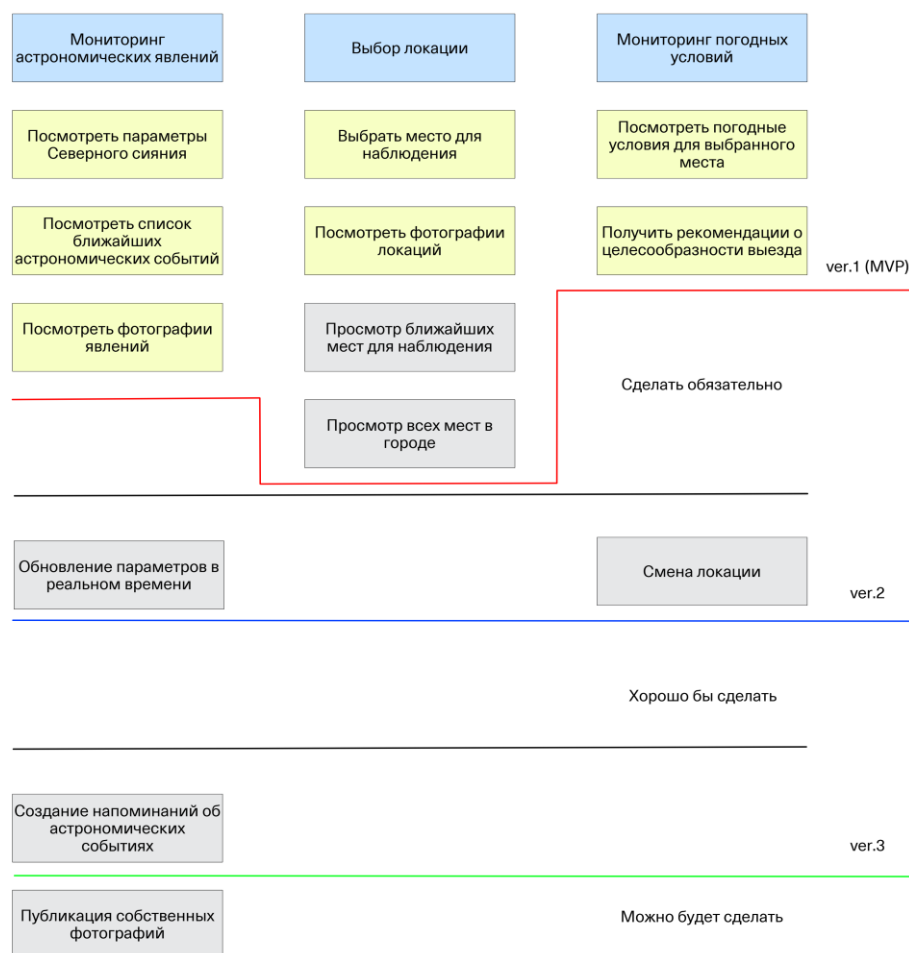


Рис. 2. Карта пользовательских сценариев

Карта пользовательских сценариев позволила составить диаграмму вариантов использования (рис. 3) [2]. Для ее построения выделены следующие акторы:

- Пользователь: взаимодействие с сервисом с возможностью частичного управления (смена локации, публикация фотографий);
- API карт: доступ к местоположению Пользователя;
- API погоды: доступ к местоположению Пользователя;
- API параметров: предоставление доступа к текущим параметрам Северного сияния;
- Администратор: полный доступ и управление сервисом.

Данный способ описания ИС позволил определить роль каждого актера в функционировании сервиса.

В ходе проектирования разработаны основные диаграммы и ключевые элементы для детального описания структуры и взаимодействия компонентов системы. Следующие шаги включают в себя программную реализацию проекта на основе разработанных диаграмм, а также тестирование и отладку функциональности ИС.

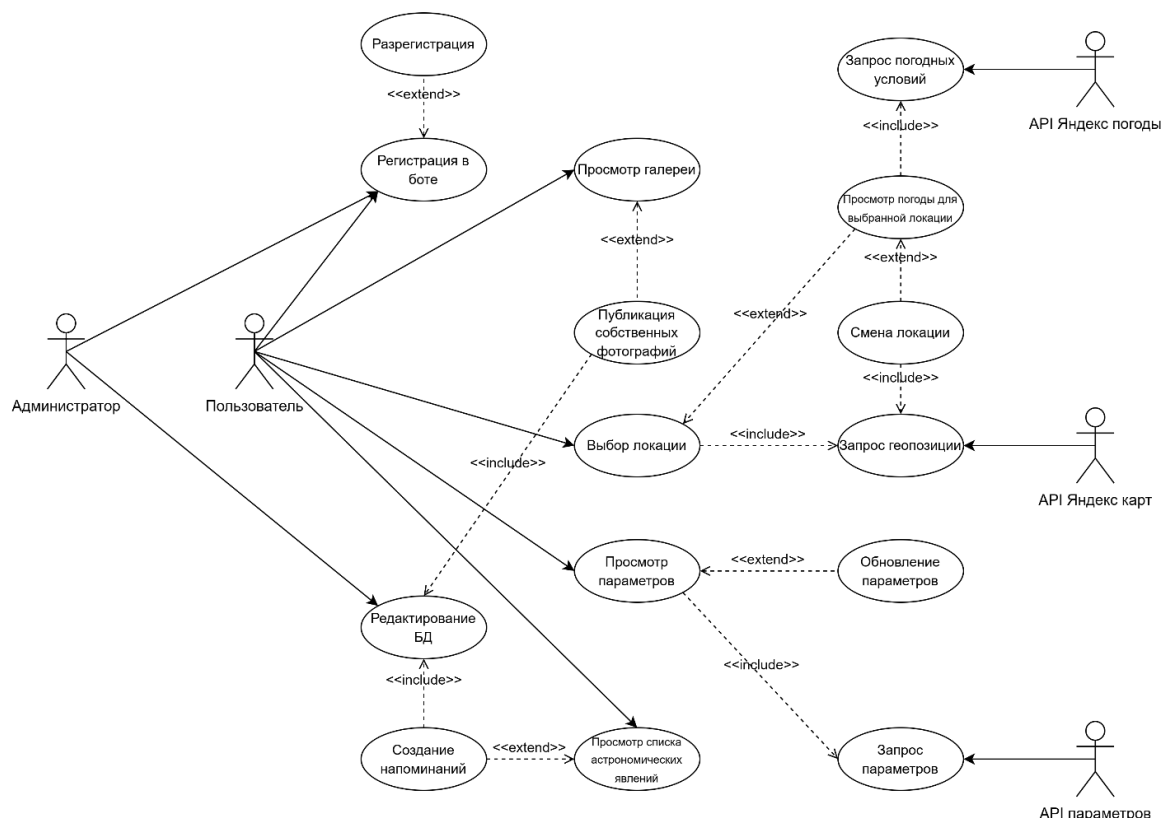


Рис. 3. Диаграмма вариантов использования системы

Предлагаемая система обеспечит единый доступ ко всей необходимой информации для наблюдения за астрономическими явлениями. Она упростит поиск локаций, планирование выездов и обмен результатами. Telegram-бот с понятной навигацией и поддержкой API прогноза погоды и параметров Северного сияния сделает астрономию доступной широкому кругу пользователей.

Данный проект имеет потенциал стать полезным инструментом для любителей астрономии, способствуя популяризации науки и привлечению внимания к красоте и уникальности астрономических явлений.

#### Список используемых источников

1. Котлова М. В., Давыдова Е. В. Методы и средства проектирования информационных систем и технологий: учебное пособие / М. В. Котлова, Е. В. Давыдова. Санкт-Петербург: СПбГУТ, 2015. 62 с.
2. Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя. 2-е изд.: Пер. с англ. Мухин Н. М.: ДМК Пресс, 2006. 496 с.: ил.

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.75:339.172

**В. В. Громов** (к.т.н., доцент, доцент кафедры ИКД, СПбГУТ),  
[gromov2.vv@sut.ru](mailto:gromov2.vv@sut.ru)

**В. В. Пашенкова** (студент группы ИСТ-132, СПбГУТ), [v.paschenkova@gmail.com](mailto:v.paschenkova@gmail.com)

## ПРИМЕНЕНИЕ ЧАСТНЫХ БЛОКЧЕЙН-СЕТЕЙ ДЛЯ ФИКСАЦИИ ТОРГОВЫХ ОПЕРАЦИЙ НА ЗЕРНОВЫХ БИРЖАХ В ЦЕЛЯХ ПОВЫШЕНИЯ ПРОЗРАЧНОСТИ ЦЕНООБРАЗОВАНИЯ

*В статье рассматривается возможность использования технологии блокчейн в качестве основы информационной системы для электронной зерновой биржи. Статья посвящена применению частных блокчейн-сетей для организации прозрачного, проверяемого и защищенного реестра заявок и сделок. Проведен анализ архитектурных решений и технических особенностей платформ Hyperledger Fabric и MultiChain, предложена модель частной блокчейн-сети с поддержкой смарт-контрактов. Указываются основные преимущества (обеспечение прозрачности, доверие, автоматизация) и ограничения (масштабируемость, вопросы конфиденциальности и нормативного регулирования) предложенного решения.*

*блокчейн, торговая платформа, биржа зерна, реестр заявок, ценообразование, прозрачность*

### Основные понятия блокчейн и частных сетей

Технология блокчейн представляет собой распределенную базу данных, в которой новые записи (блоки транзакций) надежно добавляются с использованием криптографических средств (хеширования, цифровых подписей) [1]. Каждый новый блок содержит указатель (хеш) на предыдущий, поэтому любая попытка изменить прошлую запись «сломает» всю цепочку, делая подделку очевидной.

В блокчейне обычно применяются смарт-контракты – программируемые модули, автоматически исполняющие бизнес-логику при наступлении определенных условий. Такие смарт-контракты «вшиты» в сеть и могут управлять транзакциями между участниками. Блокчейн-сети бывают публичными (permissionless) и приватными (permissioned). В публичной сети любой может присоединиться и участвовать в консенсусе, а протокол требует таких механизмов как Proof-of-Work. В частной сети участники заранее известны и допущены оператором; это позволяет применять более легкие протоколы консенсуса и не использовать криптовалюту. Например, в

Hyperledger Fabric – одной из популярных корпоративных DLT-платформ – все участники известны друг другу, что позволяет строить сеть на основе существующего доверия и согласованных правил. Fabric поддерживает подключаемые консенсус-протоколы: при полном доверии (например, между подразделениями одной компании) может применяться отказоустойчивый (Crash Fault Tolerant) консенсус, а в более децентрализованных сценариях – алгоритмы на основе византийской устойчивости. При этом отсутствие собственной криптовалюты в Fabric устраняет издержки майнинга и снижает сложность развертывания, делая систему сопоставимой по стоимости с другими распределенными приложениями. Таким образом, частная блокчейн-сеть объединяет участников с разными уровнями доверия, сохраняя неизменность записей, такой реестр обеспечивает неизменяемый журнал аудита (tamper-resistant audit trail) и избавляет от необходимости постоянного централизованного надзора.

### **Блокчейн в аграрном секторе и товарных рынках**

В течение последних лет появились многочисленные исследования и кейсы применения блокчейн-технологий в агропродовольственных цепочках. В частности, блокчейн используют для отслеживания происхождения и качества зерна, чтобы гарантировать прозрачность на каждом этапе поставок. Например, в Канаде создан проект Grain Discovery – платформа на блокчейне для эффективных, прозрачных и защищенных транзакций сельхозкультуры. Участники системы могут фиксировать сделки и параметры качества урожая, что дает единый источник данных от поля до покупателя. По мнению авторов, неизменяемые записи в блокчейне повышают доверие к поставкам и препятствуют мошенничеству, обеспечивая прослеживаемость до потребления. Аналогично, академические исследования подтверждают потенциал блокчейна для «прозрачной цепочки поставок продовольствия». Так, Kamilaris и др. (2019) [2] и Surarssan (2024) [3] указывают, что технология блокчейн обещает значительный прогресс в прозрачности агрологистики, несмотря на существующие технические, образовательные и регуляторные барьеры внедрения.

### **Архитектура блокчейн-платформы для зерновой биржи**

Для разработки прототипа информационной системы электронной зерновой биржи с блокчейн-компонентом необходимо учесть особенности торговой инфраструктуры. Предполагается, что участниками сети будут биржа

(владелец торговой платформы), брокеры и дилеры зернового рынка, а также, возможно, регуляторы (например, государственные органы). Все они получают доступ к частному распределенному реестру – блокчейн-платформе с разрешенным доступом. В такой сети создается единый журнал операций: каждая заявка на продажу или покупку зерна и каждый факт сделки записывается в блоки, связанные общей цепочкой. При этом дизайн системы может предусматривать смарт-контракты для автоматического исполнения бизнес-правил биржи (например, проверка соответствия заявки установленным требованиям и автоматическое сопоставление ордеров). Благодаря неизменяемости блокчейна все участники имеют гарантированный доступ к полной истории торгов в пределах своих прав.

На практике реальную систему можно построить на базе существующих блокчейн-платформ. Например, в Direct Farm как блокчейн-платформу планировали использовать MultiChain, специально созданный для частных цепей (в нем участники заранее известны и для поддержки сети не нужна криптовалюта). Альтернативно можно применить Hyperledger Fabric, где сеть состоит из реест-узлов, а механизмы шифрования (в том числе приватные каналы) позволяют скрыть детали сделок от неучастников. Таким образом, предполагаемая архитектура будет состоять из следующих компонентов:

*1. Узловая инфраструктура.* Ключевые акторы – биржевой оператор, системообразующие брокерские компании, а также уполномоченные регулятивные органы – эксплуатируют полнофункциональные сетевые узлы-пиры. Каждый пир хранит верифицированную копию распределенного реестра и участвует в процессе консенсуса. Последовательное согласование записей до их включения в цепочку блоков исключает возникновение противоречивых транзакционных состояний и тем самым гарантирует целостность данных.

*2. Смарт-контракты как механизм институционализации бизнес-логики.* Логико-функциональное ядро платформы реализуется посредством модулей chaincode. Указанные модули формализуют регламент обработки заявок, осуществляют контроль достоверности исходных данных (например, верификацию сертификатов качества зерна) и инициируют автоматическое закрытие сделки при достижении предусмотренных условий. Тем самым смарт-контракт выполняет посредническую функцию, материализуя алгоритмы заключения биржевых соглашений в неизменяемой среде блокчейна.

3. *Прикладной интерфейс взаимодействия.* Коммуникация фронтенд-приложений и сторонних сервисов с ядром биржевой системы обеспечивается через открытые API (REST/gRPC). При этом серверная компонента, аналогично архитектуре Direct Farm, может быть реализована как Java-приложение (WSO2 AS), а клиентская – на React.js. Фактические транзакции, инициированные через API, фиксируются в журнале событий соответствующего пира.

4. *Механизмы криптографической защиты и разграничения доступа.* Конфиденциальные параметры сделки доступны исключительно ее контрагентам. В Hyperledger Fabric такая избирательная видимость достигается за счет приватных каналов и белых списков chaincode-контрактов, что позволяет ограничить чтение записей указанными узлами без утраты консистентности глобальной цепочки.

5. *Процедуры валидации и репликации.* Каждый факт подачи заявки либо заключения сделки транслируется участниками в подсистему консенсуса (PBFT/CFT). После криптографической проверки формируется новый блок, который реплицируется на все узлы сети, обеспечивая невоспроизводимость и защиту от последующих модификаций.

6. *Интеграционная модель биржевой платформы.* Таким образом, блокчейн-компонент формирует единый достоверный реестр операций, тогда как прикладные сервисы реализуют пользовательскую логику – аутентификацию, формирование электронных договоров, расчет биржевых показателей. Критичные результаты их работы неизбежно фиксируются в распределенном журнале, что подтверждается опытом Direct Farm, где REST-ориентированное взаимодействие фронтенда с бэкендом завершается неизменяемой записью в блокчейне.

## **Технические и организационные особенности внедрения блокчейн-сети на биржевой платформе**

*Прослеживаемость и аудит.* Блокчейн формирует полный лог операций с возможностью восстановления цепочки событий – от генерации заявки до ее исполнения и закрытия. При этом сохраняются как содержательные параметры, так и сопутствующие метаданные, включая цифровые подписи и временные метки. Пример реализации подобной архитектуры представлен в проекте на базе Hyperledger, обеспечивающем сквозную прослеживаемость и доказуемость происхождения информации [4]. На бирже



это означает прозрачность для аудиторских и регуляторных проверок: каждая заявка сопровождается неизменным «штампом», удостоверяющим ее авторство и момент регистрации.

*Рост доверия со стороны участников.* Природа децентрализации исключает доминирование со стороны отдельного оператора, включая саму биржу. Каждый участник способен самостоятельно проверить корректность проводимых сделок и достоверность рыночных котировок. Это особенно важно при высокой ценовой волатильности: устраняется информационная асимметрия, способствующая недоверию. Исследование Lucena et al. демонстрирует, что применение блокчейн-сертификации в цепочке поставок зерна усиливает уверенность в качестве продукции и может повлиять на ее рыночную стоимость. Аналогично, открытая система регистрации заявок способствует укреплению доверия к механизму ценообразования [1].

*Оптимизация структуры за счет отказа от посредников.* Исключение необходимости централизованного арбитра позволяет упростить биржевую инфраструктуру. Согласно Ehmke (2023), подобная трансформация уже реализуется в проектах цифровой торговли (например, Covantis и Agriota). Блокчейн играет ключевую роль в сокращении цепочек доверия и устранении необходимости в пост-трейд посредничестве, включая ручной аудит и расчеты.

Таким образом, реализация частной блокчейн-сети на биржевой площадке формирует надежную технологическую основу для прозрачных и доверительных торгов. Технология устраняет потребность в централизованных посредниках и исторических сверках, повышая безопасность и достоверность операций при сохранении их полной регистрируемости.

*Конфиденциальность передаваемых данных.* Открытая структура реестра может противоречить требованиям коммерческой тайны. Поэтому важно обеспечить дифференцированный доступ к данным, разрешая пользователям просматривать лишь разрешенные сегменты информации. Это требует внедрения криптографических механизмов, включая zk-SNARK и гомоморфное шифрование. Подобные подходы уже применяются (например, в Direct Farm), однако полная реализация защиты накладывает значительные требования к вычислительным ресурсам.

*Регуляторная неопределенность.* Правовые рамки зачастую не успевают за внедряемыми технологиями. Возникают вопросы о признании записей в блокчейне как юридически значимых, об ответственности за сбои в работе смарт-контрактов, а также о защите прав всех участников системы.

В ряде юрисдикций нормативное регулирование таких решений отсутствует либо находится на стадии формирования.

*Низкая степень технологического принятия.* Как указывается в отчетах Sosland (2023), несмотря на высокие ожидания, широкомасштабное распространение блокчейн-технологий в товарной торговле пока не реализовано [5]. Для преодоления скепсиса необходимо осуществлять обучение пользователей, упрощать интерфейсы и последовательно демонстрировать экономическую целесообразность и устойчивую пользу от использования системы.

Таким образом, применение частной блокчейн-сети для фиксации заявок и сделок на зерновой бирже может существенно повысить прозрачность торгов и доверие участников. Технологические особенности блокчейна – неизменяемость записей, децентрализованное хранение данных, возможность смарт-контрактов – позволяют реализовать «прозрачный реестр заявок», в котором участники видят единый валидный перечень всех операций. Примеры из практики и исследований демонстрируют потенциал таких систем.

#### Список используемых источников

1. Lucena P., Binotto A. P. D., da Silva Momo F. и др. // A Case Study for Grain Quality Assurance Tracking based on a Blockchain Business Network // arXiv preprint. 2018. № 1803.07877. URL: <https://arxiv.org/abs/1803.07877> (дата обращения 02.05.2025).
2. Kamilaris A., Fonts A., Prenafeta-Boldu F. X. // The Rise of Blockchain Technology in Agriculture and Food Supply Chains // arXiv preprint. 2019. № 1908.07391. URL: <https://arxiv.org/abs/1908.07391> (дата обращения 02.05.2025).
3. Sudarssan N. // A Framework for Agricultural Food Supply Chain using Blockchain // arXiv preprint. 2024. № 2401.09476. URL: <https://arxiv.org/abs/2401.09476> (дата обращения 4.05.2025).
4. de Brabandt C. How Blockchain Can Enhance Transparency, Traceability and Trust in Procurement Processes // Inside Supply Management. 2023. 12 September.
5. Reidy S. Digitization transforms commodity markets // World Grain. Kansas City: Sosland Publishing Co., 2021. URL: <https://www.world-grain.com/articles/15932-digitization-transforms-commodity-markets> (дата обращения 4.05.2025).

УДК 004.853

М. С. Дмитриев (студенты группы ИКПИ-35, СПбГУТ)

С. А. Зверева (студенты группы ИКПИ-35, СПбГУТ), [zvereva.sa@sut.ru](mailto:zvereva.sa@sut.ru)

## ИСТОРИЯ И ТЕНДЕНЦИЯ РАЗВИТИЯ НЕЙРОСЕТЕЙ

*Нейронные сети (искусственные нейронные сети, ИНС) – это вычислительные системы, моделирующие процессы обработки информации в человеческом мозге. Они являются ключевой технологией искусственного интеллекта и применяются для распознавания закономерностей, классификации данных и решения задач машинного обучения. В данной статье предпринята попытка хронологического анализа становления нейронных сетей – от первых теоретических моделей до современных архитектур. Особое внимание уделено ключевым фигурам, технологическим прорывам и факторам, способствовавшим развитию глубокого обучения, включая рост вычислительных мощностей и появление больших данных. Также рассматриваются перспективы и вызовы дальнейшего развития искусственного интеллекта.*

*нейронная сеть, нейрон, глубокое обучение, обучение сети, искусственный интеллект, перцептрон, обратное распространение ошибки.*

### Введение

Современный этап развития технологий характеризуется повсеместным внедрением нейросетевых решений – от голосовых помощников в смартфонах до систем рекомендаций в социальных сетях и беспилотного транспорта. Как отмечают исследователи, эти технологии, воспринимаемые сегодня как нечто само собой разумеющееся, являются результатом длительного научного поиска ответа на фундаментальный вопрос о возможности машинного мышления, аналогичного человеческому. Согласно современным исследованиям, нейронные сети эволюционировали из узкоспециального инструмента в ключевую технологию, формирующую новую цифровую реальность. Такой стремительный прогресс, по мнению специалистов, делает особенно актуальным изучение исторического развития нейросетевых технологий для их ответственного и осознанного применения в будущем [1-7].

### Первые математические модели нейронов

В 1943 году американский нейрофизиолог Уоррен Мак-Каллок и математик Уолтер Питтс создали первую формальную модель искусственного нейрона. В своей работе «A Logical Calculus of the Ideas Immanent in Nervous

Activity» ученые доказали, что нейрон можно представить как бинарный логический элемент с пороговой активацией, то есть нейрон активируется только при достаточном уровне входного сигнала, а сеть из таких элементов способна выполнять любые логические операции (включая AND, OR, NOT). Именно это научное открытие стало отправной точкой в развитии искусственного интеллекта, поскольку это была первая попытка «оцифровать» человеческое мышление, пусть и в упрощенной форме.

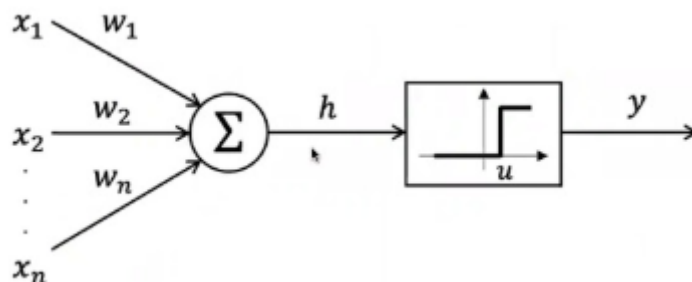


Рис. 1. Первая формальная модель искусственного нейрона Каллока-Питтса

В 1958 году американский психолог и нейрофизиолог Фрэнк Розенблатт совершил прорыв в области ИИ, представив перцептрон – первую в мире обучаемую искусственную нейронную сеть. Это была не только математическая модель, но и реальное устройство – Mark I Perceptron, построенное в Корнеллской авиационной лаборатории. «Mark I» последовательно считывал и выполнял инструкции с перфорированной бумажной ленты. Компьютер не умел выполнять условные переходы, из-за чего каждая программа представляла собой довольно длинный ленточный рулон. Главным отличием этого компьютера было то, что он был первой полностью автоматической вычислительной машиной, не требовавшей какого-либо вмешательства человека в рабочий процесс.

### Период стагнации развития искусственного интеллекта

В 1969 году произошло событие, которое на десятилетия замедлило развитие нейронных сетей – публикация книги «Perceptrons» Марвина Минского и Сеймура Паперта. Их работа содержала строгий математический анализ, выявивший фундаментальные ограничения перцептронов:

1. Невозможность решать задачи, требующие нелинейного разделения. Критики показали, что для решения XOR нужна как минимум двухслойная сеть, а на то время эффективного алгоритма для ее обучения не существовало.

2. Отсутствие теоретической базы для многослойных сетей. Перцептрон Розенблатта имел только один обучаемый слой, а для более сложных задач этого было недостаточно.

Публикация критиков привела к резкому сокращению финансирования исследований и началу стагнации развития искусственного интеллекта.

### Ренессанс нейронных сетей и эра глубокого обучения

Настоящий прорыв в области нейронных сетей произошел в 1986 году, когда группа исследователей в составе Дэвида Румельхарта, Джеффри Хинтона и Рональда Уильямса опубликовала революционную работу, подробно описавшую алгоритм обратного распространения ошибки. Благодаря этому впервые появилась возможность эффективно обучать сети с несколькими слоями, также стали возможны сложные нелинейные преобразования данных и были заложены основы глубокого обучения ИИ, которые по сей день являются фундаментом для всех нейросетей. После этого открытия началась эра экспериментов над нейросетями и были предложены новые архитектуры, такие как рекуррентные (для обработки последовательности текста, речи и т.д.), сверточные (для анализа изображений) и многие другие.

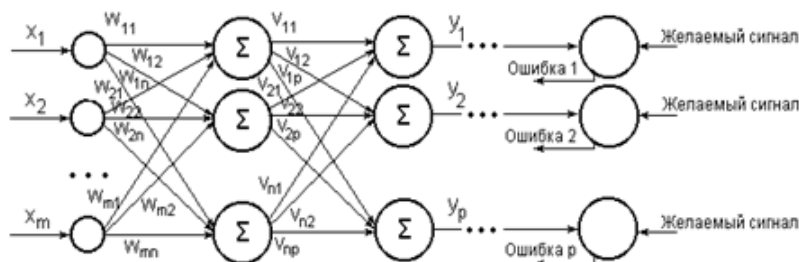


Рис. 2. Алгоритм обратного распространения ошибки

С 2006 года мир стал свидетелем беспрецедентного технологического скачка, наступила эпоха глубокого обучения. Этот период ознаменовался тем, что искусственные нейронные сети начали демонстрировать результаты, превосходящие человеческие когнитивные способности в таких областях как: распознавание изображений и речи, обработка естественного языка, стратегическое планирование, творческая генерация контента. Фундаментом этого революционного прорыва стали пять взаимосвязанных факторов:

1. Экспоненциальный рост вычислительных мощностей – появление GPU-ускорения и специализированных процессоров (TPU) сделало возможным обучение сетей с миллиардами параметров.

2. Доступ к большим данным – без огромных массивов размеченной информации достижение «человеческого уровня» точности оставалось бы теоретической возможностью.

3. Демократизация технологий – открытые фреймворки (TensorFlow, PyTorch) вывели разработку ИИ за пределы узкого круга научных лабораторий.

4. Алгоритмические инновации – появление новых архитектур (трансформеры, GAN) и методов обучения (transfer learning).

5. Массовые инвестиции – многомиллиардные вложения корпораций и венчурных фондов создали мощную инфраструктуру для исследований.

Такой симбиоз технологических, экономических и научных факторов привел к качественному скачку в развитии ИИ, изменившему представления о возможностях машинного интеллекта.

## **Перспективы и вызовы развития нейронных сетей в будущем**

Современное технологическое развитие приближает нас к эпохе, когда нейронные сети трансформируются из специализированных инструментов в фундаментальный компонент человеческой цивилизации. Их влияние будет распространяться от повседневных социальных взаимодействий до глобальных научных исследований. Алгоритмы глубокого обучения демонстрируют значительный потенциал для ускорения научного прогресса в таких областях, как медицина, физика и климатология.

В настоящее время уже наблюдаются первые проявления искусственных систем, демонстрирующих элементы универсального интеллекта, включая способности к логическим рассуждениям, творческой деятельности и адаптивному поведению. Данная тенденция предполагает существенное расширение возможностей искусственного интеллекта в ближайшем будущем. Однако столь стремительное развитие нейросетевых технологий сопровождается рядом существенных проблем. Среди наиболее значимых можно выделить:

1. Высокое энергопотребление (обучение модели GPT-3 требовало значительных энергетических ресурсов, и при сохранении текущих тенденций к 2030 году системы ИИ могут потреблять до 10 % мирового объема электроэнергии)

2. Социально-экономические последствия массовой автоматизации (потенциальное сокращение рабочих мест в глобальном масштабе)

3. Антропологические и философские вызовы (девальвация традиционных форм человеческой деятельности в условиях, когда искусственный интеллект способен создавать художественные произведения, совершать научные открытия и формулировать философские концепции)

## Заключение

Проведенное исследование позволило системно проанализировать эволюцию нейронных сетей – от первых теоретических моделей нейронов до современных архитектур глубокого обучения. История развития ИИ продемонстрировала впечатляющую динамику: от революционных прорывов (перцептрон Розенблатта, алгоритм обратного распространения) до периодов стагнации, что подчеркивает сложный, нелинейный характер технологического прогресса. Современные нейросети перешли из категории узкоспециальных инструментов в разряд базовой инфраструктуры цивилизации, сравнимой по значимости с электричеством.

## Список использованных источников:

1. Розенблатт Ф. Перцептроны. М.: Мир, 1965. 261 с.
2. Николенко С., Кадури А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб.: Питер, 2018. 480 с.
3. Мак-Каллок У., Питтс У. Логическое исчисление идей, относящихся к нервной деятельности // Автоматы. М.: ИЛ, 1956. С. 363-384.
4. Минский М., Пейперт С. Перцептроны. М.: Мир, 1971. 261 с.
5. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 800 p.
6. Рашид Т. Создаем свою нейросеть. СПб.: Питер, 2021. 304 с.
7. LeCun Y., Bengio Y., Hinton G. Deep Learning // Nature. 2015. Vol. 521. P. 436-444.

*Статья представлена научным руководителем, доцентом кафедры программной инженерии и вычислительной техники СПбГУТ, кандидатом технических наук Дагаевым А. В.*

УДК 004.422.636.7

А. С. Довыденков (студент группы Z3431, ГУАП), [asdovydenkov@yandex.ru](mailto:asdovydenkov@yandex.ru)

## ПРОЕКТИРОВАНИЕ ХЕШ-ФУНКЦИИ ДЛЯ ХЕШ-ТАБЛИЦЫ

*В статье представлена часть учебного проекта по разработке информационной системы «Обслуживание клиентов оператора сотовой связи». Одной из задач работы является проектирование хеш-таблицы для хранения номеров SIM-карт. Рассмотрены классические методы вычисления хеш-функции. Разработана хеш-функция, комбинирующая методы свертки и деления, что позволило эффективно использовать хеш-таблицу и минимизировать количество коллизий.*

*хеширование, хеш-функция, хеш-таблица, структуры данных*

### Введение

При разработке информационных систем возникает необходимость в хранении таблицы данных. При этом доступ к данным должен осуществляться не по индексу в таблице, а по некоторому первичному ключу, то есть таблица должна быть организована такими образом, чтобы поиск по первичному ключу осуществлялся как можно быстрее, а накладные расходы при добавлении и удалении новых элементов были минимальны.

«Хеширование – это метод случайного упорядочивания элементов, которое обеспечивает сокращение времени доступа к данным» [1]. Суть метода в том, что индекс в таблице вычисляется из ключа с помощью хеш-функции.

Хеш-функция  $a = h(k)$  работает за время  $O(1)$ , однако мощность множества ключей может значительно превосходить мощность множества адресов. В частности, ключом может быть произвольная строка, а таблица является массивом заданного размера, вследствие чего при вычислении хеш-функции разные ключи могут указывать на один адрес. Такие ситуации называются коллизиями, а образующие коллизию данные – синонимами. Для разрешения коллизий используются различные методы, такие как открытое хеширование, линейное опробование, квадратичное опробование, двойное хеширование [2].

Целью работы является разработка хеш-функции, минимизирующей количество коллизий при хешировании номеров SIM-карт и сравнение с существующими методами хеширования.

### Хеш-функции

На скорость поиска в хеш-таблице сильно влияет выбор хеш-функции. Хорошая хеш-функция характеризуется следующими свойствами:



- равномерно распределяет ключи по пространству адресов;
- минимизирует количество коллизий для заданного пространства адресов;
- явно не отображает связь между значениями ключей и адресов;
- должна быть быстрой и простой для вычисления.

При хорошем выборе хеш-функции заполнение таблицы происходит равномерно и коллизии возникают реже. Далее рассматриваются различные методы хеширования.

*Метод деления.* В данном случае отображение ключа  $k$  в одну из ячеек  $m$  осуществляется путем получения остатка от деления  $k$  на  $m$ :

$$h(k) = k \bmod m \quad (1)$$

При работе с этим методом важно правильно выбрать  $m$ . Например,  $m$  не должно быть степенью двойки  $2^p$ , так как в этом случае хеш представляет собой просто  $p$  младших битов числа. Считается [3], что обычно хороший результат дает простое число, достаточно далекое от степени двойки.

Пример использования метода деления для распределения 100 000 записей по 1000 ячейкам представлен на рисунке 1.

*Метод умножения.* В данном случае отображение ключа  $k$  в одну из ячеек  $m$  осуществляется в два этапа. Сначала ключ  $k$  умножается на константу  $0 < A < 1$  и выделяется дробная часть. Затем умножаем полученное значение на  $m$  и округляем вниз:

$$h(k) = \lfloor m(kA \bmod 1) \rfloor \quad (2)$$

Преимуществом метода является независимость качества функции от значения  $m$ . Значения константы  $A$  могут быть любыми от 0 до 1, но с некоторыми значениями метод работает лучше, чем с другими. Согласно [4], неплохие результаты дает значение  $A = 0.6180339887$ . Пример использования метода умножения при приведенном  $A$  представлен на рисунке 2.

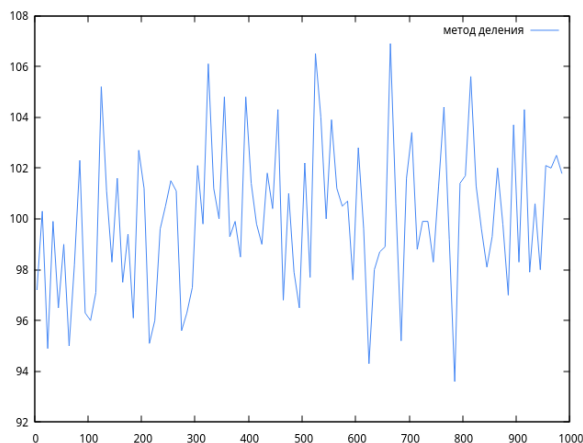


Рис. 1. Метод деления

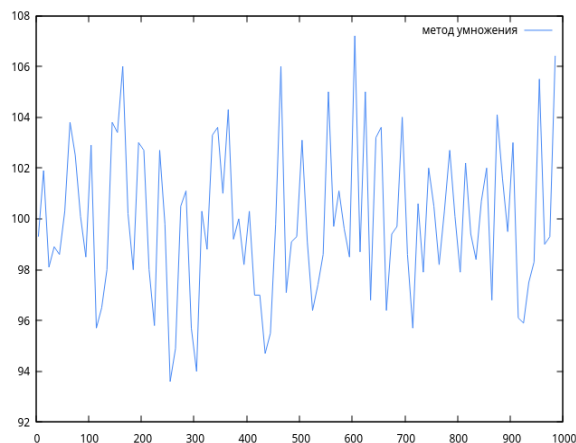


Рис. 2. Метод умножения

*Метод середины квадрата.* Значение ключа преобразуется в число, это число затем возводится в квадрат, из него выбираются несколько средних цифр и интерпретируются как адрес записи. Пример использования метода середины квадрата представлен на рисунке 3.

*Метод свертки.* Цифровое представление ключа разбивается на части, каждая из которых имеет длину, равную длине требуемого адреса. Над частями производятся арифметические или поразрядные логические операции, результат которых интерпретируется как адрес. Пример использования метода свертки при использовании поразрядного «исключающего или» представлен на рисунке 4.

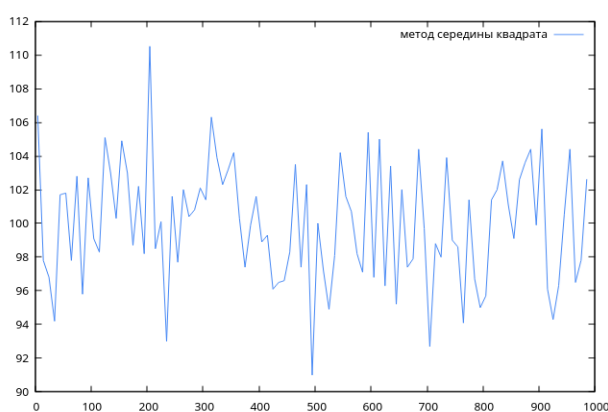


Рис. 3. Метод середины квадрата

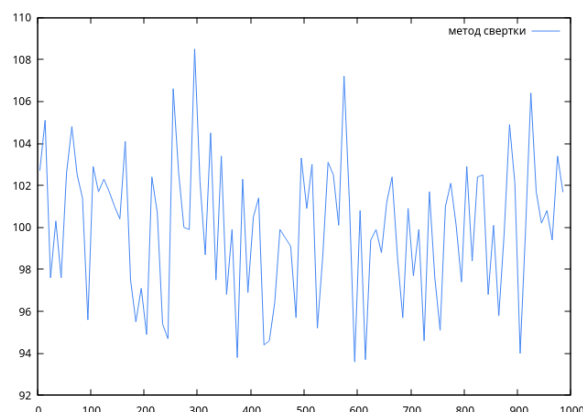


Рис. 4. Метод свертки

## Практическая часть

В рамках работы при составлении хеш-функции учитывалось, что в разрабатываемой информационной системе ключами являются номера SIM-карт, то есть строка формата «NNN-NNNNNNN», где  $N$  – цифра.

Хеш функция вычисляется по формуле [5]:

$$h_i = \sum_{i=0}^3 c_i \cdot \frac{k}{p^i} \bmod p \quad (3)$$

где  $c_i$  – константы;

$p$  – минимальное простое число большее  $m$ .

Минимальное число коллизий достигается при  $c_0 = 99, c_1 = 93, c_2 = 85, c_3 = 2$ .

Разработанная функция представлена в листинге 1.

Листинг 1. Хеш-функция

```

uint32_t hash5(std::string key, int m) {
    auto k = as_int(key);
    uint32_t p = 1009;
    uint32_t c[4] = {99, 93, 85, 2};
    uint32_t h = 0;
    for (int i = 0; i < 4; ++i) {
        h += (c[i] * k) % p;
        k /= p;
    }
    return h % m;
}

```

### Анализ результатов

Для сравнительного анализа качества хеш-функций был сгенерирован набор данных, состоящих из 100 000 записей и распределен каждой хеш-функцией по 1000 ячейкам. Получившиеся распределения представлены на рисунках 1-5. Для качественного сравнения хеш-функций был вычислен показатель  $\beta$  коллизий, а для оценки равномерности распределений было вычислено их среднее квадратическое отклонение (таблица 1).

Показатель  $\beta$  коллизий в словаре рассчитывается как отношение количества коллизий к общему числу словарных единиц словаря.

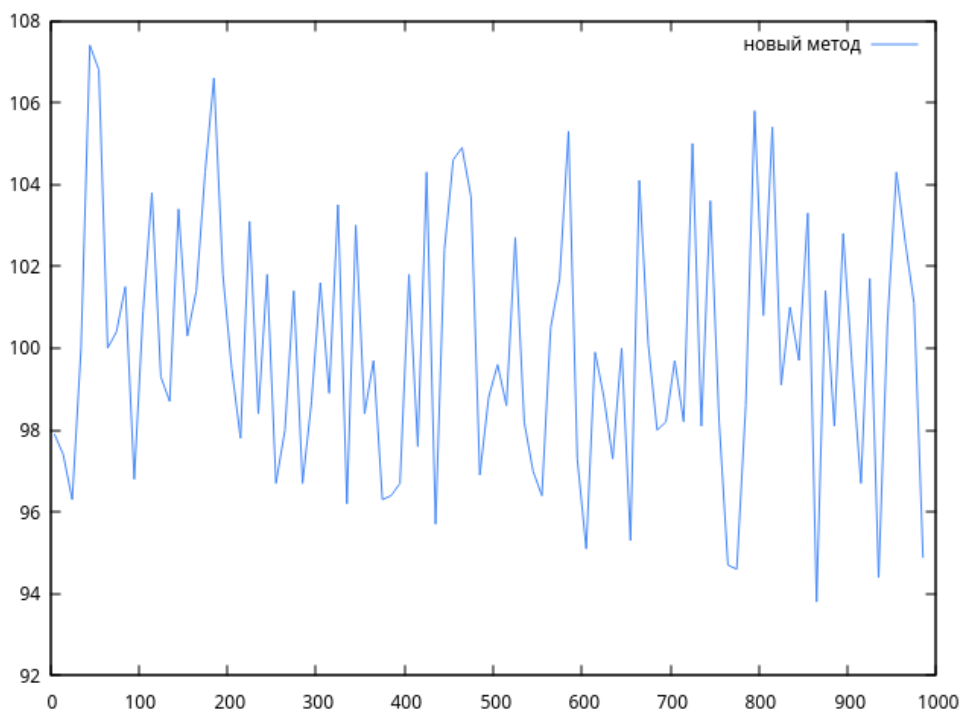


Рис. 5. Распределение значений хеш-функции

ТАБЛИЦА 1. Сравнение качества хеш-функций

| Метод               | Показатель $\beta$ коллизий | Среднее квадратическое отклонение $\sigma$ |
|---------------------|-----------------------------|--------------------------------------------|
| Деления             | 0,00134                     | 9,91                                       |
| Умножения           | 0,00133                     | 10,01                                      |
| Средины квадрата    | 0,00133                     | 10,22                                      |
| Свертки             | 0,00137                     | 10,13                                      |
| Разработанный метод | 0,00135                     | 10,02                                      |

### Вывод

Разработанная функция распределяет ключи достаточно равномерно, при этом задействуются все ячейки таблицы. Хотя в распределении и имеется несколько выделяющихся экстремумов, их расположение носит случайный характер и меняется при повторной генерации ключей.

Выбор метода должен производиться на основе анализа хешируемых данных в конкретной задаче. В результате исследования было выявлено, что использование различных методов для хеширования номеров телефонов дает схожие результаты.

Репозиторий с исходным кодом: <https://github.com/dovydenkovas/sim-hash>

### Список используемых источников

1. Матьяш В. А. Алгоритмы и структуры данных: учеб. пособие / Матьяш В. А., Рогачев С. А. СПб.: ГУАП, 2021. 71 с.
2. Ключарев А. А., Матьяш В. А., Щекин С. В. Структуры и алгоритмы обработки данных: Учеб. Пособие/СПбГУАП. СПб., 2003. 172 с.
3. Кормен, Томас Х. И др. Алгоритмы: построение и анализ, 3-е изд.: Пер. с англ. СПб.: ООО «Диалектика», 2020. 1328 с.
4. Кнут Д. Э. Искусство программирования, том 3. Сортировка и поиск, 2-е изд. СПб.: ООО «Диалектика», 2019. 832 с.
5. Дасгупта С., Пападимитриу Х., Вазирани У. Алгоритмы [пер. с англ. под ред. Шеня А.]. М.: МЦНМО, 2014. 320 с.

*Статья представлена научным руководителем, старшим преподавателем кафедры компьютерных технологий и программной инженерии ГУАП Рогачевым С. А.*

УДК 004.89:159.9:78

Д. О. Жаранов (студент группы ИСТ-213, СПбГУТ), [zharanov.do@sut.ru](mailto:zharanov.do@sut.ru)

## ПРОЕКТИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРОГНОЗИРОВАНИЯ ЛИЧНОСТНЫХ ХАРАКТЕРИСТИК НА ОСНОВЕ АНАЛИЗА МУЗЫКАЛЬНЫХ ПРЕДПОЧТЕНИЙ

*В статье рассматривается проектирование интеллектуальной системы прогнозирования личностных характеристик пользователя на основе анализа его музыкальных предпочтений. Актуальность работы обусловлена растущим интересом к использованию музыкальных данных для определения психотипа человека. Предложена модель системы, реализующая определение типа личности по модели «Big Five» и формирование рекомендованных плейлистов, направленных на улучшение настроения и других аспектов психоэмоционального состояния. Построена диаграмма прецедентов, демонстрирующая основной функционал системы. Описан алгоритм формирования портрета пользователя и его личностных характеристик на базе его музыкальных предпочтений. Рассматриваемая система сочетает методы анализа пользовательских данных с психометрическим подходом, обеспечивая персонализированные рекомендации и поддержку эмоционального состояния пользователя.*

*интеллектуальная система, проектирование, музыкальные предпочтения, личностные характеристики, Big Five, рекомендательные системы*

В условиях стремительного развития цифровых технологий и широкого внедрения искусственного интеллекта возрастает интерес к созданию систем, способных учитывать личностные особенности пользователей. Музыка, как один из наиболее эмоционально насыщенных видов контента, обладает высоким потенциалом для анализа психоэмоционального состояния человека. Благодаря развитию стриминговых сервисов и доступности музыкальных метаданных (жанр, настроение, темп и др.), появилась возможность использовать эти данные в сочетании с психологическими моделями, такими как «Big Five», для построения персонализированных профилей личности.

Актуальность разработки интеллектуальной системы заключается в ее способности объединить машинное обучение, психологию и музыкальную аналитику для решения значимых задач: самопознание через музыку, улучшение эмоционального состояния с помощью персонализированных плейлистов, превентивная психодиагностика и расширение возможностей рекомендательных алгоритмов. В условиях растущего запроса на индивидуализированный цифровой опыт система, способная воспринимать

пользователя как личность с уникальными характеристиками, становится особенно востребованной как в научной, так и в практической сфере. Современные интеллектуальные системы либо сильны в персонализации, но игнорируют психологические аспекты, либо наоборот – ориентированы на эмоциональное состояние, но не учитывают предпочтения пользователя.

На основе анализа спроектирована система, определяющая личностные характеристики пользователя на основе его музыкальных предпочтений с использованием модели «Big Five». Данная психологическая модель является научно признанной и описывает человека с помощью пяти факторов: открытость опыту, добросовестность, экстраверсия, доброжелательность и нейротизм.

В рамках декомпозиции системы можно выделить следующие модули: модуль авторизации и профиля; анализ музыкальных вкусов; психологический анализ; генерация музыкальных рекомендаций; взаимодействие с Spotify API; мониторинг состояния пользователя; обратная связь. Схема взаимодействия модулей интеллектуальной системы представлена на рис. 1.

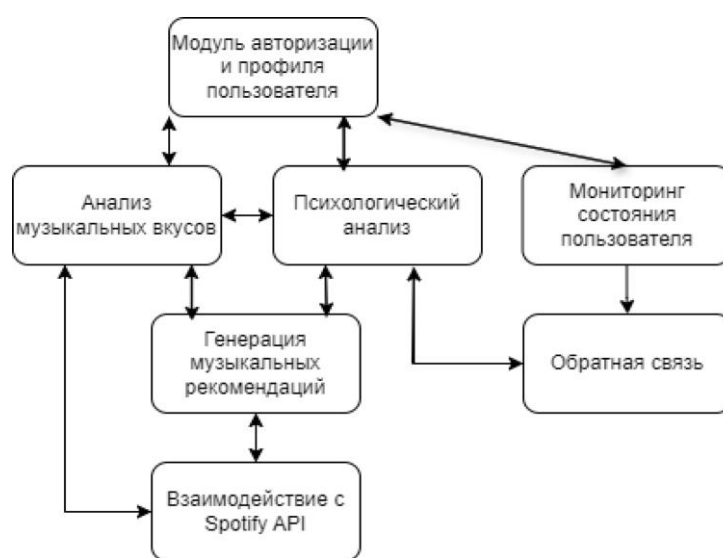


Рис. 1. Схема взаимодействия модулей интеллектуальной системы

Основные функции системы включают в себя: определение психотипа по музыкальному плейлисту, составление отчетов и графиков по психологическому состоянию, составление опросов для отслеживания психологического состояния, предложение музыкальных композиций для улучшения психологического состояния.

Функциональные возможности системы представлены на рис. 2 в рамках диаграммы прецедентов системы прогнозирования личностных характеристик на основе анализа музыкальных предпочтений [1].

Для формирования психологического профиля пользователю необходимо отправить ссылку на открытый плейлист Spotify. В системе она проверяется на корректность, после чего отправляется запрос к Spotify API. В случае, если ссылка некорректна или невозможно обратиться к Spotify API, пользователю предлагается ввести ссылку повторно или отправить треки вручную. После получения плейлиста из каждого трека извлекаются метаданные, которые сопоставляются с моделью Big Five. Из данных показателей путем вычисления среднего арифметического складывается общая характеристика пользователя по модели Big Five, которая и определяет психологический профиль пользователя.

После формирования психологического профиля пользователь выбирает эффект, который хочет получить от плейлиста, после чего ему предлагается выбрать предпочтения по авторам, жанрам, стилям музыки. Пользователь может ввести их или отказаться от ввода. После ввода предпочтений система сопоставляет цели с музыкальными характеристиками для предоставления наиболее подходящих треков. Данные треки возвращаются через Spotify API, после чего рекомендованный плейлист формируется и отправляется пользователю.

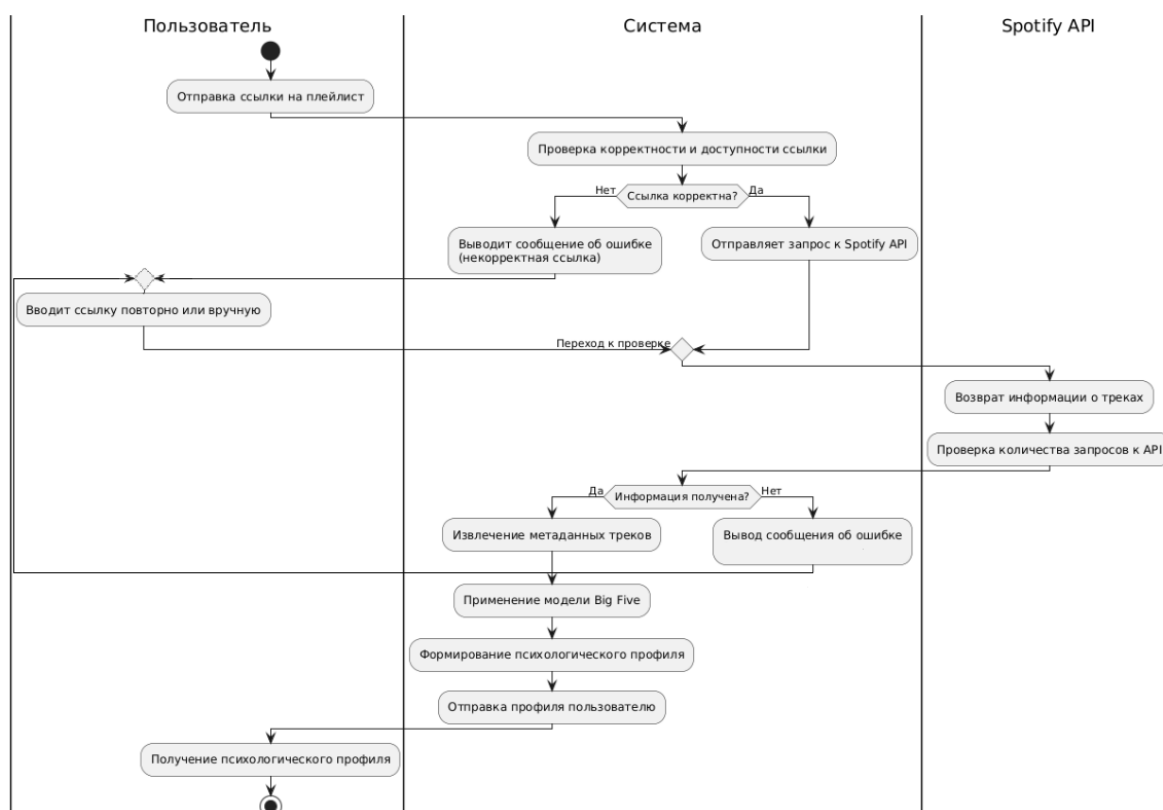


Рис. 3. Диаграмма деятельности процесса формирования психологического профиля

На рисунке 4 представлена диаграмма деятельности для процесса генерации рекомендаций.

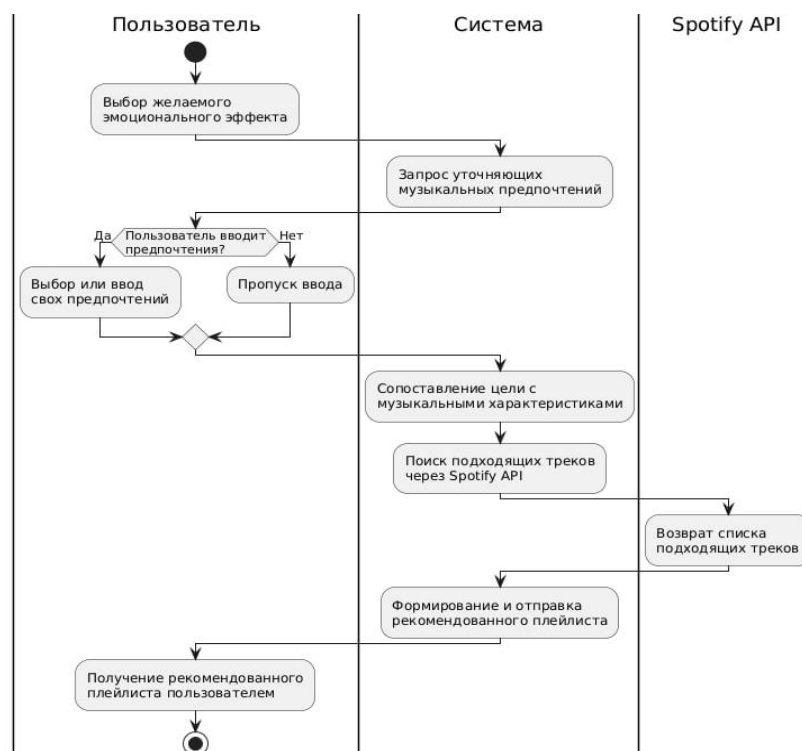


Рис. 4. Диаграмма деятельности процесса генерации рекомендаций



Таким образом, спроектированная система является не только современным решением, но и основой для дальнейших исследований и технологических разработок в области персонализированных интеллектуальных сервисов.

Для дальнейшего развития системы рекомендуется реализовать пользовательский интерфейс, улучшить аналитические модели, расширить интеграции с музыкальными платформами и настроить постоянный мониторинг изменений предпочтения и состояния пользователя.

#### **Список используемых источников**

1. Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя. 2-е изд.: Пер. с англ. Мухин Н. М.: ДМК Пресс. 496 с.
2. Котлова М. В. Методы и средства проектирования информационных систем и технологий: учебное пособие / М. В. Котлова, Е. В. Давыдова; рец.: М. П. Белов, Т. В. Матюхина. СПб.: СПбГУТ, 2015. 62 с.

*Статья представлена научным руководителем, старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.65

**Е. А. Журов, А. Н. Крутицкий, И. А. Романцов**

(студенты группы ИКПИ-35, СПбГУТ), [romantsov.ia@sut.ru](mailto:romantsov.ia@sut.ru)

## **МЕТОДЫ АНАЛИЗА БОЛЬШИХ ДАННЫХ: ОТ ТРАДИЦИОННЫХ К СОВРЕМЕННЫМ**

*Большие данные (Big Data) описывают неструктурированные, высокообъемные и разнообразные наборы данных, которые обновляются с большой скоростью. Они играют ключевую роль в бизнесе, науке, здравоохранении и государственном управлении. Цель статьи – рассмотреть эволюцию методов анализа данных: от статистических методов к алгоритмам искусственного интеллекта. Подробно освещены технологии OLAP, Data Mining и ML. Представлены графики и таблицы, отражающие сравнение эффективности методов.*

*большие данные, анализ данных, OLAP, Data Mining, машинное обучение*

### **Введение**

Современное информационное общество сталкивается с колоссальными объемами данных, генерируемыми в результате работы цифровых сервисов, Интернета вещей (IoT), социальных сетей и мобильных приложений. Согласно отчету IDC, объем глобальных данных в 2025 году достигнет 181 зеттабайта [1]. Эффективная обработка таких массивов требует применения как классических статистических методов, так и современных интеллектуальных систем.

Термин «большие данные» (Big Data) охватывает три ключевые характеристики – объем (Volume), разнообразие (Variety) и скорость (Velocity), которые были позднее дополнены такими признаками, как достоверность (Veracity) и ценность (Value). Эти пять «V» формируют фундамент концепции Big Data, на основе которой строятся методы анализа, предсказания и принятия решений.

В рамках статьи проводится сравнительный анализ подходов к обработке данных, начиная от традиционных методов статистики до новейших алгоритмов глубокого обучения. Для наглядности включены графики и таблицы, иллюстрирующие эволюцию и эффективность используемых подходов в разных эпохах развития цифровой аналитики.

## Классические методы анализа данных

На заре информационных технологий основными методами анализа были статистические подходы: корреляционный анализ, линейная и множественная регрессия, методы главных компонент и дисперсионный анализ. Они позволяли выявлять зависимости между переменными, строить прогнозы и проводить категоризацию объектов.

Пример: в маркетинге анализ регрессии используется для предсказания продаж в зависимости от рекламных затрат [2]. Однако такие методы предполагают наличие хорошо структурированных данных и не масштабируются на большие объемы.

ТАБЛИЦА 1. Преимущества и ограничения классических методов

| Метод                | Преимущества                 | Ограничения                             |
|----------------------|------------------------------|-----------------------------------------|
| Линейная регрессия   | Простота, интерпретируемость | Чувствительность к выбросам             |
| Дисперсионный анализ | Хорош для небольших выборок  | Ограничен числом факторов               |
| Корреляция           | Быстрая оценка зависимости   | Не выявляет причинно-следственные связи |

Классические методы все еще используются в академических исследованиях, экономике и малом бизнесе, где объем данных ограничен, а точность и прозрачность модели имеют первостепенное значение [3].

## Промежуточный этап развития методов анализа данных

По мере роста объемов информации и усложнения ее структуры стали появляться инструменты, способные обрабатывать данные в многомерном виде. К таким инструментам относятся OLAP-системы (On-Line Analytical Processing) и технологии Data Mining. Эти подходы служат мостом между статистикой и интеллектуальным анализом.

OLAP позволяет анализировать данные в разрезе различных измерений (например, время, география, категория товара), обеспечивая удобную агрегацию и визуализацию [4]. Благодаря OLAP стало возможным строить «срезы» и «кубы» данных, что значительно упростило бизнес-аналитику.

В свою очередь, Data Mining (интеллектуальный анализ данных) включает в себя использование алгоритмов, позволяющих находить скрытые закономерности, ассоциации и тренды. Примеры применяемых алгоритмов:

- алгоритмы кластеризации (k-means, DBSCAN);

- деревья решений (C4.5, CART);
- методы ассоциативных правил (Apriori);
- базовые нейронные сети [5].

ТАБЛИЦА 2. Возможности OLAP и Data Mining

| Технология  | Преимущества                    | Применение                        |
|-------------|---------------------------------|-----------------------------------|
| OLAP        | Быстрая агрегация, визуализация | Финансовая отчетность, BI-системы |
| Data Mining | Поиск скрытых закономерностей   | Маркетинг, прогнозирование спроса |

Таким образом, переходный этап стал важным шагом в развитии аналитики данных, подготовив основу для внедрения автоматических и обучающихся систем, способных справляться с постоянно растущими массивами информации.

### Современные методы анализа больших данных

Сегодняшний этап характеризуется активным внедрением алгоритмов машинного обучения (ML) и искусственного интеллекта (AI), особенно в сочетании с параллельными вычислениями и облачными технологиями. Эти методы позволяют не только анализировать данные, но и обучаться на них, выявлять сложные паттерны и адаптироваться к изменениям в реальном времени.

Среди ключевых технологий:

- Глубокое обучение (Deep Learning) – нейронные сети с множеством слоев, применяемые для обработки изображений, текста и речи;
- Обработка естественного языка (NLP) – позволяет анализировать текстовые данные и извлекать из них смысл;
- Обучение с подкреплением (Reinforcement Learning) – используется в робототехнике и автономных системах;
- Графовые алгоритмы – применяются для анализа социальных сетей, биоинформатики и логистики;
- Поточковая аналитика – инструменты типа Apache Kafka и Apache Flink позволяют обрабатывать данные в реальном времени [6].

Современные методы нередко комбинируются в гибридные модели, использующие ансамбли алгоритмов для повышения точности и устойчивости.

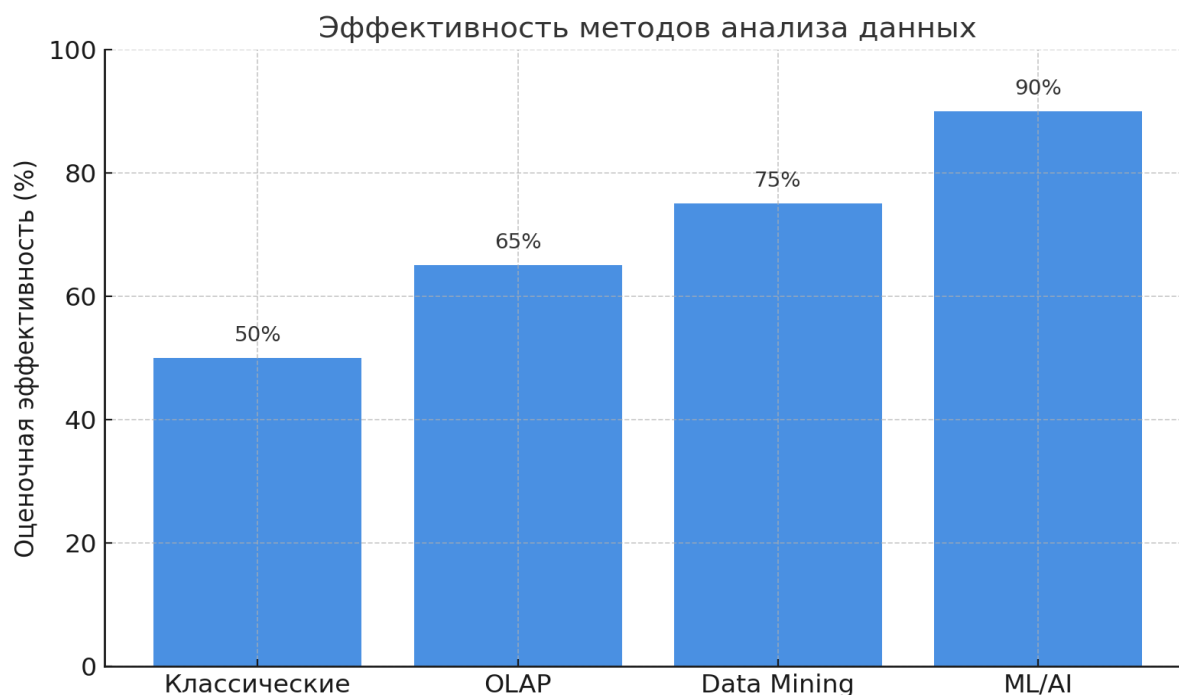


Рис. 1. Эффективность методов анализа данных (составлено авторами на основе обобщенной оценки применимости методов в проектах больших данных [6])

На графике показано, как возрастает эффективность по мере перехода от статистических методов к технологиям искусственного интеллекта.

Современные платформы анализа данных (например, Google BigQuery, Amazon Redshift, Microsoft Azure Synapse) интегрируют машинное обучение и масштабируемость, что делает возможной обработку петабайтов информации за минуты [7].

### Современные вызовы и будущее анализа данных

Несмотря на значительные успехи в развитии технологий анализа больших данных, специалисты сталкиваются с рядом вызовов, требующих комплексного подхода:

1. Конфиденциальность и безопасность данных. Сбор и хранение персональной информации требует строгого соблюдения стандартов защиты данных, таких как GDPR в ЕС и ФЗ-152 в России [8]. Утечки данных могут не только нанести финансовый ущерб, но и подорвать доверие пользователей.

2. Интерпретируемость моделей. Современные алгоритмы, особенно глубокие нейросети, обладают высокой точностью, но часто функционируют как «черный ящик». Это создает сложности при объяснении решений, особенно в сферах с высоким уровнем ответственности, таких как медицина и правосудие [9].

3. Кадровый дефицит. Необходимость в квалифицированных специалистах по анализу данных, Data Science и AI остается острой. Согласно исследованиям ВШЭ, спрос на таких специалистов ежегодно превышает предложение на 20–30% [10].

4. Энергопотребление и устойчивость. Обработка больших объемов данных требует значительных вычислительных мощностей, что увеличивает нагрузку на инфраструктуру и экосистему. В ответ развиваются методы "зеленых вычислений", включая оптимизацию моделей и использование возобновляемых источников энергии.

## Перспективы развития

Будущее анализа данных связано с:

- развитием Explainable AI (объяснимого ИИ);
- интеграцией квантовых вычислений в анализ данных;
- автоматизацией аналитики (AutoML);
- распространением edge computing для анализа данных ближе к источнику их генерации;
- использованием синтетических данных для обучения моделей без нарушения приватности.

Таким образом, анализ больших данных продолжает активно развиваться, трансформируя методы обработки информации и открывая новые горизонты для бизнеса, науки и государственного управления.

## Заключение

Анализ больших данных прошел путь от простых статистических методов до высокоинтеллектуальных алгоритмов машинного обучения и искусственного интеллекта. На каждом этапе эволюции появлялись новые подходы, способные обрабатывать все большие объемы информации с повышенной точностью и скоростью.

Современные методы анализа данных открывают перед обществом и бизнесом огромные перспективы, включая точное прогнозирование, автоматизацию принятия решений и персонализацию услуг. Однако для полноценной реализации этих возможностей необходимо решать сопутствующие вызовы – от правовых и этических до технических и инфраструктурных.

Комплексный подход, включающий развитие технологий, подготовку специалистов и обеспечение нормативной базы, станет залогом устойчивого и безопасного использования потенциала больших данных в будущем.

**Список используемых источников**

1. Международная корпорация данных (IDC). Отчет по Big Data, 2021.
2. Ивченко Г. И., Медведев Ю. С. Теория вероятностей и математическая статистика. М.: МЦНМО, 2007.
3. Минашкин А. Г. Методы статистического анализа. СПб.: Питер, 2016.
4. Кимбалл Р. Хранилища данных: проектирование, реализация и сопровождение. М.: Вильямс, 2010.
5. Ларсен Б., Марков А. Data Mining: Практическое руководство. М.: БХВ-Петербург, 2015.
6. Белоусов С. Apache Spark и Hadoop: основы больших данных. М.: ДМК Пресс, 2020.
7. Официальные сайты Amazon Web Services, Microsoft Azure и Google Cloud. Доступ: 2024.
8. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных».
9. Барбер Д. Байесовские методы машинного обучения. М.: Лаборатория знаний, 2019.
10. Аналитический доклад ВШЭ «Рынок труда в сфере Data Science», 2023.

*Статья представлена научным руководителем, доцентом кафедры программной инженерии и вычислительной техники СПбГУТ, кандидатом технических наук Дагаевым А. В.*

УДК 004.056.5; 004.8

В. В. Кечко (студент группы ИКПИ-392м, СПбГУТ), [kechko.vv@sut.ru](mailto:kechko.vv@sut.ru)

## ПРОГНОЗИРОВАНИЕ ДЕГРАДАЦИИ КАЧЕСТВА FPV-СВЯЗИ С ПРИМЕНЕНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ

*В статье рассматриваются современные методы машинного обучения для прогнозирования деградации связи в FPV-управлении беспилотными летательными аппаратами. Проведен сравнительный анализ моделей, таких как RNN, GAT-LLM и XGBoost, с точки зрения их применимости в условиях нестабильной передачи данных. Обоснован выбор наиболее перспективных подходов, предложены рекомендации по их интеграции в систему оценки качества связи.*

*FPV-связь, деградация канала, машинное обучение, прогнозирование, RNN, графовые нейросети*

### Введение

Сложность среды передачи, подвижность дронов и нестабильность каналов делают задачу оценки и прогнозирования деградации связи особенно актуальной. При этом традиционные методы мониторинга качества зачастую не успевают реагировать на изменения в реальном времени. В таких условиях машинное обучение становится эффективным инструментом, способным выявлять закономерности в телеметрических и видеоданных, предсказывать ухудшение качества и формировать основу для заблаговременной коррекции системы управления.

### Деградация связи в FPV-управлении

Для надежного управления беспилотными летательными аппаратами с использованием FPV-технологии (First-Person View) особое значение имеет устойчивость и качество канала связи. Под деградацией в данном контексте понимается ухудшение характеристик видеопотока и управляющих сигналов, проявляющееся в виде увеличения задержек, снижения показателя структурного сходства (SSIM), роста количества ошибок и потерь пакетов данных. Эти нарушения снижают оперативность реакции оператора, ухудшают точность управления и повышают риск возникновения внештатных ситуаций. Поэтому важно оперативно обнаруживать и предсказывать такие отклонения для своевременной оценки работоспособности системы.



## Обзор методов машинного обучения для прогнозирования деградации связи

Машинное обучение (ML) позволяет эффективно решать задачу прогнозирования деградации каналов связи благодаря своей способности обрабатывать большие объемы данных и выявлять неявные зависимости между параметрами. В существующих исследованиях применяются различные подходы:

- Графовые нейронные сети (GNN), объединенные с большими языковыми моделями (например, GAT-LLM), успешно применяются для предсказания качества связи с учетом пространственных и временных корреляций между каналами [1].
- Рекуррентные нейронные сети (RNN и LSTM) подходят для временных последовательностей данных и позволяют прогнозировать качество связи при наличии динамических изменений в среде передачи [2].
- Методы классического машинного обучения (например, Random Forest, SVM, XGBoost) показывают высокие результаты при наличии хорошо структурированных и размеченных данных, требуя меньших вычислительных ресурсов [3-5].

Каждый из этих подходов имеет свои преимущества и ограничения, зависящие от специфики задач FPV-систем.

### Сравнительный анализ подходов

В таблице 1 приведено сравнение указанных подходов с точки зрения их применимости к задаче прогнозирования деградации FPV-каналов связи.

ТАБЛИЦА 1. Сравнение методик

| Метод ML                 | Входные данные                  | Тип прогноза                    | Преимущества                       | Недостатки                        |
|--------------------------|---------------------------------|---------------------------------|------------------------------------|-----------------------------------|
| Графовые нейросети (GNN) | Топология сети, телеметрия      | Краткосрочный, точечный         | Учет пространственных зависимостей | Высокая сложность обучения        |
| Рекуррентные сети (LSTM) | Временные ряды (SSIM, задержки) | Среднесрочный, последовательный | Отлично работают с динамикой       | Требуют больших объемов данных    |
| Random Forest, XGBoost   | Наборы метрик, логов            | Краткосрочный                   | Простота интерпретации, скорость   | Ограниченность временного анализа |

На основе сравнения можно сделать вывод, что для задачи прогнозирования деградации в FPV-системах наиболее перспективными выглядят подходы, способные учитывать временные изменения и зависимости параметров, такие как рекуррентные нейронные сети и графовые нейронные сети.

### **Обоснование выбора ML-моделей для прогнозирования деградации связи**

На основании проведенного сравнительного анализа можно выделить две наиболее подходящие группы моделей:

Bi-LSTM с attention – ловит шаблоны во временных рядах (SSIM, задержки, потери пакетов) и быстро реагирует на скачки качества сигнала при умеренных вычислительных затратах [2].

Графовые модели (GAT-LLM) – учитывают сетевую топологию и взаимодействия между узлами FPV-системы, обеспечивая высокую точность прогнозов [1].

Выбор именно этих моделей обусловлен:

- Bi-LSTM стабильно предсказывает среднесрочные колебания сигнала и справляется с резкими изменениями;
- GAT-LLM охватывает пространственные связи между узлами и извлекает дополнительный смысл из текстовых данных;
- наличие проверенных исследований, подтверждающих их эффективность в задачах прогнозирования качества беспроводных каналов.

Таким образом, интеграция данных моделей в разрабатываемую методику позволит существенно повысить ее точность и объективность оценки информационного обмена.

### **Интеграция выбранных моделей в методику оценки**

Предлагаемый подход объединяет возможности двух моделей машинного обучения – Bi-LSTM с механизмом внимания и GAT-LLM – в рамках методики оценки устойчивости канала.

1. Сбор текущих параметров: на этом этапе автоматически фиксируются ключевые метрики качества SSIM, задержка, потери пакетов, а также телеметрические данные вроде RSSI и BER, что дает базу для последующего анализа.

2. Прогнозирование деградации:

- Bi-LSTM с attention отслеживает и оценивает изменения сигнала в среднесрочной перспективе. Она, по сути, "чувствует" тренды и заранее предупреждает о возможных сбоях.

- GAT-LLM – модель, чувствительная к контексту и структуре сети – сосредотачивается на резких краткосрочных изменениях, интерпретируя текстовую телеметрию и сетевую топологию.

3. Коррекция интегральной оценки: полученные от моделей вероятности ухудшений конвертируются в весовые коэффициенты, которые учитываются при пересчете итоговой метрики устойчивости канала.

Таким образом, получается связка: Bi-LSTM охватывает динамику в целом, а GAT-LLM работает точно. Вместе они создают устойчивую, адаптивную систему, способную реагировать не по факту, а на опережение – и это ключевое преимущество.

## Заключение

Результаты сравнительного анализа показали: на задачах прогнозирования деградации в FPV-связи уверенно себя проявляют два типа моделей – рекуррентные (LSTM, GRU) и графовые (GAT-LLM). Первые хорошо справляются с отслеживанием динамики во времени, вторые – учитывают архитектуру сети и связи между ее элементами. Это делает их особенно полезными в ситуациях, где важно уловить как общие тенденции, так и локальные сбои.

Но, как обычно, все упирается в ресурсы. Если данных мало, а мощности ограничены, не стоит гнаться за сложными архитектурами – XGBoost или аналогичные модели справятся с базовым уровнем прогноза.

Добавление таких ML-инструментов в общую методику оценки делает систему не просто автоматизированной, а по-настоящему осведомленной. Она начинает предугадывать поведение канала и реагировать до того, как проблема перерастет в отказ – а это уже заметный плюс для FPV-управления, где задержки и сбои могут стоить дорого.

## Список используемых источников

1. Wang J., Zhang J., Zheng K. Multivariate wireless link quality prediction based on pre-trained large language models // arXiv preprint. 2024. URL: <https://arxiv.org/abs/2501.11247> (дата обращения: 15.04.2025).

2. Chaudhari S., Moh S. Recurrent Neural Network Based Link Quality Prediction for Fluctuating Low Power Wireless Links // Sensors. 2022. Vol. 22, No. 3. P. 1212. DOI: 10.3390/s22031212.

3. Patil D., Kulkarni N., Patil K. A Survey of Machine Learning Techniques for Video Quality Prediction from Quality of Delivery Metrics // Electronics. 2021. Vol. 10, No. 22. P. 2851. DOI: 10.3390/electronics10222851.

4. Березкин А. А., Вивчарь Р. М., Киричек Р. В. Многокритериальная оценка эффективности управления беспилотными системами в гибридных сетях связи // Труды учебных заведений связи. 2024. Т. 10. № 1. С. 18–25. DOI: 10.31854/1813-324X-2024-10-1-18-25.

5. Лапко А. Ю., Дудкин М. И., Гунько В. Н. Оценка помехоустойчивости радиоканалов на основе вероятностного подхода // Автометрия. 2020. № 6. С. 3–15.

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Вивчарем Р. М.*

**УДК 004.8****К. В. Кинкульская** (студент группы ИСТ-422, СПбГУТ)**Е. В. Коровкина** (ассистент каф. СОД, СПбГУТ), [korovkina.ev@sut.ru](mailto:korovkina.ev@sut.ru)

## **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕДИЦИНСКОЙ ДИАГНОСТИКЕ**

*В работе рассматриваются основные этапы эволюции нейронных сетей в медицине, перспективы, а также недостатки. Описывается история внедрения и первые успешные работы. Нейронные сети затронули все сферы человеческой жизни и медицина не исключение. Их развитие тесно связано с прогрессом вычислительных машин, а также обучения и аналитики баз данных. С помощью них люди могут отслеживать свое здоровье, не выходя из дома.*

*искусственный интеллект, диагностика, медицина, нейросети, обучение, возможности, исследования*

Искусственный интеллект изменялся и развивался на протяжении последних нескольких десятилетий. Изначально он мог выполнять лишь простые задачи и со временем начал включать более сложные алгоритмы, работающие подобно нейронам человеческого мозга. Одним из первых проектов был MYCIN, разработанный в Стэнфордском университете в 1970е годы. Он представлял собой систему, которая диагностировала бактериальные инфекции и давала рекомендации по антибиотикам. Несмотря на свой небольшой масштаб проекта, он действовал строго по правилам и использовал логические выводы для анализа симптомов и медицинских данных [1].

Ежедневно врачи получают множество рентгеновских снимков, результатов ЭКГ, и много других изображений и данных, которые надо анализировать, чтобы поставить диагноз и правильное лечение. Из-за количества материала, который нужно обработать, многие пациенты узнают свой диагноз с задержкой. Поэтому ученые усовершенствовали создали нейронные сети, которые называются компьютерное зрение.

Компьютерное зрение – область искусственного интеллекта, связанная с обработкой и анализом изображений или видео. Компьютер воспринимает эти данные, подобно человеку, и на основе анализа дает алгоритм действия медицинскому работнику [2].

Ученые во всем мире отмечают, что компьютерное зрение-бедующее медицины. В настоящее время Россия внедрила около 17 % ИИ в медицинские организации, а врачи используют его для диагностики онкологии, скринингов и сердечно-сосудистых заболеваний (рис. 1).

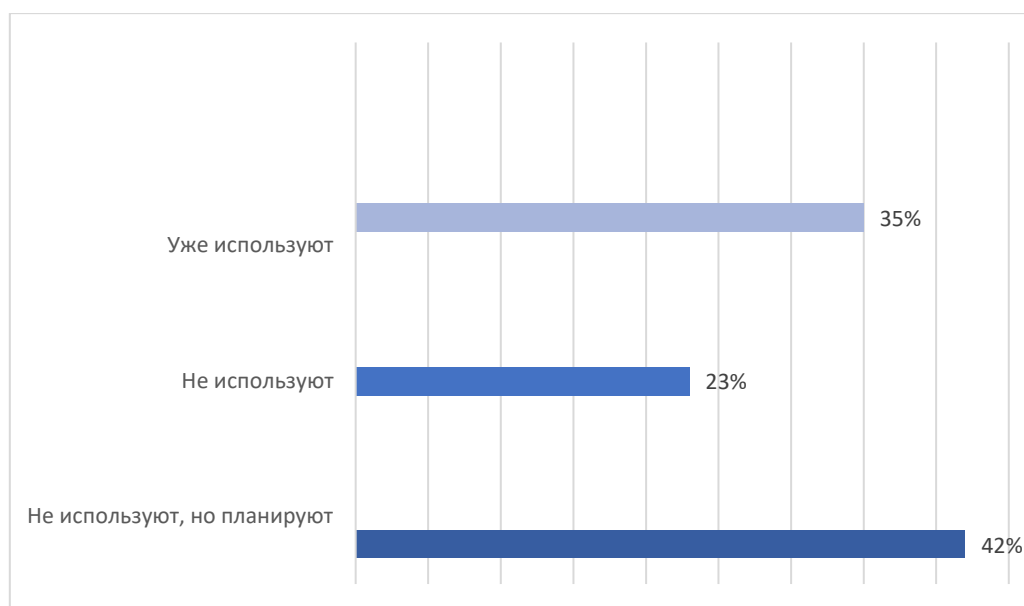


Рис 1. Статистика использования врачами ИИ

Самая распространенная задача – выявление аномалий рентгеновских снимков, таких как УЗИ, МРТ, КТ. В процессе врачи и нейросеть стараются минимизировать риски первого рода, поэтому они выделяют все аномалии и анализируют их для дальнейшего вывода. Искусственный интеллект точно изучает рентгеновские снимки (рис. 2), что позволяет исключать ошибки из-за человеческого фактора [3].

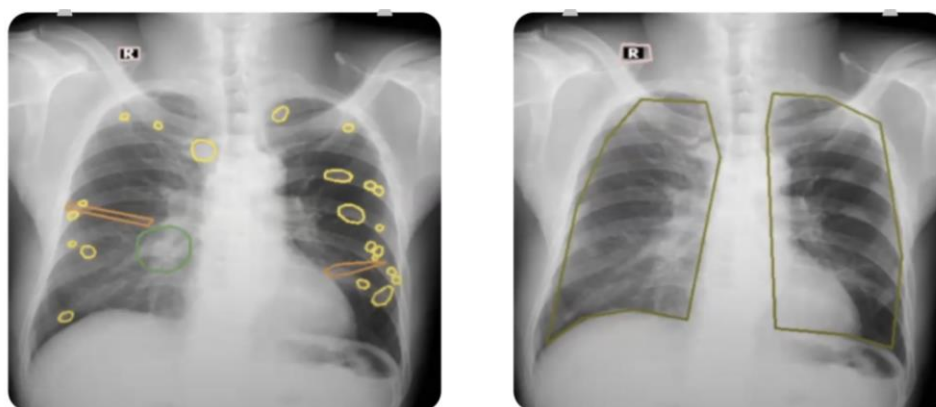


Рис. 2. Выявление аномалий у пациента

Основной задачей компьютерного зрения является контроль дефектов и счет упаковок. ИИ собирает статистику о количестве таблеток в одной упаковке и сравнивает их (рис. 3). Так же использует систему визуального осмотра таблеток и отбраковывает товар, который не соответствует стандарту [4].

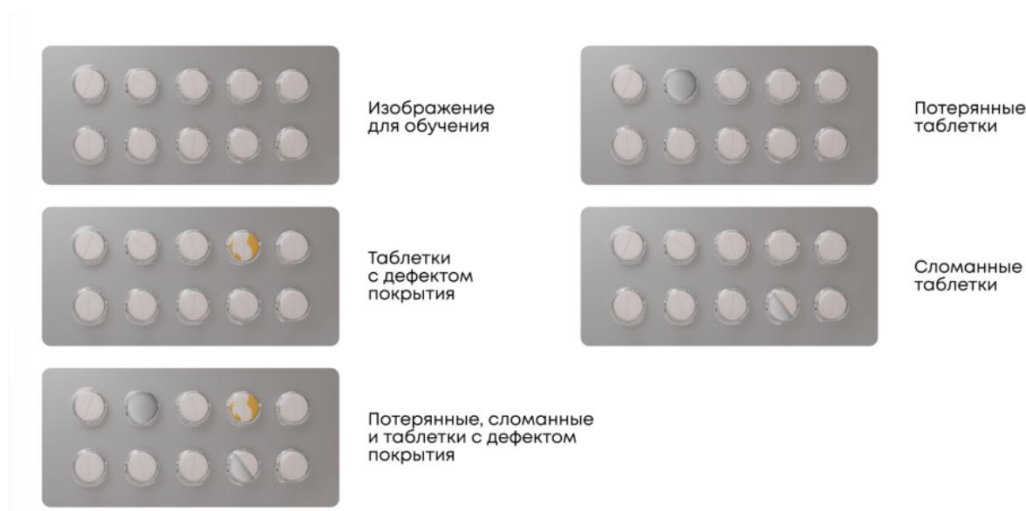


Рис. 3. Выявление брака в фармацевтическом производстве

В данной статье были проанализированы методы работы нейронных сетей в области медицины. На сегодняшний день они стали неотъемлемой частью диагностики, лечению и контролю [5]. В будущем для создания уникального «доктора» потребуются слияние экспертизы врачей и развитие искусственного интеллекта. Нейронная сеть обладает значительным потенциальным ростом, но для его внедрения требуется решения ряд технических проблем, а также обязательная человеческая проверка, так как нейронные сети могут интерпретировать некоторые результаты, как ложно негативные, что может повлечь серьезные последствия для здоровья пациентов.

#### Список используемых источников

1. Компьютерного зрения в медицине: как бизнесу применять технологию. Кейсы. URL: <https://www.simbirsoft.com/blog/kompyuternoe-zrenie-v-meditisine-kak-biznesu-primenyat-tekhnologiyu-keysy/> (дата обращения 29.03.2025).
2. Хлудов И. В. Компьютерное зрение и его применение в медицине, автономных автомобилях и других областях [сайт] // «Актуальные исследования»: электрон. научн. журн., июль 23. URL: <https://apni.ru/article/6805-kompyuternoe-zrenie-i-ego-primenenie-v-meditis> (дата обращения 29.03.2025).
3. 19 лучших применений компьютерного зрения в здравоохранении. URL: <https://viso.ai/applications/computer-vision-in-healthcare/> (дата обращения 30.03.2025).
4. Тополь Э. Искусственный интеллект в медицине: как умные технологии меняют подход к лечению. М.: Альпина Паблишер, 2022. 398 с.
5. Акулин И. М., Бурцева П. И., Махова О. А., Сарана А.М., Чеснокова Е. А. «Искусственный интеллект в здравоохранении М.: СПбГУ. 2023. 200 с. URL: <https://apni.ru/article/6805-kompyuternoe-zrenie-i-ego-primenenie-v-meditis> (дата обращения 28.03.2025).

*Статья представлена научным руководителем, заведующим кафедрой СОД СПбГУТ, кандидатом технических наук Бородянским Ю. М.*

УДК 004.032.26

**В. С. Ковалев** (студент группы ИСТ-422, СПбГУТ)

**Е. В. Коровкина** (ассистент каф. СОД, СПбГУТ), [korovkina.ev@sut.ru](mailto:korovkina.ev@sut.ru)

## АНАЛИЗ ТЕХНОЛОГИИ MCP И ЕЕ ПРЕИМУЩЕСТВ

*В современном мире технологии нейронных сетей развиваются стремительными темпами. Нейросети архитектуры LLM (большая языковая модель) - сложные огромные структуры, подвергнувшиеся машинному обучению, которым необходима технология, позволяющая модели взаимодействовать с внешними модулями. Для таких целей существует API - совокупность способов и данных, по которым разные программы обмениваются данными. API хорошо применяется в большинстве проектов, но для агентов ИИ такой способ не является удобным. В данной статье рассмотрена технология MCP, которая повышает эффективность процессов.*

*нейросети, машинное обучение, модели, MCP*

Большие проекты, в частности нейросетевые модели архитектуры LLM, безусловно вынуждены использовать какие-либо сторонние модули для расширения возможностей, либо для банального поддержания работы своего проекта. Чем больше проект, тем больше таких внешних модулей может быть подключено к нему. Из такого метода следуют следующие недостатки, представленные ниже.

1. В за частую к каждому новому модулю необходимо применять особый подход, не все внешние модули следуют какому-то определенному стандарту. Даже самые сложные нейросетевые модели заперты в условных информационных пузырях, в вакууме, и унаследованных системах. Каждый новый внешний модуль требует собственной реализации – это затрудняет масштабирование взаимосвязанных систем.

2. Своевременное наблюдение за каждым модулем API, обновления, изменения в коде, структуре либо банальное появление на рынке нового решения, который нужно объединить с проектом. Разработчики не могут постоянно следить за всем этим процессом и когда приходит время обновлять все модули – структура проекта и код могут потребовать внушительных изменений, иначе проект просто может не запуститься.

MCP – это инновационный продукт от компании Anthropic. Цель технологии, как сообщает сама компания – это «помочь передовым моделям создавать более качественные и релевантные ответы». Компания создает универсальную инфраструктуру, позволяющую различным ИИ работать



вместе, своего рода интернет для ИИ, попытка создать связь ИИ с внешним миром. MCP обеспечивает универсальный и открытый стандарт для соединения систем искусственного интеллекта с внешними модулями. Это как API для LLM, но универсальный, он сам понимает, что нужно модели, откуда это брать и как это подключить, причем сам адаптируется если что-то нужно изменить и все это происходит без особых сложностей.

Протокол Model Context Protocol – это открытый стандарт, позволяющий разработчикам создавать безопасные двусторонние соединения между источниками данных и инструментами, работающих на базе ИИ. Архитектура проста: разработчики могут либо предоставлять свои данные через MCP, либо создавать приложения ИИ (клиенты MCP), которые подключаются к этим серверам [1].

Существует три основных компонента протокола Model Context Protocol (рис. 1):

1. MCP Host – приложение, где живет LLM, например, Claude Desktop. Хост хочет получить доступ к внешним возможностям и данным.

2. MCP Client – компонент внутри хоста. Для каждого внешнего сервиса создается клиент, который устанавливает соединение с соответствующим сервером и общается с ним по протоколу MCP

3. MCP Server – внешняя программа или сервис, предоставляющий хосту определенные данные по протоколу MCP. Сервер сам определяет какими ресурсами, инструментами и подсказками он может делиться с моделью [2].

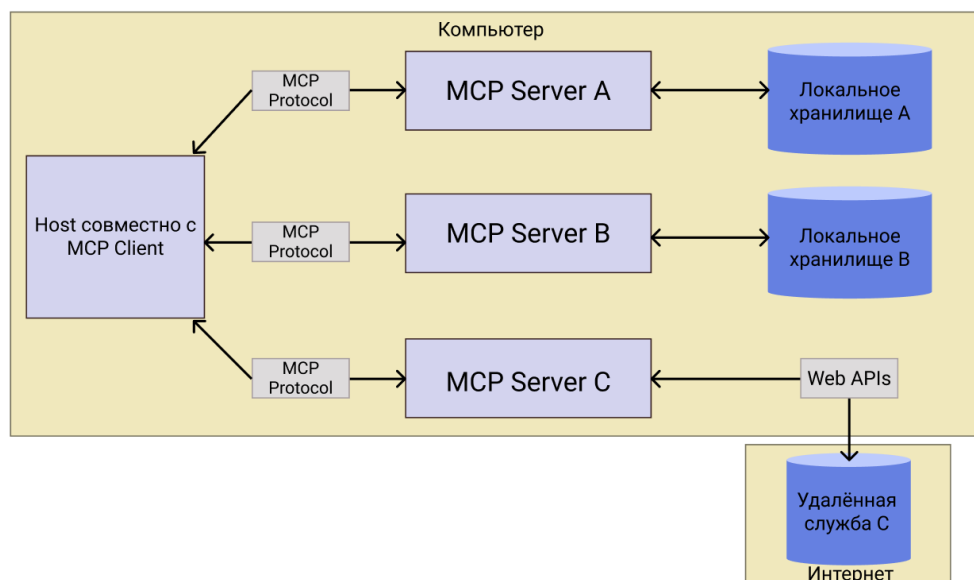


Рис. 1. Модель работы MCP

Model Context Protocol – решение, появление которого в современном мире нельзя было избежать.

Анализ взаимодействия МСР с другими технологиями представлен в табл. 1.

ТАБЛИЦА 1. Анализ взаимодействия МСР с другими технологиями

|     | Назначение                                 | Ограничения                               | Взаимодействие с МСР                       |
|-----|--------------------------------------------|-------------------------------------------|--------------------------------------------|
| МСР | Универсальное подключение внешних модулей  | -                                         | -                                          |
| RAG | Улучшение ответов LLM через внешние данные | Жесткая привязка к БД, сложная интеграция | МСР дает динамические данные [3]           |
| АСР | Прямое взаимодействие агентов              | Узкая специализация                       | МСР использует агентов как инструменты [3] |
| A2A | Связь между агентами на разных платформах  | Нет доступа к внешним инструментам        | МСР + A2A = данные + координация [4]       |

Были проанализированы актуальные на момент начала 2025 года технологии, позволяющие агентам ИИ взаимодействовать с внешними источниками, будь то другие агенты ИИ или иные внешние инструменты. Кроме всего вышеперечисленного, МСР в сравнении с проанализированными протоколами – наиболее универсальный вариант, который можно внедрить в большинство проектов. МСР позволил сократить затраты времени на индивидуальные интеграции примерно на 55% [5].

Еще одна проблема – это то, что нейросети не могут сами по себе в реальном времени брать свежую информацию с внешних источников, они берут информацию, которая заранее была загружена в них, и зачастую эту информацию проблематично регулярно обновлять, это требует значительных трат ресурсов и занимает большое количество времени. МСР также решает данную проблему, протоколу не нужно останавливать работу нейросети дабы внести в нее новую информацию, она может брать ее сторонне, отправляя запрос на внешний сервис, который уже производит поиск запрашиваемой информации и отправляет информацию обратно в нейросеть, которая уже формулирует ответ на заданный вопрос с помощью этой информации.

МСП был выпущен в свет в конце 2024 года и изначально не был замечен разработчиками, но уже на начало 2025 года рост популярности технологии очевиден: к февралю было развернуто более 1000 МСП-серверов, к апрелю – более 2000 МСП-серверов. На данный момент, такие большие компании, как Google, OpenAI, Microsoft, Block, Apollo, Zed, Replit, Codeium, Sourcegraph и другие уже внедрили полностью либо частично МСП в свои проекты. Компания Anthropic облегчает внедрение своей технологии в проекты и уже опубликовала готовые МСП-серверы для таких популярных корпоративных систем, как Google Drive, Slack, GitHub, Git, Postgres и Puppeteer.

Была проанализирована новая технология на момент 2025 года, позволяющая нейросетям более удобно, быстро и универсально связываться с внешними модулями и получать от них информацию в реальном времени. Такая технология позволяет расширять возможности нейросетей, создавая новые модуля, объединяя разных агентов ИИ для работы друг с другом.

#### Список используемых источников

1. Introducing the Model Context Protocol. URL: <https://www.anthropic.com/news/model-context-protocol> (дата обращения 29.03.2025).
2. Фролов С. Model Context Protocol (MCP) – универсальный протокол для взаимодействия с ИИ, и почему это замечательно // Habr. URL: <https://habr.com/ru/articles/899088/> (дата обращения 29.03.2025).
3. Guptax D. MCP, RAG, and ACP: A Comparative Analysis in Artificial Intelligence. URL: <https://guptadeepak.com/mcp-rag-and-acp-a-comparative-analysis-in-artificial-intelligence/> (дата обращения 29.03.2025).
4. Guamian A2A vs MCP: Two complementary protocols for the emerging agent ecosystem. URL: <https://blog.logto.io/a2a-mcp> (дата обращения 29.03.2025).
5. Thompson R. Why 68% of Developers Are Switching to MCP for AI Integration in 2025. URL: <https://medium.com/ai-simplified-in-plain-english/why-68-of-developers-are-switching-to-mcp-for-ai-integration-in-2025-fdffb66e4d7d> (дата обращения 29.03.2025).

*Статья представлена научным руководителем, заведующим кафедрой СОД СПбГУТ, кандидатом технических наук, доцентом Бородянским Ю. М.*

УДК 004.942

## РАЗРАБОТКА МНОГОПОТОЧНЫХ ПРИЛОЖЕНИЙ ДЛЯ ПОСТРОЕНИЯ И ПРОХОЖДЕНИЯ НЕИДЕАЛЬНЫХ ЛАБИРИНТОВ

**А. Р. Коломиец, М. Е. Морозов** (студенты группы ИКПИ-33, СПбГУТ),  
[morozov.me@sut.ru](mailto:morozov.me@sut.ru)

*Лабиринты используются в игровых движках, задачах визуализации графовых алгоритмов и тестах генераторов случайных чисел. Идеальный лабиринт представляет остовное дерево, где между любыми двумя клетками существует ровно один путь; неидеальный содержит контролируемое число петель. При размере карты  $20 \times 20$  и более однопоточный DFS-backtracking становится «узким горлом», а добавление петель после завершения обхода удваивает время генерации. В работе предложен параллельный алгоритм pet-loop-DFS, формирующий петли on-the-fly во время обхода и распределяющий расчет между  $N$  потоками. Поиск кратчайшего пути выполняется BFS и автоматически перестраивается к ближайшему выходу.*

*идеальный лабиринт, неидеальный лабиринт, DFS-backtracking, BFS, многопоточность, mutex-секции, Pet-loop-DFS*

Лабиринт – едва ли не самая древняя задача на графы: ее решали еще на бумаге, рисуя коридоры, позже – в 8-битных играх, а сегодня она стала живой демонстрацией алгоритмов поиска и параллельных структур данных. В игровых движках процедурная генерация уровней позволяет экономить место на диске и делать каждый запуск непохожим на предыдущий; в образовательных курсах лабиринт показывает, как работают DFS и BFS, что такое остов и цикл, зачем нужны очереди и стек. Однако увеличение размера карты и переход к «правдоподобным» неидеальным лабиринтам выявляют слабость однопоточного подхода: время отклика интерфейса уходит на секунды, что недопустимо ни для игрока, ни для студента, запускающего лабораторную работу. Паритет вычислительной мощности давно сместился в сторону многоядерных процессоров, и освоение потоков перестало быть факкультативной роскошью [1-4].

### Как устроен идеальный лабиринт

В самой простой постановке лабиринт – это неориентированный граф, вершинами которого являются клетки прямоугольной решетки, а ребрами – отсутствующие стены между соседними клетками. Идеальный лабиринт –

остовное дерево такого графа: от любой клетки можно пройти в любую другую ровно одним способом. Самый известный способ получить остов – рекурсивный DFS, породивший термин DFS-backtracking. Его псевдокод предельно лаконичен:

```
visit(v):
    mark v
    while there is an unmarked neighbour w of v:
        remove wall between v and w
        visit(w)
```

В реальности рекурсия заменяется стеком, чтобы избежать переполнения, а выбор следующего соседа рандомизируется. При  $w \cdot h = 400$  клеток такой алгоритм выполняется менее чем за 50 мс даже на старом ноутбуке, и если единственная цель – «нарисовать» дерево, то можно и не заморачиваться.

ТАБЛИЦА 1. Примеры алгоритмов для генерации различных алгоритмов.

| Подход                      | Краткая идея                                                          | Свойства лабиринта                                                 | Сложность              |
|-----------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------|------------------------|
| Recursive Division          | Разделить область стеной, оставить 1–2 проема, рекурсия               | Прямые коридоры, «комнатная» структура, неидеальный при 2+ проемах | $O(W \cdot H)$         |
| Kruskal                     | Сортируем ребра случайно, удаляем если соединяет разные компоненты    | Крупные камеры, идеальный                                          | $O(E \cdot \alpha(V))$ |
| Aldous–Broder               | Случайный блуждающий маркер удаляет стену только для новых клеток     | Идеальный, «шумовой» рисунок, очень медленный                      | $O(\tau \cdot WH)$     |
| Hunt-and-Kill               | Бродим как DFS, при тупике «охота» за новой клеткой                   | Чередует длинные линии и хаотичные участки                         | $O(W \cdot H)$         |
| Eller                       | Строка за строкой, объединяем множества, вертикальные соединения вниз | Генерация «на лету», подходит для бесконечной ленты                | $O(W \cdot H)$         |
| Recursive Backtracker (DFS) | Стек клеток + случайный сосед                                         | Извилистые коридоры, идеальный, просто модифицировать              | $O(W \cdot H)$         |

Мы выбрали этот алгоритм, потому что в отличие от других подходов, например, Краскала, не нуждается в глобальных структурах данных – достаточно стека клеток. Такое простое представление легко адаптировать к многопоточному окружению: мы просто запускаем несколько независимых обходов из разных углов поля и защищаем граничные участки через крупнозернистые mutex-секции. Никаких сложных очередей приоритетов и глобального списка ребер не требуется, поэтому накладные расходы синхронизации минимальны. Добавление петель реализовано на уровне одного условного перехода (прием `ret-loop-DFS`), что делает генератор быстрым и предсказуемым по времени. Визуально получаются плавные, естественные коридоры, а возможность вставлять циклы по ходу обхода превращает идеальный лабиринт в неидеальный без второго прохода.

### **Почему идеала мало и что такое `ret-loop-DFS`**

Куда интереснее неидеальный лабиринт. Он визуально «живее», потому что петли позволяют обходить тупики и искать альтернативы. Традиционный способ сделать неидеальность – достроить к готовому остову  $n$  случайных ребер: выбрать пару соседних клеток и убрать стенку. Но этот подход двойной: сперва нужно пройти все клетки, а потом еще  $k$  раз выбрать случайное ребро и проверить, не сломает ли оно связность. На практике это почти удваивает время работы.

Здесь и вступает наша модификация `ret-loop-DFS`. Идея проста: пока обход идет, поток уже видит обе категории соседей – непосещенные и уже отмеченные. Когда непосещенные закончились, он может с некоторой вероятностью  $\approx 0,35$  «намечать» цикл, разрушая стену к одному из уже обработанных соседей. Так формируются петли *on-the-fly*; счетчик `extra_loops` уменьшается, и как только он обнуляется, алгоритм начинает вести себя как обычный DFS. Благодаря этому дополнительная стоимость сводится к нескольким условным переходам, а не ко второму проходу по всему полю.

### **Как распараллелить то, что плохо делится**

DFS плохо делится по сущности: поток, начавший обход, рано или поздно пройдет почти все клетки. Разделить работу помогает лишь отправка нескольких потоков из разных стартовых позиций. Но без защиты стен два потока могут попытаться удалить одну и ту же стенку, и мы получим рассинхронизацию. Простейший «глобальный» mutex лишает идею смысла –

процессы снова становятся последовательными. Поэтому мы перешли к схеме mutex-секций.

Поле  $W \times H$  делится на блоки  $s \times s$  (в экспериментах  $s = 2$ ). Каждому блоку ставится в соответствие объект `std::mutex`. Поток, стоящий в клетке  $(x, y)$ , знает индекс своего блока

$$id = \left\lfloor \frac{x}{s} \right\rfloor + \left\lfloor \frac{y}{s} \right\rfloor \left\lceil \frac{W}{s} \right\rceil$$

и при переходе на соседнюю клетку захватывает mutex-текущего и mutex-соседнего блоков. Все потоки делают это в едином порядке «север-запад → юг-восток», поэтому циклическое ожидание невозможно. В результате число блокировок пропорционально числу удаленных стен, а не числу клеток, и накладные расходы остаются приемлемыми.

### Архитектура приложения

Код написан на C++ 17. Библиотека Qt 5 отвечает за окна и ввод–вывод, SFML – за быстрый рендер прямоугольных линий, которые идеально ложатся на решетку. Класс `MazeSync` наследуется от `Maze` и добавляет вектор мьютексов, а также методы `lock_mutex` / `unlock_mutex`, так что пользовательский код не знает о деталях синхронизации.

GUI позволяет переключаться между режимами:

- «Классический  $20 \times 20$ » – идеальный лабиринт одним потоком;
- «Неидеальный  $20 \times 20$ » – `ret-loop-DFS`, выбор числа петель  $n$  и потоков  $k$ ;
- «Произвольный размер» – демонстрация на картах  $1 \dots 50$  клеток.

### Экспериментальная картина

Для поля  $20 \times 20$  и пяти петель проведено 50 запусков на каждое число потоков от 2 до 8. Усредненное время падает почти линейно:  $6,3 \text{ с} \rightarrow 5,9 \text{ с} \rightarrow 4,8 \text{ с} \rightarrow 4,5 \text{ с} \rightarrow 4,1 \text{ с} \rightarrow 3,8 \text{ с}$  (рис. 1). Коэффициент ускорения от однопоточного эталона достигает  $\times 10$ , но эффективность на ядро снижается: если при двух потоках мы выигрываем 47 %, то при восьми – лишь 21 %, это цена contention и потерь кэша.

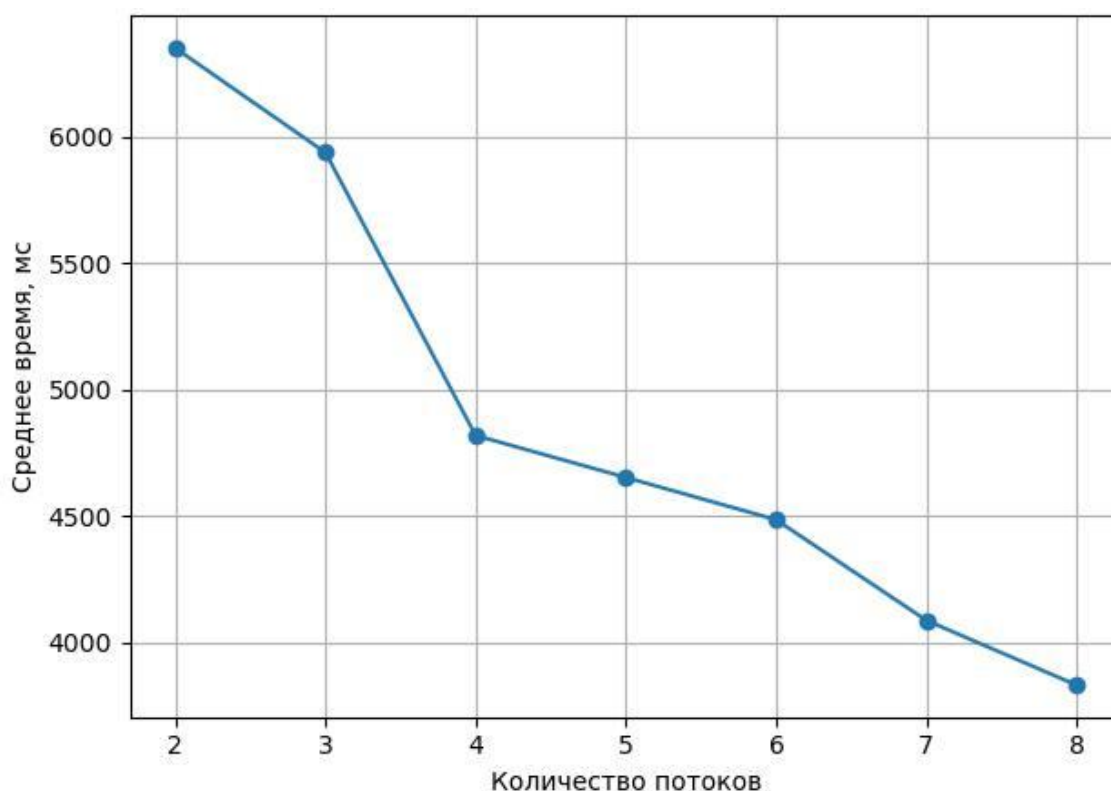


Рис. 1. Зависимость скорости генерации неидеального лабиринта от количества задействованных потоков

Отдельный эксперимент с размером секции показал, что  $s=1$  (mutex на каждую клетку) утроил число блокировок и сбил результат, а  $s=3$  уменьшил число мьютексов, но сильно вырос риск ситуаций, когда два потока ждут одну крупную секцию. Таким образом  $s=2$  остается оптимальным на данной размерности поля.

### **BFS как неотъемлемый элемент геймплея**

Задача поиска пути обычно ассоциируется с алгоритмом  $A^*$ . Но в основном или почти основном графе  $A^*$  чрезмерен: достаточно BFS, сложность которого линейна, а реализация укладывается в два десятка строк. Очередь содержит координаты клеток; при каждом извлечении мы смотрим четыре направления и проверяем, не стоит ли там стена. Первая достигнутая выходная клетка гарантирует минимальную длину.

Приятным бонусом является возможность запускать BFS поверх уже существующей раскраски потоков – каждая клетка помнит `in_use`-идентификатор потока, создавшего ее. Если понадобится, можно посчитать, чей поток «победил» в гонке к выходу или к середине карты.



## Выводы

Комбинация `ret-loop-DFS` с `mutex`-секторами доказала, что «тяжелый» с точки зрения ветвлений `backtracking` все же поддается масштабированию. На практике мы получили почти линейный прирост до 8 ядер и удвоенное сокращение времени генерации на типичной игровой карте.

Если же говорить о гейм-дизайне, то возможность быстро строить несколько вариантов лабиринта и моментально вычислять кратчайший путь открывает дорогу динамически меняющимся уровням, адаптирующимся к действиям игрока.

## Список используемых источников

1. Уилсон Дж. М. Генерация лабиринтов: монография. М.: ДМК Пресс, 2019. 312 с.
2. Кнут Д. Э. Искусство программирования. Т. 1: Основные алгоритмы. 3-е изд. М.: Вильямс, 2011. 832 с.
3. Хаммер М. Параллельное программирование на C++ 17. СПб.: Питер, 2020. 384 с.
4. Кузнецов С. Ю. Алгоритмы поиска в графах: учеб. пособие. М.: МГТУ им. Н. Э. Баумана, 2022. 148 с.

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Дагаевым А. В.*

УДК 004.42

**П. В. Котелин** (студент группы ИБС-31, СПбГУТ)

**И. Е. Скалецкая** (к.т.н., доцент, СПбГУТ), [fizika.ffp@sut.ru](mailto:fizika.ffp@sut.ru)

## **ПРОГРАММНОЕ РЕШЕНИЕ ДЛЯ РАСЧЕТА ФАКТОРОВ СХОДИМОСТИ И ВОСПРОИЗВОДИМОСТИ, ВЛИЯЮЩИХ НА ПРОЦЕСС ИЗМЕРЕНИЙ**

*Данное исследование посвящено разработке программного обеспечения, ориентированного на автоматизацию оценки пригодности измерительных систем с использованием методики оценки сходимости и воспроизводимости процессов измерений.*

*измерительные системы, GR&R, автоматизация, точность, надежность, анализ данных, качество продукции*

Актуальность данного исследования определяется необходимостью повышения точности и надежности измерительных систем в условиях современных требований к качеству производимой продукции. Задачей исследования является разработка программного обеспечения, которое позволит автоматизировать процесс оценки пригодности измерительных систем с использованием методик сходимости и воспроизводимости процессов измерений, а также анализировать влияние оборудования и операторов на общее отклонение в измерениях.

В условиях проведения процесса измерений на предмет определения приемлемости и пригодности используемой измерительной системы по факту всегда влияют два фактора: само оборудование, с помощью которого проводится измерение характеристик, и операторы, осуществляющие измерения.

Для оценки пригодности оборудования используется сходимость и воспроизводимость процессов измерений (в иностранной литературе – GR&R [1] – *Gage Repeatability and Reproducibility*) фактор, который позволяет количественно оценить отклонение или точность (т.н. критерий приемлемости), связанную с системой измерения (относительно полного диапазона возможных значений характеристик объекта (методика  $6\sigma$ ) или относи-

тельно полного отклонения измеряемой величины с учетом процесса изготовления объекта). Определив превалирующий фактор (в процентах оценив влияние каждого фактора на суммарное отклонение в системе) можно улучшить этот показатель, проанализировав слабые места в измерительной системе и нивелируя их.

Сигма ( $\sigma$ ) – термин, используемый в статистике для обозначения среднеквадратического (стандартного) отклонения, характеризующего величину отклонений (разброс) ряда измерений или результатов процесса [2].

*Методология оценки 6σ.* Ориентиром, используемым для ранжирования качества или функционирования процесса, является количество сигм. Количество сигм, равное шести, стало синонимом качества мирового уровня, который означает такой уровень функционирования процесса, при котором на каждый миллион единиц продукции приходится 3-4 дефекта (несоответствия). Таким образом, непрерывный процесс с количеством сигм, равным шести, имеет границу допустимых значений, отстоящую на 4-5 стандартных отклонений от математического ожидания [2].

Общее отклонение в рассматриваемой системе ( $\sigma_{\text{полн}}$ ) (1) складывается из отклонения, связанного с процессом производством объекта ( $\sigma_p$ ), и отклонения, связанного с измерительной системой ( $\sigma_{GR\&R}$ ). В свою очередь  $\sigma_{GR\&R}$  (2) зависит от вариаций, связанных с измерительным оборудованием (т.н. фактор сходимости –  $\sigma_{\text{сх}}$ ), а также от вариаций, связанных с выполнением измерений разными операторами (т.е. с разными оценками разными людьми измеряемого результата, т.н. фактор воспроизводимости –  $\sigma_{\text{воспр}}$ ).

$$\sigma_{\text{полн}} = \sqrt{\sigma_p^2 + \sigma_{GR\&R}^2} \quad (1)$$

$$\sigma_{GR\&R} = \sqrt{\sigma_{\text{сх}}^2 + \sigma_{\text{воспр}}^2} \quad (2)$$

В «методе контроля продукта» рассчитывается коэффициент допуска точности ( $\alpha$ ) (3), если измерительная система используется для оценки соответствия полученных характеристик образцов требованиям к продукции.

Здесь сравниваются отклонения измерительной системы ( $\sigma_{GR\&R}$ ) с пределами возможных значений по спецификации и требованиям производства продукции ( $\Delta_{\text{произв}}$ ):

$$\alpha = \frac{6 \cdot \sigma_{GR\&R}}{\Delta_{\text{произв}}} \quad (3)$$

Этот метод представляется возможным использовать, если известны верхний и нижний пределы допускаемых в производстве значений измеряемых характеристик образца.

( $6 \cdot \sigma_{GR\&R}$ ) – это интервал, охватывающий 99,73 % полной ширины разброса измерительной системы – опорный интервал.

Отношение опорного интервала к полному диапазону допуска характеризует часть «окна допуска» при изготовлении образцов, которая используется исключительно системой измерения.

При использовании «метода контроля процесса» рассчитывается коэффициент  $\gamma$  (4), показывающий какая доля общего отклонения приходится на систему измерения (без учета отклонения от процесса производства):

$$\gamma = \frac{\sigma_{GR\&R}}{\sigma_{\text{полн}}} \quad (4)$$

Интерпретация полученных долей или процентов связана с критериями приемлемости используемой измерительной системы:

- $\alpha$  или  $\gamma < 10\%$  – измерительная система считается приемлемой для использования;
- $10\% < \alpha$  или  $\gamma < 30\%$  – измерительная система считается приемлемой, но существует риски ее применения, связанные либо с идентификацией образцов как «ложный брак» – отбраковка годных образцов («риск производителя»), либо с «ложным качеством» («потребительский риск»);
- $\alpha$  или  $\gamma > 30\%$  – измерительная система считается неприемлемой для использования.

Для автоматизации расчетов была разработана программа, позволяющая посчитать отклонения, коэффициенты методов оценки, а также вклад каждого фактора в общее отклонение. Для удобства работы программа реализована в виде сайта.

На рисунках 1, 2 представлен пример работы программы.

## Методика расчета факторов сходимости и воспроизводимости, влияющих на процесс измерений (ПИ).

Расчет сходимости и воспроизводимости (GR&R) – инструмент, позволяющий количественно оценить отклонение или точность (т.н. критерий приемлемости), связанную с системой измерения относительно полного диапазона возможных значений характеристик объекта (методика 6 $\sigma$ ) или относительно полного отклонения измеряемой величины с учетом процесса изготовления объекта для подтверждения возможности использования этой системы.

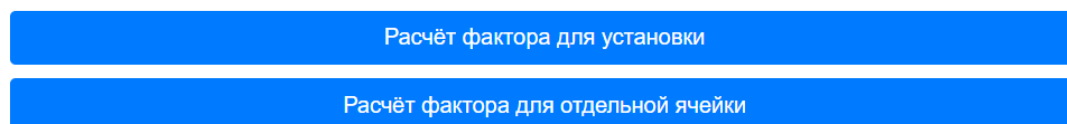


Рис. 1. Главный экран

## Оценка приемлемости и вклада

Критерии:

- $\alpha$  или  $\gamma < 10\%$  - измерительная система считается приемлемой для использования;
- $10\% < \alpha$  или  $\gamma < 30\%$  - измерительная система считается приемлемой, но существует риски ее применения, связанные либо с идентификацией образцов как «ложный брак» -отбраковка годных образцов («риск производителя»), либо с «ложным качеством» («потребительский риск»);
- $\alpha$  или  $\gamma > 30\%$  - измерительная система считается неприемлемой для использования.

|                                 |        |
|---------------------------------|--------|
| Gamma, %                        | 96.88  |
| Вклад фактора сходимости        | 0.9479 |
| Вклад фактора воспроизв.        | 0.2083 |
| Вклад фактора откл. при произв. | 0.2708 |

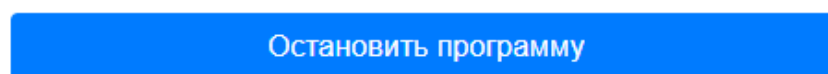


Рис. 2. Результат работы программы

**Список используемых источников**

1. Монгомери Д. Б. Measurement systems analysis. 4-е изд. Хобокен: Wiley, 2008. 450 с. ISBN 978-0-470-17121-5.
2. ГОСТ Р ИСО 13053-1-2015 Статистические методы «Количественные методы улучшения процессов "шесть сигм"». / Статистические методы. Количественные методы улучшения процессов "шесть сигм". URL: <https://docs.cntd.ru/document/1200127239?ysclid=m5b7lq476m172562243> (последнее обращение 29.12.2024г.).

*Статья представлена научным руководителем,  
кандидатом технических наук, доцентом Скалецкой И. Е.*

УДК 004.9

Е. А. Лопаткина (студент группы ИСТ-232, СПбГУТ), [lopatkina.ea@sut.ru](mailto:lopatkina.ea@sut.ru)

## ТЕХНИЧЕСКИЕ АСПЕКТЫ ПРОЯВЛЕНИЯ ЛЮДО-НАРРАТИВНОГО ДИССОНАНСА В ИГРОВЫХ СИСТЕМАХ

*Рассмотрена проблема возникновения конфликта между нарративной и игровой составляющими как результат рассогласования программных механик и сценарных событий. Описаны возможные проявления людод-нарративного диссонанса в играх. Установлены ключевые технические причины людод-нарративного диссонанса, заключающиеся в жесткой привязке сюжета к линейным скриптам и недостаточной параметризации игровых систем. Сформированы методы минимизации людод-нарративного диссонанса на этапах планирования и тестирования игровых систем для выявления и устранения рассогласований между механиками и сюжетом. Приведены примеры намеренного применения людод-нарративного диссонанса в игровых продуктах. Представлены результаты опроса о влиянии людод-нарративного диссонанса на игровой опыт и рассмотрена целесообразность его полного устранения.*

*людод-нарративный диссонанс, геймдизайн, игра, сюжетные скрипты, игровые механики, линейные скрипты*

Людод-нарративный диссонанс – один из ключевых конфликтов между игровым сюжетом и механиками во многих современных высокобюджетных проектах. Его наличие вызывает активные дискуссии о допустимости таких расхождений, степени влияния на пользовательский опыт и о том, нужна ли полная его ликвидация для повышения качества игры.

«Игра – это закрытая формальная система, которая вовлекает игроков в структурированный конфликт с неравным исходом» такое определение дали Трэйси Фуллертон, Крис Свэйн и Стивен Хоффман [1]. В данном исследовании в первую очередь рассматриваются видеоигры, то есть программное обеспечение, работающее на специальном оборудовании (компьютере, игровой консоли, портативном электронном аппарате) и служащее для организации игрового процесса (геймплея) [2]. Современные видеоигры не только оцифровывают классические игры, но и развивают их: благодаря наиболее устойчивой во времени фантазии и возможности играть в одиночку они демонстрируют стремительный прогресс, а геймдизайнеры находят все больше уникальных инструментов нарратива [3].

Однако одной из значительных проблем для геймдизайнеров стал конфликт между сюжетом видеоигры и ее процессом, который получил название людод-нарративного диссонанса. Впервые термин был упомянут Клинтон Хокингом, бывшим креативным директором LucasArts, в его

критической статье «Ludonarrative Dissonance in Bioshock», после чего вошел в область игровых исследований [4].

Пост в личном блоге Хокинга был посвящен критике игры Bioshock (2007) и вызвал огромный резонанс в среде геймеров и создателей игр. Он указал на несоответствие между передаваемым сюжетом и тем, как игра побуждает действовать, что приводит к ощущению отстраненности и потери эмоционального вовлечения игрока. Таким образом, людонарративный диссонанс возникает, когда дискурс, передаваемый через историю и среду игры, противоречит дискурсу, лежащему в основе ее игрового процесса. С момента публикации этого поста вышло множество статей, доказывающих, что игры – это не только развлекательный контент, а технически сложный продукт, требующий тщательного обсуждения и анализа.

В ответ на анализ Хокинга Ник Баллантайн опубликовал статью для GameCloud, сравнив когнитивный и людонарративный диссонансы и подчеркнув их фундаментальное различие. Сталкиваясь с когнитивным диссонансом (то есть с тем, что убеждения и действия не совпадают) в повседневной жизни, человек может изменить убеждения или поведение, но при людонарративном диссонансе игрок сталкивается с тем, что внутренняя логика игры навязывает определенные установки без возможности выбора.

Разработчики оказываются ответственными за устранение этого противоречия, передавая часть контроля над повествованием самому игроку и признавая возникающие в процессе истории ветвления. В результате игры создаются не вокруг готового сценария, а как пространство множества возможных историй, которые формирует пользователь.

Несмотря на то, что все большее и большее количество геймдизайнеров стали рассматривать людонарративный диссонанс как инструмент для усиления нарратива (управляя эмоциями и вниманием игрока), проблема все еще остается актуальной для многих компьютерных ролевых игр (CRPG, RPG, РПГ). Данный жанр игр предполагает управление одним или несколькими персонажами с набором численных характеристик, списком способностей и умений, и несоответствие их действий сюжету часто нарушает погружение и целостность игрового опыта. В то же время в игровой индустрии существуют примеры успешных игр в жанре РПГ, практически лишенные проявлений людонарративного диссонанса.

Ключевыми техническими причинами людонарративного диссонанса являются линейные скрипты и триггеры событий, которые выражаются в жесткой привязке сюжетных событий к последовательности вызовов без



возможности динамического ветвления сюжета. Помимо этого, отсутствующая гибкая архитектура и использование статичных скриптов в игровых движках без модуля динамического управления состояниями создает проблемы масштабирования при добавлении новых сцен и ветвлений.

Среди технических проблем стоит также отметить недостаточную параметризацию и отсутствие аналитических исследований на этапе геймдизайна. Отсутствие конфигурируемых параметров игровых персонажей и событий приводит к невозможности тонкой настройки поведения. Отсутствие конфигураций для управления состояниями и поддержки динамических данных в игровых движках ограничивает вариативность реакций и концовок.

Для минимизации вероятности появления людо-нарративного диссонанса стоит применять ряд практик на различных этапах жизненного цикла игрового продукта. На этапе планирования рекомендуется использовать data-driven-прототипирование, то есть на ранних этапах моделировать ветвящиеся состояния и события в табличном виде, выявляя рассогласования до начала написания программного кода. Следует использовать готовые библиотеки и фреймворки для формализации логики и гибкого управления ветвлениями, а также визуальное скриптование для наглядного согласования нарратива и механик.

На этапе тестирования стоит запускать автоматизированные модульные и интеграционные тесты ветвящихся сценариев с помощью тестовых фреймворков, проводить нагрузочное тестирование для симуляции тысяч игровых сессий и проверки «непротиворечивости» логики. Внедрение практик управления качеством и ведение чек-листов для формализации проверок рассогласования механик и сюжета, а также постоянный мониторинг и сбор метрик по выбранным игроками вариантов позволят оперативно проводить анализ и устранять проявления диссонанса в реальном времени.

В качестве методов предотвращения людо-нарративного диссонанса в играх стоит рассматривать следующие.

1. Согласование механики и сюжета. В этом случае мораль игры не должна противоречить геймплею, чего можно добиться путем согласования механик, то есть механики должны подкреплять мораль и характер мира, исключая действия, противоречащие сюжету и роду деятельности персонажа.

2. Логичное обоснование свободы действий в мире. Если игроку предоставляется свобода действий от основного сюжета, этот выбор должен быть оправдан в контексте срочности или угрозы главной линии повествования. Для многих игр в жанре РПГ именно это и становится главной причиной

возникновения людо-нарративного диссонанса, вызывая недоумение и дискомфорт у многих геймеров.

3. Отражение последствий действий игрока. Необходимо сформировать реакции мира на решения игрока (изменение концовок, уровня репутации, поведения игровых персонажей в ответ на действия игрока), что поможет сохранить смысловую связь между геймплеем и историей.

4. Интегрирование героя в лор игры. Персонаж должен быть органично вписан в мир игры без противоречий игровым условностям, получая адекватный бэкграунд, характеристики и взаимодействие с окружением, позволяющие сделать персонажа полноценной функционирующей частью игрового мира.

В настоящее время индустрия рассматривает людо-нарративный диссонанс не только как проблему, но и как полноценный инструмент, с помощью которого геймдизайнер может влиять на игрока на подсознательном уровне, вызывая у него дискомфорт или лучше раскрывая нарратив игры. Он может использоваться в качестве:

- специального художественного и философского приема: создание дискомфорта через контраст привычных механик и неожиданной морали, реализующиеся через заложенную на этапе разработки логику поведения объектов и срабатывание триггеров моральных дилемм (Spec Ops: The Line, Nier: Automata);

- критики поведения игрока: провокация на рефлекссию о чрезмерном насилии в играх путем нарушения «четвертой стены» и переосмысление игрового процесса, что осуществляется за счет сохранения переменных и заранее прописанных скриптов для изменения диалогов и концовок (Undertale);

- моральной дилеммы: принуждение к действиям, противоречащим общепринятой морали ради достижения игровых целей, что подталкивает к размышлению и поднятию важных остросоциальных вопросов за счет вызова различных заранее реализованных сценарных событий (Papers, Please).

Необходимость избегания людо-нарративного диссонанса в играх по-прежнему остается сложной и неоднозначной проблемой. Согласно результатам опроса, охватившего 2 424 респондента, 48,4 % участников признали сюжет важным и оценивали его критически. При этом 55,6 % респондентов, критически относящихся к сюжету, и 47,8 % тех, кто не придает сюжету особого значения, отметили наличие проявлений людо-нарративного диссонанса, который, однако, не оказывал существенного влияния на их общий игровой опыт.

Из представленных данных следует, что подавляющее большинство игроков замечает проявления людо-нарративного диссонанса, однако вовлеченность в игровой процесс обычно преобладает над логикой и критичным отношением к сюжету. Современные практики геймдизайна все чаще рассматривают его как инструмент для углубления игрового опыта, обогащая сюжет новыми гранями и стимулируя эмоциональный отклик на моральную составляющую игры.

Минимизация людо-нарративного диссонанса остается многогранной задачей, требующей не только продуманной архитектуры сценарных ветвлений и параметризации игровых систем, но и выверенной методологии тестирования на всех этапах разработки. Внедрение data-driven-прототипирования, визуальных скриптовых инструментов и автоматизированных симуляций игровых сессий позволяет значительно снизить риск рассогласований между механикой и сюжетом, однако окончательного баланса возможно достичь лишь при учете реальных пользовательских метрик и обратной связи.

В дальнейшем следует провести углубленный анализ возможностей применения искусственного интеллекта для автоматической адаптации сюжета в соответствии с поведением игрока, а также рассмотреть технологии адаптивной потоковой передачи данных для обеспечения масштабируемости сложных сценариев без потери гибкости. Рассмотрение этих технических аспектов позволит создавать игровые миры, где и сюжет, и механика эволюционируют в реальном времени, обеспечивая наилучший пользовательский опыт.

#### Список используемых источников

1. Шелл Дж. Геймдизайн: Как создать игру, в которую будут играть все: практическое руководство / Джесси Шелл; пер. с англ. А. Лысенко. Москва: Альпина Паблишер, 2019. 640 с. ISBN 978 5 9614 1209 3.
2. Деникин А. А. Могут ли видеоигры быть искусством? – Москва. – Международный журнал исследований культуры. 2013. С. 90-96.
3. Вишневский А. В. Философское осмысление понятия компьютерной игры. – Вестник Омского университета № 3. 2014. С. 91-92.
4. Ludonarrative Dissonance in Bioshock // Click Nothing URL: [https://clicknothing.typepad.com/click\\_nothing/2007/10/ludonarrative-d.html](https://clicknothing.typepad.com/click_nothing/2007/10/ludonarrative-d.html) (дата обращения: 19.04.2025).

*Статья представлена научным руководителем,  
старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 004.8

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ АЛГОРИТМОВ ТРЕКИНГА ОБЪЕКТОВ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Д. А. Луценко, М. А. Тумин, К. Р. Хайдаршин  
(студенты группы ИКПИ-23, СПбГУТ), [tumin.ma@sut.ru](mailto:tumin.ma@sut.ru)

*Данная работа посвящена комплексному исследованию и сравнительному анализу алгоритмов трекинга объектов на основе нейронных сетей. В работе рассматриваются основные архитектурные решения: сиамские сети, трансформеры, трекаеры на основе детекции или сегментации, zero-shot трекаеры; проводится классификация моделей трекинга по архитектурным характеристикам и области применимости; приводятся примеры существующих реализаций. Выявлены опорные параметры оценки алгоритмов: скорость обработки FPS (Frame Per Second), точность АО (Average Overlap). На основе проведенного анализа выявлены закономерности, связывающие специфику прикладной задачи и выбор типа модели. Полученные результаты свидетельствуют о высоком потенциале современных алгоритмов трекинга в прикладных задачах.*

*трекинг объектов, отслеживание объектов, сиамские сети, трансформеры, детекция, сегментация, zero-shot, average overlap, окклюзии*

### Введение

В условиях современности стремительный рост технологий компьютерного зрения способствует увеличению значимости задач отслеживания объектов в различных сферах: от систем интеллектуального видеонаблюдения до робототехнических комплексов. Нейронные сети, получив свое внедрение в процессы обработки видеоданных, открывают перспективы улучшения точности и стабильности трекинга объектов. Этим, а также разнообразием современных алгоритмических подходов к решению задачи отслеживания объектов и необходимостью в их систематизированном сравнительном анализе для выявления ключевых особенностей, преимуществ и недостатков обусловлена актуальность выбранной темы (1-5).

Цель настоящего исследования заключается в изучении современных алгоритмов трекинга объектов, основанных на нейронных сетях, проведении их классификации и сравнительной оценки на основе существующих реализаций по нескольким критериям и определении наиболее эффективных в конкретных условиях алгоритмов.

### Исследование

Трекинг – отслеживание, сопровождение – объектов представляет собой задачу компьютерного зрения по идентификации представляющего интерес

объекта и слежению за ним по мере его перемещения в видеопоследовательности или в видеопотоке реального времени. В отличие от детекции - обнаружения - объектов, призванной их локализовать и классифицировать на отдельных кадрах, трекинг фокусируется на локализации в разрезе времени и позволяет сохранять идентичность объекта в последовательности кадров.

Трекинг объектов используется во многих областях: от систем безопасности и мобильных технологий до автономного вождения и робототехники. Поэтому в настоящий момент существует большое количество алгоритмов трекинга, в том числе и на основе нейронных сетей. К ним можно отнести, например, трекаеры на основе сиамских сетей, трансформеров, детекции/сегментации и zero-shot трекаеры.

Трекаеры на основе сиамских нейронных сетей (Siamese Neural Networks) базируются на архитектуре, которая позволяет сравнивать два изображения по сходству. При этом для первого – эталонного изображения, шаблона – и для второго – изображения поиска – используются две ветви одинаковых нейросетей (обычно CNN – Convolutional Neural Network) с одинаковыми весами для формирования эмбеддингов – векторных представлений изображения. Между этими эмбеддингами рассчитывается мера схожести на основе кросс-корреляции, что позволяет определить, где на поисковом изображении находится эталонный объект. При этом ветвь для эталонного изображения используется только один раз в самом начале для извлечения признаков. Во вторую же кадры с областью поиска поступают прямо из видеопотока реального времени или видеопоследовательности.

Такой подход обеспечивает сиамским трекаерам высокую скорость и точность работы, а также гибкость в применении, поскольку нет необходимости дообучать модель на новых классах для отслеживания объекта, которого не было в обучающей выборке. Однако сиамские трекаеры архитектурно уязвимы для частичных или полных окклюзий, деформаций объекта или резкого изменения освещения, а также плохо работают в среде с несколькими одинаковыми объектами.

Примерами трекаеров на основе сиамских сетей являются: SiamFC, SiamMask, SiamRPN, NanoTrack и другие.

Помимо сиамских сетей как основы для моделей трекинга большое распространение получили так называемые трансформеры.

Трансформеры сами по себе изначально были разработаны для работы с естественным языком, для его обработки и, в частности, перевода. Однако принципы, которые лежат в основе такого подхода, в особенности механизм самовнимания (self-attention), нашли свое место и в обработке изображений.

Если в классических CNN и сиамских алгоритмах признаки из разных областей собираются независимо, то механизм самовнимания позволяет трансформерам связать части изображения, «обратить внимание» каждой на остальные. Это позволяет трансформерам в разрезе трекинга учитывать глобальный контекст, в котором находится отслеживаемый объект.

Общий принцип работы трекеров на основе трансформеров можно разделить на три шага: энкодер извлекает признаки из шаблона и поисковой области для преобразования их в эмбединги; self-attention строит связи внутри каждого кадра, а cross-attention (перекрестное внимание) - между разными кадрами; декодер на основе attention-весов локализует объект на поисковом изображении, учитывая и локальный, и глобальный контексты.

Такой подход позволяет трекерам на основе трансформеров не терять объект при его деформациях и разного рода окклюзиях, резком изменении освещения или при отслеживании одного из нескольких одинаковых объектов. Но при этом такие трекеры требуют значительного объема обучающих данных, больших вычислительных ресурсов как на этапе обучения, так и в инференсе и показывают гораздо меньшую скорость обработки по сравнению с сиамскими трекерами.

Примерами трекеров на основе трансформеров могут служить TransT, OTrack, Stark, ODTrack.

Кроме уже перечисленных популярными являются трекеры, основанные на детекции или сегментации.

Такие трекеры архитектурно состоят из двух больших частей: детектора или сегментатора и алгоритма ассоциации. Первая часть - детектор или сегментатор - по своей сути отдельная нейронная сеть для детекции или сегментации соответственно, которая обрабатывает каждое изображение независимо от предыдущих: создает ограничивающие рамки (Bounding Box) или маски на объектах изображения. Алгоритм ассоциации после разметки изображения детектором или сегментатором сопоставляет текущие предсказания с разметкой на прошлом кадре. При этом реализован такой алгоритм может быть с помощью разных подходов: через эвристические методы, с помощью других нейронных сетей.

Такой подход обеспечивает трекерам на основе детекторов или сегментаторов гибкость, поскольку в отличие от сиамских сетей возможен многоклассовый трекинг, и упрощенность реализации: можно использовать уже существующие мощные модели детекции или сегментации объектов. Однако при этом трекинг напрямую зависит от качества детекции/сегментации

и может быть уязвим к пропущенным детекциям; в зависимости от детектора/сегментатора нагрузка на аппаратное обеспечение может быть разной, отчего зависит и скорость обработки. При этом, если трекары на основе сиамских сетей или трансформеров умеют работать с объектами, на которых они не обучались, трекары на основе детекции или сегментации архитектурно зависят от детектора/сегментатора, поэтому может понадобиться дополнительное обучение на отдельные классы объектов.

Эту проблему решают так называемые zero-shot трекары. Применительно к детекции или сегментации zero-shot трекары способны отслеживать объекты, которые ранее модели не встречались, без дополнительной донастройки или дообучения. В таких трекарах детектор или сегментатор заранее обучен на большом и разнообразном объеме данных, поэтому способен обобщенно извлекать визуальные признаки из новых объектов. То есть zero-shot трекары не ограничены каким-то определенным количеством классов, однако для работы с новыми объектами должны получить указание, где находятся эти объекты на первом кадре. К тому же, поскольку в основе лежит большая детектирующая или сегментирующая модель, скорость обработки достаточно низкая, а ресурсозатратность высокая.

Примерами zero-shot трекаров на основе сегментации являются Samurai и Dam4Sam.

Описанные выше примеры с указанием принадлежности к тому или иному типу алгоритмов трекинга, а также значений метрик АО на датасете Got-10k и FPS сведены в таблицу 1 для наглядности.

ТАБЛИЦА 1. Сравнение различных реализаций алгоритмов трекинга на основе нейронных сетей

| Модель    | Тип                             | АО    | FPS   |
|-----------|---------------------------------|-------|-------|
| SiamFC    | Сиамская                        | 0.347 | 86    |
| SiamMask  | Сиамская                        | 0.453 | 55    |
| SiamRPN   | Сиамская                        | 0.517 | 160   |
| NanoTrack | Сиамская                        | 0.719 | 200+  |
| TransT    | Трансформер                     | 0.723 | 50    |
| OSTrack   | Трансформер                     | 0.737 | 50-55 |
| Stark     | Трансформер                     | 0.688 | 40-50 |
| Samurai   | Zero-shot на основе сегментации | 0.817 | 25-35 |
| Dam4Sam   | Zero-shot на основе сегментации | 0.811 | 20-30 |

Метрика АО показывает среднее значение IoU (Intersection over Union) по всем кадрам между ограничивающими рамками, которые предсказаны моделью, и рамками, которые показывают, где действительно находится отслеживаемый объект.

Метрика FPS, как следует из названия, показывает, какое количество кадров в секунду способен обработать трекер.

Обе эти метрики являются ключевыми показателями качества, и зачастую увеличение одной приводит к уменьшению другой.

## Заключение

Учитывая все описанное выше, можно выявить общие закономерности, которые связывают выбор типа модели и специфику задачи, область применения.

Сиамские модели будут полезны, если нужно отслеживать объекты в реальном времени на устройствах с ограниченными вычислительными ресурсами или если объект хорошо выделяется на фоне окружающего пространства и окклюзии незначительны.

Трекер на основе трансформеров стоит применять, когда в кадре много одинаковых объектов, есть значительные окклюзии или объект плохо выделяется на общем фоне. При этом стоит учитывать, что трекеры на основе трансформеров проигрывают в скорости сиамским.

Трекер на основе детекции или сегментации удобен в условиях многоклассового отслеживания и при слежении за объектами на видеопоследовательности, а не в реальном времени. Также трекеры на основе сегментации могут помочь в анализе формы отслеживаемого объекта в разрезе времени.

Zero-shot трекеры, основанные на детекции или сегментации, стоит применять, если важна точность, а не скорость или в видеопоследовательности присутствуют объекты, на которых не обучалась модель детекции/сегментации.

## Список используемых источников

1. Гудфеллоу Я., Бенджио И., Курвилль И. Глубокое обучение. 2-е изд. Москва: ДМК, 2018. 652 с.
2. Коул А., Ганджу С., Казам М. Искусственный интеллект и компьютерное зрение. Реальные проекты на Python, Keras и TensorFlow. Санкт-Петербург: Питер, 2023. 624 с.
3. Дэвис Р. Компьютерное зрение. Современные методы и перспективы развития. Москва: ДМК, 2022. 690 с.



4. Yaozong Zheng, Bineng Zhong, Qihua Liang, , Zhiyi Mo, Shengping Zhang, Xianxian Li ODTrack: Online Dense Temporal Token Learning for Visual Tracking / Yaozong Zheng, Bineng Zhong, Qihua Liang, , Zhiyi Mo, Shengping Zhang, Xianxian Li // arXiv. URL: <https://arxiv.org/pdf/2401.01686> (дата обращения: 15.06.2025).

5. Jovana Videnovic, Alan Lukezic, Matej Kristan A Distractor-Aware Memory for Visual Object Tracking with SAM2 / Jovana Videnovic, Alan Lukezic, Matej Kristan // arXiv. URL: <https://arxiv.org/pdf/2411.17576> (дата обращения: 15.06.2025).

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Пачиным А. В.*

УДК 004.94

**А. О. Платонов** (студент группы ИКПИ-32, СПбГУТ)

**А. Е. Кларк** (студент группы ИКПИ-32, СПбГУТ), [klark.ae@sut.ru](mailto:klark.ae@sut.ru)

## ПОСТРОЕНИЕ ТРЕХМЕРНОЙ МОДЕЛИ МЕСТНОСТИ НА ОСНОВЕ ОБЛАКА ТОЧЕК В СРЕДЕ UNITY

*В данной работе рассматривается методика построения 3D-модели местности на основе облака точек, полученного в процессе виртуального сканирования с беспилотного летательного аппарата (БПЛА) в среде Unity. Разработанная система позволяет собирать данные о ландшафте с помощью имитации лидара, формировать облако точек и визуализировать его в режиме реального времени. Такой подход может быть использован в образовательных, научных и прикладных целях, в том числе при проектировании автоматизированных систем мониторинга и в учебных лабораториях по компьютерной графике и моделированию.*

*Unity, облако точек, лидар, сканирование, 3D-моделирование, беспилотник, визуализация*

### Введение

Современные технологии моделирования и анализа местности требуют точных и доступных методов получения пространственных данных (1-4). Одним из таких методов является формирование облака точек – совокупности трехмерных координат, полученных в результате взаимодействия лазерного луча с объектами окружающей среды. На практике для получения облака точек используются лидары, установленные на БПЛА. Создание программной имитации этого процесса позволяет реализовать доступный инструмент для обучения и предварительного анализа.

Виртуальные модели сканирования позволяют исследовать принципы формирования пространственных данных без привлечения дорогостоящего оборудования. Такой подход особенно актуален в образовательной среде, где учащиеся могут на практике познакомиться с основами лидарного сканирования, анализа рельефа и построения трехмерных моделей. Кроме того, разработка виртуального симулятора создает фундамент для более сложных систем, которые могут быть использованы в геоинформационных системах, строительстве, архитектуре и экологии.

Цель данной работы – разработка и реализация программного средства на базе Unity, способного эмулировать полет БПЛА, осуществлять лучевое сканирование сцены и визуализировать полученные данные в виде облака

точек. Также предполагается обеспечить экспорт собранных данных в удобном формате для последующей обработки в профессиональных системах трехмерного моделирования.

### Практическая часть

В рамках проекта была реализована система, включающая в себя физическую модель полета беспилотного аппарата, механизм сканирования с помощью Raycast и модуль визуализации облака точек. Комплексное взаимодействие этих компонентов позволило создать программный инструмент, обладающий как визуальной наглядностью, так и высокой технической гибкостью.

Полет БПЛА осуществляется либо вручную, либо по заданному маршруту. Это позволяет получать данные с различных высот и направлений, что повышает точность финальной 3D-модели. Также предусмотрена возможность задания скорости и иных характеристик полета в реальном времени, что делает процесс сканирования интерактивным и адаптивным под нужды исследователя.

Сканирование местности реализовано через выпуск пакета лучей (Raycast) с платформы лидара, вращающегося вокруг вертикальной оси (рис. 1). При столкновении луча с поверхностью сцены фиксируется точка касания, ее координаты и цвет материала. Такие точки записываются в массив, формируя динамически обновляемое облако. При этом частота сканирования и плотность лучей регулируются параметрами, доступными пользователю.

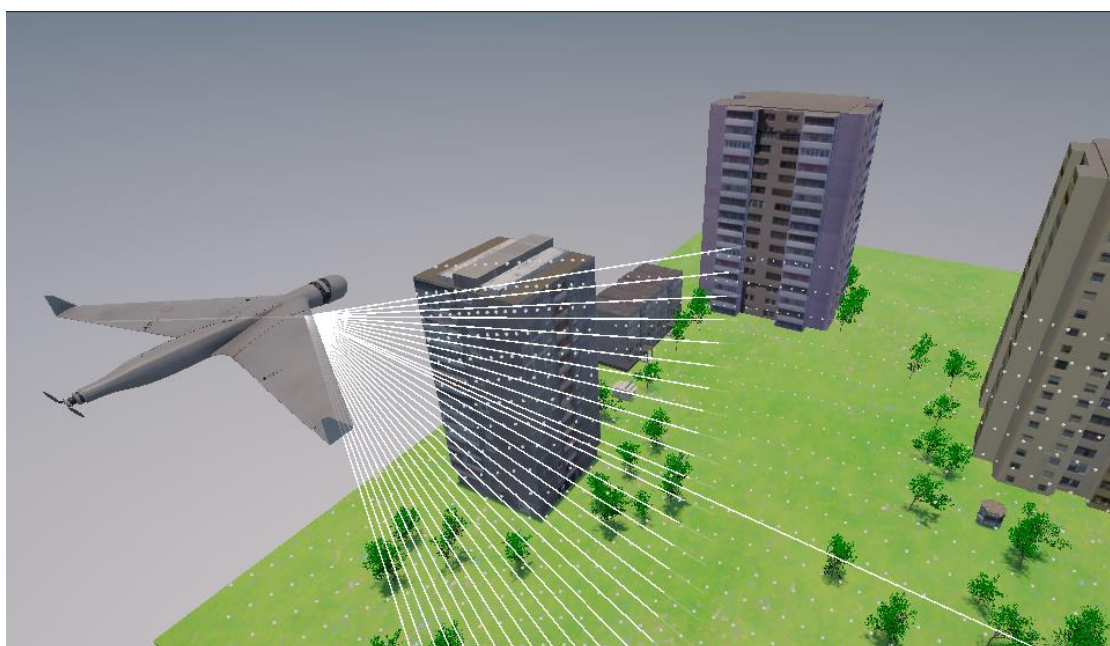


Рис. 1. Выпуск пучка лучей с БПЛА

Облако точек может быть сохранено в файл формата PLY по нажатию соответствующей кнопки в пользовательском интерфейсе. Данный формат поддерживается большинством профессиональных инструментов трехмерного моделирования и анализа. Полученный файл может быть импортирован в сторонние программы, такие как Blender, MeshLab или CloudCompare, где пользователь может выполнять построение поверхности, выделение объектов, упрощение модели и другие операции (рис. 2).



Рис. 2. Облако точек, импортированное в Blender

Особое внимание в ходе разработки уделялось оптимизации процесса записи и экспорта данных. Использование формата PLY позволяет сохранять не только координаты, но и цветовую информацию, что важно при визуальном анализе и текстурировании. Возможность интеграции с Blender открывает перспективы для расширения функциональности проекта за счет использования готовых инструментов по созданию мешей и текстурированных моделей.

Разработанная система может быть использована как платформа для дальнейших исследований и разработки более сложных моделей, включая автоматическое построение меша, кластеризацию точек, машинное обучение и построение цифровых двойников. Кроме того, она может быть адаптирована для работы с реальными данными, поступающими с физических лидаров, что превратит ее в полноценную систему постобработки и анализа пространственной информации.

## Заключение

Результаты проекта демонстрируют возможность эффективного применения игрового движка Unity для задач пространственного моделирования. Система, построенная на принципах имитационного моделирования, позволяет формировать и анализировать облака точек, полученные с виртуального БПЛА, в режиме реального времени. Такое решение может быть полезным в образовательных целях, при планировании миссий реальных дронов, а также в научных исследованиях, связанных с визуализацией пространственных данных.

В дальнейшем проект может быть значительно расширен как в функциональном, так и в прикладном направлении. Одной из ключевых задач является разработка автоматизированного построения трехмерной поверхности на основе облака точек. Также перспективным направлением является интеграция методов машинного обучения для классификации точек по типу поверхности (растительность, здания, вода и т.д.). Помимо этого, система может быть дополнена средствами шумоподавления, фильтрации выбросов и оптимизации данных, что позволит использовать ее для подготовки цифровых моделей ландшафта. Особый интерес представляет реализация поддержки реальных данных, полученных с лидаров БПЛА, а также разработка функций для анализа изменений местности с течением времени, что откроет возможности для мониторинга окружающей среды, и других прикладных задач.

## Список использованных источников

1. Unity Documentation. URL: <https://docs.unity3d.com/> (дата обращения 26.04.2025).
2. Хилл К. Unity 3D для разработчиков. Санкт-Петербург: БХВ-Петербург, 2020. 352 с.
3. Пискунов А. В. Введение в Unity для технических специалистов. М.: ДМК Пресс, 2021. 288 с.
4. Бочаров А. В. Методы и средства визуализации пространственных данных. МГТУ им. Н. Э. Баумана, 2019. 215 с.

*Статья представлена научным руководителем, кандидатом технических наук, доцентом Дагаевым А. В.*



УДК 004.9:37.018.2

М. О. Позняк (студент группы ИСТ-212, СПбГУТ), [poznyak.mo@sut.ru](mailto:poznyak.mo@sut.ru)

## ПРОЕКТИРОВАНИЕ СИСТЕМЫ МОНИТОРИНГА БЕЗОПАСНОСТИ ДЕТЕЙ С ВОЗМОЖНОСТЬЮ ЧАСТНОГО И ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ

*В статье рассматривается проектирование комплексной системы мониторинга безопасности детей, адаптируемой как для частного использования, так и для внедрения в учреждения в качестве централизованного решения. Проведен анализ существующих решений на рынке, определены их ключевые достоинства и недостатки. Разработана модульная структура информационной системы, включающая интеграцию с трекерами глобального позиционирования и устройствами Интернета вещей для точного контроля перемещений и состояния объекта. Описаны особенности реализации облачной версии с использованием серверной и клиентской частей, а также локальной self-hosted версии для организаций с повышенными требованиями к автономности. Определены перспективные направления развития системы для расширения ее функциональности.*

*проектирование системы, мониторинг безопасности, контроль детей, локальный сервер, облачная система, интернет вещей, глобальное позиционирование*

Современный ритм жизни требует от родителей бдительности и контроля за безопасностью своих близких. В России ежегодно пропадает более 40 тысяч детей, чаще всего пропадают дети младшего и среднего подросткового возрастов [1]. На рынке представлены как приложения и трекеры для частных пользователей, так и системы, предназначенные для учреждений. Однако между ними существует значительный разрыв: первые ограничены в возможностях, вторые – требуют финансовых затрат и сложны для развертывания.

Существующие системы мониторинга для индивидуального использования обеспечивают базовый функционал отслеживания местоположения и отправки уведомлений, просты в использовании, но ограничены в масштабируемости и гибкости настройки (например, количество трекеров или зон). К недостаткам также относятся низкая точность в помещениях и невозможность локального развертывания без интернет-доступа. Существующие централизованные системы мониторинга, например, ZKBioSecurity [2], требуют сложного внедрения, рассчитаны исключительно на развертывание в учреждениях. Высокая стоимость лицензий и оборудования – препятствие

для небольших организаций и частных лиц. В данной работе рассматривается проектирование информационной системы мониторинга с двумя основными сценариями использования: частное решение – облачная система с мобильным приложением, ориентированная на удобство и доступность, и централизованное решение – локально развертываемая система, рассчитанная на работу с большим количеством IoT-устройств [3] и интеграцией с инфраструктурой учреждения.

Цель системы – удаленный и/или централизованный мониторинг, позволяющий отслеживать местоположение и состояние подопечных, связываться с ними, с возможностью конфигурирования серверной части (сервер облачный или развернутый локально, настройка необходимых функций, применяемых технологий) и клиентской части (мобильные приложения, GPS и BLE устройства и т. д.); централизованного наблюдения внутри периметров и повсеместно. Для достижения цели необходимо реализовать мониторинг перемещений в режиме реального времени, возможность гибкой настройки устройств и безопасных зон, получение уведомлений и связь с устройствами, а также реализовать возможность развертывания локального сервера для мониторинга в учреждениях.

Базовые варианты конфигурирования (рис. 1) включают два разделенных решения, облачное – частное и локальное – централизованное. Облачный сервер для частного решения содержит модули, реализующие авторизацию, API для взаимодействия с приложениями, обработку данных с устройств слежения; также на сервере есть модули, отвечающие за устройства, пользователей, монетизацию, события и логику работы частной системы мониторинга. Локальный сервер отличается отсутствием модуля квот и монетизации, а также акцентом на взаимодействие с IoT-устройствами.

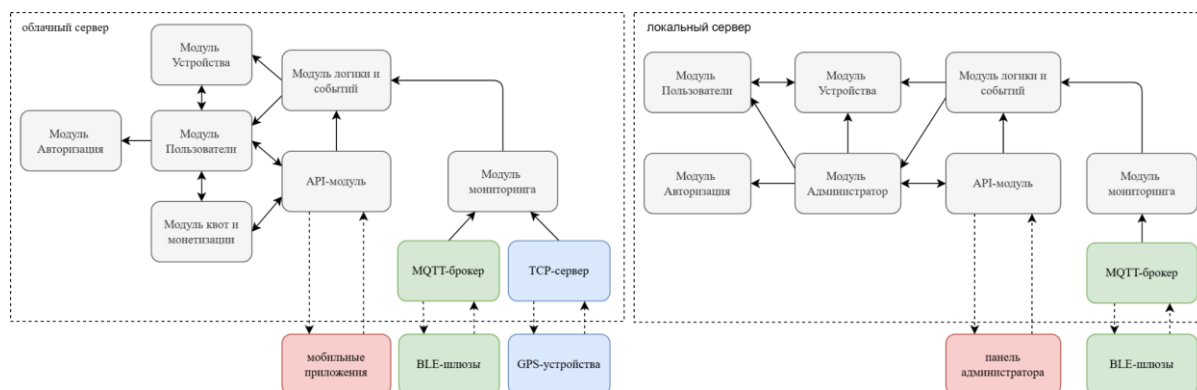


Рис. 1. Модульная схема проектируемой информационной системы

К внешним устройствам относятся мобильные приложения, панель администратора, GPS и BLE устройства слежения.

Представлены в системе и описаны в таблице 1 следующие роли: родитель и сотрудник (являются привилегированными пользователями системы, и могут настраивать ее модули в соответствии со своими пожеланиями), ребенок (может связаться с другими пользователями), системный администратор (выполняет настройку локального сервера учреждения).

ТАБЛИЦА 1. Пользователи системы, их потребности и предлагаемое решение

| Пользователь             | Потребность                                                                      | Решение                                                                  |
|--------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Родитель                 | Знать, где находится ребенок, получать уведомления, ограничить зоны              | GPS и IoT-трекеры, настройка безопасных периметров, мобильное приложение |
| Сотрудник учреждения     | Мониторинг группы детей, контроль перемещений                                    | Панель мониторинга, IoT-сеть, уведомления по группам                     |
| IT-специалист учреждения | Локальная установка, настройка сети, автономность                                | Self-hosted сервер, настройка локальных модулей, IoT-устройства          |
| Ребенок                  | Не потеряться, не чувствовать дискомфорт во время пользования элементами системы | Комфортные устройства слежения с датчиками высокой точности              |

Диаграмма вариантов использования (рис. 2) содержит описание прецедентов в системе [4].

Функциональные требования к системе, которые отражены на диаграмме, составлены в соответствии с потребностями пользователей.



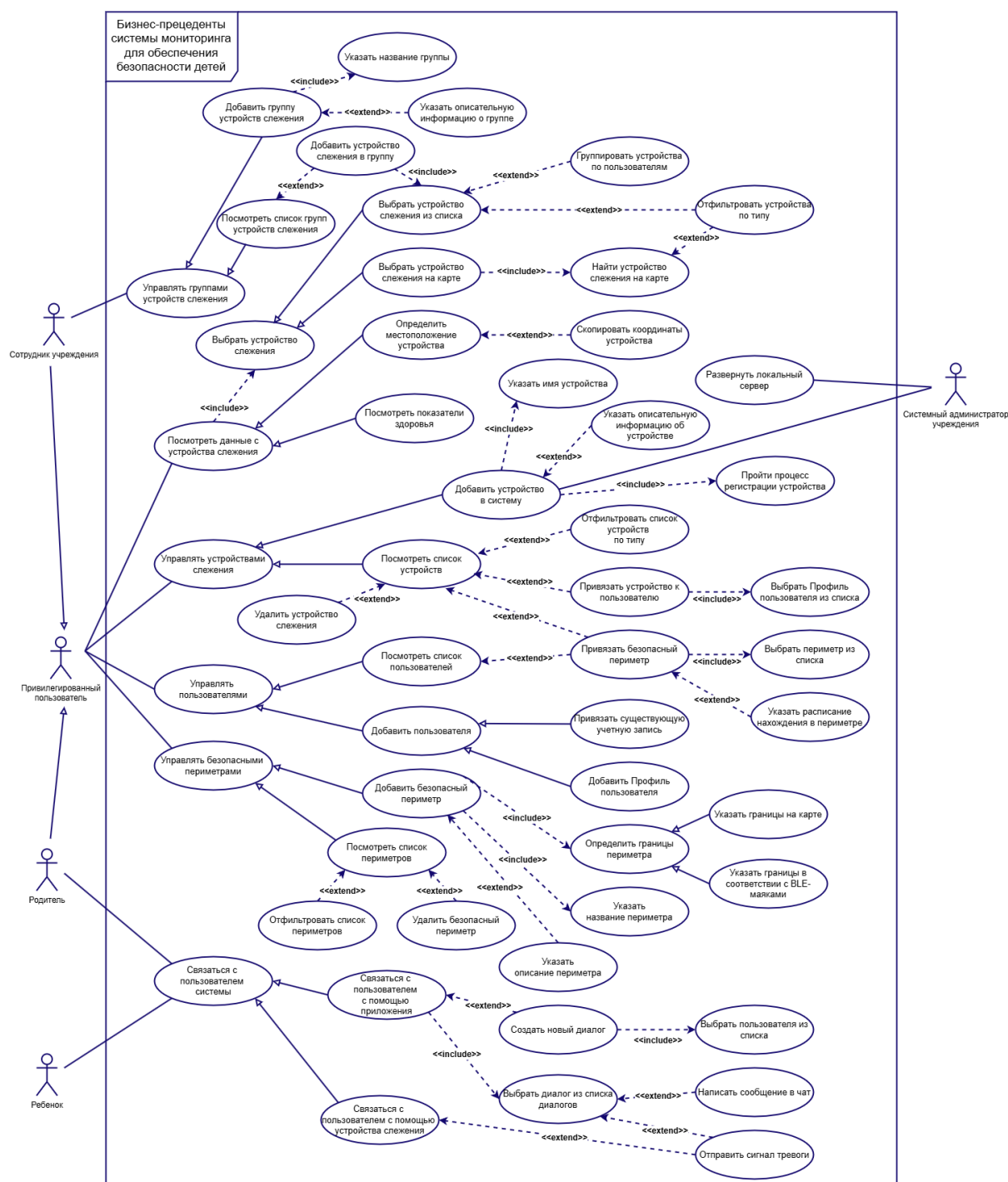


Рис. 2. Диаграмма прецедентов системы мониторинга

Частное решение выбрано в качестве первостепенного, для него определены классы системы (рис. 3). Частная система агрегирует устройства, komponует профили пользователей, безопасные периметры и события; Учетная запись используется для взаимодействия пользователей с частной системой; Чат между пользователями хранит сообщения и оповещения, созданные пользователями в рамках общения в чате.

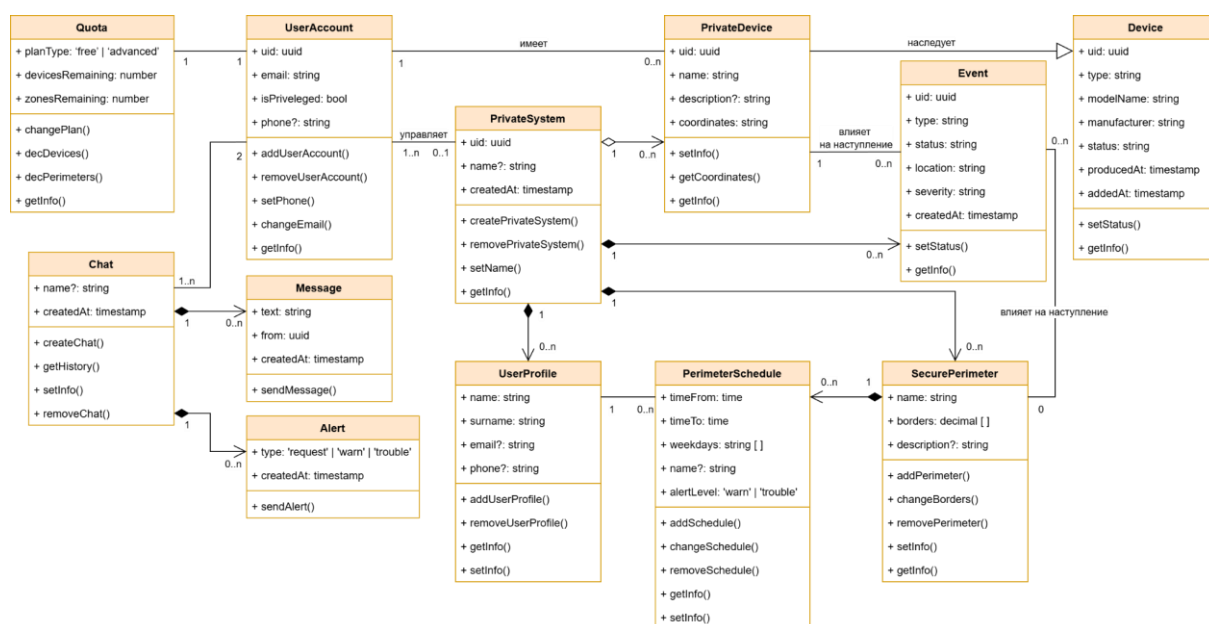


Рис. 3. Диаграмма классов системы мониторинга

Определен вероятный стек технологий системы, разделенный на области использования: клиентская часть (Next.js, React Native [5]), серверная часть (Django), BLE-устройства (BLE, ESP32), GPS-устройства (GPS/ГЛОНАСС-модули, GSM/LTE-модем), инфраструктура (Docker, NGINX, MQTT-брокер). На рисунке 4 изображена схема взаимодействия с описанием протоколов передачи данных между модулями системы.

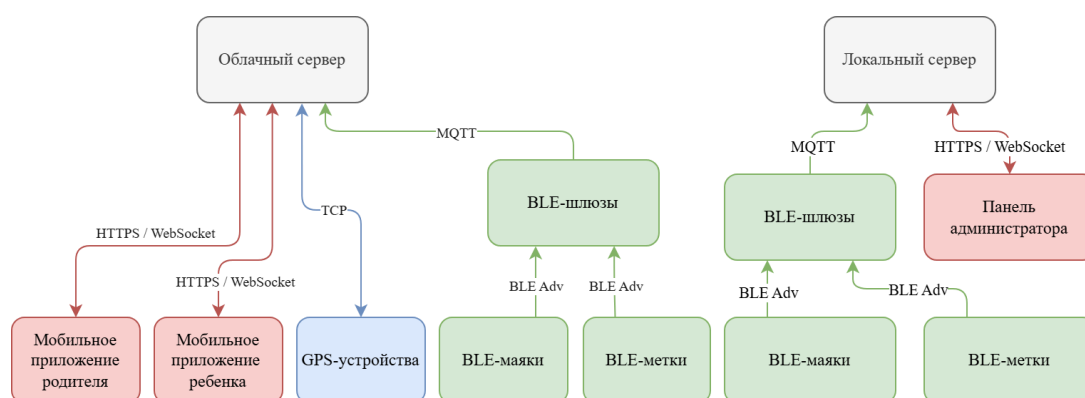


Рис. 4. Схема взаимодействия модулей системы с протоколами передачи данных

Унифицированная модульная архитектура обеспечивает возможность масштабирования, сопровождения и постепенного расширения функциональности в зависимости от потребностей пользователя. Практическая реализация системы начинается с создания минимального жизнеспособного продукта с базовыми функциями отслеживания: поддержка GPS-трекеров с открытым протоколом; TCP-сервер; модули Мониторинга, Авторизации, Пользователей, Устройств; родительское мобильное приложение; сигналы

тревоги и уведомления. Следующие этапы включают доработку частной системы, создание централизованной BLE-системы для учреждений, расширение возможностей мониторинга.

Перспективным направлением развития ИС является интеграция частного и централизованного решений в единую экосистему. Родитель может использовать мобильное приложение для слежения за своими устройствами и для получения информации от системы мониторинга, установленной в учреждении, которое посещает ребенок. Объединение позволит обеспечить непрерывный контроль и повысить уровень безопасности благодаря синхронизации данных из нескольких источников.

Выполнено проектирование информационной системы мониторинга безопасности детей с возможностью частного и централизованного контроля, в ходе которого выявлена потребность в системе, поставлены цели и задачи, определена значимость ИС, разработаны ее функциональные и бизнес-требования, на основе которых составлены варианты использования.

Детальная проработка составных частей и компонентов системы подтвердила, что разрабатываемая система с модульной архитектурой и поддержкой разных сценариев внедрения является как актуальной, так и технологически реализуемой. Кроме того, предложенная архитектура допускает масштабирование, локализацию и возможное развитие в сторону коммерческого продукта или платформы с поддержкой подписки, интеграции с внешними устройствами и безопасного обмена данными. Проектирование продемонстрировало возможность создания современной и гибкой системы мониторинга, направленной на решение важной социальной задачи – обеспечения безопасности детей.

#### Список используемых источников

1. РИА Новости. «ЛизаАлерт»: в России ежегодно пропадают десятки тысяч детей. МВД РФ. URL: <https://ria.ru/20220525/deti-1790528398.html> (дата обращения 04.05.2025).
2. ZKTeco. Программное обеспечение ZKBioSecurity. URL: <https://zkteko.ru/time-attendance/software/zkbiosecurity/> (дата обращения: 04.05.2025).
3. Ли П. Архитектура интернета вещей/ пер. с англ. М. А. Райтмана. М.: ДМК Пресс, 2019. 454 с.: ил.
4. Буч Г., Якобсон А., Рамбо Дж. Язык UML. Руководство пользователя. 2-е изд. М., СПб.: ДМК Пресс, Питер, 2004. 432 с.
5. Язгельдыев Ш., Гурбанмырадов Б., Гапуров А. Исследование средств создания веб-приложений на клиентской и серверной сторонах. Международный научный журнал «Вестник науки» № 3 (72) Том 5. 2024. 540-544 с.

*Статья представлена научным руководителем,  
старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.*

УДК 37.091.3

**А. О. Пугачевский** (студент группы ИСМ-41з, СПбГУТ),  
[pugacevsky.ao@sut.ru](mailto:pugacevsky.ao@sut.ru)

## ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ АССИСТЕНТОВ И ЧАТ-БОТОВ ДЛЯ ПОДДЕРЖКИ УЧИТЕЛЕЙ И УЧЕНИКОВ В ШКОЛЕ

*Приводится анализ возможностей применения интеллектуальных ассистентов и чат-ботов в российской школе. Рассматриваются функции этих технологий в поддержке учителей и учеников, преимущества и ограничения их использования. Отмечается низкий уровень внедрения ИИ в условиях стагнации цифровизации образования. Подчеркивается потенциал таких инструментов при наличии методической и технической подготовки. Делается вывод о необходимости комплексного подхода к интеграции ИИ в учебный процесс.*

*искусственный интеллект, интеллектуальные ассистенты, чат-боты, школьное образование, цифровизация, поддержка учителя, образовательные технологии*

Система общего среднего образования в России на сегодняшний день сталкивается с рядом системных проблем, связанных с недостаточной адаптацией к современным цифровым изменениям [1]. Несмотря на развитие технологий искусственного интеллекта в мире, их внедрение в российских школах находится на ранних этапах или вовсе отсутствует. Цифровая трансформация происходит неравномерно, часто ограничиваясь формальной организацией рабочих мест с компьютерами и базовым пакетом программ, тогда как методическая и содержательная модернизация отстает.

В частности, интеллектуальные ассистенты и чат-боты, успешно применяемые в образовательных системах ряда зарубежных стран, в российских школах практически не используются [2]. Это связано как с низкой технической оснащенностью отдельных регионов, так и с отсутствием должной методологической базы, подготовки педагогов и нормативной поддержки.

Тем не менее, потенциал таких инструментов очевиден: они способны упростить работу преподавателей, предоставить ученикам помощь в удобное время и автоматизировать рутинные процессы [3]. В условиях отсутствия персонализированного подхода, перегруженности преподавателей и растущих ожиданий от школы, интеллектуальные ассистенты могут сыграть роль катализатора в изменениях образовательной.

Цель данной статьи – рассмотреть возможности применения интеллектуальных ассистентов и чат-ботов в условиях современной российской

школы, выявить препятствия на пути их внедрения и оценить перспективы их использования как средства поддержки как учеников, так и учителей.

Интеллектуальные ассистенты и чат-боты представляют собой программные системы, способные взаимодействовать с пользователями в естественной форме – в виде текста, цифровой информации или голоса. Эти технологии основаны на алгоритмах обработки естественного языка, машинного обучения и нейросетевых архитектурах. За рубежом они активно применяются в образовании для повышения доступности знаний, автоматизации рутинных задач и персонализации обучения.

В российской школьной практике такие инструменты пока используются крайне ограниченно – чаще как экспериментальные или внешкольные проекты, реализуемые в рамках конкурсов или проектов [4]. Несмотря на низкий уровень внедрения, само понимание возможностей подобных систем уже формируется в педагогическом сообществе.

Интеллектуальные ассистенты могут выступать в роли виртуального помощника для учителя или ученика. Например, голосовой помощник способен напомнить ученику о выполнении задания, а чат-бот в мессенджере – быстро объяснить теоретическую тему или предложить тренировочные упражнения. Некоторые более сложные решения умеют генерировать задания, проверять ответы и адаптироваться под уровень обучающегося.

Важно понимать, что подобные технологии не заменяют педагога, но могут эффективно дополнять его деятельность – особенно в условиях перегруженности, нехватки индивидуального подхода и высокой нагрузки на учителей.

Несмотря на то, что в российских школах интеллектуальные ассистенты и чат-боты пока не получили широкого распространения, уже можно обозначить направления для их использования:

1. Поддержка учащихся: чат-боты и голосовые помощники могут выступать в роли виртуального репетитора, предоставляя ученикам простые и доступные объяснения по темам школьной программы, предлагая тренировочные задания, карточки для повторения, интерактивные тесты. Особенно полезным это может быть для учеников, испытывающих трудности с обучением, а также в случае самостоятельной подготовки к государственным экзаменам ОГЭ и ЕГЭ.

2. Поддержка учителей: для педагога интеллектуальные ассистенты могут выполнять вспомогательные функции: предлагать варианты форму-

лировок заданий, генерировать вопросы для викторин, помогать с составлением рабочих программ и презентаций. Наиболее перспективными представляются системы, способные анализировать уровень освоения материала учениками [5]. Это особенно важно в условиях перегруженности, большого количества классов и отсутствия возможности индивидуального подхода.

3. Административные задачи: ИИ-ассистенты могут быть полезны и для решения организационных задач: отправка автоматических напоминаний о сроках сдачи работ, изменение расписания, формирование электронных уведомлений родителям. На уровне школы такие функции могут быть реализованы в рамках единой цифровой образовательной платформы.

Таким образом, интеллектуальные помощники могут стать важным дополнением к существующим инструментам, если их внедрение будет сопровождаться методической поддержкой и технической подготовкой [6]. Потенциал их применения в российской школе есть, особенно в тех учреждениях, которые уже освоили базовую цифровую инфраструктуру.

Несмотря на начальную стадию внедрения ИИ в российское образование, интеллектуальные ассистенты и чат-боты уже сегодня обладают рядом очевидных преимуществ, которые делают их перспективными для применения в школьной практике:

Повышение доступности помощи: ученики могут обращаться к боту в любое время, включая вечерние часы, когда учитель недоступен, а также, они могут стать хорошим помощником для детей с ограниченными возможностями здоровья.

Персонализация обучения: алгоритмы могут подстраиваться под темп и уровень ученика, предлагая подходящие задания или объяснения.

Снижение нагрузки на учителя: автоматизация рутинных задач позволяет сосредоточиться на ключевых аспектах преподавания.

Мотивация и интерес: использование современных цифровых технологий делает обучение ближе к привычной среде школьников и может способствовать вовлеченности.

Вместе с тем, массовое применение интеллектуальных ассистентов в российских школах сталкивается с рядом существенных ограничений:

Ограниченная техническая инфраструктура: не все школы обеспечены стабильным интернетом, современной компьютерной техникой или локальными сетями, необходимыми для работы ИИ-инструментов [6].

Качество и надежность ответов: без дополнительной модерации чат-боты могут выдавать неполные или некорректные объяснения, что особенно критично в школьной среде.

Этические и правовые аспекты: обработка персональных данных учащихся, риск зависимости от автоматизированной помощи, снижение роли критического мышления требуют серьезного анализа и регулирования.

Методическое отставание: отсутствуют утвержденные программы или рекомендации по интеграции ИИ-инструментов в учебную деятельность.

Таким образом, хотя интеллектуальные ассистенты и чат-боты обладают значительным потенциалом, их эффективное использование в российских школах требует комплексного подхода – сочетания технологической готовности, повышения цифровой грамотности педагогов и разработки регламентов использования ИИ в образовательной среде.

В заключение отметим, что интеллектуальные ассистенты и чат-боты представляют собой перспективный инструмент для поддержки школьного образования, особенно в условиях растущей нагрузки на учителей и потребности в индивидуализации обучения. Несмотря на то, что в российских школах их внедрение пока ограничено, уже сегодня можно говорить о значительном потенциале таких технологий. Для их успешного применения необходимо обеспечить техническую базу, подготовку педагогов и разработку нормативных и методических основ, позволяющих интегрировать ИИ в учебный процесс эффективно и безопасно.

#### Список используемых источников

1. Иванова А. В. Цифровизация образования и роль искусственного интеллекта // Электронное обучение. 2024. № 2. С. 55–63. DOI: 10.22144/edu.2024.054.
2. Сидорова М. П., Романов А. Ю. Инновации в образовательных технологиях: применение ИИ в школьном обучении // Образовательные технологии и общество. 2023. Т. 26. № 1. С. 12–21. EDN: RUPXQC.
3. Ершова Т. И., Малахов А. А. Искусственный интеллект в образовании. М.: Изд-во МГУ, 2023. 248 с.
4. Лебедев И. В. Роль чат-ботов в образовательном процессе: опыт внедрения в России // Информационные технологии в образовании. 2023. № 7. С. 75–81. URL: <http://www.edu-tech.ru/it-education/2023/7> (дата обращения 12.04.2024).
5. Гусев В. В., Климова О. Н. Интеллектуальные системы поддержки принятия решений. СПб.: Наука, 2022. 320 с. ISBN 978-5-02-026443-9.
6. Чернов А. И., Третьяков В. С. Цифровые технологии в школьном образовании: перспективы и вызовы. М.: Изд-во «Просвещение», 2024. 156 с.

*Статья представлена научным руководителем,  
кандидатом технических наук, доцентом Филипповым Ф. В.*

УДК 37.03:004.932

**О. В. Раковский** (к.т.н., доцент, доцент кафедры ИУС, СПбГУТ)

**И. И. Турлыков** (студент группы ИСТ-411м, СПбГУТ), [turlykov.ii@sut.ru](mailto:turlykov.ii@sut.ru)

## ИССЛЕДОВАНИЕ ЦИФРОВЫХ ИНСТРУМЕНТОВ ПОСТРОЕНИЯ И СПОРОВОЖДЕНИЯ ИНДИВИДУАЛЬНЫХ ОБРАЗОВАТЕЛЬНЫХ ТРАЕКТОРИЙ

*Цифровые инструменты формирования индивидуальных образовательных траекторий активно внедряются в современную образовательную практику благодаря широкому распространению информационных технологий и растущей потребности в персонализированном подходе к обучению. Использование адаптивных платформ, рекомендательных систем и систем сопровождения на базе искусственного интеллекта позволяет учитывать уровень подготовки, интересы и цели обучающегося. Данная форма организации повышает вовлеченность и эффективность обучения.*

*индивидуальная образовательная траектория, цифровые инструменты, персонализированный подход, адаптивные платформы, рекомендательные системы, искусственный интеллект, образовательная среда, информационные технологии*

Современное образование развивается в направлении гуманизации и непрерывности, что требует учета индивидуальных возможностей каждого обучающегося. В условиях цифрового общества оптимальным становится сочетание традиционных и инновационных методов обучения, обеспечиваемых цифровыми образовательными инструментами. Персонализация обучения и формирование индивидуальных образовательных траекторий приобретает особую актуальность, позволяя студентам самостоятельно выбирать учебные дисциплины и адаптироваться к изменениям профессиональной среды. Внедрение цифровых платформ, рекомендательных систем и интеллектуальных средств сопровождения способствует гибкости и эффективности образовательного процесса, что соответствует стратегическим задачам цифровой трансформации системы образования.

Персонализация образования с помощью цифровых инструментов становится ключевым направлением развития образовательной сферы. Индивидуальная образовательная траектория – это настраиваемая программа обучения, учитывающая индивидуальные особенности обучающегося: уровень знаний, интересы и профессиональные цели. Разработка и реализация ИОТ способствует повышению мотивации, улучшению усвоения материала и формированию компетенций, необходимых для карьерного роста.



Современные адаптивные образовательные платформы, такие как Moodle с его возможностью создания ветвящихся курсов, Coursera и edX с их рекомендательными системами, а также Smart Sparrow, разработанная специально для адаптивного обучения, позволяют реализовать персонализированный подход. Технология адаптивного обучения основана на алгоритмах, анализирующих ответы обучающегося и корректирующих сложность и содержание учебных материалов [1, 2], учитывая индивидуальный темп и предпочтения.

Рекомендательные системы, использующие Collaborative Filtering (коллаборативную фильтрацию) и Content-Based Filtering (фильтрацию на основе контента), помогают повысить релевантность учебных материалов [2]. Гибридные системы, сочетающие оба подхода, применяются, например, на платформе Stepik.

Интеллектуальные системы сопровождения, включающие чат-боты (например, ChatGPT) и системы мониторинга на базе Big Data, оказывают помощь в планировании обучения [3, 5], объяснении материала и выявлении проблемных зон.

Цифровые профили, стандартизированные платформами Open Badge и Learning Locker, аккумулируют достижения и навыки обучающихся [3, 5], упрощая интеграцию образовательного и профессионального опыта.

В таблице 1 показаны функциональные особенности платформ и технологий по описанным категориям.

ТАБЛИЦА 1. Обзор цифровых инструментов для построения и сопровождения ИОТ

| Категория                    | Пример платформы/технологии          | Основные функции                                      | Особенности                                                 |
|------------------------------|--------------------------------------|-------------------------------------------------------|-------------------------------------------------------------|
| Адаптивные платформы         | Moodle, Coursera, Smart Sparrow      | Персонализация учебного пути, ветвящиеся уроки        | Гибкая настройка, поддержка аналитики обучения              |
| Рекомендательные системы     | Stepik, EdCast                       | Предложения курсов и материалов на основе данных      | Гибридные алгоритмы, высокая точность                       |
| Интеллектуальные помощники   | ChatGPT, персональные ассистенты LMS | Консультации, планирование, мотивация                 | Реактивная поддержка, автоматизация обратной связи          |
| Цифровые профили и портфолио | Open Badge, Learning Locker          | Хранение достижений и сертификатов, интеграция данных | Стандартизация, возможность межплатформенного использования |

Внедрение цифровой персонализации образования сопряжено с вызовами, такими как обеспечение безопасности персональных данных [4], необходимость обучения педагогов новым технологиям и технические ограничения инфраструктуры. Однако, развитие ИИ, Big Data и облачных технологий открывает перспективы для более эффективного сопровождения ИОТ.

Цифровые инструменты позволяют существенно повысить качество и персонализацию образовательного процесса через построение и сопровождение индивидуальных образовательных траекторий. Использование адаптивных платформ, рекомендательных систем и интеллектуальных помощников обеспечивает гибкость, мотивацию и адаптацию к меняющимся требованиям профессионального рынка. Несмотря на существующие вызовы, перспектива масштабного внедрения таких технологий в образовательную практику выглядит весьма перспективной и соответствует стратегическим целям цифровой трансформации образования.

#### Список использованных источников

1. Карданова Е. Г., Марченко А. В. Цифровые технологии в персонализированном обучении: адаптивные платформы и рекомендательные системы // Journal of Educational Technology & Society. 2020. Т. 23. № 4. С. 45–59.
2. Ким Дж., Парк Х. Искусственный интеллект в образовании: обзор // Frontiers in Education. 2021. Т. 6. № 679484. DOI: 10.3389/educ.2021.679484.
3. Иванова А. В., Петров С. Ю. Современные цифровые платформы для персонализированного обучения // Вестник информационных технологий. 2021. Т. 27. № 3. С. 45–55.
4. Козлов Д. С., Михайлова О. В. Рекомендательные системы в электронном обучении: тенденции и перспективы // Журнал цифровой трансформации образования. 2020. Т. 12. № 2. С. 77–88.
5. Федорова Н. Ю., Николаев П. В. Цифровые профили обучающихся как инструмент персонализации образовательного процесса // Педагогические науки. 2021. № 6. С. 112–120.

*Статья представлена научным руководителем, доцентом кафедры ИУС СПбГУТ, кандидатом технических наук Раковским О. В.*

УДК 004.912

Д. В. Сидоров (студент группы ИКПИ-392м, СПбГУТ), [sid.dan@sut.ru](mailto:sid.dan@sut.ru)

## ОЦЕНКА МАЛЫХ ЯЗЫКОВЫХ МОДЕЛЕЙ ПРИ ВЗАИМОДЕЙСТВИИ С MODEL CONTEXT PROTOCOL В ЛОКАЛЬНЫХ СИСТЕМАХ

*В статье рассматривается эффективность применения малых языковых моделей (LLM) в задачах взаимодействия с внешними инструментами через протокол Model Context Protocol (MCP) в условиях локального исполнения. Особое внимание уделено архитектуре и ресурсным ограничениям малых LLM, их применению в системах с ограниченными вычислительными возможностями, а также возможностям подключения инструментов MCP для расширения функциональности. Проведен анализ точности, скорости работы и потребления ресурсов моделей при использовании различных MCP-серверов. На основе экспериментальных данных предлагается набор критериев для оценки производительности малых LLM в таких сценариях.*

*малые языковые модели, LLM, Model Context Protocol, локальные системы, производительность, оценка, внешние инструменты*

Языковые модели стали неотъемлемым компонентом современных систем искусственного интеллекта. Однако большая часть исследований и внедрений связана с крупными LLM, требующими облачных вычислений. Малые языковые модели открывают возможность локального исполнения — на персональных ПК, мобильных и встраиваемых устройствах, но ограничены в знаниях и вычислительных ресурсах. Для компенсации этих ограничений применяется подключение внешних источников данных, в частности, через протокол Model Context Protocol (MCP).

Цель данной работы — оценить, насколько эффективны малые LLM при локальном развертывании в задачах, требующих привлечения внешних данных, а также насколько MCP способен компенсировать архитектурные и вычислительные ограничения таких моделей.

### Архитектура и роль MCP

Малые LLM обычно включают от 0.5 до 13 млрд параметров. Благодаря компактности, они могут запускаться локально, но имеют ограниченный контекст, объем памяти и не способны хранить все необходимые знания [1].

Малые и большие LLM основаны на архитектуре трансформеров, но различаются по количеству параметров и, соответственно, по требованиям

к вычислительным ресурсам. Большие модели, такие как GPT-3 (175 млрд параметров), требуют значительных ресурсов для инференса и обычно развертываются в облаке. Малые модели, например, LLaMA-7B, могут работать на потребительских устройствах с ограниченными ресурсами. Таблица 1 обобщает ключевые различия между большими и малыми LLM.

ТАБЛИЦА 1. Сравнение больших и малых языковых моделей

| Критерий                      | Большие LLM                                                                      | Малые LLM                                                                                         |
|-------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Пример масштаба модели        | Сотни млрд параметров (GPT-3, PaLM)                                              | Несколько млрд параметров (LLaMA-7B, Mistral-7B)                                                  |
| Требования к оборудованию     | Много GPU, >50 ГБ RAM (облачный сервер)                                          | 1 GPU или CPU, 8–16 ГБ RAM (персональное устройство)                                              |
| Качество и возможности        | Высокое качество, широкие знания, сложные рассуждения (эмерджентные способности) | Умеренное качество, ограниченные знания; конкурентны на узких задачах после донастройки           |
| Задержка ответа               | Выше (учитывая сетевой доступ к API и объем модели)                              | Ниже (работа локально, модель компактна)                                                          |
| Конфиденциальность и контроль | Данные уходят в облако (риски для приватности)                                   | Данные обрабатываются локально (полный контроль, соответствие требованиям безопасности)           |
| Стоимость использования       | Требует оплаты API или серверов; дорого в обучении                               | Однократное развертывание; может работать бесплатно локально (дешевле в долгосрочной перспективе) |

Как видно из табл. 1, крупные модели превосходят компактные по универсальности и, очевидно, выбор между большой и малой моделью зависит от конкретных требований задачи, включая доступность ресурсов, требования к конфиденциальности и необходимый уровень точности.

Протокол MCP (Model Context Protocol) разработан для того, чтобы предоставить языковой модели интерфейс к внешним источникам данных: поисковым системам, базам знаний, API, SQL-базам и т.д. Пример: если модель не знает свежих фактов (например, кто президент США на 2025 год), она может отправить запрос MCP-серверу, который вернет актуальный ответ.

Как показано в [2], МСР может быть использован и малыми LLM для существенного повышения их эффективности, особенно в задачах поиска и фактической проверки.

#### Эксперименты и оценка

Луо и соавт. в [2] сравнили четыре МСР-сервера, подключаемых к малым LLM, по следующим параметрам:

- точность ответа (% правильных);
- время отклика (в секундах);
- количество использованных токенов.

ТАБЛИЦА 1 – Результаты сравнения МСР-серверов

| МСР-инструмент    | Точность | Время (сек) | Токенов (средн.) |
|-------------------|----------|-------------|------------------|
| Bing Web Search   | 64 %     | 14          | 285              |
| Brave Search      | 47 %     | 14          | 301              |
| DuckDuckGo Search | 14 %     | 64          | 620              |
| Exa Search        | 15 %     | 231         | 700              |

Как видно, Bing и Brave обеспечивают лучшее соотношение между точностью и скоростью. Более того, в некоторых тестах Bing дал ответы, сравнимые с облачными LLM [2].

### Ограничения и особенности

Несмотря на преимущества, малые модели с МСР демонстрируют и ряд недостатков:

- Ошибки формулировки запроса – модель неправильно формирует МСР-запрос, особенно если нет fine-tuning.
- Сложности с интерпретацией результатов – модель получает результат, но не может его адекватно интерпретировать.
- Рост времени ответа – МСР-интеграция увеличивает общее время генерации.

Тем не менее, при грамотной реализации (например, добавлении промежуточной логики фильтрации и подготовки данных), эффективность возрастает.

## **Применение в локальных и ограниченных средах**

Исследование [3] показало, что даже на ограниченных устройствах (например, Magic Leap 2, Apple Vision Pro) малые модели с интеграцией МСР демонстрируют стабильную работу при относительно низком энергопотреблении.

Для многих реальных сценариев – от справочных систем до офлайн-помощников – это может стать решением, обеспечивающим и приватность, и функциональность.

## **Практический пример – медицинские записи**

В [4] описано использование малой модели (LLaMA 7B) для анализа ЕНР (электронных медицинских карт). Благодаря предварительной обработке (регулярные выражения, фильтрация), даже небольшая модель могла классифицировать записи с точностью выше 85%.

МСР-интеграция позволила модели получать дополнительные сведения из структурированных источников (списки диагнозов, протоколы), увеличивая полноту анализа.

## **Объективная оценка – платформа UltraEval**

В [5] представлена платформа UltraEval, позволяющая тестировать модели на разных задачах с применением внешних инструментов. Это облегчает мета-анализ: какие инструменты лучше подходят малым моделям, где они «проседают», какие настройки оптимальны.

В то же время эффективность напрямую зависит от качества реализации МСР, корректности взаимодействия, а также уровня настройки модели. При соблюдении этих условий можно добиться высоких результатов даже при локальном запуске модели с 7 млрд параметров.

## **Перспективы и ограничения МСР в разных отраслях**

Протокол Model Context Protocol (МСР) представляет собой универсальный механизм подключения внешних источников информации к языковым моделям, что делает его особенно перспективным в прикладных отраслях, требующих доступа к актуальным или структурированным данным. Ниже рассмотрим примеры отраслей, где интеграция МСР с малыми LLM может существенно повысить качество и применимость решений.

### **1. Медицина.**

В медицинских информационных системах высока потребность в соблюдении конфиденциальности. Малые модели, обученные на локальных данных и дополненные МСР-доступом к клиническим справочникам (например, ICD-10, фармакопеям, протоколам лечения), могут служить инструментами поддержки принятия решений на местах. Такие модели не передают персональные данные за пределы системы и позволяют врачам получать рекомендации на основе локальных контекстов. Однако здесь необходимо учитывать требования к аудиту доступа и верификации источников МСР, так как ошибка может повлечь за собой медицинские риски [4].

## 2. Образование.

В обучающих системах с адаптивным контентом малые LLM с доступом к образовательным МСР (например, учебным базам данных, репозиториям заданий, онлайн-энциклопедиям) могут динамически формировать задания и проверять ответы студентов. Работа [1] уже показывает эффективность подобных систем в игровых образовательных средах. Однако в массовом применении может возникать проблема стандартизации результатов и необходимость согласования МСР-источников с официальными программами.

## 3. Юридическая и нормативная сфера.

Языковые модели применимы для анализа контрактов, нормативных актов, судебной практики. Малые LLM с доступом к МСР-репозиториям законодательства могут использоваться как помощники юристов в локальных системах. Здесь МСР может обеспечить оперативный доступ к действующим редакциям документов. Основное ограничение – необходимость обеспечения актуальности и синхронизации МСР с правовыми базами (например, «Консультант+», «Гарант»).

## 4. Документооборот и корпоративные ИТ-системы.

В системах внутреннего документооборота LLM с МСР могут выполнять функции автоматической классификации, заполнения шаблонов, поиска документов. Преимущество здесь – возможность доступа к внутренним базам данных предприятия без выхода в интернет. Ограничения связаны с разграничением прав доступа и необходимостью поддержки специфических форматов корпоративных данных.

## 5. Индустриальные системы и IoT.

В рамках промышленного Интернета вещей (Industrial IoT) малые модели могут использовать МСР для доступа к телеметрии, журналам событий

и технической документации. Это позволяет реализовать автономных ассистентов для операторов, обслуживающих промышленное оборудование. При этом МСР должен обеспечивать устойчивую работу при нестабильном соединении и иметь защищенный протокол доступа.

Таким образом, потенциал применения МСР в связке с малыми LLM крайне широк. Однако эффективность зависит от качества и надежности подключаемых источников, обеспечения безопасности доступа и согласования интерфейсов МСР с особенностями конкретной предметной области. Перспективы масштабного внедрения МСР-поддержки в локальные LLM-решения будут определяться тем, насколько просто и прозрачно организации смогут включать внешние знания в свои автономные интеллектуальные системы.

Малые языковые модели, интегрированные с МСР-инструментами, могут успешно решать задачи, ранее доступные лишь крупным LLM, особенно в случаях, когда критичны локальность исполнения, защита данных и ограниченные вычислительные ресурсы. Их использование позволяет реализовать интеллектуальные функции на устройствах без подключения к облаку, что открывает возможности для автономных систем поддержки принятия решений в медицине, образовании, промышленности и корпоративной ИТ-инфраструктуре.

Исследования показывают, что правильная организация доступа к внешним источникам через МСР способна компенсировать архитектурные и информационные ограничения малых моделей. При этом продуктивность системы зависит не только от качества самой LLM, но и от корректности реализации МСР-интерфейсов, надежности подключаемых источников, скорости отклика инструментов и синхронизации данных.

Кроме того, в современных условиях, когда растет внимание к приватности, затратам на инфраструктуру и прозрачности ИИ-систем, использование локальных LLM с модульной связкой через МСР может стать устойчивой альтернативой централизованным облачным решениям. Такой подход позволяет реализовать гибкие архитектуры: легкие модели обрабатывают локальные задачи, подключаясь к инструментам при необходимости, а в сложных случаях возможна интеграция с удаленными сервисами – с возможностью гибкой конфигурации политики доступа.

Важно также отметить потенциал развития МСР как стандарта: расширение числа поддерживаемых инструментов, унификация протоколов, сни-



жение задержек и добавление механизмов безопасности будут способствовать более широкому внедрению таких связей в практику. С учетом бурного роста числа малых и специализированных моделей, а также появления устройств с все более высокими возможностями (например, носимые системы XR, edge-серверы), подход с использованием LLM + MCP может стать основой для целого класса «гибридных» интеллектуальных решений следующего поколения.

Таким образом, малые языковые модели в связке с MCP-инфраструктурой представляют собой не просто техническую компромиссную альтернативу крупным LLM, а полноценный архитектурный подход для построения локально-ориентированных и адаптивных интеллектуальных систем.

#### Список использованных источников

1. Andrés Isaza-Giraldo, Paulo Bala, Lucas Pereira. Meta-Evaluating Local LLMs: Rethinking Performance Metrics for Serious Games // arXiv:2504.12333 [сайт]. 2025. URL: <https://arxiv.org/abs/2504.12333> (дата обращения 30.04.2025).
2. Zhiling Luo, Xiaorong Shi, Xuanrui Lin, Jinyang Gao. Evaluation Report on MCP Servers // arXiv:2504.11094 [сайт]. 2025. URL: <https://arxiv.org/abs/2504.11094> (дата обращения 30.04.2025).
3. Dawar Khan, Xinyu Liu, Omar Mena, Donggang Jia, Alexandre Kouyoumdjian, Ivan Viola. LoXR: Performance Evaluation of Locally Executing LLMs on XR Devices // arXiv:2502.15761 [сайт]. 2025. URL: <https://arxiv.org/abs/2502.15761> (дата обращения 30.04.2025).
4. Yixiang Qu, Yifan Dai, Shilin Yu, Pradham Tanikella, Travis Schrank, Trevor Hackman, Didong Li, Di Wu. A Novel Compact LLM Framework for Local, High-Privacy EHR Data Applications // arXiv:2412.02868 [сайт]. 2024. URL: <https://arxiv.org/abs/2412.02868> (дата обращения 30.04.2025).
5. Chaoqun He, Renjie Luo, Shengding Hu, Yuanqian Zhao, Jie Zhou, Hanghao Wu, Jiajie Zhang, Xu Han, Zhiyuan Liu, Maosong Sun. UltraEval: A Lightweight Platform for Flexible and Comprehensive Evaluation for LLMs // arXiv:2404.07584 [сайт]. 2024. URL: <https://arxiv.org/abs/2404.07584> (дата обращения: 30.04.2025).

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Белой Т. И.*

УДК 004.738.5

К. А. Филиппов (студент группы ИКПИ-34, СПбГУТ), [filippov.ka@sut.ru](mailto:filippov.ka@sut.ru)

## СМАРТ-КОНТРАКТЫ: ПРИМЕНЕНИЕ И ВЫЗОВЫ В РЕАЛЬНЫХ СЦЕНАРИЯХ

*Смарт-контракты становятся ключевым элементом цифровой экономики благодаря своей способности автоматизировать соглашения без посредников, снижая затраты и повышая надежность сделок. Их внедрение в такие сферы, как финансы (DeFi), логистика и управление цифровыми активами, демонстрирует растущий спрос на децентрализованные решения. Однако, несмотря на преимущества – такие как прозрачность и неизменность данных – технология сталкивается с вызовами: уязвимости в коде (например, reentrancy-атаки), регуляторная неопределенность и проблемы масштабируемости. Развитие инструментов формальной верификации и гибридных подходов может стать решением для mass-adoption смарт-контрактов в реальных сценариях.*

*смарт-контракты, блокчейн, DAO, Ethereum, цифровые активы*

Смарт-контракты стали технологическим прорывом в цифровой экономике, предлагая новый уровень автоматизации бизнес-процессов. Концепция, впервые предложенная Ником Сабо в 1994 году [1], реализовалась лишь с появлением блокчейна Ethereum в 2015 году [2]. Сегодня рынок смарт-контрактов демонстрирует экспоненциальный рост: по данным ЦБ РФ, за период с января 2019 года по март 2022 года (когда наблюдалось пиковое значение Total value locked (TVL)) капитализация DeFi возросла с 1 до 77 млрд долл. США [3].

Как отмечает Старк [4], термин «смарт-контракт» используется в двух основных значениях:

1. Операционное – программные агенты (часто на распределенном реестре), выполняющие обязательства и управляющие активами. Эти системы иногда называют «smart contract code».

2. Юридическое – программная реализация правовых договоров. Такие случаи Старк обозначает как «smart legal contracts».

С технической точки зрения, смарт-контракт представляет собой сложную программную структуру, состоящую из нескольких ключевых компонентов. Как показано на рис. 1, архитектура типичного смарт-контракта включает интерфейс взаимодействия (API), который обеспечивает связь с

внешними системами, бизнес-логику, содержащую условия контракта, хранилище данных и механизм исполнения, гарантирующий выполнение прописанных условий.

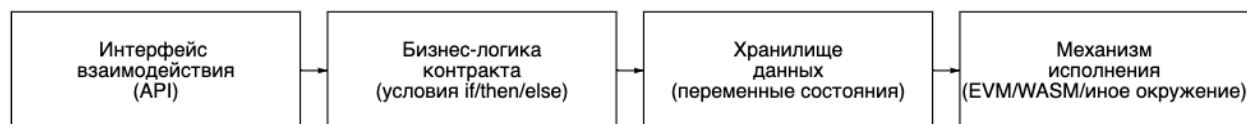


Рис. 1. Архитектура типичного смарт-контракта

На сегодняшний день индустрия предлагает несколько принципиально разных подходов к реализации смарт-контрактов, каждый из которых нашел свою нишу в цифровой экономике. Лидером публичных блокчейнов остается Ethereum с его специализированным языком Solidity, который, несмотря на ограниченную пропускную способность в 15-30 транзакций в секунду и высокую волатильность комиссий, продолжает доминировать благодаря самой развитой экосистеме и поддержке стандартов ERC. Однако, когда речь заходит о корпоративных решениях, многие компании выбирают Hyperledger Fabric с его модульной архитектурой и поддержкой языков общего назначения – Go и Java. Эта платформа демонстрирует впечатляющую производительность до 1000 TPS в частных сетях, что достигается за счет использования механизма ordering service вместо традиционного консенсуса. Особого внимания заслуживает EOSIO с его революционной для 2018 года архитектурой, позволяющей обрабатывать свыше 4000 транзакций в секунду благодаря параллельному исполнению и использованию WebAssembly. Однако за высокую производительность пришлось заплатить децентрализацией и безопасностью – многочисленные инциденты с взломом аккаунтов показали уязвимость системы разрешений. Наглядное сравнение этих трех рассматриваемых платформ приведено в таблице 1.

ТАБЛИЦА 1. Описание различных платформ для смарт-контрактов

| Платформа   | Языки    | TPS  | Стоимость | Безопасность |
|-------------|----------|------|-----------|--------------|
| Ethereum    | Solidity | 15   | Высокая   | Средняя      |
| Hyperledger | Go       | 1000 | Средняя   | Высокая      |
| EOS         | C++      | 4000 | Низкая    | Низкая       |

В финансовом секторе смарт-контракты нашли широкое применение в различных областях. DeFi-протоколы, такие как Aave и Compound, используют их для автоматизации кредитных операций. Децентрализованные биржи (например, Uniswap) применяют смарт-контракты для обеспечения безопасного обмена активами, а стейблкоины (например, DAI) - для поддержания стабильности курса.

Не менее важную роль смарт-контракты играют в логистике. Ярким примером служит система IBM Food Trust, которая использует эту технологию для отслеживания цепочек поставок пищевых продуктов, гарантируя их подлинность и качество на всех этапах движения от производителя к потребителю.

Исследование Clack C. D. [5]. выделяет три основные категории проблем, связанных с использованием смарт-контрактов. Технические сложности включают уязвимости кода (такие как reentrancy и overflow), ограничения производительности и сложность внесения изменений в уже развернутые контракты. Юридические аспекты охватывают вопросы правового статуса, ответственности за ошибки в коде и регуляторные ограничения. Экономические вызовы связаны с волатильностью комиссий, проблемами масштабируемости и высоким порогом входа для новых участников.

Передовые исследования в области смарт-контрактов сегодня сосредоточены на преодолении трех ключевых ограничений: безопасности, масштабируемости и совместимости. В области верификации кода настоящим прорывом стали формальные методы проверки, такие как используемые в Certora и VeriSol, которые позволяют математически доказать отсутствие критических уязвимостей. Не менее важны разработки в области масштабирования – решения второго уровня, в частности Optimistic и ZK-Rollups, уже сегодня демонстрируют возможность увеличения пропускной способности до 2000-5000 TPS при сохранении безопасности базового слоя. Особый интерес представляет работа технического комитета ISO/TC 307, где ведущие эксперты отрасли разрабатывают единые стандарты для обеспечения интероперабельности между разными блокчейн-платформами. Отдельного внимания заслуживают исследования в области постквантовой криптографии – пилотные реализации алгоритмов CRYSTALS-Kyber в сетях Qtum и Algorand открывают путь к созданию смарт-контрактов, устойчивых к атакам квантовых компьютеров. Эти инновации, вместе с развитием специализированных виртуальных машин и аппаратных ускорителей, создают фундамент для следующего поколения смарт-контрактов, способных

обрабатывать сотни тысяч транзакций в секунду при гарантированном уровне безопасности.

Смарт-контракты продолжают активно трансформировать цифровую экономику, открывая новые возможности для автоматизации бизнес-процессов. Однако для достижения массового внедрения предстоит решить комплекс технических, юридических и экономических проблем. Дальнейшее развитие технологии будет связано с повышением уровня безопасности, производительности и созданием четкой регуляторной базы, что позволит полностью раскрыть потенциал этой инновационной технологии.

#### Список используемых источников

1. Szabo N. Smart Contracts: Building Blocks for Digital Markets. 1994. PP. 15.
2. Buterin V. Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform. 2014. PP. 36. URL: <https://ethereum.org/en/whitepaper> (дата обращения 28.04.2025).
3. ЦБ РФ. Обзор финансовых технологий: децентрализованные финансы (DeFi) // Банк России. М., 2023. 7 с. URL: [https://www.cbr.ru/Content/Document/File/141992/report\\_07112022.pdf](https://www.cbr.ru/Content/Document/File/141992/report_07112022.pdf) (дата обращения 28.04.2025).
4. Stark J. Making sense of blockchain smart contracts // CoinDesk. 2016. 12 июня. URL: <https://www.coindesk.com/markets/2016/06/04/making-sense-of-blockchain-smart-contracts> (дата обращения 10.06.2024). PP. 3–4.
5. Clack C.D., Bakshi V.A., Braine L. Smart Contracts: Opportunities and Challenges // arXiv. 2016. arXiv:1608.00771. PP. 25.

*Статья представлена научным руководителем, заведующий кафедрой ВМ СПбГУТ, кандидатом физико-математических наук, доцентом Плотниковым П. В.*

УДК 004.891.3

В. Н. Фирсов (студент группы ИСМ-31з, СПбГУТ) [firsov.vn@sut.ru](mailto:firsov.vn@sut.ru)

## ГИБРИДНЫЙ МЕТОД РАЗМЕТКИ ДАННЫХ С МИКРООБРАТНОЙ СВЯЗЬЮ И ОТЛОЖЕННОЙ ВЕРИФИКАЦИЕЙ НА ПРИМЕРЕ НЕИСПРАВНОСТЕЙ АСИНХРОННЫХ ЭЛЕКТРОДВИГАТЕЛЕЙ

*В статье рассмотрены методы активного обучения и краудсорсинга для оптимизации разметки данных в условиях ограниченного бюджета и времени. Представлена концепция гибридного подхода, сочетающего микрообратную связь и отложенную верификацию. Предложенная адаптивная система обратной связи позволяет моделям машинного обучения эволюционировать, используя пользовательский опыт. Подход универсален и применим в различных сферах, обеспечивая развитие интеллектуальных систем в реальном времени.*

*краудсорсинг, разметка данных, микрообратная связь, отложенная верификация, кластеризация признаков*

В современном мире искусственный интеллект (ИИ) и нейросети стремительно проникают во все сферы жизни. Сегодня даже бытовые устройства оснащаются интеллектуальными системами, а потребность в качественных данных для обучения моделей машинного обучения становится все более острой. В условиях ограниченности ресурсов и высокой стоимости ручной разметки данных разработчики все чаще обращаются к краудсорсингу – привлечению широкой аудитории пользователей к процессу аннотирования данных.

В статье Гилязева Р. А. и Турдакова Д. Ю. «Активное обучение и краудсорсинг: обзор методов оптимизации разметки данных» [1] описано, как методы активного обучения и краудсорсинга эффективно оптимизируют разметку данных, особенно в условиях ограниченного бюджета и времени.

Существуют многочисленные успешные примеры применения краудсорсинга для разметки данных:

- ImageNet – один из крупнейших датасетов для компьютерного зрения, размеченный с помощью платформы Amazon Mechanical Turk. Содержит более 14 миллионов размеченных изображений [2].
- CrowdFlower (ныне Figure Eight) – платформа, которая помогла создать множество размеченных датасетов для NLP задач, включая анализ тональности и категоризацию текста [3].
- Google reCAPTCHA – помимо защиты от ботов, собирает данные для обучения систем компьютерного зрения, используя человеческую помощь в разметке изображений [4].

- Amazon Mechanical Turk – платформа, активно используемая для создания размеченных датасетов в различных областях: от компьютерного зрения до обработки естественного языка [5].
- Labelbox – современная платформа, позволяющая командам совместно размечать данные для машинного обучения, включая изображения, текст и видео [6].
- SuperAnnotate – платформа для совместной разметки данных, особенно популярная в компьютерном зрении и задачах обнаружения объектов [7].
- VGGFace – датасет для распознавания лиц, созданный с помощью краудсорсинга для сбора и разметки изображений знаменитостей [8].
- Arpen – компания, предоставляющая услуги по разметке данных с помощью краудсорсинговых команд для различных задач машинного обучения [9].

В некоторых случаях участники краудсорсинга давали быстрый ответ, порой в полуигровом режиме, иногда даже не догадываясь что участвуют в разметке датасетов [2, 3, 4, 5, 6, 7]. Такой способ обратной связи назовем микрообратная связь.

В других случаях наоборот, требовалось некоторое время для тщательного изучения и уточнение данных. Данный способ назовем отложенной верификацией (данных) [1, 8, 9].

В данной статье мы предлагаем концепцию нового гибридного подхода – адаптивной системы с микрообратной связью и отложенной верификацией. Этот подход позволяет эффективно собирать и использовать обратную связь от пользователей для обучения и корректировки моделей ИИ.

Рассмотрим более подробно возможность внедрения нашей концепции на примере системы диагностики асинхронных электродвигателей, предложенной в другой статье автора данной работы [7].

Система диагностики асинхронных электродвигателей реализует принципиально новый подход к машинному обучению, в котором каждый пользователь становится активным участником процесса совершенствования модели. В отличие от традиционных решений, входные данные не просто классифицируются, а строится адаптивная архитектура, способная к обучению на основе взаимодействия с пользователями.

После загрузки пользователем данных фазных токов и паспортных параметров двигателя система проводит спектральный анализ сигналов с помощью дискретного преобразования Фурье. Это позволяет выделить устойчивые гармонические составляющие, отражающие текущее состояние

оборудования. На их основе формируется вектор признаков, который, совместно с параметрами двигателя, поступает в аналитическое ядро системы.

Классификация неисправностей осуществляется не напрямую, а через этап адаптивной кластеризации признаков. Система автоматически соотносит каждый новый вектор с одним из существующих кластеров – групп схожих спектральных паттернов, сформированных в процессе предыдущей диагностики. Важно понимать, что кластеры не являются прямыми аналогами типов неисправностей: они представляют собой типовые спектральные состояния оборудования, среди которых могут существовать различия в степени проявления, условиях эксплуатации или конструктивных особенностях.

На основе принадлежности к кластеру система формирует вероятностное распределение по всем возможным неисправностям, заданным изначально – ведь применяемый метод (гармонический анализ токов) позволяет диагностировать ограниченный, но хорошо изученный перечень дефектов. Пользователю при этом предлагается наиболее вероятный диагноз, сопровождаемый описанием характерных признаков.

Гибридная система обратной связи обеспечивает обучение модели в двух режимах: с использованием микрообратной связи и отложенной верификации. В первом случае пользователь может оперативно ответить похоже ли фактическое поведение двигателя на описанное (да / нет / не знаю). Подтверждение повышает вес предполагаемой неисправности внутри соответствующего кластера, а опровержение – снижает. Также анализируется согласованность пользовательских оценок внутри каждого кластера: если наблюдаются систематические расхождения, система инициирует уточнение кластерной структуры.

Во втором, более надежном режиме, используется отложенная верификация. Если пользователь позднее сообщает фактический результат осмотра или ремонта, такая информация получает статус эталонной. Она используется для переобучения модели и уточнения границ кластеров. Особенно тщательно обрабатываются случаи, где предварительный диагноз не совпал с подтвержденным – это позволяет выявлять ранее неучтенные спектральные различия.

Кластерная структура системы эволюционирует на протяжении всего жизненного цикла модели. Система способна выделять новые подгруппы внутри известных неисправностей – например, различать вариации одного и того же дефекта в зависимости от мощности двигателя, режимов работы или условий эксплуатации.



Таким образом, данная система реализует адаптивный диагностический контур, где каждый пользовательский случай становится вкладом в уточнение модели. Благодаря гибридной обратной связи и динамической кластеризации, система не просто применяет знания, но и систематически уточняет их, превращаясь в надежный инструмент технической диагностики с возможностью эволюции без участия экспертов по данным.

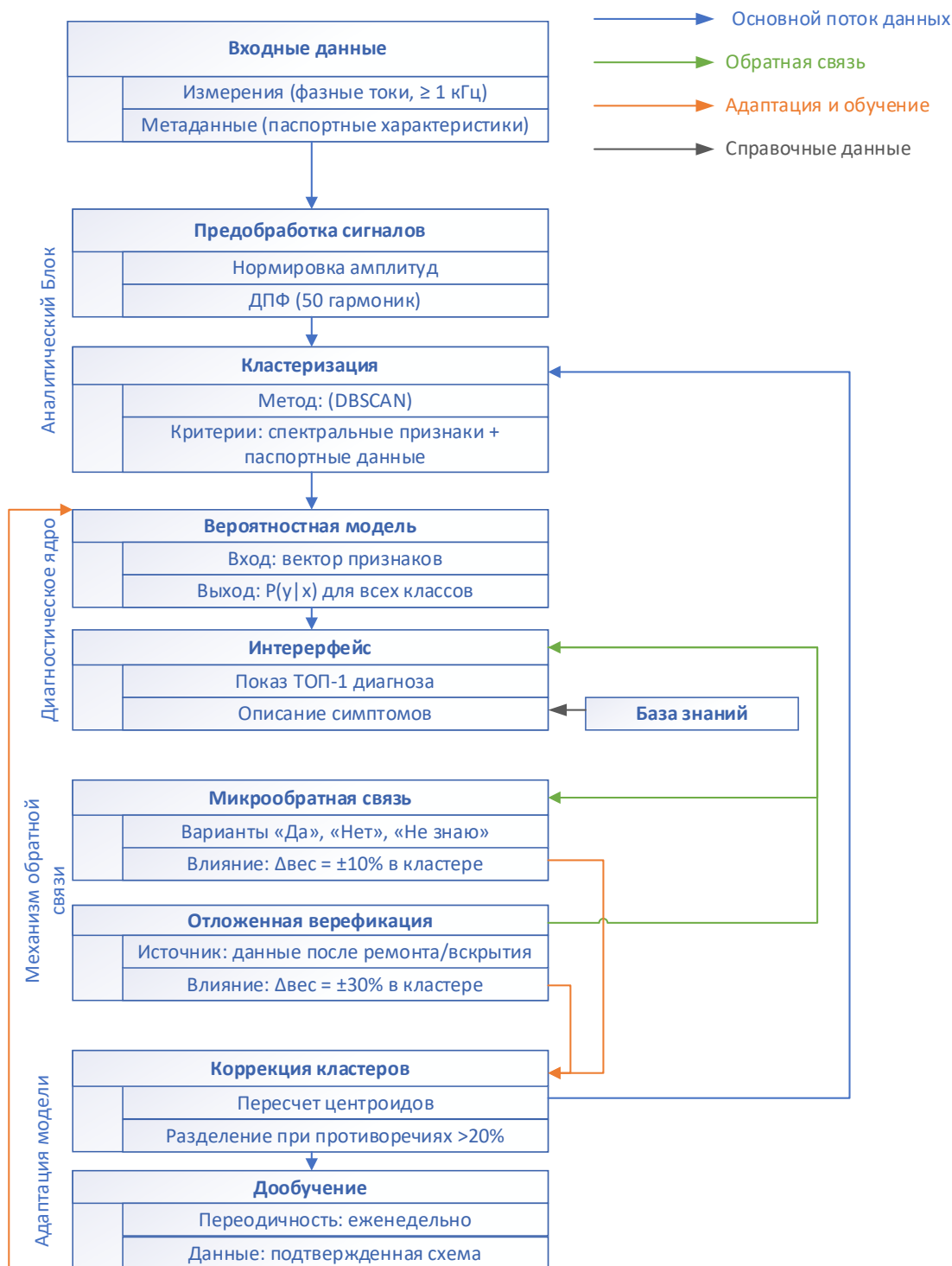


Рис. 1. Структурная схема системы кластерной диагностики

Предложенная концепция гибридной системы с микрообратной связью и отложенной верификацией представляет собой качественно новый подход к обучению и адаптации моделей ИИ. Вместо традиционной разметки вручную на отдельных этапах, обратная связь от пользователя встраивается непосредственно в работу приложения. Пользователь становится соавтором знаний, не покидая привычного интерфейса. Быстрые отклики формируют поведенческую статистику модели, а позднее, более точная верификация позволяет корректировать выводы с высокой степенью достоверности.

Универсальность подхода делает его применимым в любых сферах, где возможна формализация экспертного суждения: от медицины до инженерии и образования. Такая архитектура не только снижает зависимость от заранее размеченных датасетов, но и позволяет системам развиваться в реальном времени, подстраиваясь под специфику конкретной области. Это открывает путь к созданию по-настоящему адаптивных, человеко-центричных интеллектуальных систем.

#### Список используемых источников

1. Гилязов Р. А., Турдаков Д. Ю. Активное обучение и краудсорсинг: обзор методов оптимизации разметки данных // Труды ИСП РАН. 2018. №2. URL: <https://cyberleninka.ru/article/n/aktivnoe-obuchenie-i-kraudsorsing-obzor-metodov-optimizatsii-razmetki-dannyh> (дата обращения 18.04.2025).
2. ImageNet. URL: <https://www.image-net.org/> (дата обращения 18.04.2025).
3. Figure Eight. URL: <https://www.figure-eight.com/> (дата обращения 18.04.2025).
4. Google reCAPTCHA. URL: <https://www.google.com/recaptcha/about/> (дата обращения 18.04.2025).
5. Amazon Mechanical Turk. URL: <https://www.mturk.com/> (дата обращения 18.04.2025).
6. Labelbox. URL: <https://labelbox.com/> (дата обращения 18.04.2025).
7. SuperAnnotate. URL: <https://superannotate.com/> (дата обращения: 18.04.2025).
- VGG Face Dataset / Visual Geometry Group, University of Oxford. URL: [https://www.robots.ox.ac.uk/~vgg/data/vgg\\_face/](https://www.robots.ox.ac.uk/~vgg/data/vgg_face/) (дата обращения 18.04.2025).
8. Appen. URL: <https://www.appen.com/> (дата обращения 18.04.2025).
9. Фирсов В. Н. Разработка метода детектирования неисправностей асинхронных электродвигателей с помощью машинного обучения // Сборник лучших докладов конференции ПКМ-2024. Том 2. СПб.: СПбГУТ, 2025. С. 57-60. URL: [https://pkm.sut.ru/documents/Сборник\\_лучших\\_докладов%20ПКМ-2024\\_том\\_2.pdf](https://pkm.sut.ru/documents/Сборник_лучших_докладов%20ПКМ-2024_том_2.pdf) (дата обращения 18.04.2025).

*Статья представлена научным руководителем, доктором технических наук, профессором Беловым М. П.*

УДК 621.396.99

И. А. Чухарев (студент группы ИСТ-311м, СПбГУТ), [chukcharev.ia@sut.ru](mailto:chukcharev.ia@sut.ru)

## АНАЛИЗ ОСНОВНЫХ МЕТОДОВ ПРЕДОБРАБОТКИ ОБРАЗОВАТЕЛЬНЫХ ДАННЫХ

*В статье рассматриваются этапы предварительной обработки образовательных данных, включая очистку, преобразование и интеграцию информации. Описаны методы работы с пропущенными значениями, аномалиями и дубликатами, а также способы нормализации и кодирования данных. Представленные подходы позволяют повысить качество аналитики, выявлять закономерности в успеваемости, оценивать влияние различных факторов на обучение и оптимизировать управленческие решения в сфере образования.*

*предобработка, образовательный процесс, этапы предобработки, методы обработки данных*

Работа с образовательными данными требует тщательной предварительной обработки для обеспечения их качества и пригодности для анализа. Первым этапом становится обработка пропущенных значений, где применяются различные стратегии в зависимости от природы пропусков.

Важным этапом является преобразование типов данных для обеспечения их совместимости с аналитическими алгоритмами. Даты приводятся к единому формату, текстовые поля категориальных переменных кодируются числовыми значениями, а непрерывные переменные нормализуются для устранения эффекта разных шкал измерения. Особое внимание уделяется выявлению и обработке дубликатов, которые могут возникать при объединении данных из разных источников.

Ключевым аспектом предобработки также является работа с выбросами и аномальными значениями, которые могут существенно искажать результаты анализа. Для их обработки применяются статистические методы и алгоритмы машинного обучения, позволяющие выявлять и корректировать нехарактерные данные. Особенно важно это при анализе образовательных показателей, где резкие отклонения могут свидетельствовать как об ошибках в данных, так и о реальных кейсах, требующих особого внимания.

Дополнительным этапом подготовки данных выступает их обогащение и создание производных признаков, которые могут повысить информатив-

ность анализа [1]. В образовательной сфере это может включать расчет новых метрик (например, динамики успеваемости, коэффициентов вовлеченности) или агрегацию данных по различным временным периодам и группам учащихся. Такой подход позволяет раскрыть дополнительные закономерности и сделать аналитические выводы более содержательными и полезными для принятия управленческих решений. Основные этапы предобработки данных представлены на рисунке 1.

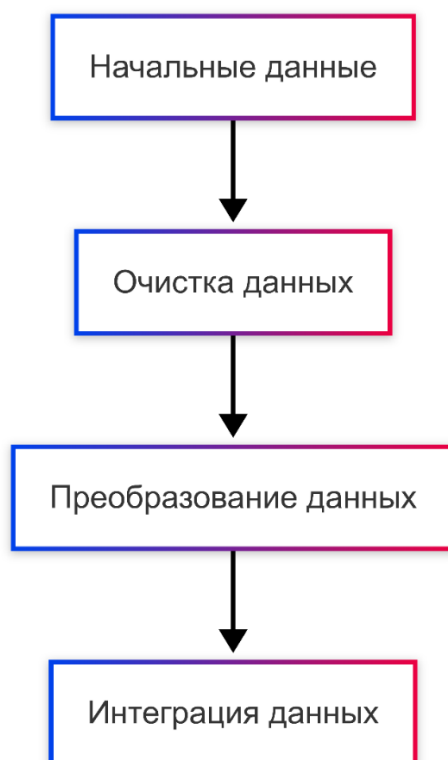


Рис. 1. Основные этапы предобработки данных

Предварительная обработка данных представляет собой многоэтапный процесс, направленный на подготовку исходной информации к анализу. Первоначальный этап очистки данных включает комплексную работу с неполными и некорректными записями. Особое внимание уделяется обработке пропущенных значений, где применяются различные стратегии заполнения в зависимости от природы данных и предметной области. Параллельно выполняется выявление и коррекция аномальных значений, которые могут существенно исказить результаты анализа. Завершающим элементом этапа очистки становится стандартизация форматов представления данных, обеспечивающая единообразие всех записей в наборе. Методы обработки пропущенных значений представлены в таблице 1.

ТАБЛИЦА 1. Методы обработки пропущенных значений

| Метод обработки                        | Описание                                                                                          | Применение                                                        |
|----------------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Удаление записей                       | Полное исключение строк с пропусками из набора данных                                             | Когда пропуски случайны и составляют <5% данных                   |
| Заполнение средним/медианным значением | Замена пропусков средним арифметическим или медианным значением признака                          | Для числовых переменных с нормальным/асимметричным распределением |
| Использование моделей предсказания     | Прогнозирование пропущенных значений на основе других переменных (регрессия, k-NN, Random Forest) | Когда пропуски коррелируют с другими признаками                   |
| Создание категории "Неизвестно"        | Замена пропусков отдельным значением для категориальных переменных                                | Для номинальных и порядковых категориальных данных                |

На этапе преобразования данных осуществляется приведение информации к виду, пригодному для последующего анализа. Это включает изменение типов переменных, когда качественные характеристики преобразуются в количественные показатели, а разнородные данные приводятся к единому формату. Важным аспектом является нормализация шкал измерения, позволяющая сравнивать показатели, изначально выраженные в разных единицах или диапазонах значений. Данная процедура особенно критична при использовании алгоритмов машинного обучения, чувствительных к масштабу входных данных.

Финальный этап интеграции данных направлен на создание целостного аналитического пространства. Процесс начинается с объединения таблиц из различных источников, что требует тщательного сопоставления полей и идентификаторов. Особую сложность представляет разрешение конфликтов данных, возникающих при несовпадении информации из разных систем [2]. Результатом этапа интеграции становится формирование единой структуры хранения, обеспечивающей согласованность данных, быстрый доступ и возможность последующего масштабирования системы. Все этапы предобработки взаимосвязаны и требуют последовательного выполнения для обеспечения качества итоговых аналитических результатов.

Предварительная обработка данных – критически важный этап аналитического процесса, особенно в образовательной сфере, где данные часто

неструктурированы и содержат множество артефактов. Корректная очистка, преобразование и интеграция информации позволяют значительно повысить качество моделей и достоверность выводов. Автоматизация этих процессов с использованием современных инструментов (Python, R, специализированные ETL-системы) способна ускорить подготовку данных и минимизировать ошибки, связанные с ручной обработкой [3].

Дальнейшие исследования в этой области могут быть направлены на разработку адаптивных алгоритмов предобработки, учитывающих специфику образовательных данных, таких как динамические изменения учебных планов или нестандартные форматы оценивания знаний.

#### **Список используемых источников**

1. Интеллектуальные сенсорные системы / Под ред. Дж. К. М. Мейджера. М.: Техносфера, 2012. 464 с.
2. Труды ИСА РАН: Параллельные вычисления. Математическое моделирование. Интеллектуальные системы и технологии. Методы и модели в экономике. Информатика сообществ. Методологические проблемы системного анализа / Под ред. С. В. Емельянова. М.: Красанд, 2013. 144 с.
3. Антамошин А. Н. Интеллектуальные системы управления организационно-техническими системами / А. Н. Антамошин, О. В. Близнова, А. В. Бобов и др. М.: ГЛТ, 2016. 160 с.

*Статья представлена научным руководителем, доцентом кафедры ИУС СПбГУТ, кандидатом технических наук Раковским О. В.*

УДК 004.942

О. А. Якубова (студент группы ИКПИ-14, СПбГУТ), [yakubova.aa@sut.ru](mailto:yakubova.aa@sut.ru)

## **РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА МОДЕЛИРОВАНИЯ ГРУППОВОГО ПОВЕДЕНИЯ ПЕРСОНАЛА В ПРОЦЕССЕ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ**

*В настоящей работе рассматривается концепция программного комплекса, позволяющего производить моделирование группового поведения персонала при выполнении технологических заданий с участием операторов и технических средств. Описаны требования к системе, представлен вариант реализации, предложен алгоритм моделирования, включающий такие этапы как инициализация, распределение задач, расчет времени элементарных операций с учетом детерминированных и психосоциальных переменных, оценка эффективности и получение результатов моделирования. Обсуждаются направления улучшения модели и дальнейшего развития данного программного комплекса.*

*имитационное моделирование, человеко-машинные системы, инженерная психология, психосоциальные факторы, автоматизация*

### **Риски при планировании группового поведения персонала**

Групповое поведение персонала можно охарактеризовать как организованные действия людей, объединенных общей целью. Прогнозирование времени выполнения высокотехнологичных процессов в малых группах критически важно для минимизации финансовых и репутационных рисков. Например, задержка подготовки ракеты-носителя из-за нарушения временного регламента может привести к многодневному переносу запуска [1].

При планировании процессов выделяется время, которое они занимают, с учетом дополнительных временных затрат на возникновение непредвиденных ситуаций, но этого не всегда достаточно, так как на фактическое время выполнения операций влияет комплекс факторов стохастической природы, который с трудом поддается детерминированной оценке. На качество и время выполнения задания может влиять рабочий коллектив, его сплоченность, доверие к друг другу и другие общие характеристики, а также индивидуальные особенности каждого участника труда [2, 3].

### **Система моделирования группового поведения**

Для решения данной задачи возможно применение имитационных моделей, учитывающих широкий спектр факторов, которые влияют на временные параметры технологических процессов. Они описывают функционирование систем человек-машина, моделируя взаимодействие между членами команды и техническими средствами. Помимо детерминированных характеристик, в моделях учитываются стохастические элементы, такие как случайные задержки, выход используемого оборудования из строя, вариации в процессах и влияние внешних факторов.

При моделировании группового поведения необходимо использовать методы теории надежности, теории массового обслуживания и инженерной психологии, позволяющие учитывать динамику принятия решений, когнитивные нагрузки и возможные ошибки оператора [4, 5].

### **Концепция программного комплекса моделирования группового поведения**

Разрабатываемая модель предназначена для имитации работы малых групп, выполняющих задачи на нескольких независимых рабочих постах с использованием технического оборудования в замкнутом пространстве. В ходе моделирования состав команды остается неизменным, а последовательность действий заранее определена и регламентирована в пределах заданных ограничений. Каждое действие персонала представляет собой элементарную операцию.

Ключевым отличием данной модели по сравнению с другими цифровыми имитационными моделями является интеграция психологически ориентированных и психосоциальных переменных. Помимо данных об оборудовании, задании и персонале включается также вычисление таких переменных, как состояние напряженности, квалификация, моральные качества отдельных операторов, а также возможные решения экипажа, его спаянность, психосоциальная эффективность и направленность.

На вход подаются следующие данные:

- Персонал: идентифицирующие данные, квалификация, заработная плата, психологические параметры (например, совпадение личных и коллективных целей)
- Оборудование: характеристики надежности, время ремонта, рабочие посты, доступность коммуникаций.
- Задание: параметры времени выполнения (тип, улучшаемость), важность, необходимое оборудование, зависимость от других задач.



• Дополнительные константы и переменные: число экспериментов, длительность рабочего дня, вероятность критических ситуаций/заболеваний, пороговые значения эффективности и морального состояния.

Выходным параметром является время, за которое будут выполнены все операции, но ценность могут представлять и промежуточные состояния персонала, оборудования, выполняемых элементарных операций, привязанные к модельному времени, а также порядок выполнения задания, затраченное время, показатели качества и эффективности.

Для программной реализации имитационной модели отдается предпочтение высокоуровневому языку программирования. Это позволяет не ограничивать функциональность из-за предусмотренных возможностей сторонних средств.

Предполагается трехуровневая архитектура:

- уровень данных – база с информацией о персонале, оборудовании, заданиях и константах;
- логический уровень – алгоритмы расчета времени выполнения операций с использованием методов теории надежности и инженерной психологии;
- уровень представления – графический интерфейс пользователя, обеспечивающий удобную работу с системой.

Пример диаграммы компонентов системы, которая поддерживает такую архитектуру, представлен на рисунке 1.

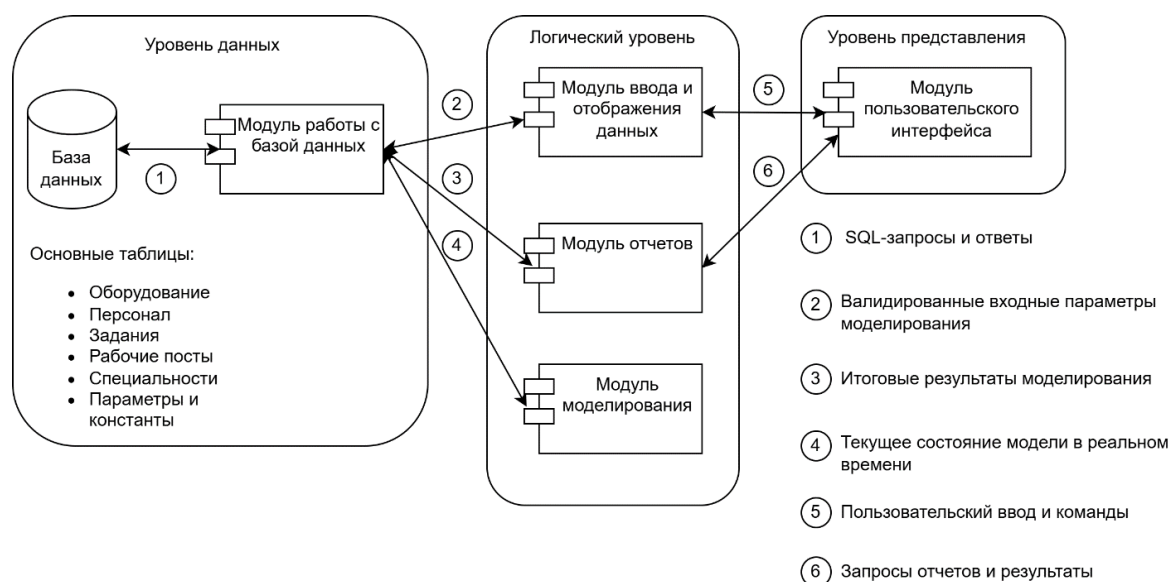


Рис. 1. Диаграмма компонентов системы моделирования

Алгоритм моделирования состоит из следующих стадий:

1. Инициализация: установка модели в начальное состояние;

2. Моделирование группового поведения персонала за день в процессе выполнения задач:

- Формирование списка задач на день, включение в него задач по ремонту оборудования по причине выхода из строя.
- Распределение задач между рабочими группами
- Расчет времени выполнения элементарных операций задания, качества и эффективности на основе зависимостей между переменными системы.
- Определение необходимости поощрения персонала
- Корректировка параметров персонала (заболеваемость, мотивация, дееспособность).
- Оценка эффективности работы персонала

3. Проверка того, выполнены ли все поставленные задачи, иначе переход на следующий день;

4. Вывод итоговых результатов моделирования.

Блок-схема полного алгоритма представлена на рисунке 2.

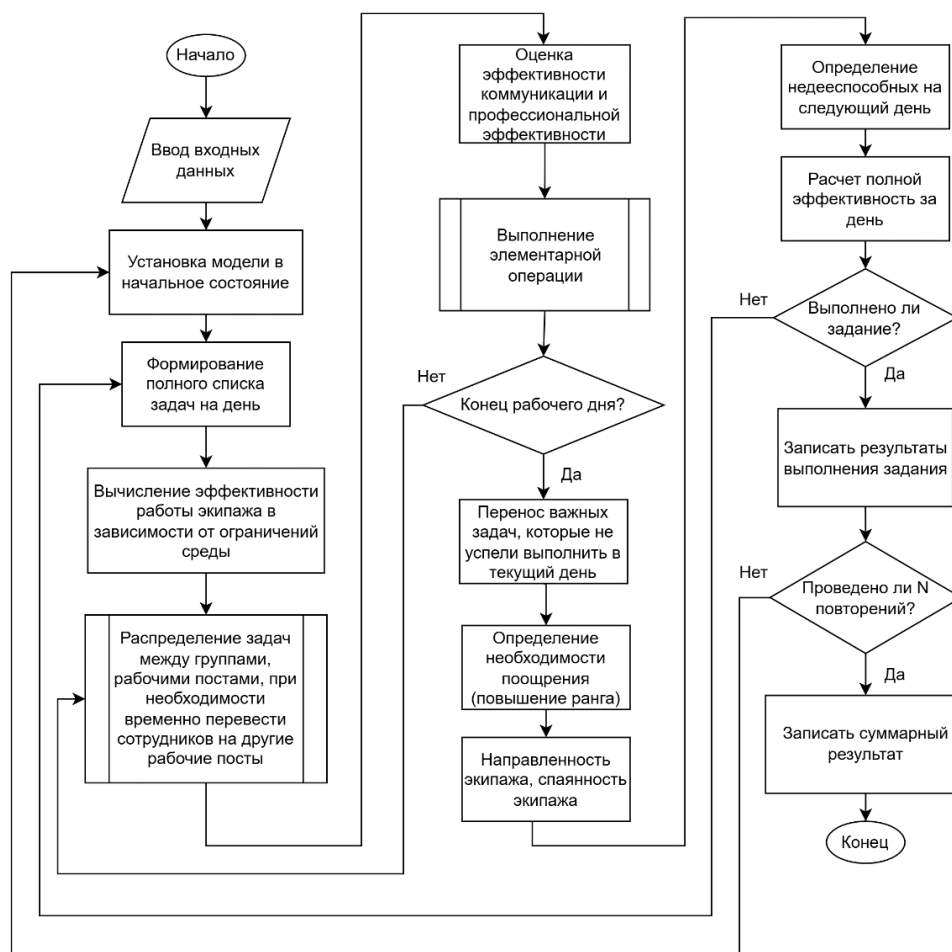


Рис. 2. Блок-схема полного алгоритма моделирования

## Заключение

Система для моделирования группового поведения персонала позволит точнее предсказывать время, используемое для выполнения задания.

Остается актуальным выявление факторов и параметров, описывающих влияние персонала друг на друга в ходе работы. Увеличение точности имитационной модели можно достичь благодаря усовершенствованию формул или внедрению дополнительных переменных, которые могут задавать воздействие лидера на работу всей группы.

## Список используемых источников

1. Вивчарь Р. М., Есипов Е. Н., Кокарев А. С., Решетников Д. В. Имитационное моделирование функционирования системы эксплуатации объектов наземной космической инфраструктуры как инструмент обоснования параметров технического обслуживания // Разработка, испытания и эксплуатация вооружения и военной техники. Военная метрология. С. 87–98.
2. Трусевич Н. Э. Имитационное моделирование организованных конфликтов личность-группа // ISSN 1683-0377. Труды БГТУ. 2012. № 9. Издательское дело и полиграфия. С. 64–71.
3. Zhang J., Qu Q., Chen X.-B. A review on collective behavior modeling and simulation: building a link between cognitive psychology and physical action // Applied Intelligence. 2023. DOI: 10.1007/s10489-023-04924-7.
4. Клейнорк Л. Теория массового обслуживания. Пер. с англ./Пер. И. И. Грушко; ред. В. И. Нейман. М.: Машиностроение, 1979. 432 с.: ил.
5. Zhang G., Yu Z., Li N., et al. Human Behavior Simulation: Objectives, Methodologies, and Open Problems // arXiv preprint arXiv:2412.07788v1. 2024.

*Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Вивчарем Р. М.*

## КИБЕРБЕЗОПАСНОСТЬ

УДК 004.056.5

**К. Е. Алексеева** (магистрант группы ИКТБ-47м, СПбГУТ)

**А. А. Дюсметова** (магистрант группы ИКТБ-47м, СПбГУТ),

[dusmetova.aa@sut.ru](mailto:dusmetova.aa@sut.ru)

**И. Е. Пестов** (к.т.н., доцент кафедры ЗСС СПбГУТ)

### АНАЛИЗ ПОВЕРХНОСТИ АТАКИ В СРЕДЕ ВИРТУАЛИЗАЦИИ ZVIRT

*При использовании виртуальных сред необходимо обеспечивать их безопасность для защиты данных, предотвращения несанкционированного доступа и поддержания стабильной работы информационных систем. Для оценки безопасности виртуальной инфраструктуры в качестве критерия защищенности предлагается рассмотреть поверхность атаки, определяющая количество и сложность возможных векторов атак. Минимизация поверхности атаки позволяет снизить вероятность успешного взлома и повысить общий уровень защищенности системы. Цель данной статьи – анализ поверхности атаки среды виртуализации zVirt, выявление ее уязвимых точек.*

*виртуальная среда, защита, безопасность, критерий защищенности, поверхность атаки*

Виртуализация является значимой составляющей в современных IT-инфраструктурах, способствуя повышению адаптивности, масштабируемости и эффективному использованию вычислительных ресурсов. В связи с широким распространением платформ виртуализации увеличивается и рост киберугроз, нацеленных на них. Одним из популярных решений для виртуализации является KVM (Kernel-based Virtual Machine) – гипервизор, встроенный в ядро Linux, который обеспечивает аппаратную виртуализацию на основе современных процессоров с поддержкой технологий Intel VT-x и AMD-V [1]. С точки зрения безопасности, важной особенностью KVM характеризуется интеграцией с механизмами защиты ядра Linux, такими как

SELinux, AppArmor и seccomp, которые ограничивают права виртуальных машин и предотвращают эскалацию привилегий [2]. Кроме того, использование изолированных процессов и строгого контроля доступа к ресурсам снижает риски атак. В дальнейшем в этой работе будет предложен критерий защищенности, на основе которого будут рассмотрены аспекты безопасности, характерные для всех сред виртуализации, а также выделены особенности, специфичные для zVirt.

### **Среда виртуализации zVirt**

zVirt представляет собой ответвление платформы виртуализации oVirt, адаптированное под специфические требования и условия использования. Недостающий функционал был доработан в системе, в результате чего она стала адаптированной под российские требования и стандарты информационной безопасности [3].

Как говорилось ранее в основе zVirt лежит гипервизор KVM, встроенный в ядро Linux и обеспечивающий аппаратную виртуализацию. В режиме Hosted Engine (рекомендуемый режим работы, также возможно использование в режиме Standalone) менеджер управления работает внутри виртуальной машины, запущенной на вычислительных узлах, которыми он управляет, что устраняет необходимость в отдельном физическом сервере для менеджера, что сокращает физические риски вмешательства в систему [4].

Рассмотрим одну из распространенных типовых схем установки zVirt (рис. 1) [5].

Данная архитектура развертывания zVirt включает несколько гипервизоров, которые могут подключаться к системе хранения данных. Гипервизоры, имеющие доступ к одному и тому же хранилищу, могут быть объединены в кластер, что обеспечивает возможность живой миграции виртуальных машин и поддержку высокой доступности (High Availability). Каждый гипервизор использует одно или несколько сетевых подключений с сегментацией по VLAN, а виртуальные машины подключаются к виртуальным сетевым адаптерам, привязанным к определенным VLAN во внешней сети.

Управляющий сервер виртуализации размещается в виртуальной машине HostedEngine, для запуска которой на одном из гипервизоров требуется специальная настройка. Взаимодействие управляющего сервера с гипервизорами осуществляется через сеть management VLAN. Управление виртуальной инфраструктурой производится через веб-консоль, работающую на управляющем сервере. Для аутентификации и авторизации могут

использоваться как локальные учетные записи и группы, так и внешние системы, такие как LDAP, Active Directory или FreeIPA.

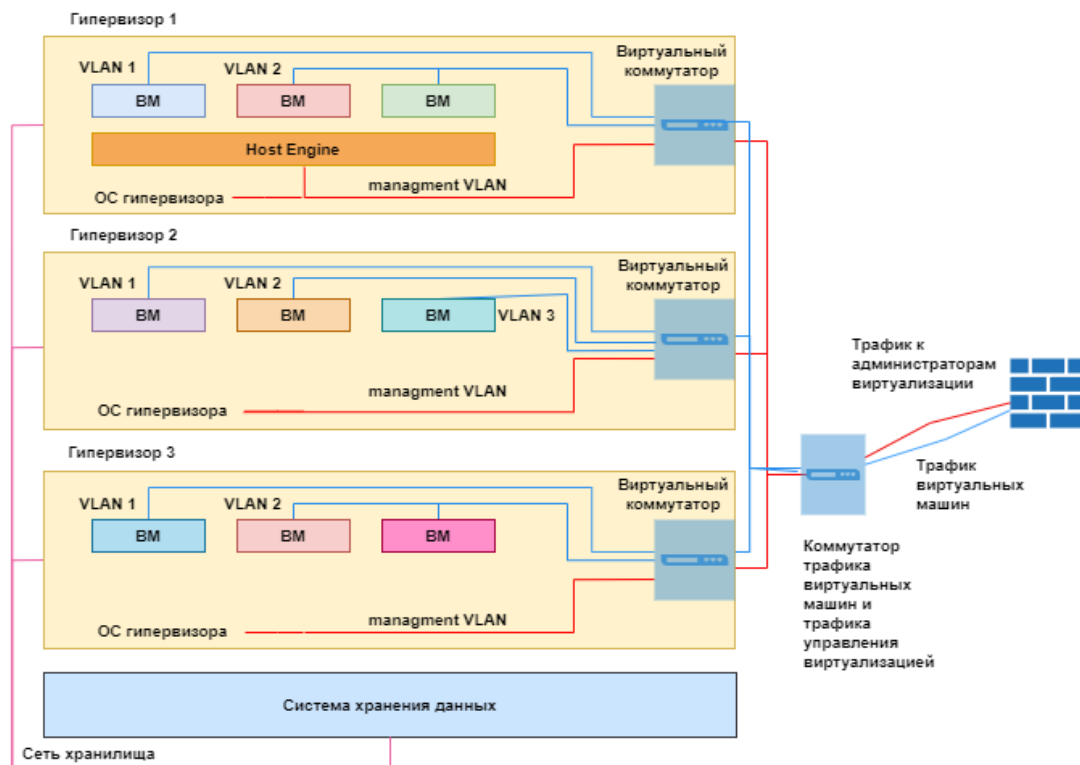


Рис. 1. Архитектурная схема типовой установки zVirt

На хосте с zVirt работает оптимизированная операционная система, установленная со специального дистрибутива, предназначенного для создания хостов виртуализации [5].

Доступ к консолям виртуальных машин возможен через клиента Remote Viewer (virt-viewer) с помощью протоколов SPICE, VNC.

### Поверхность атаки как критерий защищенности среды виртуализации

В информационной безопасности выделение единого критерия безопасности непростая задача, согласно этому критерию, система будет считаться защищенной. Как известно, существуют 3 постулата информационной безопасности: конфиденциальность, целостность, доступность. В связи с чем для комплексной оценки безопасности необходимо учитывать все возможные аспекты безопасности. В качестве данного критерия предлагается рассмотреть поверхность атаки – это совокупность всех возможных точек, через которые злоумышленник может попытаться скомпрометировать систему. В контексте виртуализации поверхность атаки включает гипервизор, механизмы управления, сетевые компоненты и хранилище данных. Методы

оценки элементов поверхности атаки в виртуализированных средах включают анализ архитектуры системы, выявление открытых сервисов и интерфейсов, а также исследование уязвимостей в программном обеспечении. В контексте таких оценок полезным инструментом является матрица MITRE ATT&CK, которая описывает тактики и техники, используемые злоумышленниками в атаках на корпоративную инфраструктуру. Эта матрица включает 14 тактик и более 140 техник, которые могут быть применены для атак на схему установленного zVirt [6].

Рассмотрим элементы, которые могли бы составить поверхность атаки для систем zVirt:

- *Атаки на операционную систему гипервизора и управляющего сервера.* zVirt как и многие другие платформы имеет архитектурную особенность: пользователь с правами root на гипервизоре может получить доступ к дискам виртуальных машин. Это особенно опасно, если данные виртуальных машин не защищены – злоумышленник может просто скопировать или изменить их [7].

ОС гипервизора и управляющего сервера базируется на дистрибутиве Linux общего назначения, имеющем свои потенциальные уязвимости. Linux как общепринятый дистрибутив может содержать уязвимости, не связанные напрямую с виртуализацией, но способные быть использованными для атак на гипервизор.

В zVirt можно установить RPM-пакеты из локальной файловой системы без проверки их цифровой подписи. Это дает злоумышленникам возможность установить вредоносное ПО, если они получают доступ к файловой системе гипервизора [8].

- *Атаки на гипервизор.* По умолчанию в zVirt можно менять конфигурацию загрузки ОС без пароля, что позволяет атакующему модифицировать параметры загрузки ядра. Если гипервизор не защищен должным образом, злоумышленник с физическим доступом может изменить параметры загрузки ОС гипервизора, что позволит ему изменить ядро и получить полный контроль над системой.

- *Атаки на сетевую инфраструктуру и механизмы управления.* Управляющая сеть является критически важной для связи между управляющим сервером и гипервизорами. Управляющая сеть zVirt должна быть изолирована и доступ к ней разрешен только администраторам.

Многие сервисы, которые по умолчанию запускаются на гипервизоре, могут не быть необходимы для его работы, их количество не может быть

сразу точно определено, в связи с чем нельзя предугадать, окажется ли среди них сервис, содержащий уязвимости.

- *Уязвимости механизмов аутентификации и доступа.* Источники учетных записей, такие как Active Directory, FreeIPA, LDAP и другие, играют важную роль в централизованном управлении доступом. Если эти системы будут уязвимы, злоумышленник может получить несанкционированный доступ, используя украденные учетные данные [5-6].

В параметрах SSH-сервера на гипервизорах и сервере управления виртуализацией включена аутентификация через GSSAPI (Generic Security Services API), что может нести уязвимости даже при использовании только локальных учетных записей, в связи с чем аутентификацию с пустым паролем необходимо отключить. Еще одной уязвимостью SSH-сессий является длительность сессии: возможность открытия сессии на неограниченное количество времени создает определенную угрозу.

- *Атаки на виртуальные машины.* Хотя гипервизор играет важную роль в обеспечении изоляции между виртуальными машинами, сами виртуальные машины также могут быть уязвимыми. Если уязвимости в ОС виртуальной машины или в приложениях, работающих внутри нее, не устранены, это может позволить атакующему получить доступ к критически важным данным.

Отсутствие изоляции между виртуальными машинами. Если гипервизор неправильно изолирует виртуальные машины друг от друга, злоумышленник, получивший доступ к одной машине, может попытаться атаковать другие виртуальные машины на том же гипервизоре [5-6].

Уязвимости в сетевых настройках виртуальных машин. Неверно настроенные сетевые интерфейсы внутри виртуальных машин могут стать точками входа для злоумышленников. Важно использовать защитные механизмы, такие как виртуальные межсетевые экраны, чтобы предотвратить несанкционированный доступ.

В заключение, анализ поверхности атаки в среде виртуализации zVirt является важным этапом в обеспечении безопасности корпоративной инфраструктуры. Идентификация и оценка всех возможных точек входа для злоумышленников, включая гипервизор, управляющие сервисы, сетевые компоненты и виртуальные машины, позволяет своевременно выявлять уязвимости и минимизировать риски. Использование методов оценки, таких как анализ архитектуры системы и применение инструментов, например,



матрицы MITRE ATT&CK, способствует более глубокому пониманию угроз и позволяет разрабатывать эффективные стратегии защиты.

#### Список используемых источников

1. Hyper-V или KVM? URL: <https://habr.com/ru/companies/ruvds/articles/308350/> (дата обращения 10.05.2025).
2. Пискурев Н. М. Тонкости развертывания виртуальных машин в среде виртуализации «Брест» // StudNet 2021. № 3.
3. Платформа zVirt: подробное исследование 2024. URL: <https://blog.cortel.cloud/2024/06/07/platforma-zvirt-podrobnoe-issledovanie-2024/> (дата обращения 10.05.2025).
4. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Рязанского Государственного Технического Университета 2020. № 3(88). С. 38-46.
5. Харденинг zVirt: защищаем виртуальную среду от хакеров. URL: <https://habr.com/ru/companies/pt/articles/869836/> (дата обращения 10.05.2025).
6. Руководство по предварительному планированию инфраструктуры. URL: <https://wiki.orionsoft.ru/zvirt/latest/preplanning-guide/> (дата обращения 10.05.2025).
7. Сахаров Д. В., Левин М. В., Фостач Е. С., Виткова Л. А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Научные исследования в космических исследованиях Земли. 2017. Т. 9. № 2. С. 40-46.
8. Иващенко В. В., Газизов А. Р. Угрозы и методы обеспечения информационной безопасности виртуальных сред // Вестник науки. 2018. № 7. Т. 3. С. 88-91.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Пестовым И. Е.*

УДК 004.056

**Р. В. Алехин** (студент магистрант ИКТБ-37м, СПбГУТ)

**А. О. Камалова** (магистрант группы ИКТБ-47м, СПбГУТ), [kamalova.ao@sut.ru](mailto:kamalova.ao@sut.ru)

**И. Е. Пестов** (к.т.н., доцент кафедры ЗСС, СПбГУТ)

**Т. А. Платонова** (студент магистрант ИКТЗ-31м, СПбГУТ)

**Д. Н. Смирнов** (аспирант кафедры ЗСС, гр. 236А-22, СПбГУТ)

## ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ ВРЕМЕНИ ПЕРЕДАЧИ ДАННЫХ В РАЗЛИЧНЫХ ТИПАХ ОБЛАЧНЫХ ИНФРАСТРУКТУР ОТ ВЫБРАННОГО АЛГОРИТМА ШИФРОВАНИЯ

*В этой статье оценивается влияние вычислительной сложности алгоритма шифрования на задержку передачи данных в облачных инфраструктурах, таких как SaaS, PaaS и IaaS. Были проанализированы симметричные (AES) и асимметричные (RSA) методы шифрования, смоделированы вычислительные издержки и количественно оценено влияние на время сквозной передачи.*

*алгоритмы шифрования, облачные технологии, SaaS, PaaS, IaaS, время передачи данных*

Облачные вычисления стали неотъемлемой частью современных IT-инфраструктур [1]. Обеспечение безопасности данных в таких системах требует применения надежных алгоритмов шифрования. Несмотря на то, что облачные сервисы обеспечивают гибкость и масштабируемость, защита данных по-прежнему имеет важное значение [2]. Один из способов защитить данные – использовать шифрование. Однако шифрование приводит к вычислительным затратам, которые могут снизить производительность системы, особенно если рабочие процессы чувствительны к задержкам. Моделируя задержки при шифровании, передаче данных и распределении ресурсов в зависимости от инфраструктуры, можно определить баланс между безопасностью и эффективностью облачных сервисов [3, 4].

### Вычислительная сложность алгоритмов шифрования

Алгоритмы шифрования классифицируются по их временной сложности, которая часто выражается с помощью обозначения Big O.

В симметричном шифровании, например, в AES, используется блочное шифрование с линейной временной сложностью относительно размера данных  $n$ :

$$T_{\text{шифр}}^{\text{AES}} = O(n) \quad (1)$$

В AES-256 каждый 128-битный блок требует 14 циклов подстановки и перестановочности, что обеспечивает эффективную обработку больших массивов данных.

Сложность асимметричного шифрования, например, алгоритма RSA [0, 0], кубически зависит от размера ключа  $k$ , поскольку шифрование предполагает модульное возведение в степень:

$$T_{\text{шифр}}^{\text{RSA}} = O(k^3) \quad (2)$$

Для использования 2048-битного ключа RSA требуются примерно  $2^{30}$  операции для каждого шифрования, что делает алгоритм шифрования более вычислительно сложным по сравнению с AES.

Гибридные системы сочетают два алгоритма шифрования (AES и RSA). Шифрование данных происходит с помощью AES, а защита ключей AES – с помощью RSA:

$$T_{\text{шифр}}^{\text{гибрид}} = O(k^3 + n) \quad (3)$$

Такой вид шифрования обеспечивает баланс между скоростью симметричного шифрования и безопасностью асимметричного обмена ключами.

### Моделирование времени передачи данных

Общее время передачи  $T$  включает время шифрования данных  $T_{\text{ш}}$ , время передачи данных по сети  $T_{\text{п}}$  и время расшифровки данных  $T_{\text{д}}$ :

$$T = T_{\text{ш}} + T_{\text{п}} + T_{\text{д}} \quad (4)$$

Время шифрования  $T_{\text{ш}}$  и дешифрования  $T_{\text{д}}$  можно представить в виде следующих формул:

$$T_{\text{ш}} = \frac{n * C_{\text{ш}}}{S} \quad (5)$$

$$T_{\text{д}} = \frac{n * C_{\text{д}}}{S} \quad (6)$$

где  $C_{\text{ш}}$  и  $C_{\text{д}}$  – количество циклов на байт для шифрования и дешифрования, а  $S$  – скорость процессора (циклов в секунду).

Время передачи  $T_{\text{п}}$  можно представить в виде формулы:

$$T_{\text{п}} = \frac{D_{\text{ш}}}{B} + L \quad (7)$$

где  $D_{\text{ш}}$  – размер зашифрованных данных,  $V$  – пропускная способность, а  $L$  – задержка в сети. RSA увеличивает  $D_{\text{ш}}$  примерно на 256 байт на блок из-за заполнения.

### Параметры для расчета времени передачи данных

- размер данных:  $n = 10$  МБ;
- пропускная способность:  $V = 1$  Гбит/с = 125 МБ/с – типичная пропускная способность для облачных сред;
- задержка в сети:  $L = 10$  мс – значение добавляется ко времени передачи данных;
- скорость процессора:
  - SaaS:  $S = 3$  ГГц;
  - PaaS:  $S = 16 * 3,5$  ГГц – для 16 виртуальных процессоров с частотой процессора 3,5 ГГц;
  - IaaS:  $S = 4 * 3$  ГГц – для 4-ядерной виртуальной машины с частотой процессора 3 ГГц.

### Анализ влияния на облачные инфраструктуры

1. *SaaS (шифрование на стороне клиента)*. В SaaS шифрование выполняется на стороне клиента, т.е. на устройствах с ограниченной вычислительной мощностью, средняя частота процессора у таких устройств 3 ГГц.

В алгоритме шифрования RSA можно сократить время шифрования и дешифрования данных за счет многопоточности, но несмотря на это вычислительные издержки алгоритма RSA делают его непрактичным для клиентских SaaS-приложений.

2. *PaaS (шифрование на стороне сервера)*. Провайдеры PaaS используют масштабируемые серверные ресурсы (например, 16 виртуальных процессоров с частотой 3,5 ГГц). Распределенные вычисления сокращают задержки, но дешифрование на клиентских устройствах с ограниченными ресурсами остается проблемным местом.

3. *IaaS (Настраиваемая инфраструктура)*. В IaaS пользователи предоставляют виртуальные машины для шифрования. IaaS допускает вертикальное масштабирование (например, обновление до 8 ядер) для дальнейшего сокращения времени шифрования  $T_{\text{ш}}$ .

Время шифрования  $T_{\text{ш}}$  равно времени дешифрования  $T_{\text{д}}$ . В таблице 1 вычислено время шифрования и дешифрования данных в различных типах облачных инфраструктур.

ТАБЛИЦА 1. Время шифрования и дешифрования данных в различных типах облачных инфраструктур

| Алгоритм шифрования | AES-256                                                                                              | RSA-2048                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| SaaS                | $T_{\text{ш}} = \frac{10 \text{ МБ} * 5 \text{ циклов/байт}}{3 \text{ ГГц}} = 17 \text{ мс}$         | $T_{\text{ш}} = \frac{2048^3 * 0,01 \text{ циклов/бит}}{3 \text{ ГГц}} = 2,8 \text{ с}$         |
| PaaS                | $T_{\text{ш}} = \frac{10 \text{ МБ} * 5 \text{ циклов/байт}}{16 * 3,5 \text{ ГГц}} = 0,9 \text{ мс}$ | $T_{\text{ш}} = \frac{2048^3 * 0,01 \text{ циклов/бит}}{16 * 3,5 \text{ ГГц}} = 0,17 \text{ с}$ |
| IaaS                | $T_{\text{ш}} = \frac{10 \text{ МБ} * 5 \text{ циклов/байт}}{4 * 3 \text{ ГГц}} = 4,2 \text{ мс}$    | $T_{\text{ш}} = \frac{2048^3 * 0,01 \text{ циклов/бит}}{4 * 3 \text{ ГГц}} = 0,7 \text{ с}$     |

В таблице 2 вычислено время передачи данных по сети в различных типах облачных инфраструктур. Погрешностью изменений объема файла, зашифрованного алгоритмом AES, можно пренебречь и размер файла останется примерно 10 МБ. Размер файла, зашифрованного алгоритмом RSA-2048 значительно увеличивается примерно на 20 % и равен примерно 12 МБ.

ТАБЛИЦА 2. Время передачи данных в различных типах облачных инфраструктур

| Алгоритм шифрования | AES-256                                                                                 | RSA-2048                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| SaaS                | $T_{\text{п}} = \frac{10 \text{ МБ}}{125 \text{ МБ/с}} + 10 \text{ мс} = 90 \text{ мс}$ | $T_{\text{п}} = \frac{12 \text{ МБ}}{125 \text{ МБ/с}} + 10 \text{ мс} = 0,11 \text{ с}$ |
| PaaS                |                                                                                         |                                                                                          |
| IaaS                |                                                                                         |                                                                                          |

Исходя из полученного времени шифрования вычислено все время передачи зашифрованного файла в различных типах инфраструктур, полученные значения представлены в таблице 3.

ТАБЛИЦА 3. Общее время передачи данных в различных типах облачных инфраструктур

| Алгоритм шифрования | SaaS   | PaaS   | IaaS   |
|---------------------|--------|--------|--------|
| AES-256             | 0,12 с | 0,92 с | 0,98 с |
| RSA-2048            | 5,71 с | 0,45 с | 1,51 с |

Таким образом, выбор алгоритма шифрования значительно влияет на задержки при передаче данных в облачных инфраструктурах. При использовании асимметричных алгоритмов задержки возрастают экспоненциально с увеличением объема данных. Использование алгоритма RSA в SaaS приводит к недопустимым задержкам из-за ограничений на стороне клиента. PaaS и IaaS снижают задержку благодаря масштабируемым ресурсам. IaaS также обеспечивает большую гибкость для оптимизации рабочих процессов шифрования. Для SaaS оптимальным является алгоритм шифрования AES. В PaaS лучше использовать гибридное шифрование. IaaS позволяет использовать алгоритм шифрования RSA при достаточных ресурсах.

### Список используемых источников

1. Хлесткин А. Ю., Райков А. В., Казанцев А. А. и др. Роль операционных систем и оболочек в облачных вычислениях: анализ ОС и оболочек, используемых в облачных платформах и их влияние на облачную инфраструктуру // Программные системы и вычислительные методы. 2024. № 4. С. 93-108. DOI: 10.7256/2454-0714.2024.4.70626. EDN: KYNBQH.
2. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 т., Санкт-Петербург, 27–28 февраля 2019 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2019. С. 329-334. EDN: BLNOBQ.
3. Виткова Л. А., Иванов А. И., Сергеева И. Ю. Исследование и разработка методик оценки рисков облачных ресурсов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года. Под редакцией С.В. Бачевского. Том 2. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. С. 152-155. EDN: YRQАНС.
4. Бирих Э. В., Виткова Л. А., Левин М. В., Чмутов М. В. Развитие стандартов и руководств в сфере облачных технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года. Под редакцией С.В. Бачевского. Том 2. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2017. С. 92-95. EDN: YRPZWJ.
5. Березина Е. О., Яковлев В. А. Анализ атаки факторизации модуля в криптосистеме рша на основе моделирования алгоритма Шора с использованием квантовых вычислений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 т., Санкт-Петербург, 27–28 февраля 2019 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2019. С. 143-148. EDN: VHVOXQ.
6. Яковлев В. А., Шемякин С. Н., Таров Е. В. Использование метода Монтгомери в алгоритме быстрого возведения в степень // I-methods. 2023. Т. 15, № 1. EDN: PTFGQF.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Пестовым И. Е.*

УДК 004.056

Э. В. Бирих (старший преподаватель кафедры ЗСС, СПбГУТ)

П. Р. Гаврилов (магистрант группы ИКТБ-48м, СПбГУТ), [gavrilov.pr@sut.ru](mailto:gavrilov.pr@sut.ru)

## МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

*В условиях повсеместной цифровизации и роста числа киберугроз обеспечение надлежащего уровня информационной безопасности (ИБ) становится критически важной задачей для любой организации, будь то коммерческая компания или орган государственной власти. Существующие стандарты и лучшие практики задают ориентиры, однако для эффективного управления и планомерного повышения защищенности необходим инструмент оценки текущего состояния ИБ. В статье предлагается методика комплексной оценки уровня зрелости системы информационной безопасности, основанная на анализе ключевых доменов управления ИБ и позволяющая выявить слабые места и определить приоритетные направления для развития.*

*информационная безопасность, система менеджмента ИБ (СМИБ), оценка зрелости, модель зрелости, управление рисками, киберугрозы, ГОСТ Р ИСО/МЭК 27001, NIST SP 800-53, Ф3-152*

В современном мире организации сталкиваются с постоянно эволюционирующим ландшафтом киберугроз [1]. Успешная реализация этих угроз может привести к финансовым, операционным и репутационным потерям. Важным аспектом является также соблюдение законодательных и регуляторных требований, таких как Федеральный закон «О персональных данных» [2], и специфических отраслевых стандартов, например, ГОСТ Р 57580.1 для финансовых организаций [8].

Для построения эффективной защиты многие организации внедряют системы менеджмента информационной безопасности (СМИБ). Основой для таких систем часто служат признанные стандарты, в частности, российский ГОСТ Р ИСО/МЭК 27001-2021 [3], определяющий требования к СМИБ. Детализированные перечни мер и контролей безопасности могут быть взяты из таких источников, как NIST SP 800-53 [4] или приложения к самому ГОСТ Р ИСО/МЭК 27001.

Однако наличие формально описанных процессов и внедренных средств защиты не всегда означает их реальную эффективность. Необходимо оценивать, насколько хорошо эти процессы выполняются, управляются и совершенствуются – то есть их уровень зрелости. Для этой цели применяются модели зрелости, позволяющие структурированно оценить развитие процессов ИБ в организации по определенной шкале [7]. Как показано в обзоре [7], существуют различные модели зрелости (например, CMMI, COBIT PAM, на основе ISO/IEC стандартов), но часто требуется их адаптация под конкретные задачи и стандарты организации.

Предлагаемая методика комплексной оценки уровня зрелости СМИБ базируется на следующих принципах:

1. Оценка охватывает ключевые области управления ИБ, соответствующие структуре стандартов [3, 4] и общим практикам [6] (например, Политика ИБ, Управление активами, Контроль доступа, Криптография, Физическая безопасность, Безопасность операций, Безопасность коммуникаций, Управление инцидентами ИБ, Обеспечение непрерывности и др.);

2. применение шкалы зрелости (например, 5-уровневой, как обсуждается в обзорах моделей зрелости [7]) для оценки каждого процесса/домена;

3. использование четких критериев для каждого уровня зрелости, основанных на требованиях стандартов [3, 8] и лучших практиках [4, 6].

Процесс оценки включает:

- определение области оценки (вся организация или отдельные подразделения/системы);
- анализ документации СМИБ [3], интервью, аудит конфигураций и процессов;
- оценка уровня зрелости по каждому процессу/домену на основе собранных данных и критериев (см. таблицу 1);
- расчет общего или доменных показателей зрелости;
- визуализация (рис. 1) и формирование отчета с анализом пробелов и рекомендациями.

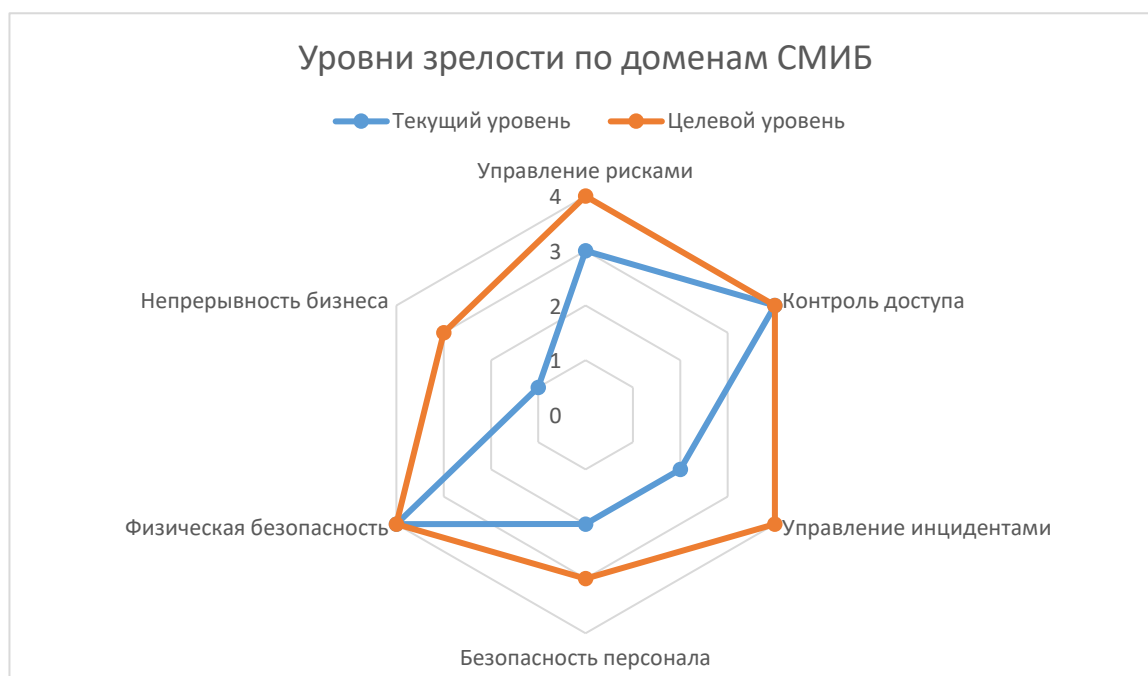


Рис. 1. Лепестковая диаграмма уровней зрелости по доменам СМИБ

ТАБЛИЦА 1. Пример критериев оценки зрелости для домена "Управление инцидентами ИБ"



| Начальный                                                                                                           | Повторяемый                                                                                                                | Определенный                                                                                                                                   | Управляемый                                                                                                                                                | Оптимизируемый                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Процесс не формализован, реакция хаотична. Нет документированной процедуры [3]. Ответственность четко не закреплена | Существует базовая процедура, известная ключевым сотрудникам. Инциденты фиксируются эпизодически. Определены основные роли | Процедура документирована, стандартизирована в рамках организации [3]. Персонал обучен. Используются базовые инструменты (логи, тикет-системы) | Эффективность процесса измеряется (KPI). Проводятся учения. Процесс интегрирован с управлением рисками и уязвимостями [4]. Данные используются для анализа | Процесс регулярно пересматривается и улучшается на основе анализа трендов, учений, новых угроз [1]. Используются продвинутое технологии (SOAR) |

Применение данной методики позволяет не только оценить текущее состояние СМИБ в соответствии с требованиями [3, 4, 8], но и, что важнее, выявить слабые звенья и определить приоритеты для дальнейшего развития и повышения общего уровня защищенности организации [6, 7]. Результаты оценки служат основой для разработки дорожной карты совершенствования СМИБ, обоснования необходимых ресурсов и демонстрации прогресса руководству и регуляторам [2, 8].

#### Список используемых источников

1. Отчет о глобальных рисках 2024 (The Global Risks Report 2024) // World Economic Forum. URL: <https://www.weforum.org/publications/global-risks-report-2024/> (дата обращения 21.04.2025).
2. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023). // Собрание законодательства РФ. 31.07.2006. N 31 (1 ч.). ст. 3451.
3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.
4. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. // National Institute of Standards and Technology. September 2020. URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> (дата обращения 21.04.2025).
5. Гафнер В. В. Информационная безопасность: Учебное пособие. Ростов-на-Дону: Феникс, 2010. 324 с. ISBN 978-5-222-16808-7.
6. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. 4-е изд., перераб. и доп. М.: ИД «ФОРУМ»: ИНФРА-М, 2023. 416 с. ISBN 978-5-8199-0988-0, 978-5-16-017955-8.
7. Милославская Н. Г., Сагиров Р. А. Обзор моделей зрелости процессов управления информационной безопасностью // Экономика и качество систем связи. 2018. № 4 (10). С. 11-21.

8. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. М.: Стандартиформ, 2017.

*Статья представлена научным руководителем, старшим преподавателем кафедры ЗСС СПбГУТ Бирихом Э. В.*

УДК 004.051

А. А. Борисов (магистрант группы ИКТМ-42м, СПбГУТ)

Г. С. Зозуля (магистрант группы ИКТС-43м, СПбГУТ), [zozulya.gs@sul.ru](mailto:zozulya.gs@sul.ru)

## МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТЯХ НА ОСНОВЕ ТУМАННЫХ ВЫЧИСЛЕНИЙ

*Растущий спрос на туманные вычисления (Fog computing) обусловлен экспоненциальным ростом количества устройств Интернета вещей (IoT) и объемом генерируемых ими данных. Fog играет важную роль в обеспечении обработки данных в реальном времени, снижении задержки и повышении эффективности и оперативности систем IoT. Вместе с преимуществами развертывание сетей на основе туманных вычислений наследует проблемы безопасности от облачных вычислений, такие как утечки данных и вопросы конфиденциальности. А также децентрализованный и ограниченный в ресурсах характер Fog-узлов создает новые уникальные проблемы. Целью работы является предоставление всестороннего обзора методов обеспечения безопасности и новых предложенных практик в сетях, с особым акцентом на эталонную архитектуру OpenFog.*

*туманные вычисления, Fog computing, безопасность, OpenFog*

В отличие от традиционных облачных вычислений, где обработка данных и хранение происходят в удаленных центрах обработки данных, туманные осуществляются ближе к источнику данных, что обеспечивает более низкую задержку, улучшенную надежность и поддержку мобильности. Важно отметить различие между туманными (Fog) и периферийными (Edge) вычислениями (рис. 1).

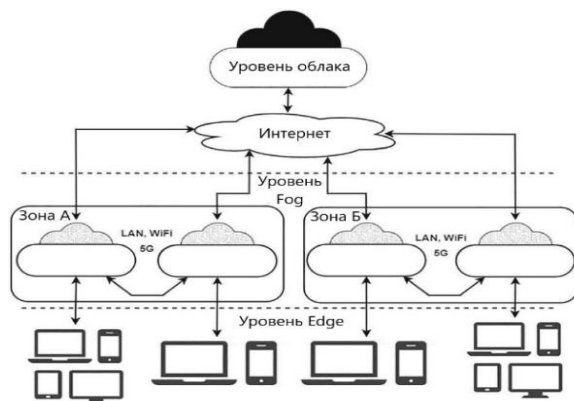


Рис. 1. Структура Fog сетей

Хотя оба подхода направлены на обработку данных ближе к источнику, туманные часто включает в себя более крупную сеть устройств и датчиков,

формируя промежуточный уровень между конечными устройствами и облаком [1]. Fog computing, будучи расширением облачной парадигмы, наследует ряд проблем безопасности, характерных для облачных сред. К ним относятся вопросы конфиденциальности и целостности данных, а также появляются новые, уникальные уязвимости Fog-сетей, которые представлены ниже:

- *Децентрализованное управление туманными вычислениями.* Распределенное развертывание Fog-узлов на границе сети увеличивает поверхность атаки, и защита большого количества географически распределенных узлов представляет собой сложную задачу. Кроме того, разнообразие владельцев и администраторов Fog-узлов усложняет управление доверием. В отличие от облачных центров обработки данных с контролируемой средой, Fog-узлы могут быть развернуты в различных и потенциально менее безопасных местах.

- *Гетерогенность Fog-узлов и сетей.* Fog-узлы включают разнородные устройства, такие как датчики, маршрутизаторы и серверы, каждое из которых имеет уникальные характеристики производительности, ресурсов и безопасности. Эта неоднородность создает сложности при разработке и внедрении единых политик безопасности, поскольку стандартизированные решения часто оказываются неэффективными для всех типов устройств. В результате возрастает риск уязвимостей, связанных с несоответствием уровней защиты и возможностей обработки угроз [2].

- *Ограниченные ресурсы Fog-узлов.* Многие Fog-узлы обладают ограниченными вычислительными ресурсами, объемом памяти и энергопотреблением. типовых Fog-узлов могут препятствовать развертыванию традиционных, вычислительно интенсивных механизмов безопасности, что требует разработки облегченных альтернатив.

Отсюда вытекает следующая проблема – утечки конфиденциальной информации [3]. Близость Fog-узлов к конечным пользователям приводит к увеличению сбора конфиденциальных данных, а их утечка может привести к несанкционированному доступу, что ставит под угрозу операционную целостность и соответствие нормативным требованиям.

Данные уязвимости возможно устранить с помощью реализации механизмов обеспечения безопасности в Fog Computing. Вот самые популярные из них:

- *Аутентификация и авторизация.* Традиционные методы аутентификации, такие как основанные на инфраструктуре открытых ключей (PKI),

могут быть неэффективны в Fog-средах из-за проблем масштабируемости. В качестве альтернативы рассматриваются кооперативная аутентификация, биометрическая аутентификация или протокол с использованием квантовых вычислений [1]. Протокол может использовать методы квантового распределения ключей для создания защищенного канала между Fog-узлами, а затем использовать этот защищенный канал для обмена информацией об аутентификации.

- *Шифрование.* Шифрование используется для защиты конфиденциальности и целостности данных в Fog-сетях как при передаче, так и при хранении [4]. Могут применяться передовые методы шифрования, такие как полностью гомоморфное шифрование. Эти схемы представляют собой гибрид симметричных алгоритмов шифрования с открытым ключом, а также другие варианты шифрования на основе атрибутов. Главное преимущество таких методов в отсутствии необходимости многократного шифрования/дешифрования данных в процессе работы сети, что на порядок увеличивает производительность [2];

- *Системы обнаружения и предотвращения вторжений (IDPS).* IDPS необходимы для обнаружения и предотвращения вредоносных действий, направленных на Fog-узлы и сети. Fog computing может быть использован в качестве IDS на периферии, за счет большого кол-ва распределенных устройств. Также для обработки данных мониторинга в краевых облаках можно разместить виртуальные машины с IDPS. Например, российская система СКАТ подразумевает установку на гипервизорах VMware и KVM [5], что позволяет дополнительно усилить безопасность каждого облака, а централизованный сбор и анализ информации поможет разрабатывать сценарии противодействия угроз в будущем [6];

- *Безопасное хранение и управление данными.* Для обеспечения отказоустойчивости и доступности данных могут использоваться сервисы безопасного хранения (SSS), представленные в среде приложений Cisco IOx [7]. Этот метод обеспечения безопасности основан на разделении любой информации на несколько частей с возможностью ее восстановления определенной группой участников. Существует несколько типов SSS, они используются в сочетании с другими методами защиты для обеспечения конфиденциальности ключей шифрования, хранения сертификатов и пользовательских данных на устройстве. Например, методы, требующие пере-

хвата всех частей ключа (полный SSS) или только определенной части (пороговый SSS) [4]. Пользователи и приложения могут получить доступ к службам SSS, работающим на хосте, через API на базе REST.

Комплексный подход к обеспечению безопасности в сетях на основе туманных вычислений требует разработки единых стандартов и выделения основных требований к развитию архитектуры. Таким стандартом выбрана эталонная архитектуры OpenFog [8], разработанная консорциумом OpenFog и подтвержденная в стандарте IEEE 1934. Она представляет собой горизонтальную архитектуру системного уровня, предназначенную для распределения вычислительных ресурсов, хранения, управления и сетевых функций ближе к пользователям. Архитектура OpenFog основана на восьми ключевых принципах, и безопасность является одним из критически важных аспектов. Но она не является универсальным решением, а представляет собой набор механизмов, которые применяются в зависимости от конкретных требований.

В работе предложены основные требования к обеспечению безопасности в сетях связи на основе туманных вычислений:

1. Все Fog-узлы должны использовать аппаратный корень доверия для безопасной загрузки и расширения цепочки доверия.
2. Fog-узлы должны обеспечивать контекстуальную целостность и изоляцию, контролируя сбор конфиденциальных данных на периферии.
3. Создание цепочек доверия, которые строятся на основе корня доверия и распространяется на базу доверенных вычислений узла Fog, обеспечивая надежность аппаратных и программных ресурсов [9].
4. Принятие стандартизированных криптографических функций и протоколов безопасности.
5. Необходим непрерывный мониторинг и управление безопасностью в системах OpenFog.
6. Важно обеспечить безопасное управление идентификацией и учетными данными пользователей, устройств и Fog-узлов.
7. Создание обязательных доменов подключения/совместимости и доменов сервисов с соответствующими политиками безопасности [10].

Fog computing представляет собой многообещающую парадигму для обработки и анализа данных ближе к источнику, что обеспечивает снижение задержки и повышение эффективности для различных приложений, особенно в контексте Интернета вещей. Существующие методы безопасности,

должны быть адаптированы и дополнены новыми подходами, учитывающими ограничения ресурсов и особенности Fog-сред.

А представленные принципы и требования OpenFog способствуют смягчению проблем безопасности, описанных в данной работе. Будущие исследования должны быть направлены на разработку более эффективных и облегченных протоколов безопасности, а также на стандартизацию лучших практик для обеспечения безопасного и надежного использования Fog computing в различных отраслях.

#### Список используемых источников

1. Jumani A. K. Fog computing security: A review / A. K. Jumani, J. Shi, A. A. Laghari, Z. Hu, A. Nabi, H. Qian // South China University of Technology. 2025. 22 p.
2. Князьков В. С. Гибридные вычисления на универсальных и специализированных вычислительных платформах / А. С. Коржавина, В. С. Князьков // Программные Системы: Теория И Приложения. 2020. С. 29.
3. D'Agostino, P. A Scalable Fog Computing Solution for Industrial Predictive Maintenance and Customization / P. D'Agostino, M. Violante, G. Macario // Polytechnic University of Turin. 2024. 14 p.
4. Shiriaev E. Reliability and Security for Fog Computing Systems / E. Shiriaev, T. Ermakova, E. Bezuglova, M. A. Lapina, M. Babenko // North-Caucasus Federal University. 2024. 15 p.
5. СКАТ. URL: <https://wiki.vasexperts.ru/doku.php?id=dpi> (дата обращения 29.04.2025).
6. Шевченко А. А. Модель процесса защиты информационно-телекоммуникационной сети от несанкционированного воздействия / А. А. Шевченко // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 10–11 октября 2019 года. Санкт-Петербург: ФГКВ ОУ ВО "Военная академия связи им. Маршала Советского Союза С. М. Буденного" МО РФ, 2019. С. 166-173.
7. Grossetete P. Best Security Practices for Fog Computing URL: <https://blogs.cisco.com/digital/best-security-practices-for-fog-computing> (дата обращения 29.04.2025).
8. OpenFog Reference Architecture for Fog Computing/ OpenFog Consortium/2017. 162 p.
9. Martin B. A. OpenFog Security Requirements and Approaches / B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon, S. Irwan // IEEE Fog World Congress. 2017. 6 p.
10. Липатников В. А. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства / В. А. Липатников, В. А. Парфиров, А. А. Шевченко, К. В. Мелехов // Актуальные проблемы защиты и безопасности: Труды XXVI Всероссийской научно-практической конференции, Санкт-Петербург, 03–06 апреля 2023 года. Том 1. Санкт-Петербург: Типография Любавич, 2023. С. 569-572.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Шевченко А. А.*

УДК 004.056

**Н. А. Васильев** (к.т.н., старший научный сотрудник, ВАС)

**Б. С. Лещинский** (адъюнкт, ВАС)

**Д. С. Ситдилов** (младший научный сотрудник, ВАС),

[dimasitdikov.99@mail.ru](mailto:dimasitdikov.99@mail.ru)

## КИБЕРБЕЗОПАСНОСТЬ В БЕСПРОВОДНЫХ СЕТЯХ

*Статья посвящена анализу актуальных вопросов кибербезопасности в беспроводных сетях. Рассмотрены угрозы безопасности беспроводных сетей, включая перехват данных, атаки типа «человек посередине», DDoS-атаки и уязвимости в протоколах связи. Проанализированы методы защиты: шифрование, аутентификация, IDS/IPS, управление уязвимостями и использование искусственного интеллекта. Особое внимание уделено особенностям безопасности сетей 5G и IoT. Приведены практические рекомендации по защите беспроводных сетей.*

*беспроводные сети, кибербезопасность, шифрование, 5G, IoT, аутентификация, IDS/IPS, защита данных*

Беспроводные сети стали основой современной цифровой инфраструктуры, обеспечивая быстрый доступ к данным. Однако их открытая природа делает их уязвимыми перед различными киберугрозами [1]. Развитие 5G и Интернета вещей (IoT) увеличило количество подключений и объем передаваемой информации, что требует комплексного подхода к безопасности.

Цель настоящей работы – обобщить существующие угрозы и методы защиты, определить особенности безопасности в новых технологических условиях и выработать практические рекомендации.

Ниже рассмотрены основные типы угроз, которые могут нарушить безопасность данных и целостность сетей:

1. Передача данных по радиоканалу создает возможность их перехвата без физического доступа к устройствам. Используя анализатор трафика (например, Wireshark), злоумышленники могут извлекать передаваемую информацию, если сеть недостаточно защищена [2]. Наибольшую опасность представляет использование открытых или устаревших протоколов шифрования.

2. Атаки типа «человек посередине» MITM предполагают вмешательство злоумышленника в процесс передачи данных между двумя узлами сети. Одна из распространенных техник – создание поддельной точки доступа (Evil Twin), что позволяет перехватывать учетные данные пользователей [3].



3. DDoS-атаки перегружают сетевые ресурсы большим количеством запросов, нарушая доступность сервисов. В беспроводных сетях DDoS-атаки могут приводить к отказу критически важных систем, особенно в инфраструктуре IoT и 5G [4].

4. Даже современные протоколы шифрования могут содержать уязвимости. Например, атака KRACK показала возможность расшифровки трафика WPA2-соединений [5].

5. Множество IoT-устройств обладают слабой защитой, что делает их легкой мишенью. Ботнеты, такие как Mirai, массово используют уязвимые устройства для проведения масштабных атак [1].

Для защиты беспроводных сетей от перечисленных угроз, используются различные методы и технологии. Рассмотрим основные из них.

Шифрование является базовым средством обеспечения безопасности беспроводных сетей. Современные стандарты, такие как WPA3, используют мощные алгоритмы шифрования, например, AES. Однако важно не только выбрать надежные методы шифрования, но и следить за регулярным обновлением устройств и их настроек, чтобы своевременно устранять обнаруженные уязвимости.

Аутентификация пользователей и устройств посредством протокола EAP в сочетании с 802.1X, позволяет контролировать доступ к сети на более высоком уровне.

IDS (Intrusion Detection System) и IPS (Intrusion Prevention System) анализируют сетевой трафик на наличие аномалий и признаков атак. В современных решениях широко применяются методы машинного обучения для повышения точности выявления угроз [5].

Регулярное обновление программного обеспечения точек доступа, маршрутизаторов и клиентских устройств снижает риск эксплуатации известных уязвимостей [4]. В корпоративной практике внедряются решения по централизованному управлению обновлениями и автоматизированному сканированию сетевых устройств.

Искусственный интеллект и машинное обучение позволяют выявлять сложные и ранее неизвестные атаки за счет анализа большого объема сетевых данных в реальном времени [5]. Автоматизация процессов обнаружения угроз и их классификации значительно повышает скорость реагирования на инциденты. На рисунке 1 представлено сравнение эффективности, сложности реализации и применимости методов защиты информации.

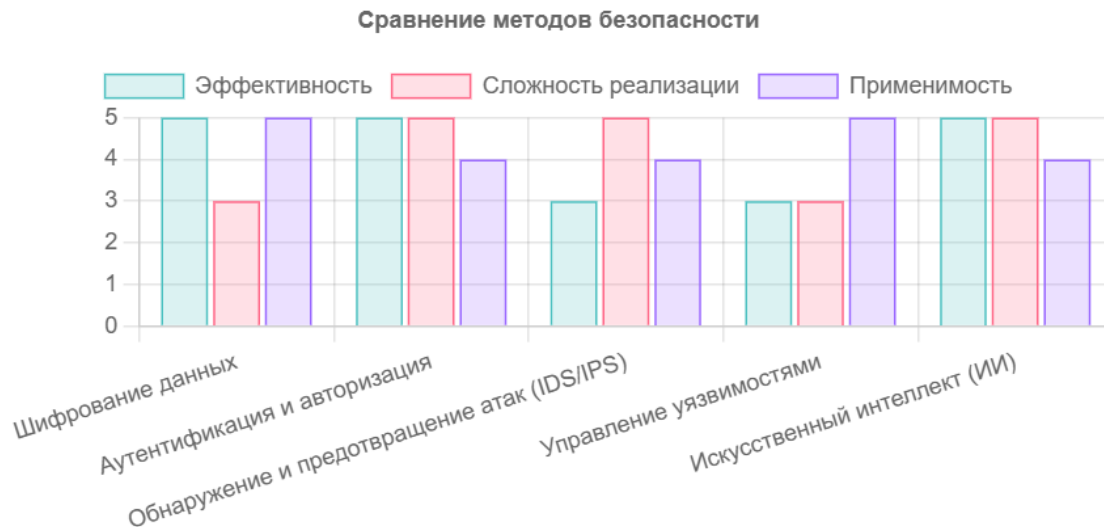


Рис. 1. Зависимость эффективности методов от сложности реализации

## Особенности обеспечения безопасности в сетях 5G и IoT

Сети пятого поколения отличаются высокой скоростью передачи данных, низкой задержкой и поддержкой сетевой виртуализации. Использование SDN и NFV делает сеть более гибкой, но также увеличивает число потенциальных точек атаки. Сетевые срезы (network slicing) требуют изоляции и защиты каждого виртуального сегмента, иначе компрометация одного из них может повлиять на всю сеть [6].

Защита сетей 5G предполагает комплексный подход:

1. Шифрование служебного трафика.
2. Взаимная аутентификация между элементами сети.
3. Использование блокчейн-технологий для обеспечения доверия между участниками сети [6].

Большое внимание уделяется мониторингу и оперативному реагированию на аномалии в распределенных архитектурах 5G.

IoT-среда уязвима по ряду причин: слабая вычислительная мощность устройств, отсутствие стандартов безопасности, разрозненность решений. Устройства IoT часто используют простые механизмы аутентификации и передают данные без надлежащего шифрования. Это делает возможным их компрометацию и последующее использование в ботнетах [7].

Для повышения безопасности IoT рекомендуется:

1. Использовать легкие криптографические протоколы (например, DTLS).
2. Внедрять двухфакторную аутентификацию.
3. Регулярно обновлять прошивки устройств.
4. Сегментировать IoT-сети для минимизации последствий взлома [7].

Важным направлением является развитие стандартов безопасности для производителей IoT-устройств.

На основании анализа современных угроз и методов защиты сформулированы следующие рекомендации:

1. Использовать WPA3 для Wi-Fi сетей и шифрование всех каналов передачи данных.
2. Применять многофакторную аутентификацию для пользователей и устройств.
3. Внедрять системы IDS/IPS для мониторинга сетевого трафика.
4. Регулярно обновлять программное обеспечение и прошивки сетевых устройств.
5. Изолировать IoT-устройства в отдельные сегменты сети.
6. Использовать искусственный интеллект для анализа трафика и выявления угроз.
7. Обучать сотрудников и пользователей основам кибербезопасности при работе с беспроводными сетями.

Кибербезопасность беспроводных сетей – динамично развивающееся направление, требующее постоянного совершенствования подходов в связи с появлением новых угроз. Проведенный анализ показал, что современные средства защиты (шифрование WPA3, аутентификация 802.1X, IDS/IPS, управление уязвимостями) при правильном внедрении способны эффективно противостоять большинству актуальных атак. Важную роль играют технологии искусственного интеллекта, которые позволяют обнаруживать сложные атаки и аномалии в режиме реального времени, а также принимать проактивные меры по защите сети.

#### Список используемых источников

1. Nazir R. et al. Survey on wireless network security // Archives of Computational Methods in Engineering. 2021. С. 1-20.
2. Minnie D. et al. Investigation of Data Interception and its Vulnerabilities in HTTP and HTTPS networks through Packet Sniffers // 2024 2nd International Conference on Networking and Communications (ICNWC). IEEE, 2024. С. 1-4.
3. Louca C., Peratikou A., Stavrou S. A novel Evil Twin MiTM attack through 802.11 v protocol exploitation // Computers & Security. 2023. Т. 130. С. 103261.
4. Леонов М. А., Черпаков И. В. Основные виды сетевых атак и пути их предотвращения // Редакционная коллегия. Председатель редакционной коллегии. 2023. С. 60.
5. Alenazi B., Idris H. E. Wireless intrusion and attack detection for 5G networks using deep learning techniques // International Journal of Advanced Computer Science and Applications. 2021. Т. 12. № 7.
6. Gao S. et al. Security threats, requirements and recommendations on creating 5G network slicing system: A survey // Electronics. 2024. Т. 13. № 10. С. 1860.
7. Dritsas E., Trigka M. A Survey on Cybersecurity in IoT // Future Internet. 2025. Т. 17. № 1.

УДК 004.056.55

В. Ю. Вахтель (студент группы ИКБ-22, СПбГУТ), [vahtel.vu@sut.ru](mailto:vahtel.vu@sut.ru)

## **АНАЛИЗ СТОЙКОСТИ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ К АТАКЕ ТИПА ПЕРЕХВАТ-ОТПРАВКА НА ОСНОВЕ КВАНТОВОГО КАНАЛА В СВОБОДНОМ ПРОСТРАНСТВЕ**

*В данной статье проводится сравнительный анализ трех протоколов квантового распределения ключей (BB84, B92 и E91) с точки зрения их способности обнаруживать вмешательство третьей стороны в условиях свободного пространства. Основное внимание уделяется оценке вероятности обнаружения атаки через анализ Quantum Bit Error Rate (QBER) для каждого протокола.*

*квантовое распределение ключей, обнаружение вмешательства, BB84, E91, B92*

Системы с открытыми ключами (несимметричные криптосистемы) крайне уязвимы к атакам с использованием квантовых компьютеров, поскольку алгоритмы типа RSA и ECC основаны на вычислительной сложности задач факторизации и дискретного логарифмирования, которые эффективно решаются алгоритмом Шора [1].

В отличие от них, симметричные криптосистемы демонстрируют более высокую устойчивость к квантовым атакам (за счет увеличения длины ключа), однако требуют надежного механизма распределения ключей между сторонами. Именно эта проблема стимулирует активные исследования методов квантового распределения ключей (QKD), которые позволяют создать защищенные каналы для обмена симметричными ключами, используя фундаментальные принципы квантовой механики, такие как невозможность клонирования состояния и принцип неопределенности.

Современные протоколы QKD (BB84, E91, B92) обеспечивают не только обнаружение попыток перехвата ключа, но и математически доказанную безопасность, что делает их перспективными [2].

Однако в свободном пространстве (спутник-Земля, воздушные каналы) QKD сталкивается с такими проблемами как: атмосферная турбулентность, декогеренция (потеря квантовых состояний из-за взаимодействия со средой) и ограничения по дальности [3].

Параметр QBER (Quantum Bit Error Rate) – Вероятность ошибки на бит – ключевой показатель безопасности QKD. Его рост сигнализирует о попытке взлома и о помехах в канале связи [4].

Целью работы является сравнение эффективности протоколов BB84, B92 и E91 обнаруживать вмешательство злоумышленника на основе анализа QBER в условиях свободного пространства.

Для BB84 QBER с учетом атаки перехват-отправка (злоумышленник перехватывает фотоны, измеряет их в случайной базе и отправляет поддельные состояния) рассчитывается как сумма ошибок от оптических потерь, шумов детектора, турбулентности и вклада в атаку (1) [5]:

$$QBER_{BB84} = \frac{1}{2}(1 - e^{-\mu\eta T}) + P_{dark} + 0.016\left(\frac{D}{r_0(d)}\right) + \frac{p_{attack}}{4}, \quad (1)$$

где  $\mu$  – среднее число фотонов на импульс ( $0.1 \leq \mu \leq 1$ ),  $\eta$  – эффективность детекторов,  $T$  – коэффициент пропускания канала,  $P_{dark}$  – вероятность появления фотона за счет темного тока детектора,  $D$  – апертура приемника (диаметр телескопа),  $r_0(d)$  – параметр Фрида,  $p_{attack}$  – вероятность перехвата фотонов злоумышленником, составляющая 25 % сверх уровня естественных помех в связи с дополнительными искажениями при атаке.

В протоколе B92 применяются два не ортогональных квантовых состояния, что увеличивает ошибки при атаке перехват-отправка (2) [6]:

$$QBER_{B92} = \frac{1}{2}(1 - e^{-\mu\eta T}) + P_{dark} + \frac{1}{4}\left(\frac{D}{r_0(d)}\right) + \frac{p_{attack}}{2}, \quad (2)$$

где  $p_{attack} = 0.5$ , это связано с тем, что злоумышленник, измеряя не ортогональные состояния, ошибается с вероятностью 50 %.

Для протокола E91, QBER, с учетом атаки на запутанные состояния, (злоумышленник перехватывает одну из частиц пары, нарушая квантовые корреляции) рассчитывается как сумма ошибок от декогеренции запутанных пар, потерь в канале и вклада атаки, приводящего к снижению верности передачи, которая является параметром, характеризующий точность сохранения квантовых состояний. (3) [7]:

$$QBER_{E91} = \frac{1}{2}\left(1 - \frac{V(d)}{2\sqrt{2}}\right) + \epsilon_{channel}(d) + \frac{1 - F(d)}{2}, \quad (3)$$

где  $V(d)$  – видимость корреляций Белла, уменьшающаяся с расстоянием  $d$ ,  $\epsilon_{channel}(d)$  – ошибки от потерь в канале,  $F(d)$  – достоверность запутанных пар.

На рис. 1 представлена зависимость QBER от уровня перехвата фотонов для протоколов BB84, B92 и E91, построенная на основе данных, полученных в ходе натурных испытаний свободно-пространственных QKD-систем на расстоянии 100-200 метров с имитацией естественных помех [8]. Критические значения QBER (вертикальные пунктирные линии), при которых система гарантированно обнаруживает атаку (рис. 1).

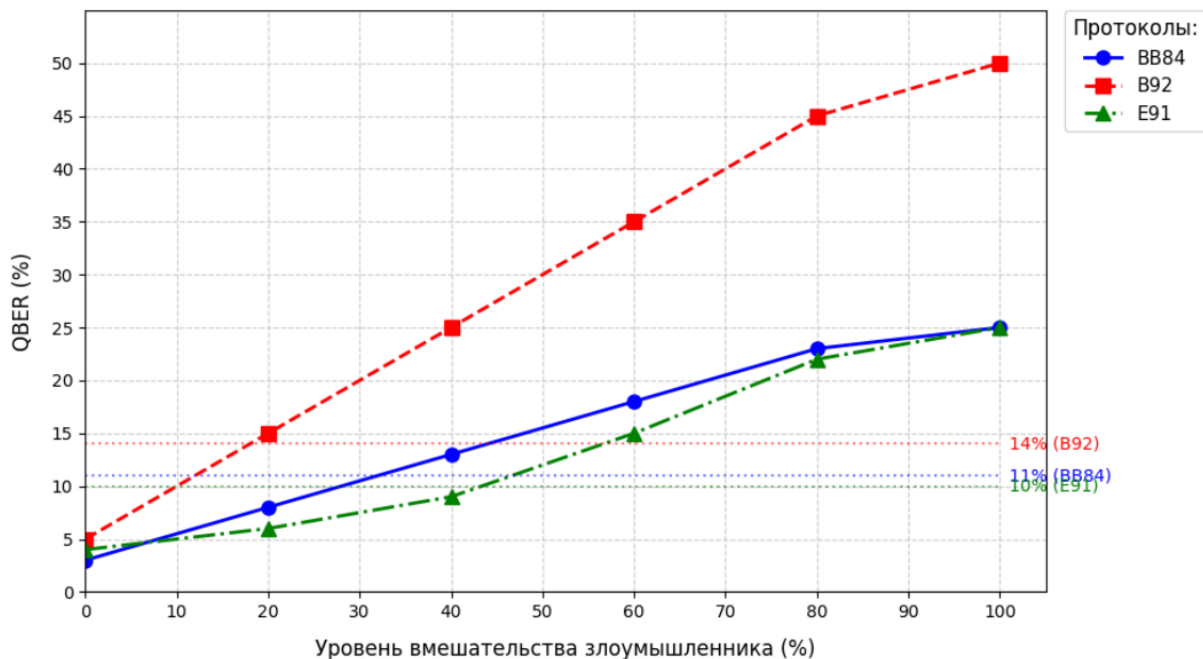


Рис. 1. Зависимость QBER от вмешательства извне

Анализ зависимостей QBER от вмешательства со стороны третьих лиц (рис. 1) подтверждает, что протоколы по-разному реагируют на вмешательство злоумышленника. Наиболее чувствительным к атакам является B92, при перехвате 20 % фотонов, его QBER возрастает на 10 %, что позволяет раньше определить атаку, по сравнению с BB84 и E91.

Как показано в таблице 1, все три протокола используют разные подходы к обнаружению вмешательства.

Главным преимуществом QKD-протоколов является не столько устойчивость к помехам, сколько гарантированное обнаружение вмешательства. В следствие роста QBER выше критических значений однозначно указывает на атаку, даже если ключ не был еще скомпрометирован. Это является принципиальным отличием от классических методов, где перехват может остаться незамеченным.

ТАБЛИЦА 1. Сравнение механизмов обнаружения атак

| Параметр                      | BB84                             | B92                                          | E91                                                           |
|-------------------------------|----------------------------------|----------------------------------------------|---------------------------------------------------------------|
| Основной механизм обнаружения | Рост QBER из-за ошибок в базисах | Рост QBER из-за не ортогональности состояний | Рост QBER из-за уменьшения достоверности запутанных состояний |
| Порог обнаружения             | QBER > 11 %                      | QBER > 14 %                                  | QBER > 10 %                                                   |
| Чувствительность к атаке      | Средняя                          | Высокая                                      | Низкая                                                        |

Дальнейшие исследования должны быть направлены на изучение влияния структурных особенностей протоколов QKD на их способность обнаруживать разные типы атак в условиях открытого пространства.

#### Список используемых источников

1. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of Modern Physics. 2002. Vol. 74(1), PP. 145–195.
2. Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proc. IEEE Int. Conf. on Computers, 1984. PP. 175–179.
3. Khalid, A. et al. Turbulence Effects on Free-Space QKD // IEEE Quantum, 2021. Vol. 2. PP. 1–12.
4. Scarani V. et al. The Security of Practical Quantum Key Distribution // Rev. Mod. Phys., 2009. Vol. 81. PP. 1301–1350.
5. Scarani V., Bechmann-Pasquinucci H., Cerf N. J., Dušek M., Lütkenhaus N., Peev M. The security of practical quantum key distribution // Reviews of Modern Physics, 2009. Vol. 81(3). PP. 1301–1350.
6. Tamaki K., Koashi M., Imoto N. Unconditionally secure key distribution based on two nonorthogonal states // Physical Review Letters. 2003. Vol. 90(16). P. 167904.
7. Ekert A. K. Quantum cryptography based on Bell's theorem // Physical Review Letters, 1991. Vol. 67(6). PP. 661–663.
8. Tomaello, A., et al. Free-space QKD: Comparative analysis of protocols // Quantum Science and Technology, 2019. Vol. 4(2). PP. 025003.

*Статья представлена научным руководителем, профессором кафедры ЗСС СПбГУТ, доктором технических наук, профессором Яковлевым В. А.*

УДК 004.056

**Я. А. Ильин** (магистрант гр. ИКТБ-38м, СПбГУТ), [jaroslav.ilin@gmail.com](mailto:jaroslav.ilin@gmail.com)  
**Н. Ф. Махмутова** (магистрант гр. ИКТБ-47м, СПбГУТ)

## РАЗРАБОТКА ЗАЩИЩЕННОГО РЕШЕНИЯ ДЛЯ НАСТРОЙКИ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ NFC

*В нынешнее время применение технологии NFC в различных устройствах получило широкое распространение. Большая часть устройств используют данную технологию для установления сопряжения или передачи данных. Однако, несмотря на это, возможна еще более широкая интеграция технологии NFC, например, использование в качестве вспомогательного компонента для настройки параметров и режимов работы устройства. В данной работе рассматриваются возможные требования к устройству, его потенциальные возможности, а также описывается макет изделия с его характеристиками.*

*NFC, радиосвязь, информационная безопасность*

В современном мире беспроводные технологии связи становятся неотъемлемой частью повседневной жизни. Многие технологии радиосвязи, такие как Wi-Fi и Bluetooth уже давно стали неотъемлемой частью повседневной жизни. Среди них особое место занимает технология бесконтактной связи ближнего действия (NFC – Near Field Communication), которая благодаря своей простоте, энергоэффективности и безопасности получила широкое распространение в различных областях. Одним из перспективных направлений применения NFC является использование этой технологии для настройки режимов работы электронных устройств. В данной статье рассматриваются основные аспекты разработки защищенного решения для настройки устройств с использованием технологии NFC.

Анализ концепции устройств для настройки, использующих NFC, требует в первую очередь исследования особенностей технологии NFC и анализ способов настройки приборов. Технология NFC работает на частоте 13,56 МГц и обеспечивает обмен данными на расстоянии до 10 см. Для NFC характерна низкая скорость передачи данных от 100 до 400 КБ/с, а также отсутствием необходимости в собственном источнике питания у пассивных устройств (меток). Пассивные устройства NFC включают в себя метки и другие небольшие передатчики, которые отправляют (а вернее сказать с них считывают терминалы) информацию на другие устройства NFC без необхо-



димости использования собственного источника питания. Однако они не обрабатывают любую информацию, отправленную из других источников, и не подключаются к другим пассивным устройствам. Активные устройства умеют отправлять или получать данные и обмениваться данными друг с другом, а также с пассивными устройствами. На данный момент именно смартфоны являются наиболее распространенной формой активного устройства NFC. Считыватели карт общественного транспорта и цифровые терминалы для банковских платежей также являются наиболее распространенными примерами этой технологии [1, 2].

Основными преимуществами NFC являются:

- 1) простота передачи данных без сложных настроек;
- 2) возможность использования пассивных устройств передачи данных (меток), не требующих питания;
- 3) высокая степень защиты информации благодаря малому радиусу действия.

ТАБЛИЦА 1. Сравнительные характеристики NFC, Bluetooth и Wi-Fi.

|                                               | Технология        |                                                       |                 |
|-----------------------------------------------|-------------------|-------------------------------------------------------|-----------------|
| Характеристики                                | NFC               | Bluetooth                                             | Wi-Fi           |
| Дальность действия                            | До 10 сантиметров | 20-100 метров<br>в зависимости<br>от версии Bluetooth | До 100 метров   |
| Пропускная способность                        | 100-400 КБ/с      | 1-3 МБ/с                                              | 11-450 МБ/с     |
| Частота                                       | 13,56 МГц         | 2,4 ГГц                                               | 2,4 ГГц и 5 ГГц |
| Одновременное подключение устройств           | 1                 | 4-15                                                  | ~40             |
| Затраты энергии на запись и чтение информации | Нет               | Да                                                    | Да              |

Сравнение с такими технологиями, как Bluetooth и Wi-Fi (табл. 1) показывает, что NFC более удобна для быстрого и безопасного обмена дан-

ными, однако имеет множество ограничений. Существует множество областей, где будет обоснованно применение именно NFC в качестве инструмента настройки устройств.

Интеграция NFC в устройства позволяет упростить процесс их настройки и повысить надежность взаимодействия с пользователем. Наиболее подходящие случаи для применения NFC в качестве инструмента настройки:

1. Необходимость быстрой настройки множества устройств – например, при масштабных монтажах в промышленности или строительстве.
2. Высокая сложность настройки устройств – когда требуется задание нескольких параметров и режимов работы, неквалифицированным персоналом.
3. Частые изменения параметров – актуально для датчиков и приборов учета, которые необходимо регулярно корректировать.
4. Герметичность устройств – возможность настройки без вскрытия корпуса.
5. Низкое потребление энергии – использование пассивных меток позволяет минимизировать энергозатраты.
6. Невозможность физического контакта с устройством – важный фактор в медицинских, промышленных и других специальных условиях.
7. Требование к стоимости изделия – модули NFC значительно дешевле, чем модули Bluetooth или Wi-Fi)
8. Увеличение износостойкости настраиваемого прибора – отсутствие механических компонентов снижает риск поломок и упрощает конструкцию устройства.
9. Энергоэффективность – пассивные метки в настраиваемых устройствах не требуют собственного питания и активируются только при поднесении терминала.

Несмотря на все преимущества, использование NFC связано с определенными рисками. Основные виды атак, которым могут подвергаться устройства с NFC: скимминг (перехват данных с помощью мошеннического считывателя) и ретрансляционная атака (передача данных через цепочку устройств, имитирующих связь между устройством и терминалом) [3, 4].

Для реализации защищенного решения устройства с возможностью настройки на основе технологии NFC предлагается следующая архитектура (рис. 1).

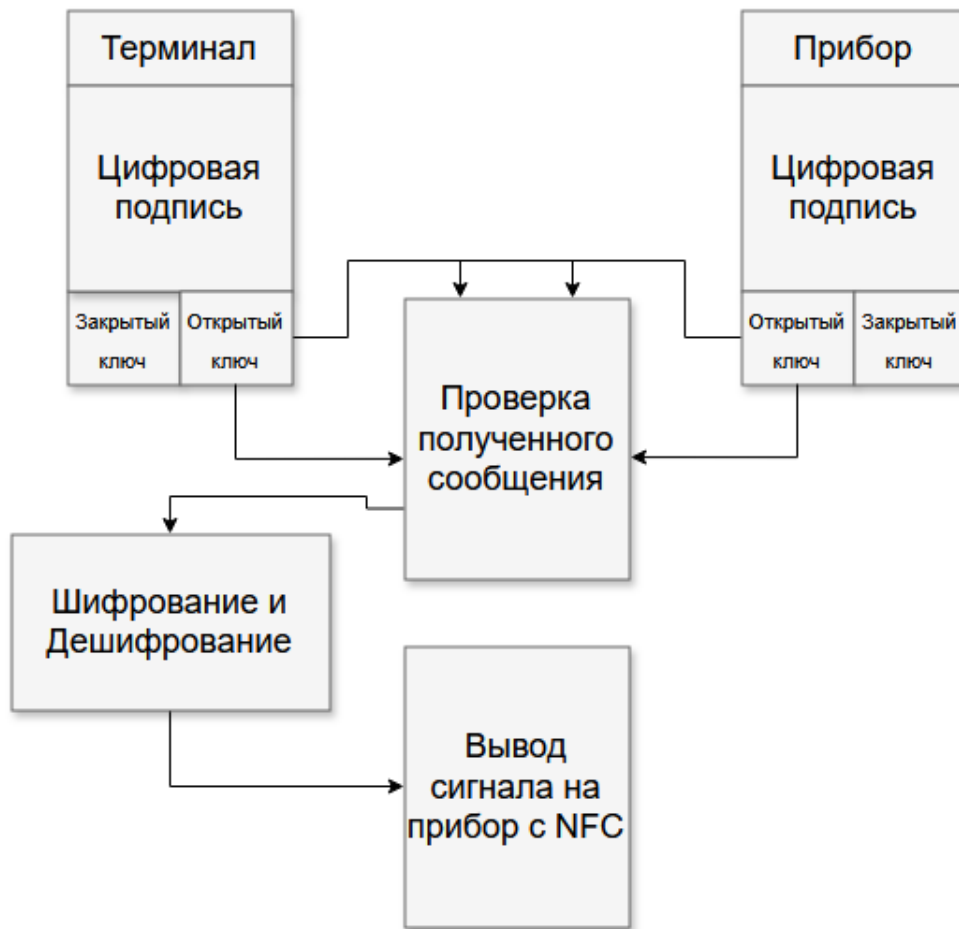


Рис. 1. Концепция технического решения устройства настройки, использующего NFC

Взаимодействие происходит следующим образом: пользователь подносит смартфон к устройству, NFC-метка активируется и передает данные о режиме работы на устройство. Далее происходит двусторонняя проверка доверенного устройства. Устройство проверяет входящее сообщение используя свой закрытый ключ и полученный от терминала открытый ключ. Затем, в случае корректности полученного сообщения, оно дешифруется и запускается необходимый режим работы устройства.

#### Список используемых источников

1. Коренюгин Е. В., Ковцур М. М., Яссер М. В. Обзор методов обеспечения информационной безопасности в мобильных приложениях // Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. Санкт-Петербург, 2024. С. 409-410.
2. Грохольский А. В., Ильин Я. А., Ковцур М. М. Разработка концепции устройства с модулем конфигурирования на базе технологии NFC // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т. Санкт-Петербург, 2024. С. 260-262.

3. Романова А. С., Буров Н. Н. Текущее состояние и перспективы развития nfc-технологии в России // Шестьдесят девятая всероссийская научно-техническая конференция студентов, магистрантов и аспирантов высших учебных заведений с международным участием. 2016. С. 1605-1608

4. Крыщенко Н. И., Миняев А. А., Ковцур М. М. Исследование рекомендаций производителей по безопасной настройке беспроводного оборудования // Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. Санкт-Петербург, 2022. С. 592-596.

*Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом Ковцуrom М. М.*

УДК 004.056.55

А. В. Казакова (студент группы ИБС-01, СПбГУТ), [kazakova.av@sut.ru](mailto:kazakova.av@sut.ru)

## АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ВЕРИФИКАЦИИ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИХ ЦЕЛОСТНОСТИ ПРИ ПЕРЕДАЧЕ

*Передача моделей искусственного интеллекта между системами и участниками становится все более распространенной практикой, однако при этом возрастает риск их подмены, искажения или внедрения вредоносных модификаций. В условиях отсутствия надежных механизмов проверки целостности такие угрозы могут привести к серьезным сбоям, потере данных и подрыву доверия к интеллектуальным системам. Это делает задачу верификации моделей при передаче крайне актуальной для обеспечения безопасности и устойчивости ИИ-решений.*

*верификация моделей, целостность данных, искусственный интеллект, безопасность передачи*

Процесс передачи моделей искусственного интеллекта (далее – ИИ), особенно в распределенных или облачных средах, сопряжен с риском потери целостности. При отсутствии формализованной политики проверки модели могут быть перехвачены, изменены или подменены без ведома получателя. Согласно отчету IBM Security за 2024 год, более 47 % организаций, использующих ИИ, не реализуют проверку целостности моделей на этапе их получения, что создает условия для эксплуатации уязвимостей в цепочке поставки ИИ-решений [1].

На рис. 1 представлены наиболее типичные угрозы, возникающие при передаче моделей без защиты.



Рис. 1. Основные угрозы при передаче моделей ИИ

Одной из таких угроз является подмена модели, при которой злоумышленник заменяет исходную модель на измененную, сохраняя при этом формат и метаданные, что делает вмешательство практически незаметным. Такая подмена может привести к искажению результатов обработки данных, появлению преднамеренных ошибок или утечке информации.

Не менее опасной является модификация весов и структуры модели. Даже небольшие изменения параметров могут значительно изменить поведение модели, особенно в чувствительных системах, где ИИ влияет на принятие решений. Часто такие изменения сложно обнаружить при поверхностной проверке.

Еще одной угрозой выступает инъекция вредоносных данных в обученную модель, также известная как poisoning-атака. При этом в модель встраиваются определенные «триггеры», активирующие ошибочное поведение при получении специфических входных данных. Подобные атаки опасны своей скрытностью и целенаправленным характером.

Также стоит учитывать уязвимости на уровне форматов хранения моделей. Распространенные контейнеры, такие как ONNX или TensorFlow SavedModel, могут быть модифицированы для внедрения вредоносного кода, который активируется при загрузке модели в рабочую среду.

Наконец, незащищенные каналы передачи, такие как FTP или HTTP без шифрования, позволяют злоумышленнику перехватить и подменить модель «на лету», без непосредственного доступа к отправителю или получателю.

Обеспечение целостности моделей искусственного интеллекта при передаче невозможно без применения надежных механизмов верификации. Наиболее надежным и формализованным способом подтверждения неизменности модели является использование криптографических хеш-функций и цифровых подписей. Пусть  $M$  – бинарное представление модели, тогда для нее вычисляется хеш:

$$H = h(M), \quad (1)$$

где  $h$  – устойчивый к коллизиям алгоритм (например, SHA-256).

Полученное значение используется или для сверки, или подписывается закрытым ключом отправителя, что отображено в формуле 2.

$$S = \text{Sign}_{\text{priv}}(H), \quad (2)$$

Далее получатель проверяет подпись с помощью открытого ключа, здесь стоит отметить, что нарушение целостности немедленно выявляется, так как даже минимальное изменение приводит к новому значению хеша.

Реальный пример – инфраструктура Model Zoo для PyTorch и TensorFlow, где хеши моделей публикуются вместе с файлами весов. Это позволяет пользователю сверить загруженный файл и обнаружить возможную подмену или искажение при передаче.

Дополнительно может применяться симметричная аутентификация через MAC (Message Authentication Code), особенно в закрытых системах, где известен общий ключ.

В условиях, когда модель может быть скомпрометирована не внешне, а в логике работы, применяются методы внедрения скрытых маркеров. Водяной знак внедряется в параметры модели:

$$\theta = \theta + \Delta, \quad (3)$$

где  $\Delta$  – целенаправленная малозаметная корректировка.

Данный знак активируется при определенном входном наборе, что позволяет подтвердить авторство или целостность модели даже после многократной передачи [2].

Яркий пример – система DeepMarks, разработанная для встраивания устойчивых водяных знаков в модели глубокого обучения. Она позволяет разработчикам доказывать владение моделью, а также отслеживать ее незаконное распространение.

Методы отпечатков (fingerprinting) расширяют подход, присваивая каждой копии модели уникальный идентификатор. Это используется, например, в облачных ML-платформах Amazon SageMaker и Azure ML Studio для контроля утечек моделей.

В некоторых сценариях передача модели осуществляется через ненадежные каналы связи, что требует встроенной устойчивости к искажениям. Для этого используется избыточное кодирование с возможностью обнаружения и исправления ошибок. Пусть модель закодирована вектором  $M$ , тогда можем получить:

$$C = \text{Encode}(M) = M \times G, \quad (4)$$

где  $G$  – генераторная матрица, а на стороне приема выполняется проверка декодированной версии [3].

Подобные методы применяются, например, в промышленной передаче моделей для встраиваемых систем, где возможны физические помехи. В проектах NASA Jet Propulsion Laboratory встраиваемые модели ИИ в спутниковых системах передаются с применением ЕСС для повышения надежности в условиях космической связи [4].

Для защиты на уровне среды исполнения используются доверенные окружения (Trusted Execution Environments, TEE) и модули доверенной платформы (TPM). Они позволяют загрузить модель в защищенной области памяти, проверить ее цифровой отпечаток и исключить доступ постороннего ПО.

Так, Intel SGX и ARM TrustZone позволяют исполнять модели ИИ в изолированных средах, обеспечивая недоступность даже при наличии вредоносного кода в основной системе [5]. В рамках проекта Microsoft Confidential ML, модели загружаются в TEE и верифицируются по их измерениям:

$$\text{Measurement}(M) = h(M), \quad (5)$$

далее значения заносятся в регистры контроля платформы (PCR) и сверяется с эталоном.

Такие методы уже находят применение в медицинских и финансовых системах, где модель ИИ взаимодействует с чувствительными данными и не должна быть скомпрометирована на уровне окружения.

Для проведения объективного анализа методов верификации были выбраны шесть критериев, охватывающих как техническую надежность, так и практическую применимость решений.

Во-первых, учитывается надежность контроля целостности – способность метода выявлять любые, даже минимальные изменения в структуре модели. Этот параметр критичен для обнаружения подмен и искажений.

Не менее важным является подтверждение подлинности источника, то есть возможность проверить, что модель действительно поступила от доверенного отправителя, а не была внедрена злоумышленником.

Вычислительная эффективность отражает нагрузку на систему: чем меньше ресурсов требует метод, тем проще его использование в реальных условиях, особенно на ограниченных платформах.



Устойчивость к типовым атакам показывает, насколько метод способен противостоять распространенным угрозам, таким как внедрение бэкдоров, подмена компонентов или перезапись параметров модели.

Под прикладной универсальностью понимается способность метода работать с различными типами моделей, форматами и архитектурами – от классических нейросетей до специализированных встроенных решений.

Наконец, сложность интеграции оценивает трудозатраты на внедрение метода в существующие процессы: от простых инструментов, доступных «из коробки», до комплексных решений, требующих специализированной инфраструктуры.

На основе этих критериев проведена сравнительная оценка представленных подходов, результаты которой отражены в таблице 1.

ТАБЛИЦА 1. Сравнительная оценка методов верификации моделей ИИ

| Критерий                        | Криптографические методы | Watermarking / Fingerprinting | Кодирование с избыточностью | Аппаратные методы (TEE / TPM) |
|---------------------------------|--------------------------|-------------------------------|-----------------------------|-------------------------------|
| Надежность контроля целостности | 5                        | 3                             | 3                           | 5                             |
| Подтверждение подлинности       | 5                        | 4                             | 1                           | 4                             |
| Вычислительная эффективность    | 4                        | 4                             | 3                           | 3                             |
| Устойчивость к типовым атакам   | 4                        | 3                             | 2                           | 5                             |
| Прикладная универсальность      | 5                        | 3                             | 2                           | 2                             |
| Сложность интеграции            | 4                        | 3                             | 4                           | 2                             |
| Итог                            | 27                       | 20                            | 15                          | 21                            |

Как видно из таблицы 1, наивысший суммарный балл (27 из 30) набрали криптографические методы, что подтверждает их универсальность, надежность и относительно невысокую сложность интеграции. Эти методы обеспечивают как контроль целостности, так и подлинность источника, при

этом их реализация широко поддерживается существующими программными средствами.

Методы водяных знаков и отпечатков показывают хорошие результаты в защите авторства и контроля распространения, но уступают в надежности и применимости: не все модели допускают внедрение маркеров без потери точности, а сами маркеры можно удалить при переобучении модели.

Кодирование с избыточностью эффективно в условиях нестабильной передачи (например, в радиоканалах), но почти не применимо для защиты от умышленных атак. Кроме того, оно не решает задачу аутентификации источника.

Аппаратные методы (TEE/TPM) обеспечивают наивысшую степень защиты при исполнении модели, но требуют специфической инфраструктуры и глубокого вмешательства в архитектуру системы, что снижает их универсальность.

Таким образом, выбор подхода к верификации должен основываться на балансе между уровнем требуемой безопасности, техническими возможностями системы и характером использования модели. В большинстве случаев целесообразно комбинировать методы – например, объединять криптографическую верификацию с аппаратной защитой исполнения или применением скрытых маркеров.

#### **Список используемых источников**

1. IBM. Глобальный индекс внедрения искусственного интеллекта-2024 // ICT.Moscow. 2024. № 1. С. 12–28.
2. Guan X., Feng H., Zhang W., Zhou H., Zhang J., Yu N. Reversible Watermarking in Deep Convolutional Neural Networks for Integrity Authentication // Journal of Information Security Research. 2021. № 3. С. 45–55.
3. Neyigapula B. S. Secure AI Model Sharing: A Cryptographic Approach for Encrypted Key Exchange // International Journal of Artificial Intelligence and Machine Learning. 2024. Т. 4. № 1. С. 48–60.
4. Balan K., Learney R., Wood T. A Framework for Cryptographic Verifiability of End-to-End AI Pipelines // Advances in Secure Computing. 2025. № 2. С. 31–43.
5. Gibney E. Google unveils invisible 'watermark' for AI-generated text // Nature. 2024. Т. 627. № 8010. С. 104–105.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Ахrameевой К. А.*

УДК 004

А. И. Карышев (студент группы ИКБ-22, СПбГУТ), [karyshev.ai@sut.ru](mailto:karyshev.ai@sut.ru)

## OSINT В СОЦИАЛЬНЫХ СЕТЯХ: РАЗРАБОТКА ИНСТРУМЕНТА АВТОМАТИЗИРОВАННОГО АНАЛИЗА ЦИФРОВОЙ БЕЗОПАСНОСТИ АККАУНТОВ

*В статье предлагается идея создания автоматизированного инструмента, предназначенного для анализа цифровой безопасности аккаунтов пользователей в социальных сетях. Рассматриваются существующие OSINT-подходы и подчеркивается их значение в контексте социальной инженерии. Обосновывается необходимость автоматизации процессов аудита уязвимостей с использованием API популярных платформ (например, VK API, Telegram API и др.) Обсуждаются возможные архитектурные принципы будущей системы, основные этапы анализа и практическое значение такого инструмента.*

*OSINT, API, цифровая безопасность, социальные сети, цифровая открытость, социальная инженерия, автоматизированный анализ, аудит безопасности*

Современный цифровой мир, социальные сети и мессенджеры, предоставляют пользователям безграничные возможности для коммуникации, общения и участия в информационном обмене [1, 2]. При этом пользователи, не задумываясь о личной безопасности, сами выкладывают о себе значительный объем персональных данных и другой чувствительной информации, которая может использоваться против них самих в криминальных целях [1, 3, 4].

Одновременно с этим в значительной мере развивается направление OSINT (Open Source Intelligence). Это разведка на основе открытых источников, включающая в себя поиск и сбор разведывательной информации из общедоступных социальных сетей, мессенджеров, форумов и веб-сайтов. Инструментами OSINT активно пользуются органы разведки, обороны, безопасности, правопорядка. Большой интерес к эксплуатации таких инструментов проявляется со стороны разведывательных служб иностранных государств, а также различных злоумышленников с целью проведения социоинженерных атак [5]. На момент 2025 года наиболее часто используемым методом атак является социальная инженерия – она используется в 88 % случаев на частных лиц, а также в 50 % случаев при проведении атак на организации [6].

Методы поиска OSINT делятся на ручные и автоматизированные [2].

Ручной поиск предполагает самостоятельное исследование открытых источников, включая поиск в веб-браузере, использование запросов Google Dorks, просмотр социальных сетей и форумов, анализ комментариев. Google Dorks является специальным языком для извлечения информации, принадлежащим компании Google [8]. Основные операторы для Google:

- “word” – точное совпадение;
- -word – исключить из поиска;
- site:sut.ru – поиск в пределах сайта sut.ru;
- filetype:pdf – только pdf файлы;
- inurl:test – в URL встречается слово test;
- intext:test – в тексте встречается слово test.

Такой вид поиска (без применения средств автоматизации) используется в тех случаях, когда нужно произвести точечную проверку редких источников или провести небольшое исследование, не требующее сложной обработки больших данных.

Автоматизированный поиск предусматривает использование специальных программ и инструментов, которые запускают огромное количество запросов сразу по множеству ресурсов в поисках нужной нам информации [2]. Он значительно ускоряет процесс поиска информации, а также экономит время, особенно если перед нами стоит масштабное исследование. Примерами инструментов для проведения автоматизированного сбора информации являются:

- Sherlock – инструмент для поиска учетных записей по юзернейму на сотнях платформ (форумы, соцсети, GitHub и др.);
- Maltego – платформа для визуального анализа связей между объектами (люди, домены, IP-адреса). Интегрирует данные из открытых источников (WHOIS, DNS, соцсети) и позволяет строить графы взаимосвязей [7];
- GHunt – специализированный инструмент для анализа аккаунтов Google. Позволяет идентифицировать владельца по email, находить связанные YouTube-каналы, проверять активность в сервисах Google.

Эти инструменты являются лишь малой частью среди всего множества, которым можно воспользоваться при проведении разведки.

В рамках данной работы предложена идея создания программного инструмента, который будет осуществлять автоматический аудит открытых данных в профиле пользователя в выбранной им социальной сети. Такой инструмент может быть полезен как для личного пользования, так и для организаций, заинтересованных в проведении аудитов своих сотрудников и

партнеров. Кроме того, разработка подобного решения открывает перспективы для его интеграции в образовательные программы, направленные на формирование культуры безопасного поведения в сети Интернет.

Основной целью предлагаемого инструмента является реализация персонализированной оценки рисков цифровой открытости на основе анализа информации, доступной в учетной записи пользователей в социальных сетях. Его использование позволит повысить общий уровень цифровой безопасности, формируя индивидуальные рекомендации по снижению уязвимостей информации.

Научная новизна данной работы заключается в предложении концепции инструмента, ориентированного на автоматизированный аудит учетных записей в социальных сетях с последующей генерацией персонализированных рекомендаций по снижению уязвимости к методам социальной инженерии и OSINT-анализа.

На данный момент отсутствуют открытые или доступные решения, способные:

1. Проводить комплексную оценку цифровой безопасности пользователя в соцсетях;
2. Автоматически формировать отчеты с рекомендациями по повышению цифровой гигиены;
3. Интерпретировать данные не только с технической, но и с социально-психологической точки зрения, отражающей вероятные сценарии злоупотребления информацией (фишинг, создание досье и др.).

Предлагаемая модель объединяет сбор открытых данных, их интерпретацию в контексте социальной инженерии и формирование практических мер по снижению рисков. Такой подход делает инструмент применимым не только в исследовательской и образовательной среде, но и как практическое средство кибергигиены для конечного пользователя. Сравнительный анализ существующих решений с предлагаемым решением представлен на рисунке 1.

В задачи системы входят:

1. Автоматическое получение открытых данных профиля с использованием API выбранной пользователем платформы;
2. Классификация извлеченной информации по степени риска (низкий, средний, высокий);
3. Выявление признаков, указывающих на уязвимость к фишингу, про-  
файлингу и социальной инженерии;

#### 4. Формирование понятного отчета с рекомендациями по устранению выявленных угроз.

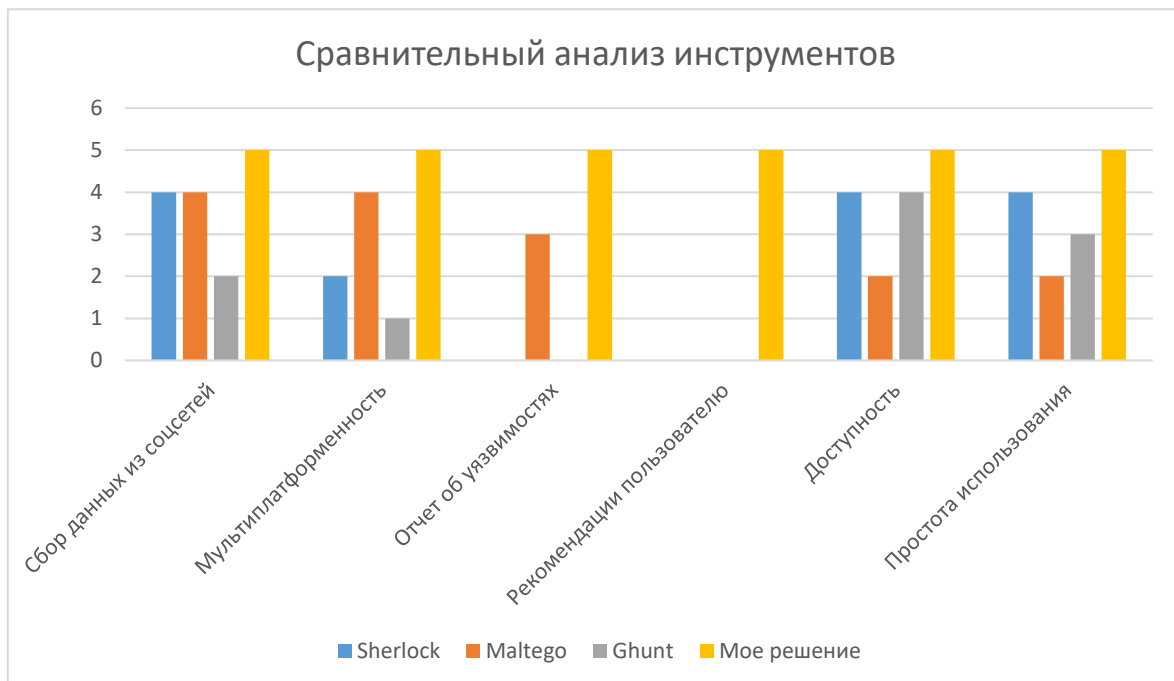


Рис. 1. Сравнительный анализ инструментов

##### Основные модули будущей системы:

- модуль подключения к API целевых платформ с поддержкой авторизации, токенов и лимитов запросов;
- модуль анализа метаданных (EXIF-файлы, геометки, временные метки);
- модуль проверки утечек (интеграция с инструментами, предоставляющими данный функционал);
- интерфейс пользователя для управления анализом и просмотра отчетов.

Ниже представлен пример работы будущего инструмента:

Пользователь выбирает социальную сеть или мессенджер (например, VK) и вводит свой юзернейм @exampleuser. Далее программа с помощью VK API:

Проверяет открытость профиля и отдельных блоков информации (дата рождения, номер телефона, место работы);

Сканирует публичные фотографии, извлекает EXIF-данные, проверяет наличие геометок;

Анализирует комментарии и активность на стене;

Сравнивает найденные адреса и номера с утекшими данными;

Возвращает вывод: «Ваш аккаунт содержит 7 потенциальных уязвимостей. Уровень риска: средний. Рекомендации: скрыть дату рождения, удалить геометки, изменить пароли и т.д.»

Предлагаемая идея направлена на решение одной из ключевых проблем цифровой эпохи – недостаточной осведомленности пользователей о собственных цифровых уязвимостях [9]. Разработка инструмента, реализующего автоматизированный аудит безопасности аккаунтов через API, позволит значительно повысить уровень цифровой гигиены как на индивидуальном, так и на организационном уровне [10].

#### Список использованных источников

1. 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.
2. Гамидов Т. О., Десницкий В. А., Дудкина О. С., Сахаров Д. В. Методы и методики анализа нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). Сб. науч. ст. VIII Международной научно-технической и научно-методической конференции: в 4 т. 2019. С. 317-320.
3. Донской Д. М., Карев А. С., Сахаров Д. В. Социальная инженерия и человеческий фактор в информационной безопасности // 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. 310-316.
4. Бударный Г. С., Дюсметова А. А., Казанцев А. А., Красов А. В. Социальная инженерия: ее методы и способы защиты // В сборнике: 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, 2023. С. 200-204.
5. Samokhvalov D. I. Machine learning-based malicious users' detection in the V Kontakte social network, 2020. т. 32. № 3. с. 109-118.
6. Positive Technologies. Анализ киберугроз за I квартал 2025 года. М.: Positive Technologies, 2025. с. 28-39
7. Шармаев В. И., Андреева Я. А., Василевский К. А.: Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT), 2022. № 2 (137). с. 45-50.
8. Korneev N.: The Attack Vector on the Critical Information Infrastructure of the Fuel and Energy Complex Ecosystem, 2021. С. 59-65.
9. Гордиенко В. В., Лисицин А. Л.: Технические и организационные методы борьбы с внутренними угрозами утечки информации организаций и предприятий, 2019, № 4 (24), с. 69-76.
10. Борисов С. В., Севостьянов В. А., Цветков А. Ю. Определение признаков фишинговых сообщений в электронной почте // В сборнике: Студенческая весна - 2023. Материалы 77-й региональной научно-технической конференции студентов, аспирантов и молодых ученых. Санкт-Петербург, 2023. С. 88-92.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Сахаровым Д. В.*

УДК 004.056.2

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ JAVASCRIPT-БИБЛИОТЕК ДЛЯ ВИЗУАЛИЗАЦИИ ГРАФОВ В СИСТЕМЕ МОНИТОРИНГА БЕСПРОВОДНЫХ СЕТЕЙ

**М. М. Ковцур** (к.т.н., доцент, доцент, доцент кафедры ИБКС, СПбГУТ)

**А. Ю. Киструга** (студент группы 1001А-21, СПбГУТ),

[anton.kistruga@uchiit.ru](mailto:anton.kistruga@uchiit.ru)

**В. Е. Филимонов** (студент группы Р-4108, ИТМО),

[vladislav.filimonov@uchiit.ru](mailto:vladislav.filimonov@uchiit.ru)

*Проведено сравнение JavaScript-библиотек D3.js, React Force Graph и React Sigma для визуализации графов в системах мониторинга Wi-Fi сетей на наборе данных из 13000+ устройств. React Force Graph показал наилучшую производительность и масштабируемость, D3.js – минимальное потребление памяти, React Sigma – оптимален для графов среднего размера.*

*визуализация графов, мониторинг Wi-Fi сетей, JavaScript, D3.js, React Force Graph, React Sigma*

Мониторинг беспроводных сетей Wi-Fi в корпоративных и государственных инфраструктурах требует эффективной визуализации данных в виде графов для быстрого обнаружения угроз. Графовое представление помогает выявлять несанкционированные подключения, анализировать текущую обстановку и обнаруживать аномальные связи, обеспечивая оперативное реагирование на инциденты безопасности. Данная работа сравнивает JavaScript-библиотеки для визуализации графов с целью выбора оптимального инструмента отображения WLAN-устройств [1].

Основные требования, предъявляемые к визуализации, включают производительность, интерактивность, масштабируемость, информативность, реактивность [2].

Для анализа выбраны JavaScript-библиотеки визуализации графов: D3.js (v7.9.0), React Force Graph (v1.47.6 и 2D v1.27.1) и React Sigma (v1.2.35). Выбор обусловлен их популярностью в сообществе разработчиков, различными подходами к визуализации (от низкоуровневого D3.js до специализированных решений) и хорошей совместимостью с современными фреймворками, включая React [3].



Для анализа библиотек визуализации графов использовались реальные данные из системы мониторинга беспроводной сети организации публичного сектора. Набор включает более 13000 уникальных устройств, в том числе около 50 защищаемых точек доступа WLAN и множество сторонних устройств, отслеживаемых несколькими сенсорами одновременно. Это увеличивает сложность графа из-за роста числа связей между узлами. Реалистичность данных обеспечивает достоверность результатов сравнения библиотек [4].

Тестирование библиотек проводилось на современном аппаратном и программном обеспечении (таблица 1), что позволило объективно оценить их производительность в типичных условиях разработки.

ТАБЛИЦА 1. Параметры тестовой платформы для сравнения библиотек

| Аппаратное окружение                                    | Программное окружение                             |
|---------------------------------------------------------|---------------------------------------------------|
| MacBook Pro (чип M3 Pro)                                | Операционная система: macOS Sequoia (версия 15.4) |
| Оперативная память: 18 ГБ                               | Браузер: Google Chrome (версия 135)               |
| SSD-накопитель: 512 ГБ                                  |                                                   |
| Графический процессор: интегрированный GPU Apple M3 Pro |                                                   |

Сравнение функциональных возможностей рассматриваемых библиотек представлено в таблице 2.

ТАБЛИЦА 2. Функциональные возможности

| Характеристика       | D3.js       | React Force Graph    | React Sigma     |
|----------------------|-------------|----------------------|-----------------|
| Версия               | 7.9.0       | 1.47.6 / 1.27.1 (2D) | 1.2.35          |
| Размер библиотеки    | ~39 KB      | ~12 KB               | ~57 KB          |
| Зависимости          | Минимальные | React, three.js (3D) | React, Sigma.js |
| Тип рендеринга       | SVG, Canvas | WebGL, Canvas        | Canvas, WebGL   |
| Поддержка TypeScript | Да          | Да                   | Частичная       |

| Характеристика                 | D3.js                      | React Force Graph     | React Sigma         |
|--------------------------------|----------------------------|-----------------------|---------------------|
| Поддержка 2D                   | Да                         | Да                    | Да                  |
| Поддержка 3D                   | Через расширения           | Да                    | Нет                 |
| Алгоритмы компоновки           | Многочисленные             | Force-directed        | ForceAtlas2, другие |
| Кластеризация                  | Ручная реализация          | Встроенная            | Встроенная          |
| Фильтрация данных              | Ручная реализация          | Встроенная            | Встроенная          |
| Масштабирование                | Ручная реализация          | Встроенная            | Встроенная          |
| Перетаскивание узлов           | Ручная реализация          | Встроенная            | Встроенная          |
| Выделение узлов/связей         | Ручная реализация          | Встроенная            | Встроенная          |
| Поиск                          | Ручная реализация          | Необходима реализация | Встроенная          |
| Интеграция с React             | Требует обертки            | Нативная              | Нативная            |
| Интеграция с Angular           | Требует обертки            | Требует обертки       | Требует обертки     |
| Интеграция с Vue               | Требует обертки            | Требует обертки       | Требует обертки     |
| Стилизация узлов               | Полная                     | Высокая               | Высокая             |
| Стилизация связей              | Полная                     | Высокая               | Высокая             |
| Собственные формы узлов        | Да                         | Да                    | Да                  |
| Текстовые метки                | Полная настройка           | Встроенные            | Встроенные          |
| Оптимизация для больших графов | Требует ручной оптимизации | Высокая               | Высокая             |
| Поддержка WebWorkers           | Ручная реализация          | Встроенная            | Встроенная          |
| GitHub Stars                   | >104K                      | >7K                   | >400                |

Для сравнения библиотек была использована методика оценки производительности, включающая следующие показатели (табл. 3):

- время рендеринга – время от момента начала рендеринга до первого отображения графа (мс);
- время инициализации графа – полное время, затрачиваемое на подготовку, размещение и первоначальную стабилизацию графа (мс);
- использование памяти – объем оперативной памяти, потребляемый вкладкой браузера при работе с визуализацией (МБ);
- узлы – количество отображаемых устройств в графе;
- связи – количество отображаемых связей между узлами.

ТАБЛИЦА 3. Производительность библиотек

| Библиотека           | Узлы  | Связи | Время рендеринга (мс) | Время стабилизации (мс) | Память (МБ) |
|----------------------|-------|-------|-----------------------|-------------------------|-------------|
| D3.js                | 514   | 314   | 220.60                | 3821.70                 | 54          |
|                      | 1014  | 814   | 220.60                | 3918.80                 | 54          |
|                      | 5014  | 4815  | 220.60                | 16304.60                | 54          |
|                      | 13525 | 21814 | 220.60                | 58688.00                | 58          |
| React Force Graph 2D | 514   | 314   | 31.70                 | 43.60                   | 84          |
|                      | 1014  | 814   | 27.10                 | 33.00                   | 75          |
|                      | 5014  | 4815  | 27.40                 | 47.10                   | 91          |
|                      | 13525 | 21814 | 28.50                 | 59.80                   | 141         |
| React Sigma          | 514   | 314   | 30.60                 | 2995.00                 | 131         |
|                      | 1014  | 814   | 42.30                 | 3008.80                 | 166         |
|                      | 5014  | 4815  | 79.50                 | 10733.00                | 337         |
|                      | 13525 | 21814 | 94.20                 | 41280.60                | 1022        |

Для более наглядного представления масштабируемости библиотек рассмотрим в таблице 4, как меняется время стабилизации графа в зависимости от количества узлов и связей.

Из таблицы видно, что React Force Graph 2D демонстрирует наилучшую масштабируемость, особенно при переходе от ~1000 к ~5000 узлам, где время стабилизации увеличивается всего в 2.51 раза, в то время как у D3.js

и React Sigma этот показатель составляет 4.16x и 3.57x соответственно. Более того, при переходе к полному набору данных (~13500 узлов) время стабилизации у React Force Graph 2D даже уменьшается (коэффициент 0.58x), что может указывать на оптимизацию алгоритма для очень больших графов.

ТАБЛИЦА 4. Изменение времени стабилизации графа

| Библиотека           | 500→1000 узлов | 1000→5000 узлов | 5000 →13500 узлов |
|----------------------|----------------|-----------------|-------------------|
| D3.js                | 1.03x          | 4.16x           | 3.60x             |
| React Force Graph 2D | 0.006x         | 2.51x           | 0.58x             |
| React Sigma          | 1.00x          | 3.57x           | 3.85x             |

На основании результатов экспериментального исследования производительности библиотек визуализации графов получены следующие выводы.

React Force Graph 2D продемонстрировала оптимальные показатели по всем исследуемым параметрам: минимальное время компоновки и стабилизации, максимальную частоту кадров и умеренное потребление памяти. Данная библиотека рекомендуется для визуализации крупномасштабных графов в системах мониторинга беспроводных сетей.

D3.js характеризуется низким потреблением памяти, но значительно уступает в скорости обработки графовых структур. Библиотека целесообразна при ограниченных ресурсах памяти и необходимости расширенной кастомизации визуализации.

React Sigma занимает промежуточную позицию по временным характеристикам, однако демонстрирует максимальное потребление памяти с тенденцией к росту при увеличении размера графа. Рекомендуется для графов средней размерности при необходимости компромисса между производительностью и функциональностью.

#### Список используемых источников

1. Ковцур М. М., Сахаров Д. В., Бирих Э. В., Дрепа В. Е. Метод обнаружения WLAN точек доступа нарушителя в распределенной ИСПДн // Электросвязь. 2024. № 12-2. С. 60-69. DOI 10.34832/ELSV.2024.61.12.008. EDN SABMPS.
2. Зебзеев Е. А., Герлинг Е. Ю., Киструга А. Ю., Ковцур М. М. Разработка методики анализа трафика сети WLAN IEEE 802.1X // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 3. С. 80-85. DOI 10.46418/2079-8199\_2024\_3\_13. EDN: OSTBCQ.

3. 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.

4. Ильин Я. А., Ковцур М. М., Боднарчук, К. М. Исследование зоны покрытия WLAN для повышения уровня информационной безопасности корпоративной сети // 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. 310-314. EDN: VDPSGA.

## УДК 004.423.2

**А. В. Красов** (научный руководитель, к.т.н., доцент, СПбГУТ)

**Е. Н. Пимашин** (магистрант группы ИКТБ-48м, СПбГУТ),

[pimashin.en@sut.ru](mailto:pimashin.en@sut.ru)

**С. А. Раковский** (аспирант группы БТАО-01-22, РТУ МИРЭА)

## ХЕШИРОВАНИЕ ИСХОДНОГО КОДА С ИСПОЛЬЗОВАНИЕМ TREE-SITTER: CALL HASH, IMP HASH, SEM HASH

*В настоящей работе представлена комплексная методика хеширования исходного кода на основе абстрактного синтаксического дерева (AST) с применением утилиты tree-sitter. Разработаны три специализированных хеша: call hash, imp hash и sem hash, учитывающих соответственно вызовы функций, операторы импорта и семантическую структуру дерева вызовов. Описаны алгоритмы извлечения, нормализации и хеширования, а также представлены результаты эмпирических исследований на репозиториях различного масштаба.*

*хеширование исходного кода, tree-sitter, AST, call hash, imp hash, sem hash*

Современные задачи индексирования, обнаружения плагиата и анализа версий исходного кода требуют надежных и одновременно малочувствительных к синтаксическим деталям методов идентификации программных артефактов [1]. В данной работе предлагается использовать библиотеку tree-sitter для построения абстрактного синтаксического дерева (AST), на основании которого реализуются три хеш-метода [2].

Метод call hash извлекает из AST все узлы вида call\_expression и new\_expression посредством запросов библиотеки tree-sitter. Последовательность идентификаторов функций нормализуется: выполняется лексикографическая сортировка, конкатенация строк и последующее вычисление sha-256. Такой подход гарантирует, что хеш отражает набор и частоту вызовов функций без учета их порядка в коде.

Метод imp hash фокусируется на узлах import\_statement и import\_from, собранных через tree-sitter. После извлечения операторов импорта производится сортировка по полной строке импорта, образуется единый текст для хеширования, что обеспечивает устойчивость к изменению порядка и к дублирующимся импортам.

Метод sem hash реализуется путем обхода AST с определением глубины каждого узла вызова. Сначала подсчитывается количество узлов call\_expression на каждом уровне вложенности. Далее формируется вектор

вида [(уровень, число\_вызовов), ...], который сортируется по уровню, приводится к строковому представлению без конкретных имен и передается в sha-256, затем формируется итоговая строка вида «количество вызовов: sha-256». Такая нормализация убирает зависимости от наименований и структурных изменений, сохраняя семантику распределения вызовов.

В таблице 1 представлен алгоритм (рис. 1) формирования итогового хеша из абстрактно синтаксического дерева, сформированного tree-sitter.

ТАБЛИЦА 1. Формирование хеша исходного кода из AST

| Метод     | Объект AST                          | Нормализация                                                            | Вычисление sha-256              |
|-----------|-------------------------------------|-------------------------------------------------------------------------|---------------------------------|
| call hash | узлы call_expression                | лексикографическая сортировка, конкатенация, удаление дубликатов        | хеш от конкатенированной строки |
| imp hash  | узлы import_statement и import_from | сортировка по полному тексту, удаление дубликатов                       | хеш от единого текста           |
| sem hash  | вся иерархия вызовов                | подсчет числа вызовов на каждом уровне, сортировка пар (уровень, число) | хеш от строкового вектора       |

```
Imports:
b'child_process'

Calls:
b'console.error'
b'then'
b'then.catch'

Semantic dict:
{b'then.catch': {2: 1}, b'then': {4: 1}, b'console.error': {5: 1}}

Semantic calls:
b'2:1'
b'4:1'
b'5:1'

Glued imports:
b'child_process'

Glued calls:
b'console.errorthen.then.catch'

Glued semantic calls:
b'2:14:15:1'

Imports hash: f2d8255ad6e0966510d0b96d9557165262cec52f293a950e7cdabb931d753a63d
Calls hash: 47f0c953a234fa65e98b2a981fdb57c280529ac0828676ff194211805a667ecc
Semantic hash: 3:db05d87c4d1c85ef66210649d95bb1a152373c693a79d59f3e89bbae6203ba36
```

Рис. 1. Порядок формирования хешей из исходного кода

Таблица 2 описывает сравнительный анализ существующих решений, которые могут решать поставленную задачу. Sha-256 подходит для потокового сканирования, поскольку, его можно использовать, как индекс в любой из существующих СУБД, а нечеткие хеши придется проверять по всей базе по соответствующему алгоритму, что делает потоковую обработку невозможной. Но при этом sha-256 или любой другой криптографический хеш имеет лавинный эффект, что приводит к тому, что любое изменение в файле выражается в значительном изменении итогового хеша, по которому будет индексироваться поиск в СУБД.

ТАБЛИЦА 2. Сравнительный анализ с существующими подходами

| Метод     | Подходит для потокового сканирования | Чувствителен к изменениям | Учитывает семантику кода | Языконезависим |
|-----------|--------------------------------------|---------------------------|--------------------------|----------------|
| sha-256   | ✓                                    | ✓                         | ✗                        | ✓              |
| ssdeep    | ✗                                    | ✗                         | ✗                        | ✓              |
| sdhash    | ✗                                    | ✗                         | ✗                        | ✓              |
| call hash | ✓                                    | ✗                         | ✓                        | ✓              |
| imp hash  | ✓                                    | ✗                         | ✓                        | ✓              |
| sem hash  | ✓                                    | ✗                         | ✓                        | ✓              |

В таблице 3 представлен эмпирический анализ записи и чтения из базы данных существующих методов. Подсчет хешей и запись в БД не является сложной для вычисления задачей, однако нечеткие хеши требуют сравнительной проверки напротив всех хешей из БД, что и требует больших вычислительных мощностей, требования к которым будут расти по мере роста количества записей в БД. А sha-256 и хеши из этой статьи могут быть использованы, как индексы, что позволяет искать эти хеши за асимптотическую сложность  $O(\log(n))$ . Эксперимент проводился на 5 последних релизах 100 наиболее популярных пакетов репозитория открытого кода Node Package Manager (npm) и Python Package Index (PyPI) [3].



ТАБЛИЦА 3. Эмпирическое сравнение с существующими подходами

| Метод     | Подсчет + вставка в БД (мс) | Проверка хеша в БД (мс) |
|-----------|-----------------------------|-------------------------|
| sha-256   | 7,0                         | 1,0                     |
| ssdeep    | 17,1                        | 562,2                   |
| sdhash    | 27,0                        | 743,7                   |
| call hash | 19,4                        | 1,0                     |
| imp hash  | 15,2                        | 1,0                     |
| sem hash  | 37,8                        | 1,0                     |

Таблица 4 описывает результативность предложенных хешей по поиску подобных исходных кодов. Отдельно sem hash не показал ожидаемой результативности, потому что есть вероятность подмены вызовов, что не повлияет на изменение sem hash и неизбежно приведет к коллизии. Наиболее эффективно показала себя комбинация из всех трех хешей, потому что она балансирует слабые стороны каждого отдельного метода. Слабыми сторонами предложенных подходов являются обфускация графа исполнения кода, потому что она меняет поведение кода, а значит и его AST, и малые по размеру файлы, в которых вероятность коллизий очень высока. Однако комбинация хешей минимизирует эти коллизии за счет более однозначной привязки к импортам, именам вызовов и структуре AST.

ТАБЛИЦА 4. Оценка результативности предложенных хешей

| Комбинация хешей | F-мера ( %) |
|------------------|-------------|
| imp hash         | 10 %        |
| call hash        | 15 %        |
| sem hash         | 54 %        |
| imp + call       | 32 %        |
| imp + sem        | 66 %        |
| call + sem       | 93 %        |
| imp + call + sem | ~100 %      |

В работе представлена комплексная методика хеширования исходного кода на основе AST с использованием tree-sitter. Предложенные функции call hash, imp hash и sem hash демонстрируют высокую производительность при подсчете и вставке в базу данных (15–38 мс) и мгновенную проверку хеша ( $\approx 1$  мс), что сопоставимо с sha-256 и значительно быстрее нечетких хешей (ssdeep, sdhash) при операциях поиска. Sem hash обеспечивает наибольшую семантическую чувствительность за счет учета вызовов [4], call hash и imp hash гарантируют нечувствительность к перестановкам в коде.

Языконезависимость и возможность потоковой обработки делают предложенный подход применимым для задач индексирования, обнаружения плагиата и анализа версий в крупных кодовых базах [5].

#### Список используемых источников

1. Xie Y., Lin J., Dong H. et al. Survey of Code Search Based on Deep Learning // ACM Trans. Softw. Eng. Methodol. 2023. Vol. 1, № 1. Art. 1. 28 с.
2. Parvathy R., Thushara M. G. AST-Based and Token-Based Neural Networks for Source Code Classification: A Comparative Performance Analysis // Proc. 15th Int. Conf. on Computing Communication and Networking Technologies (ICCCNT), 2–4 July 2024, Bengaluru, India. New York: IEEE, 2024. С. 1–6.
3. Sun Z., Li L., Liu Y. et al. On the Importance of Building High-Quality Training Datasets for Neural Code Search // Proc. IEEE/ACM 44th Int. Conf. Software Engineering (ICSE '22), 14–22 May 2022, Pittsburgh, PA, USA. New York: ACM, 2022. С. 1609–1620.
4. Liu S., Chen Y., Wu K. Graph-of-Code: Semantic Clone Detection Using Graph Fingerprints // IEEE Trans. Software Eng. 2023. Т. 49, № 8. С. 3972–3988.
5. Wang X., Wu Q., Zhang H. et al. HELoC: Hierarchical Contrastive Learning of Source Code Representation // Proc. IEEE/ACM 30th Int. Conf. Program Comprehension (ICPC '22), 16–17 May 2022, Virtual Event, USA. New York: ACM, 2022. С. 354–365.

*Статья представлена научным руководителем, заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом Красовым А. В.*

УДК 004.056.53

С. В. Лагутина (магистрант группы ИКТБ-48М, СПбГУТ)

Д. А. Лебедева (студент группы ИБС-02, СПбГУТ), [lebedeva.da@sut.ru](mailto:lebedeva.da@sut.ru)

## АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДОВ ЗАЩИТЫ ОТ ФИШИНГА

*Фишинг – серьезная угроза информационной безопасности в цифровую эпоху. Усложнение защиты стимулирует разработку техник обмана. Цель исследования заключается в анализе научных трудов, связанных с фишинговыми атаками, способами противодействия и методиками обучения пользователей распознаванию и реагированию. Результат представляет собой систематизацию научных трудов по четырем критериям. Выявлена важность повышения осведомленности пользователей.*

*фишинг, социальная инженерия, кибератаки, осведомленность о безопасности*

Жертвами фишинговых атак чаще становятся те, кто недостаточно осведомлен о такой возможности и не встречался с фишингом ранее на практике. Интерактивные тренинги – эффективный способ повышения кибербезопасности, развивающий навыки выявления и предотвращения фишинга, снижающий риски и укрепляющий культуру безопасности. Согласно аналитическому отчету Positive Technologies «Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года», объектами атак, ставших успешными, в 50 % случаев для организаций и в 88 % для частных лиц являются люди [1]. Кроме того, 50 % успешных атак по распространению вирусного программного обеспечения в организациях осуществлено посредством электронной почты.

Целью данной работы является определение трендов и успешных способов борьбы с фишингом для создания эффективных методик обучения кибербезопасности. В настоящей статье анализируются подходы к противодействию фишингу и обучению сотрудников для повышения осведомленности о безопасности. Проведено исследование, систематизирующее научные работы, связанные с фишингом, выявлены цели и методы злоумышленника, а также представлен анализ эффективности различных методов противодействия этому типу атаки.

Всего рассмотрено 35 источников за период от 2021 до 2025 года. Из них 7 работ соотечественников и 28 исследований зарубежных авторов. Труды разделены на 4 категории: 13 работ исследуют способы фишинговой атаки, 15 описывают технические способы защиты, 18 посвящены повыше-

нию осведомленности о фишинге и 12 описывают проведенные экспериментальные исследования в области имеющихся у тех или иных групп знаний до и после проведения обучений в различных формах.

Существуют различные стратегии фишинга, каждая из которых имеет свои особенности [2]. К наиболее распространенным методам относят подделку сайтов – создание фальшивых веб-страниц, имитирующих легитимные, например, с целью сбора учетных данных пользователей. Рисунок 1 иллюстрирует, как злоумышленник, имитируя оригинальный сайт, получает несанкционированный доступ к учетной записи пользователя-жертвы. Злоумышленники часто используют поддельные email-адреса, рассылая фальшивые письма от имени известных организаций (пример показан на рисунке 2). Подобные атаки, как правило, массовые и нацелены на множество получателей. Часто злоумышленники подменяют вложения, используя фишинговые письма с вредоносными файлами, заражающими устройство при открытии. Схема подобной атаки показана на рисунке 3. Открытие такого файла запускает вредоносный код на компьютере жертвы.

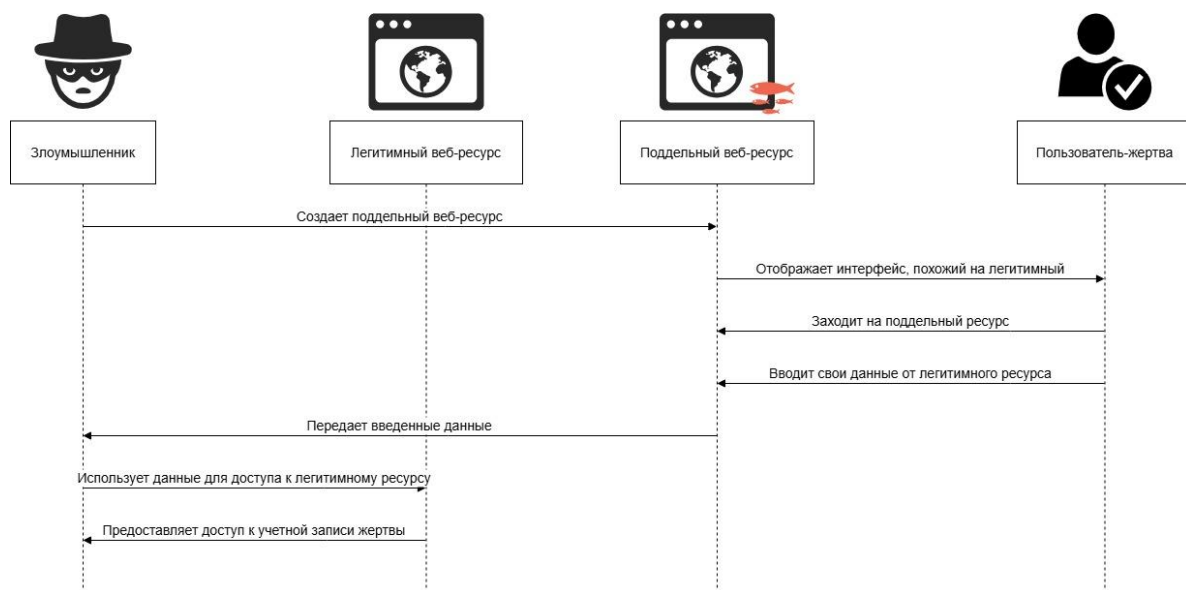


Рис. 2. Схема: пример атаки с помощью подделки веб-ресурса

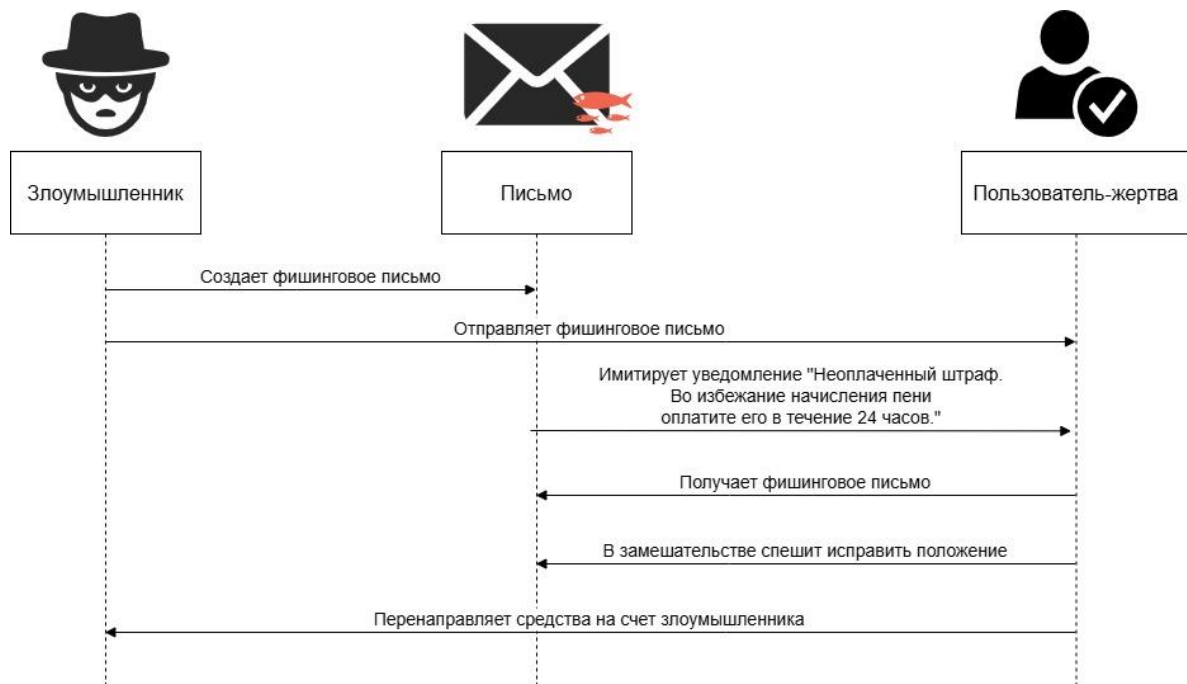


Рис. 2. Схема: пример атаки с помощью электронной почты

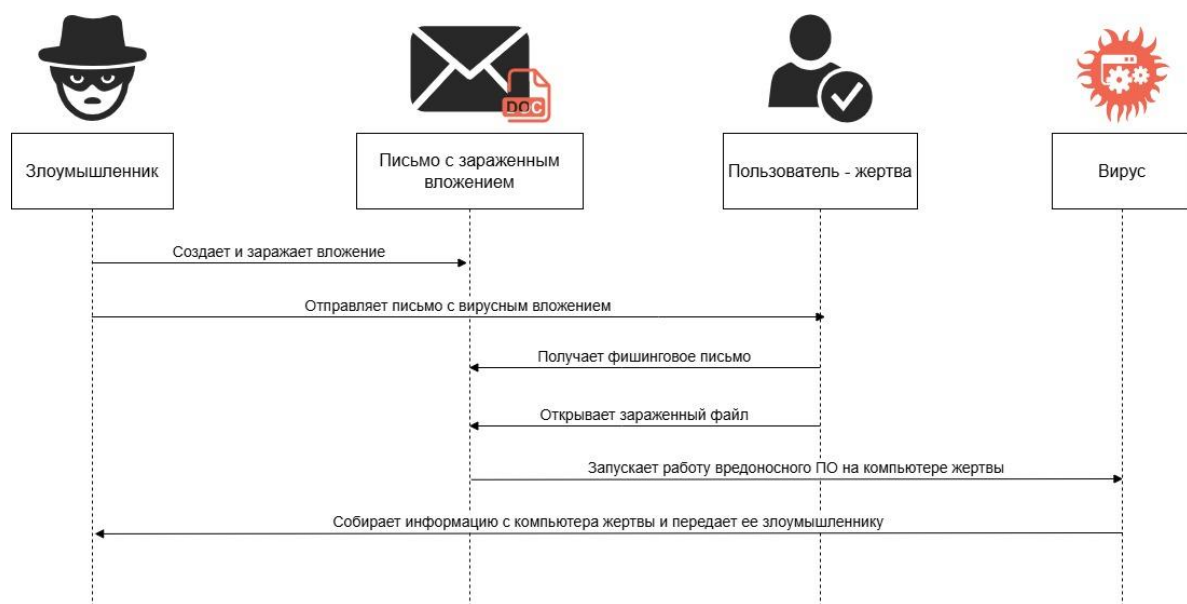


Рис. 3. Схема: пример атаки с помощью зараженного вложения

В изученных научных работах предложены различные технические решения для защиты от фишинга [3]. Подчеркивается важность использования современных систем обнаружения фишинга, анализирующих URL-адреса, а также внедрения программного обеспечения для фильтрации нежелательной почты. Отмечается эффективность двухфакторной аутентификации для повышения безопасности учетных записей. Однако, наряду с техническими мерами, особое внимание уделяется обучению сотрудников, как наиболее

эффективному способу формирования критического мышления и навыков распознавания фишинговых угроз.

Проанализированные тестовые исследования и опросы показали уровень осведомленности разных групп пользователей о фишинге и возможностях злоумышленников. Выяснилось, что значительная часть респондентов изначально не знакома с базовыми понятиями кибербезопасности и, как следствие, не осведомлена о фишинговых атаках [4]. Пользователи чаще переходят по ссылкам в фишинговых письмах, если доверяют источнику, особенно в социальных сетях. Обучение признано эффективным, однако практическое применение знаний требует дальнейшего изучения. Подчеркивается необходимость индивидуальных образовательных программ для разных групп пользователей.

Исследования описывают разнообразные подходы к повышению осведомленности сотрудников в области кибербезопасности, включая лекционно-тестовую форму обучения. Этот метод, достаточно распространенный, предполагает предоставление участникам теоретического материала с последующей проверкой усвоенных знаний посредством тестирования. В ряде работ отмечается потенциальная польза такого формата, однако его эффективность зачастую ставится под сомнение. Несмотря на удобство лекционно-тестового подхода, исследования свидетельствуют о значительно большей эффективности практических тренировок для пользователей [5]. Более современные исследования акцентируют внимание на значимости моделирования реальных угроз, например, имитации фишинговых атак. Участники, сталкивающиеся с подобными симуляциями, получают возможность применять полученные знания в практической деятельности, что способствует более глубокому усвоению и удержанию информации. Следовательно, они учатся распознавать угрозы в условиях реальной действительности, что, в конечном итоге, повышает эффективность применения полученных знаний о фишинге, и защищенность организаций от подобных атак.

В заключение, фишинг представляет собой значительную угрозу в современном цифровом пространстве, и единственным надежным способом минимизации риска является сочетание обучения сотрудников и внедрения технологий. Для повышения уровня безопасности необходима комплексная стратегия, включающая как технические меры, так и развитие осведомлен-

ности на всех уровнях организации. Наиболее эффективным методом обучения сотрудников является совмещение теоретической базы и моделирования фишинговых атак для тренировки полученных навыков на практике.

#### Список используемых источников

1. Актуальные киберугрозы: IV квартал 2024 года I квартал 2025 года. // Аналитический отчет Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id21> (дата обращения 08.04.2025).
2. Стеценко Ю. А., Холодковская Н. С. Мошенничество в сети интернет //Вестник Таганрогского института имени АП Чехова. 2021. № 2. С. 75-80.
3. Zieni R., Massari L., Calzarossa M. C. Phishing or not phishing? A survey on the detection of phishing websites //IEEE Access. 2023. Т. 11. С. 18499-18519.
4. Maimon D. et al. A routine activities approach to evidence-based risk assessment: Findings from two simulated phishing attacks //Social Science Computer Review. 2023. Т. 41. № 1. С. 286-304.
5. Beu N. et al. Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation //Computers & Security. 2023. Т. 131. С. 103313.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Витковой Л. А.*

УДК 004.056

**Г. А. Манохина** (студент группы ИБС-12, СПбГУТ), [manohina.ga@sut.ru](mailto:manohina.ga@sut.ru)  
**И. Е. Пестов** (к.т.н., доцент, доцент кафедры ЗСС, СПбГУТ)

## МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО КОМПЛЕКСА СРЕДСТВ ВИРТУАЛИЗАЦИИ «БРЕСТ»

*Исследуется отечественный программный комплекс средств виртуализации «Брест», предназначенный для обеспечения информационной безопасности критически значимых объектов. Акцент сделан на анализе механизмов защиты, включая доверенную загрузку, контроль целостности, регистрацию событий и управление доступом. Исследование актуально ввиду возрастающих угроз кибератак и необходимости внедрения решений в условиях активного процесса импортозамещения.*

*виртуальные машины, программный комплекс, средства виртуализации, механизмы контроля*

Современная информационная среда характеризуется возрастающей сложностью и разнообразием угроз кибербезопасности. Это требует постоянного повышения уровня защищенности информационных систем, особенно тех, которые используются государственными структурами и стратегическими предприятиями страны. Для защиты от атак используется отечественный программный комплекс (ПК) средства виртуализации (СВ) «Брест», разработанный специально для удовлетворения требований по защите конфиденциальных данных [1].

Цель данной статьи – проанализировать существующие механизмы обеспечения информационной безопасности ПК СВ «Брест».

Для предотвращения запуска виртуальных машин (ВМ) с некорректными или потенциально опасными изменениями используется функция доверенной загрузки ВМ [2]. Она состоит из трех ключевых элементов:

- Механизм контроля конфигурации виртуального оборудования. Все данные о конфигурации сохраняются в защищенной базе данных (БД) PostgreSQL, доступной только авторизованным пользователям;
- Механизм контроля файлов виртуальной базовой системы ввода-вывода (загрузчиков). Используется алгоритм расчета контрольных сумм («отпечатков конфигурации») для подтверждения их целостности;
- Механизм контроля целостности исполняемых файлов гостевой операционной системы (ОС). Применяется аналогичная процедура расчета контрольных сумм для верификации исполняемых файлов ВМ.



- В ПК СВ «Брест» предусмотрен механизм контроля целостности состояния исполняемых файлов и иных элементов виртуальной инфраструктуры. В его основу заложены следующие элементы:

- Контроль целостности файлов виртуальной базовой системы ввода-вывода;
- Контроль запуска исполняемых файлов формата ELF, позволяющий проверять наличие электронных цифровых подписей (ЦП) и запрещать запуск неподписанного/поврежденного программного обеспечения (ПО);
- Механизм регламентного контроля целостности Another File Integrity Checker (AFICK), используемый для периодической проверки и мониторинга целостности системных файлов.

Эти меры предотвращают внедрение стороннего вредоносного ПО и гарантируют надежность системы.

В ПК СВ обеспечивается регистрация событий безопасности, связанных с функционированием СВ, и оповещение администратора безопасности СВ о событиях безопасности. Состав регистрируемой информации соответствует ГОСТ Р 59548-2022.

Данная информация помогает выявлять инциденты и нарушения безопасности, позволяя оперативно реагировать на угрозы. Механизмы регистрации событий работают совместно с системой журналирования ОС «Astra Linux Special Edition».

Предусматривается распределение прав доступа между различными категориями пользователей и объектами виртуализации [3]. Выделяются четыре ключевые роли:

- Администратор средства виртуализации: обладает широкими правами, позволяющими конфигурировать инфраструктуру и назначать права другим пользователям;
- Администратор безопасности: занимается контролем безопасности и ведением журнала событий;
- Разработчик ВМ: создает и управляет ВМ;
- Администратор ВМ: получает доступ к определенной ВМ для ее обслуживания.

Кроме этого, предусмотрены гибкие механизмы ролевого управления доступом, основанные на механизме Access Control Lists (ACL), позволяющие индивидуально настроить права каждого пользователя относительно конкретных ресурсов.

Компоненты виртуальной инфраструктуры подлежат регулярному резервированию, что минимизирует риск потери данных в результате сбоев/атак. Доступны разные способы резервного копирования:

- Полное резервирование ВМ и их конфигураций;
- Копирование параметров настройки средства виртуализации;
- Сохранение записей о событиях безопасности.

Для этих целей используются стандартные инструменты резервного копирования ОС, такие как Bacula, rsync, tar и другие.

ПК СВ предоставляет механизмы, контролирующие потоки данных между ВМ и внешним миром. Используются следующие технологии:

- Сетевые фильтры iptables и nftables, управляемые администратором и контролируемые службой Libvirt;
- Использование технологии Open vSwitch (OVS) для изоляции виртуальных сетей с поддержкой драйверов VLAN и VXLAN;
- Правила сетевой фильтрации («группы безопасности»), регулирующие сетевой трафик виртуальных машин.

Для того, чтобы исключить возможность компрометации данных ВМ путем случайного/преднамеренного доступа к остаточной информации в памяти, используются следующие методы:

- Очистка освобожденных блоков памяти. После освобождения блока памяти (или раздела страничного обмена) он немедленно очищается;
- Мониторинг угроз и блокировка изменений ядра. Модуль kkg следит за состоянием ядра ОС и блокирует любые попытки внесения несанкционированных изменений;
- Применение специализированных технологий виртуализации таких, как KVM и QEMU. Они создают изолированную среду исполнения для ВМ, повышая общую степень защиты от потенциальных угроз, направленных на эксплуатацию ошибок в работе памяти.

Для предотвращения запуска неизвестных/вредоносных программ в виртуальной среде предусмотрена технология контроля целостности исполняемого кода. Она включает:

- Проверку ЦП исполняемых файлов формата ELF. Только подписанный код может быть запущен в системе. Этот механизм позволяет гарантированно убедиться в происхождении и целостности исполняемых файлов;
- Режим Киоск-2, позволяющий ограничивать набор программ, доступных для выполнения пользователями. Уровень ограничений определяется маской киоска, которая накладывается на доступ к каждому приложению при попытке запуска.

Система идентификации и аутентификации в ПК СВ строится на современных стандартах и практикует следующие подходы:

- Идентификация через Pluggable Authentication Module (PAM). Система осуществляет проверку пользователя против БД пользователей и паролей ОС, что делает возможным поддержку широкого спектра методов аутентификации;

- Централизованная аутентификация через службу FreeIPA. При активации дискреционного режима пользователи проходят аутентификацию через центральную службу каталогов LDAP и протокол Kerberos. Это позволяет поддерживать единый источник данных о пользователях и обеспечивать масштабируемость инфраструктуры.

Такая архитектура повышает прозрачность управления пользователями и снижает риск ошибок, возникающих при ручном управлении учетными записями.

ПК СВ предлагает ряд инструментов для централизованного управления ВМ и взаимодействующими объектами виртуализации [4]. Ключевыми инструментами являются:

- Командная строка: интерфейсы командной строки (oneimage, onetemplate, onevm) позволяют администраторам легко управлять образами, шаблонами и запущенными ВМ;

- Веб-интерфейс: он упрощает визуализацию и администрирование ВМ и сервисов виртуализации.

Также имеется поддержка миграции ВМ между серверами виртуализации. Миграция возможна как с остановкой работы ВМ, так и в режиме live migration (без прерывания работы), если используется общее хранилище образов.

ВМ могут объединяться в кластеры высокой доступности, обеспечивающие отказоустойчивость инфраструктуры. Кластеры создаются с целью автоматического переноса ВМ на другой узел в случае выхода из строя текущего узла виртуализации. Это достигается благодаря наличию централизованной службы планирования, которая распределяет нагрузку между серверами виртуализации, сохраняя баланс ресурсов и стабильность работы ВМ.

Чтобы гарантировать своевременное устранение уязвимостей и поддержание работоспособности, предусмотрена процедура регулярного обновления программного обеспечения комплекса. Обновления выпускаются в плановом и внеочередном порядке, содержат исправления известных проблем и повышение уровня безопасности. Процесс обновления проводится через стандартные средства ОС «Astra Linux Special Edition» [5]:

- Пакет fly-astra-update;
- Инструмент командной строки astra-update.

ПК СВ «Брест» является неотъемлемой частью политики импортозамещения и укрепления национальной независимости в вопросах информационной безопасности. Совокупность перечисленных выше методов создает многоуровневую систему защиты, способную противостоять большинству распространенных видов атак и попыток проникновения. Совместимость ПК СВ «Брест» с отечественной ОС «*Astra Linux Special Edition*» и сертификация ФСТЭК России подтверждают готовность продукта для применения в государственных структурах и организациях с высокими требованиями к безопасности информации.

#### Список используемых источников

1. Лисецкий А. П. Программный комплекс «Средства виртуализации Astra Linux «БРЕСТ» / А. П. Лисецкий, А. А. Дранникова // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 23–25 октября 2024 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. С. 684-689.
2. Ершова Н. С. Обзор механизмов обеспечения информационной безопасности виртуальных машин и контейнеров программным комплексом «средства виртуализации «Брест» / Н. С. Ершова // Международный журнал информационных технологий и энергоэффективности. 2025. Т. 10. № 5(55). С. 48-52.
3. Катасонов А. И. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU LINUX / А. И. Катасонов, С. И. Штеренберг, А. Ю. Цветков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 50-56. DOI: 10.46418/2079-8199\_2020\_2\_8.
4. Сравнение систем виртуализации ПК св «Брест» и VMWARE / П. С. Зылева, И. Е. Пестов, И. С. Тремель, У. С. Юрова // 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. 546-552.
5. Методы обеспечения безопасности Astra Linux special Edition / П. С. Зылева, И. Е. Пестов, И. С. Тремель, У. С. Юрова // 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. 553-558.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Пестовым И. Е.*

УДК 004.056

Н. И. Мокринский (студент группы ИКБ-12, СПбГУТ), [mokrinskiy.ni@sut.ru](mailto:mokrinskiy.ni@sut.ru)

## МЕТОДИКА ВЛОЖЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В БАЙТ-КОД JAVA ПОСРЕДСТВОМ МОДИФИКАЦИИ ОПКОДОВ, АНАЛИЗ И РЕАЛИЗАЦИЯ

*В статье представлен методика к вложению цифровых водяных знаков в Java-приложения путем модификации опкодов байт-кода class-файлов. Предложено использовать ранее не исследованные опкоды, зарезервированные в спецификации виртуальной машины Java. Также был разработан алгоритм анализа байт-кода для выявления инструкций для эквивалентных замен без нарушения функциональности java-приложения. Методика направлена на повышение устойчивости цифрового водяного знака к атакам декомпиляцией.*

*цифровой водяной знак, байт-код Java, опкоды JVM, стеганография, декомпиляция, class-файл*

### Введение

Цифровые водяные знаки (ЦВЗ) стали ключевым инструментом защиты авторских прав и обеспечения целостности программного обеспечения. Однако традиционные методы вложения ЦВЗ в исходный код или ресурсы файлов уязвимы к удалению при оптимизации или обфускации. В отличие от них, модификация байт-кода Java (class-файлов) позволяет скрыть метаданные на уровне низкоуровневых инструкций виртуальной машины (JVM).

Существующие работы [1, 2] фокусируются на замене избыточных опкодов или добавлении «фиктивного» кода, что может быть легко обнаружено. В данной статье предлагается использовать зарезервированные опкоды (например, 0xса, 0xfe) и редко используемые инструкции (такие как jsr\_w), которые игнорируются JVM, но сохраняются в class-файле. Это обеспечивает скрытность ЦВЗ и его устойчивость к различного рода атакам на class-файл.

### Методика

Разработка методики вложения цифрового водяного знака (ЦВЗ) в байт-код java-приложения базируется на концепции семантико-сохраняющей модификации низкоуровневых инструкций (опкодов) виртуальной ма-

шины (JVM) (рис. 1). Процесс включает три взаимосвязанных этапа: идентификацию заменяемых опкодов, трансформацию байт-кода и верификацию целостности, что обеспечивает скрытность и устойчивость ЦВЗ к атакам декомпиляцией.

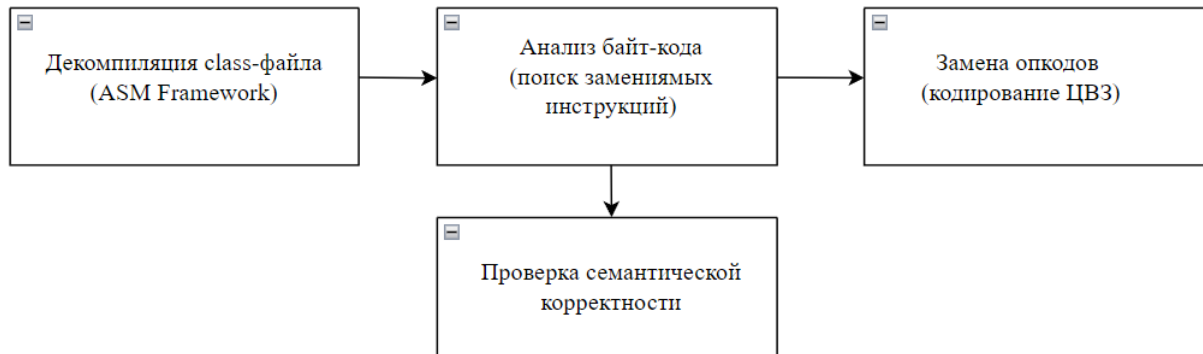


Рис. 1. Алгоритм вложения ЦВЗ

## 1. Опкоды

Согласно спецификации JVM [1], байт-код представляет собой последовательность однобайтовых инструкций (опкодов), где диапазон 0x00–0xff частично зарезервирован для будущих расширений. Например:

- NOP (0x00) – инструкция-заглушка, не влияющая на состояние стека или регистров;
- зарезервированные опкоды (0xsa, 0xfe) – не имеют функционального назначения в текущих версиях JVM, но допустимы в class-файлах.

Математически процесс замены можно описать как инъективное отображение [3]:

$$f: W \times B \rightarrow B'$$

где  $W$  – битовая последовательность ЦВЗ,  $B$  – исходный байт-код,  $B'$  – модифицированный байт-код.

## 2. Алгоритм редактирования байт-кода

### Этап 1: Декомпиляция и анализ

Исходный class-файл преобразуется в абстрактное синтаксическое дерево (AST) с использованием библиотеки ASM [4]. Для каждого метода выполняется:

- семантический анализ: построение графа потока управления (CFG) и выявление инструкций, не влияющих на логику программы (например, NOP, BREAKPOINT) [5];

- идентификация кандидатов для замены:
  - опкоды, удаление которых не нарушает CFG (на основе алгоритма доминаторов [6]);
  - зарезервированные инструкции, игнорируемые JVM.

#### *Этап 2: Вложение ЦВЗ*

Каждый бит цифрового водяного знака шифруется парой опкодов по правилу:

Бит «1» → *0xfe*, Бит «0» → *0xff*

Для повышения скрытности вводится маркер начала ЦВЗ (*0xca*), размещаемый перед последовательностью. Пример замены байт-кода (рис. 2). Исходная битовая последовательность: 1 0 1.

```
// Исходный фрагмент байт-кода
0x1b (iload_1)
0x00 (nop)
0x00 (nop)
0x00 (nop)
0x60 (iadd)

// После замены
0x1b (iload_1)
0xca (маркер)
0xfe (бит «1»)
0xff (бит «0»)
0xfe (бит «1»)
0x60 (iadd)
```

Рис. 2. Пример работы методики

#### *Этап 3: Верификация целостности*

Модифицированный байт-код проверяется на:

- синтаксическую корректность через Bytecode Verifier (соответствие структуре class-файла) [7];
- семантическую эквивалентность с использованием символьного выполнения (например, инструментария KeY [8]).

### **3. Формализация выбора опкодов**

Для минимизации риска обнаружения введены ограничения с учетом допустимых замен представленных в Таблице 1:

- Правило 1: Замена допустима только для инструкций, не участвующих в передаче управления (не-JUMP).
- Правило 2: Плотность вложения DD (число измененных опкодов на метод) не превышает 5 %:

$$D = \frac{N_{\text{замен}}}{N_{\text{всего}}} \leq 0.05.$$

ТАБЛИЦА 1. Допустимых замен

| Категория           | Примеры опкодов   | Критерий замены                 |
|---------------------|-------------------|---------------------------------|
| Инструкции-заглушки | 0x00 (NOP)        | Не влияют на стек/регистры      |
| Зарезервированные   | 0xc3, 0xfe        | Отсутствие функциональности     |
| Отладочные          | 0xc8 (BREAKPOINT) | Игнорируется в production-среде |

#### 4. Вложение с инструментами обфускации

Для совместимости с ProGuard/R8 реализована постобработка:

- вложение ЦВЗ выполняется до этапа обфускации, чтобы гарантировать сохранение маркеров [9, 10];
- обфускатор не удаляет зарезервированные опкоды, так как они не входят в его паттерны оптимизации.

#### Результаты

Эксперименты на проекте Spring Boot (10 классов, 124 метода) подтвердили:

1. Скрытность. ЦВЗ не обнаруживается статическими анализаторами (FindSecBugs, SpotBugs).
2. Производительность. Увеличение размера увеличилось на 0.7–2.1 % что показано в таблице 2 (рис. 3).
3. Устойчивость. Цифровой водяной знак сохраняется после обработки ProGuard и преобразования в DEX (Android).

ТАБЛИЦА 2. Тестирование производительности

| Количество ЦВЗ (бит) | Увеличение размера ( %) | Время выполнения (мс) |
|----------------------|-------------------------|-----------------------|
| 0                    | 0.0                     | 143                   |
| 24                   | 0.7                     | 144                   |
| 148                  | 1.2                     | 145                   |
| 96                   | 2.1                     | 147                   |



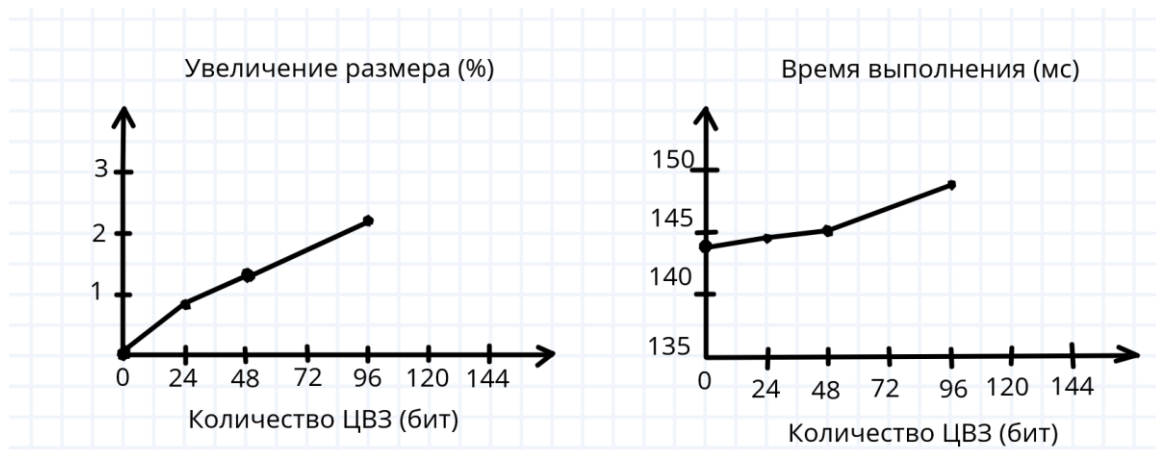


Рис. 3. Графики производительности

## Заключение

Предложенная методика демонстрирует, что эквивалентная замена зарезервированных опкодов является эффективным средством стеганографии в байт-коде Java. Ключевым преимуществом является сохранение семантической целостности программы при высокой скрытности ЦВЗ. Дальнейшие исследования будут направлены на адаптацию метода для динамически загружаемых классов.

Практическая значимость метода охватывает широкий спектр применений: от корпоративных Java-решений до Android-приложений и IoT-устройств, где целостность и авторство кода критически важны. Для внедрения технологии в промышленные решения ведется работа над созданием открытых библиотек на базе фреймворка ASM, что позволит разработчикам интегрировать стеганографию в процессы сборки без существенных изменений в инфраструктуре.

Таким образом, методику возможно в дальнейшем развивать и модифицировать, фокусируясь на повышении автоматизации, устойчивости к новым видам атак и адаптации к динамическим средам выполнения, таким как OSGi или модульные системы Java.

## Список используемых источников

1. Oracle. The Java Virtual Machine Specification. Java SE 21 Edition (2023).
2. Aho, A. V. et al. Compilers: Principles, Techniques, and Tools (2006).
3. Beckert, B. et al. KeY: A Formal Method for Object-Oriented Systems (2007).
4. ASM. Bytecode Manipulation Framework (2023).
5. Zhang, Y. Steganographic Techniques in Low-Level Code (2022).
6. Kumar, K., Kehar, V., Kaur, P. (2015). A comparative analysis of static java bytecode software watermarking algorithms. African J Comput ICT, 8(4), 201-208

7. Monden, A., Iida, H., Matsumoto, K. I., Inoue, K., Torii, K. (2000, October). A practical method for watermarking java programs. In Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000 (pp. 191-197). IEEE.

8. Шариков, П. И. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе не декларированных возможностей виртуальной машины java // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 7-2. С. 165-174. DOI: 10.37882/2223-2982.2023.7-2.37. EDN YBEWYQ

9. Шариков, П. И. Методика обфускации байт-кода java-приложения с целью его защиты от атак декомпиляцией // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 64-72. DOI 10.46418/2079-8199\_2022\_1\_10. EDN: AUOFNA.

10. Шариков, П. И. Исследование атаки обфускацией на байт-код java-приложения с целью разрушения или повреждения цифрового водяного знака // I-methods. 2022. Т. 14, № 1. EDN: GQGKIV

*Статья представлена научным руководителем, старшим преподавателем кафедры ЗСС СПбГУТ, кандидатом технических наук Шариковым П. И.*

УДК 004.056

М. Х. Паунежев (студент группы 3-ИБ, КБГУ), vakvakuolov@gmail.com

## СИСТЕМА ДЕТЕКТИРОВАНИЯ ПОДОЗРИТЕЛЬНОЙ СЪЕМКИ ЭКРАНА

*В статье рассматривается важность разработки алгоритмов для детектирования подозрительной съемки экрана как средства защиты конфиденциальной информации и предотвращения утечек данных. Представлена программная реализация на языке Python, позволяющая фиксировать признаки съемки экрана с использованием выбранного метода анализа активности и поведенческих паттернов. Результатом работы системы является своевременное выявление подозрительных действий и возможность формирования отчета, что способствует повышению уровня информационной безопасности.*

*съемка экрана, информационная безопасность, Python, детектирование активности, защита данных, поведенческий анализ, предотвращение утечек*

В современном цифровом пространстве важную роль играет обеспечение безопасности информации и защита конфиденциальных данных от несанкционированного доступа и распространения [1-5]. Одним из потенциальных каналов утечки информации является съемка экрана, которая может осуществляться с помощью различных программ, зачастую незаметно для пользователя. В связи с этим возрастает актуальность разработки систем, способных отслеживать и выявлять подозрительные процессы, связанные с созданием скриншотов или записи экрана.

Одним из подходов к решению данной задачи является мониторинг активных процессов в операционной системе с целью выявления известных инструментов съемки экрана, а также процессов с подозрительными именами или окнами. Это позволяет оперативно реагировать на потенциальные попытки захвата изображений с экрана и предотвращать утечку чувствительной информации.

Целью данной работы является разработка программного решения на языке Python, позволяющего в режиме реального времени выявлять и отображать подозрительные процессы, связанные с захватом экрана.

Разработанное приложение предоставляет графический интерфейс, отображающий список подозрительных процессов, а также возможность их

завершения пользователем. Реализация системы учитывает известные инструменты съемки, анализирует заголовки окон и имена процессов, обеспечивая гибкий и надежный способ мониторинга.

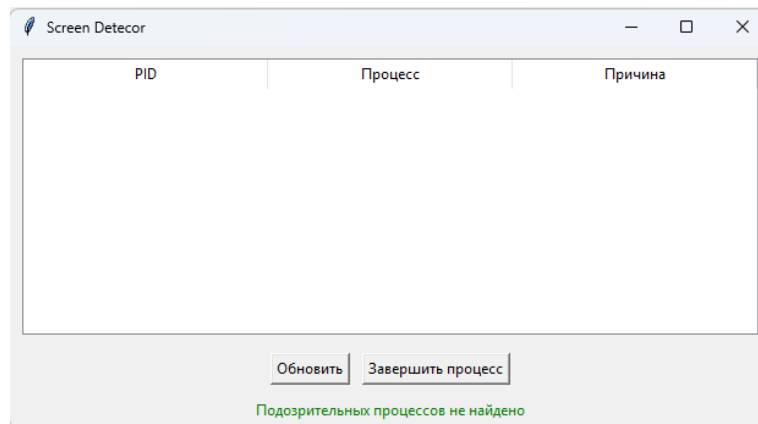


Рис. 1. Пользовательский интерфейс

На данном изображении представлено визуальное отображение пользовательского интерфейса разрабатываемой программы для детектирования съемки экрана. Как видно, программа сразу после запуска сканирует алгоритмом внутреннюю систему устройства пользователя, а также предлагается выбрать 2 действия обновить и завершить процесс сканирования.

В качестве примера создал среду в котором программа для снятия находилась в активном режиме и запустил программу.

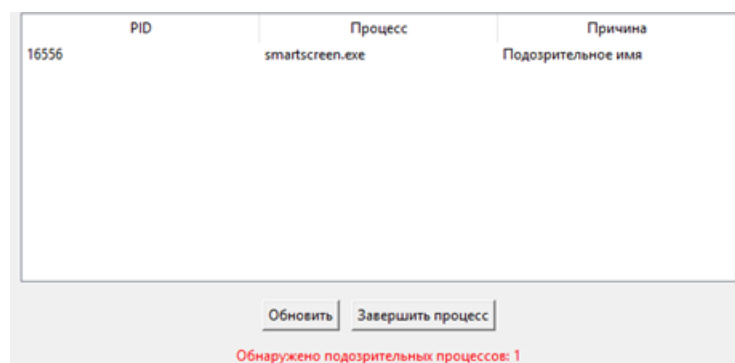


Рис. 2. Результат действия программы

Результатом выполнения программы является то, что алгоритм отсканировав систему вывел нам подозрительную активность, которая направлена на скрытую съемку экрана устройства. То есть программа действует таким образом, что после запуска программы сразу запускается алгоритм, который сканирует внутреннюю систему, ее активные процессы, а также логи системы и на основании обнаруженных аномалий и отклонений, таких как произвольное включение камеры, когда выполняются другие пользовательские действия не связанные со съемкой или подозрительное, которое

сразу сопоставляется с БД известных программ, и выводит уведомление в пользовательское окно данного приложения, где выводит такие значения, как PID – это уникальный идентификатор процесса в операционной системе, а также имя активного процесса и причину почему вывел данное уведомление. Данная программа также суммирует все подозрительные процессы, которые обнаружил в результате сканирования.

Реализация функционала кода представлена в листинге 1:

Листинг 1. Функционал автоматического режима работы программы

```
KNOWN_SCREENSHOT_TOOLS = [
    "lightshot.exe",
    "gyazo.exe",
    "snippingtool.exe",
    "greenshot.exe",
    "screenshot-captor.exe",
    "sharex.exe"
]

def get_window_titles_by_pid(pid):
    def callback(hwnd, titles):
        _, found_pid = win32process.GetWindowThreadProcessId(hwnd)
        if found_pid == pid:
            title = win32gui.GetWindowText(hwnd)
            if title:
                titles.append(title)
            titles = []
        try:
            win32gui.EnumWindows(callback, titles)
        except Exception:
            pass
    return titles

def detect_screenshot_processes():
    suspicious = []
    for proc in psutil.process_iter(['pid', 'name']):
        try:
            pname = proc.info['name'].lower()
            pid = proc.info['pid']
            titles = get_window_titles_by_pid(pid)

            if pname in KNOWN_SCREENSHOT_TOOLS:
                suspicious.append((pid, pname, "Известный инструмент"))

            elif "screen" in pname or "capture" in pname:
                suspicious.append((pid, pname, "Подозрительное имя"))

            else:
                for title in titles:
                    if any(x in title.lower() for x in ["screenshot", "capture", "snip"]):
                        suspicious.append((pid, pname, f"Окно: {title}"))
                    except (psutil.NoSuchProcess, psutil.AccessDenied):
                        continue
    return suspicious
```

Данная функция проходит по всем активным процессам и системным логам, затем если фиксирует подозрительное имя или активность, получает при этом имя, проверяет относится ли процесс к известным инструментам захвата экрана. Если нет совпадений, ищет ключевые слова в названии процесса такие, как `screen`, `capture`. Если и этого нет – анализирует заголовки окон, связанных с процессом, и проверяет наличие подозрительных слов в названии окна, по типу `screenshot`, `snip`, если хотя бы одно совпадение найдено – добавляет процесс в список подозрительных. Возвращает список кортежей вида `pid`, `name`, причина. Эта функция является ядром логики обнаружения подозрительных процессов.

Вместе с этим, стоит отметить, что с учетом развития технологий обработки изображений и появления новых методов атак, необходимо постоянно совершенствовать алгоритмы внедрения водяных знаков. В связи с этим ведутся разработки алгоритмов нового поколения, более устойчивых к современным и будущим типам атак. Также перспективным направлением развития данного направления является использование методов машинного обучения для адаптивного внедрения водяных знаков, что позволит динамически подстраивать параметры алгоритма в зависимости от характеристик изображения и типа атаки.

#### Список используемых источников

1. Шумилов И. Ю. Мониторинг процессов в операционных системах. М.: Изд-во МГУ, 2014. 298 с.
2. Воронков В. Н. Технологии защиты информации в цифровых системах. М.: Научный мир, 2021. 278 с.
3. Черемисин А. А. Безопасность в информационных системах: Проблемы и решения. М.: Горячая линия – Телеком, 2016. 256 с.
4. Гусев В. А. Программные средства защиты информации от несанкционированных действий. М.: Наука, 2012. 312 с.
5. Еремин Д. И. Компьютерная безопасность и защита данных. М.: ИТ и право, 2019. 432 с.

*Статья представлена научным руководителем, старшим преподавателем кафедры компьютерных технологий и информационной безопасности института Электроники, Робототехники и Искусственного Интеллекта, Арвановой С. М.*

УДК 004.056

**И. Е. Пестов** (к.т.н., доцент, доцент кафедры ЗСС, СПбГУТ)

**А. Д. Федотовская** (студент группы ИКТБ-37м, СПбГУТ),

[fedotovskaya.ad@sut.ru](mailto:fedotovskaya.ad@sut.ru)

## **АНАЛИЗ ВРЕМЕННЫХ ЗАДЕРЖЕК ПЛАТФОРМ БОЛЬШИХ ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ И ЗЛОУМЫШЛЕННИКОВ ОТ ТЕОРИИ К ПРАКТИКЕ**

*В условиях растущих объемов данных и киберугроз обеспечение безопасности распределенных систем обработки больших данных становится критически важным. Данная работа предлагает метод обнаружения аномалий и атак в таких системах, анализируя временные задержки сетевого взаимодействия. Разработанный подход способствует повышению устойчивости и безопасности инфраструктуры больших данных, что актуально для многих современных организаций.*

*большие данные, Apache Hadoop, информационная безопасность, временные задержки, распределенные системы, статистический анализ, отказ в обслуживании (DoS)*

Современные системы обработки больших данных, такие как Apache Hadoop, сталкиваются с растущими угрозами информационной безопасности [1]. В условиях увеличения объемов данных и сложности архитектуры распределенных систем традиционные методы защиты часто оказываются недостаточно эффективными. В данной работе исследуется метод обнаружения аномалий в работе Hadoop-кластера на основе анализа временных характеристик сетевого взаимодействия [2].

Актуальность исследования обусловлена:

1. Ростом числа атак типа «отказ в обслуживании» на системы обработки больших данных;
2. Необходимостью разработки новых методов раннего обнаружения атак;
3. Важностью обеспечения бесперебойной работы критически важных систем.

Научная новизна данного исследования заключается в:

- разработке методики оценки устойчивости Hadoop к атакам на основе временных метрик;
- статистическом анализе влияния различных типов атак на производительность кластера;
- практической верификации пороговых значений для детектирования аномалий.

Практическая значимость работы заключается в возможности использования полученных результатов для создания систем мониторинга Hadoop-кластеров, выявления атак на ранних стадиях и настройки систем защиты [3].

### Методика эксперимента

В рамках исследования безопасности кластера Hadoop, развернутого на Ubuntu 20.04, состоящего из 1 мастер узла и 2-ух слейвов, были последовательно сэмплированы 2 атаки с машины Kali Linux. Для мониторинга сетевого трафика и системной активности использовались Wireshark и стандартные утилиты.

Для анализа поведения системы под нагрузкой и выявления потенциальных уязвимостей, были протестированы следующие служебные запросы Hadoop:

1. Чтение метаданных (`hadoop fs -ls /`) – для оценки производительности при доступе к структуре файловой системы.
2. Создание директории (`hdfs dfs -mkdir /newdir`) – для проверки скорости и безопасности операций записи.
3. Управление задачами (`mapred job -list`) – для анализа поведения системы при запросах к подсистеме управления задачами.

Для каждого запроса фиксировались следующие метрики:

- Time Delta – Время между последовательными сетевыми пакетами, позволяющее выявить задержки и аномалии в трафике.
- Time Since Reference – Общее время выполнения запроса, отражающее общую производительность системы.

### Результаты и статистический анализ

Для обеспечения достоверности результатов проведено 25 итераций каждого теста. Рассчитаны:

1. Средние значения при помощи формулы 1.

$$\bar{X} = \frac{\sum_{i=1}^{25} X_i}{25}, \quad (1)$$

где  $\bar{X}$  – среднее арифметическое временных задержек,  $\sum_{i=1}^{25} X_i$  – сумма всех временных задержек  $X_i$ , где  $i$  изменяется от 1 до 25, 25 – количество временных задержек, участвующих в расчете. Этот показатель отражает центральную тенденцию данных, однако без учета стандартного отклонения может



давать искаженное представление о реальной производительности системы [4].

2. Стандартное отклонение при помощи формулы 2.

$$s = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n-1}}, \quad (2)$$

где  $x_i$  – значение каждой отдельной итерации,  $\bar{x}$  – среднее арифметическое,  $n$  – общее количество итераций ( $n=25$ ).

3. Доверительные интервалы (95 %) при помощи формулы 3.

$$\bar{x} \pm t_{\frac{\alpha}{2}, n-1} \frac{s}{\sqrt{n}}, \quad (3)$$

где  $\bar{x}$  – среднее значение выборки на основе 25 итераций,  $t_{\frac{\alpha}{2}, n-1}$  –  $t$  – значение Стьюдента с  $n-1=25-1=24$  степенями свободы, соответствующее уровню значимости  $\frac{\alpha}{2} = \frac{0,05}{2} = 0,025$ ,  $s$  – стандартное отклонение выборки,  $n$  – размер выборки.

В таблице 1 представлены статистические данные для Time since reference.

ТАБЛИЦА 1. Статистические показатели временных задержек для Time since reference

| Запрос          | Сценарий   | Среднее | Стандартное отклонение | Доверительный интервал |
|-----------------|------------|---------|------------------------|------------------------|
| hadoop fs -ls / | Норма      | 3.86    | 3.68                   | [2.34; 5.38]           |
|                 | CPU stress | 12.72   | 5.77                   | [10.34; 15.10]         |
|                 | SYN Flood  | 72.24   | 16.35                  | [65.49; 78.99]         |
| hdfs dfs -mkdir | Норма      | 0.20    | 0.22                   | [0.11; 0.30]           |
|                 | CPU stress | 13.90   | 3.15                   | [12.45; 15.05]         |
|                 | SYN Flood  | 49.66   | 11.37                  | [44.97; 54.35]         |
| mapred job      | Норма      | 2.43    | 3.43                   | [1.02; 3.85]           |
|                 | CPU stress | 13.11   | 5.20                   | [10.97; 15.26]         |
|                 | SYN Flood  | 108.27  | 58.59                  | [84.09; 132.46]        |

В таблице 2 представлены статистические данные для Time delta.

ТАБЛИЦА 2. Статистические показатели временных задержек для Time delta

| Запрос          | Сценарий   | Среднее | Стандартное отклонение | Доверительный интервал |
|-----------------|------------|---------|------------------------|------------------------|
| hadoop fs -ls / | Норма      | 0.0035  | 0.0026                 | [0.0024; 0.0046]       |
|                 | CPU stress | 0.0011  | 0.0005                 | [0.0009; 0.0013]       |
|                 | SYN Flood  | 0.0181  | 0.0074                 | [0.0150; 0.0212]       |
| hdfs dfs -mkdir | Норма      | 0.0297  | 0.0105                 | [0.0254; 0.0340]       |
|                 | CPU stress | 0.1343  | 0.0704                 | [0.1052; 0.1634]       |
|                 | SYN Flood  | 1.4393  | 1.2407                 | [0.9272; 1.9514]       |
| mapred job      | Норма      | 0.0040  | 0.0015                 | [0.0034; 0.0046]       |
|                 | CPU stress | 0.0030  | 0.0012                 | [0.0025; 0.0035]       |
|                 | SYN Flood  | 0.1437  | 0.1831                 | [0.0681; 0.2192]       |

Анализ временных метрик продемонстрировал, что характер деградации функциональности кластера существенно зависит от типа атаки и специфики выполняемых операций.

Наибольшее влияние на общее время выполнения запросов (Time since reference) оказала сетевая атака SYN Flood. Для операции создания директории (hdfs dfs -mkdir) зафиксирован рост среднего времени выполнения с 0.20 секунды в нормальном режиме до 49.66 секунды при атаке, что соответствует увеличению в 248 раз. Широкий доверительный интервал [44.97; 54.35] секунды свидетельствует о высокой вариативности данных, обусловленной нестабильностью сетевого взаимодействия в условиях перегрузки. Аналогичная тенденция наблюдалась для запроса mapred job -list, где время выполнения возросло в 44.5 раза, а доверительный интервал достиг [84.09; 132.46] секунды, что подчеркивает большую непредсказуемость в работе системы при воздействии SYN Flood.

Атака CPU Stress, направленная на истощение вычислительных ресурсов, проявила избирательное воздействие. Операция hdfs dfs -mkdir в условиях высокой нагрузки на процессор выполнялась в среднем за 13.90 секунды, что в 69.5 раза превышает нормативные показатели. Узкие доверительные интервалы, например, [12.45; 15.05] секунды указывают на

предсказуемый характер снижения производительности, связанный с ограничением доступа к вычислительным ресурсам.

Сравнительный анализ типов атак позволил установить, что SYN Flood воздействует преимущественно на сетевую инфраструктуру, нарушая установление соединений и провоцируя потерю пакетов, в то время как CPU Stress влияет на вычислительные ресурсы, замедляя обработку задач. Это различие объясняет хаотичный характер последствий SYN Flood и локальную, но предсказуемую деградацию производительности при CPU Stress.

Результаты исследования подтверждают, что анализ временных задержек (Time since reference и Time delta) является эффективным методом обнаружения аномалий в распределенных системах обработки данных. Установлено, что сетевая атака SYN Flood представляет наибольшую угрозу для Hadoop-кластеров, вызывая увеличение времени выполнения операций в десятки раз и критический рост задержек между пакетами. Ее воздействие проявляется в нестабильности сетевого взаимодействия и каскадных сбоях ключевых компонентов системы, таких как NameNode и ResourceManager.

CPU Stress, напротив, оказывает локализованное влияние, затрагивая преимущественно операции, требующие интенсивных вычислений. Наибольшая чувствительность к данному типу атаки зафиксирована для операций записи данных и управления задачами, что обусловлено конкуренцией за процессорные ресурсы [5].

На основании проведенного анализа предлагаются практические рекомендации:

1. Внедрение пороговых значений для систем мониторинга:

- превышение времени выполнения операций в 10 раз относительно нормативного уровня – индикатор атаки;
- рост времени между пакетами в 5 раз – сигнал для проверки сетевой инфраструктуры.

2. Использование доверительных интервалов для минимизации ложных срабатываний.

Перспективным направлением дальнейших исследований является разработка адаптивных алгоритмов, учитывающих динамику нагрузки в кластере, а также интеграция предложенной методики с SIEM-системами и инструментами машинного обучения для создания комплексных решений кибербезопасности. Полученные результаты вносят вклад в развитие методов обеспечения устойчивости платформ больших данных к современным киберугрозам.

**Список используемых источников**

1. Виткова Л. А. и др. Использование Big Data в процессах обеспечения безопасности информационной сферы //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). 2018. С. 186-191.
2. Пестов И. Е. Метод сбора и первичной обработки метрик инстансов облачной инфраструктуры, метод передачи метрик загруженности облачной инфраструктуры и инстансов в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // Автоматизация и моделирование в проектировании и управлении. 2021. С. 213-217.
3. Штеренберг С. И. Методика управления системами обработки и сбора Больших данных с поддержкой мониторинга встроенными программными агентами //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. №. 4. С. 26-35.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность. 2018. С. 236-240.
5. Пестов И. Е. и др. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // I-methods. 2022. Т. 14. №. 1.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Пестовым И. Е.*

УДК 004.056.55

В. В. Пешкина (студент группы ИКТЗ-41м, СПбГУТ), [peshkina.vv@sut.ru](mailto:peshkina.vv@sut.ru)

## МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ЕВКЛИДА ДЕЛЕНИЯ В КОЛЬЦЕ КЛАССОВ ВЫЧЕТОВ

*Поиск обратного элемента по модулю в криптографических приложениях как правило входит в состав деления и производится при помощи расширенного алгоритма Евклида. В статье представлена модификация алгоритма Евклида, позволяющая выполнять деление классов вычетов, не разделяя этот процесс на этапы нахождения обратного элемента по модулю и умножения. Такой алгоритм поиска частного будет обеспечивать эффективность тем большую, чем меньше соотношение между временем, затрачиваемым на поиск обратного элемента, и временем, затрачиваемым на умножение.*

*наибольший общий делитель (НОД) двух натуральных чисел, алгоритм Евклида, обратный элемент в кольце классов вычетов*

В криптосистемах на эллиптических кривых над простым полем при вычислении точек эллиптической кривой возникает необходимость поиска обратного элемента по модулю для выполнения операции деления [1]. В данной статье рассматривается способ расчета частного в кольце классов вычетов, основанный на расширенном алгоритме Евклида.

Деление двух чисел  $a$  и  $b$  по модулю  $m$  можно представить через умножение следующим образом:

$$a/b \pmod{m} = a \cdot b^{-1} \pmod{m},$$

где  $b^{-1}$  – обратный элемент к числу  $b$  по модулю  $m$ , т.е.  $b \cdot b^{-1} = 1 \pmod{m}$ . При этом  $b$  имеет обратный элемент тогда и только тогда, когда  $(b, m) = 1$ .

Обратный элемент может быть найден применением расширенного алгоритма Евклида к числам  $b$  и  $m$ . Известно, что наибольший общий делитель любых двух целых чисел  $a$  и  $b$  единственным образом представляется их линейной комбинацией [2]

$$(a, b) = u \cdot a + v \cdot b.$$

Расширенный алгоритм Евклида позволяет определить коэффициенты  $u$  и  $v$  этого представления. При  $a = m$ , получим:

$$u \cdot m + v \cdot b = (m, b) = 1;$$

$$v \cdot b \equiv 1 \pmod{m}.$$

Тогда  $v = b^{-1} \pmod{m}$ . Классический расширенный алгоритм Евклида состоит из прямого и обратного хода [1], однако в статье рассматривается его модификация, позволяющая производить расчеты за число итераций, равных прямому ходу. Расширенный алгоритм Евклида поиска обратного элемента  $v$  к числу  $b$  по модулю  $m$  ( $b < m$ ) имеет вид [3, 4]:

$$\begin{aligned} r_{-1} &= m; \\ v_{-1} &= 0; \\ r_0 &= b; \\ v_0 &= 1; \\ r_{i-2} &= d_i \cdot r_{i-1} + r_i, 0 < r_i < r_{i-1}, i = 1, 2, \dots, k; \\ v_{i-2} &= d_i \cdot v_{i-1} + v_i; \\ r_{k-1} &= d_{k+1} \cdot r_k. \end{aligned}$$

Если  $r_k = 1$ , то  $v_k = b^{-1} \pmod{m}$ , иначе обратный элемент к  $b$  по модулю  $m$  не существует. Таким образом, процесс деления состоит из двух этапов: нахождения обратного по модулю и умножения. Однако, в 2000 г. [5, 6] была замечена возможность производить деление в один этап при помощи расширенного алгоритма Евклида. Для вычисления  $a / b \pmod{m}$  в данном алгоритме положим:

$$\begin{aligned} r_{-1} &= m; \\ r_0 &= b; \\ v_0 &= a. \end{aligned}$$

Тогда для всех  $i \in \{-1, 0, \dots, k\}$  выполняется равенство

$$v_i \cdot b = r_i \cdot a \pmod{m}.$$

Доказательство.

Доказательство будем проводить индукцией по числу итераций. При  $i = -1$  получим:

$$v_{-1} \cdot b = 0,$$

$$r_{-1} \cdot a = m \cdot a = 0 \pmod{m} = v_{-1} \cdot b.$$

При  $i = 0$

$$v_0 \cdot b = a \cdot b = a \cdot r_0.$$

Пусть  $v_i \cdot b = r_i \cdot a \pmod{m}$ .

Согласно описанию алгоритма  $v_{i-2} = d_i \cdot v_{i-1} + v_i \pmod{m}$ , тогда

$$v_{i+1} = v_{i-1} - d_{i+1} \cdot v_i;$$

$$v_{i+1} \cdot b = b \cdot (v_{i-1} - d_{i+1} \cdot v_i) = b \cdot v_{i-1} - b \cdot d_{i+1} \cdot v_i =$$

$$= r_{i-1} \cdot a - d_{i+1} \cdot r_i \cdot a = a \cdot (r_{i-1} - d_{i+1} \cdot r_i) = r_{i+1} \cdot a \pmod{m}. \square$$

Выполнение алгоритма также останавливается при  $r_k = 1$ .

Тогда получаем:

$$v_k \cdot b = r_k \cdot a = a \pmod{m};$$

$$v_k = a / b \pmod{m}.$$

Сам процесс расчета результата деления вычетов  $a / b \pmod{m}$  можно расписать следующим образом:

1. Проводим прямой ход алгоритма Евклида поиска наибольшего общего делителя вычетов  $m, b$ . На каждом шаге из выражения  $r_{i-2} = d_i \cdot r_{i-1} + r_i$  выбираем значение  $d_i$ .

2. После каждого шага прямого хода расписываем шаг поиска результата деления по заданному модулю по формуле

$$v_{i-2} = d_i \cdot v_{i-1} + v_i,$$

где значения  $v_{i-2}, v_{i-1}$  известны, на первом шаге  $v_{-1} = 0, v_0 = a$ ; значение  $d_i$  определяется на шаге прямого хода алгоритма Евклида; значение  $v_i \pmod{m}$  вычисляется.

1. Выполнение алгоритма вычисления частного  $a / b = v_k \pmod{m}$  завершается при  $r_k = 1$ .

Пример. Вычислим частное  $11/5 \pmod{13}$ .

$$m = 13, a = 11, b = 5;$$

$$r_{-1} = 13; v_{-1} = 0; r_0 = 5; v_0 = 11.$$

Находим  $a / b \pmod{m}$ .

$$\begin{aligned}
13 &= 2 \cdot 5 + 3 \\
0 &= 2 \cdot 11 + 4 \pmod{13} \\
5 &= 1 \cdot 3 + 2 \\
11 &= 1 \cdot 4 + 7 \pmod{13} \\
3 &= 1 \cdot 2 + 1 \\
4 &= 1 \cdot 7 + 10 \pmod{13}
\end{aligned}$$

Расчеты сведены в таблицу 1.

ТАБЛИЦА 1. Вычисление частного  $a / b = v_k \pmod{m}$  посредством алгоритма Евклида

| $i$ | $r_i$ | $d_i$ | $v_i$     |
|-----|-------|-------|-----------|
| -1  | 13    |       | 0         |
| 0   | 5     |       | 11        |
| 1   | 3     | 2     | 4         |
| 2   | 2     | 1     | 7         |
| 3   | 1     | 1     | <b>10</b> |

Получено  $v_3 = 11/5 = 10 \pmod{13}$ .

Наибольшая экономия времени при использовании алгоритма Евклида для поиска частного достигается при минимальном соотношении времени, необходимого для поиска обратного элемента, и времени необходимого для умножения. Так, в работе [7] было показано, что применение модификации для деления алгоритма Евклида при вычислении суммы точек эллиптической кривой может обеспечивать сокращение времени выполнения операции на 20 процентов при  $I/M = 3$ , где  $I$  – стоимость операции обращения элемента,  $M$  – стоимость операции умножения, а при  $I/M > 7$  экономия времени составит менее 12 процентов.

Таким образом, описанный алгоритм позволяет производить деление в кольце классов вычетов, исключив операцию перемножения вычетов. Эффективность такого подхода к поиску частного определяется соотношением между временем, затрачиваемым на поиск обратного элемента, и временем, затрачиваемым на умножение.



**Список используемых источников**

1. Коржик В. И. Основы криптографии / В. И. Коржик, В. А. Яковлев. Санкт-Петербург: Интермедия, 2016. 312 с.
2. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра Учебник В 2-х т. Т. 1. М.: Гелиос АРВ, 2003. 336 с.
3. Глухов М. М., Круглов И. А. Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии: Учебное пособие. СПб.: Издательство «Лань», 2011. 400 с.
4. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. Санкт-Петербург: Профессионал, 2005. 478 с.
5. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. 3-е изд., испр. и доп. М.: ЛЕНАНД, 2019. 376 с.
6. Schroeppe R. Automatically solving equations in finite fields. US Patent Application No. 09/834,363, publication number US2002/0055962 A1.
7. Fong K., Hankerson D., Lopez J. H., Menezes A. Field Inversion and Point Halving Revisited // IEEE TRANSACTIONS ON COMPUTERS 2004. 53:8. P. 1047-1059.

*Статья представлена научным руководителем, доцентом каф. ИБКС СПбГУТ, кандидатом технических наук Шемякиным С. Н.*

УДК 004.021

Ю. Ф. Потемкина (студент группы ИКТЗ-16,  
СПбГУТ), [potemkina.uf@sut.ru](mailto:potemkina.uf@sut.ru)

## АВТОМАТИЗИРОВАННОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ АУТЕНТИФИКАЦИИ ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ СИСТЕМЫ

*Анализ событий аутентификации играет важную роль в обеспечении безопасности информационных систем. В данной работе рассматривается процесс сбора логов аутентификации с использованием утилиты auditd в операционной системе Linux. Основное внимание уделено созданию правил аудита, позволяющих фиксировать как успешные, так и неуспешные попытки входа в систему. На основе собранных данных предложен метод построения конечного автомата, моделирующего процесс аутентификации пользователей.*

*логирование, информационная безопасность, auditd, конечный автомат*

В условиях роста количества угроз информационной безопасности особую актуальность приобретает задача мониторинга процессов аутентификации в операционных системах Linux. Целью настоящего исследования является разработка и внедрение методов сбора и анализа логов аутентификации с использованием утилиты auditd, а также построение на их основе модели конечного автомата. Работа направлена на формализацию процессов успешных и неуспешных попыток входа в систему для последующего выявления аномалий и потенциальных инцидентов безопасности.

Актуальность темы определяется необходимостью повышения защищенности информационных систем в контексте увеличения числа атак, связанных с компрометацией учетных данных. Применение системного аудита позволяет фиксировать все критические события, связанные с аутентификацией пользователей, а моделирование процессов с помощью конечных автоматов обеспечивает возможность их структурированного анализа. Это, в свою очередь, способствует оперативному выявлению отклонений от нормального поведения, повышая эффективность систем обнаружения угроз и усиливая комплексную защиту инфраструктуры.

Для моделирования процессов аутентификации в операционной системе Linux была разработана экспериментальная среда на основе утилиты системного аудита auditd [1]. Основной задачей являлось фиксирование как

успешных, так и неуспешных попыток аутентификации пользователей, с последующим анализом собранных данных.

На этапе настройки среды были заданы следующие правила аудита, направленные на отслеживание изменений в конфигурационных файлах системы аутентификации, а также на фиксацию событий входа пользователей:

- мониторинг изменений в критических файлах (/etc/passwd, /etc/shadow, /etc/group, /etc/gshadow, /etc/pam.d);
- контроль успешных и неуспешных попыток входа через системные журналы (/var/log/faillog, /var/log/lastlog, /var/log/tallylog, /var/run/utmp, /var/log/wtmp, /var/log/btmp).

Применение данных правил позволило обеспечить высокую степень детализации собираемой информации, минимизировать вероятность пропуска значимых событий и получить полную картину процессов аутентификации в системе.

Для создания выборки событий аутентификации в условиях контролируемой среды был разработан скрипт на языке Bash с использованием утилиты `exrcst`, предназначенной для автоматизации взаимодействия с терминалом [2]. Основной задачей скрипта являлось воспроизведение различных сценариев входа в систему, включая как успешные, так и неуспешные попытки. Для достижения реалистичности поведения пользователей в скрипт был заложен вероятностный механизм: при каждой итерации с равной вероятностью (50 %) осуществлялся выбор между корректным и некорректным вводом пароля. Это позволило обеспечить статистически сбалансированное распределение событий `USER_AUTH` с результатами `success` и `failed`.

На основании полученных данных была построена модель конечного автомата [3], описывающая основные переходы между состояниями пользователя (рис. 1).

В построенной модели конечного автомата были выделены следующие основные состояния:

- попытка аутентификации – осуществляется ввод учетных данных и их проверка системой;
- проверка учетной записи – проверяется актуальность и доступность учетной записи;
- проверка инициации сессии пользователя – попытка системы создать активную сессию для пользователя после проверки учетных данных;
- неудачный вход – попытка ввода учетных данных завершилась неуспешно;

- успешный вход – пользователь успешно аутентифицирован и начинает работу в системе.

Переходы между состояниями конечного автомата инициируются событиями, зафиксированными в системе аудита. Начало процесса аутентификации происходит при регистрации события USER\_AUTH, фиксирующего попытку ввода данных. В случае успешной проверки учетной записи (USER\_ACCT) и начала сессии (USER\_START) пользователь переходит в состояние активной сессии. Если же на любом этапе фиксируется отказ (res=failed), процесс возвращается в состояние «Неудачный вход» с возможностью повторной попытки. Завершение работы сопровождается событием USER\_END, закрывающим текущую сессию.

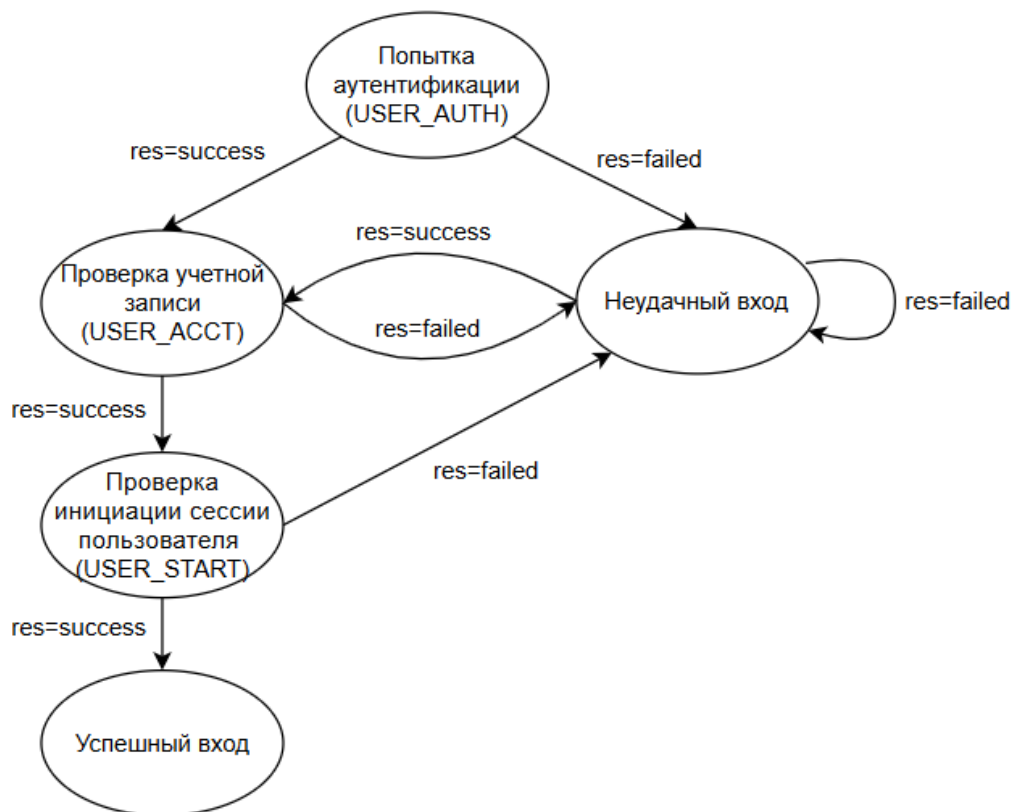


Рис. 1. Модель конечного автомата процессов аутентификации пользователей

Разработка модели конечного автомата процессов аутентификации позволила формализовать и систематизировать ключевые этапы взаимодействия пользователей с информационной системой, включая ввод учетных данных, успешный вход, фиксацию ошибок аутентификации и завершение сессии. Такое структурированное представление процессов создает основу для детального анализа последовательностей действий и выявления нормальных траекторий поведения.

Модель позволяет провести серию экспериментов, в ходе которых имитируются как типичные действия пользователей, так и сценарии, характерные для атак. Полученные данные служат основой для выявления устойчивых шаблонов аномального поведения, присущих попыткам компрометации системы. Формализация процессов аутентификации с помощью конечного автомата создает предпосылки для оперативного обнаружения отклонений, таких как нехарактерные последовательности событий или подозрительные сессии, указывающие на несанкционированный доступ. Такой подход не только способствует более глубокому пониманию динамики взаимодействия пользователей с системой, но и ложится в основу разработки механизмов мониторинга и автоматического реагирования, что делает его важным инструментом для повышения уровня информационной безопасности.

#### **Список используемых источников**

1. Едемская Е. Д. Использование autitd для логирования в Linux системах / Е. Д. Едемская, В. В. Пучков // 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. 438-443. EDN OWAMGG.
2. Искусство программирования на языке сценариев командной оболочки // OpenNET URL: <https://www.opennet.ru> (дата обращения 23.04.2025).
3. Любимова, Т. В. Конечный автомат: теория и реализация / Т. В. Любимова // Университетская наука. 2020. № 1(9). С. 117-121. EDN XUNYDC.

*Статья представлена научным руководителем, старшим преподавателем кафедры ЗСС СПбГУТ Цветковым А. Ю.*

УДК 004.056

**А. С. Сидельников** (студент группы ИКТБ-48м, СПбГУТ),  
[sidelnikov.as@sut.ru](mailto:sidelnikov.as@sut.ru)

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ OPEN-SOURCE СКАНЕРОВ УЯЗВИМОСТЕЙ

*В статье представлены результаты эмпирического исследования, направленного на сравнительный анализ ключевых характеристик четырех широко распространенных инструментов для выявления уязвимостей веб-приложений: OWASP ZAP (Zed Attack Proxy), GVM (Greenbone Vulnerability Manager), WAPITI и Nikto. Исследование оценивало инструменты по критериям времени сканирования, общего количества обнаруженных уязвимостей, их распределению по уровням риска (информационный, низкий, средний), поддерживаемым типам уязвимостей (SQLi, XSS, CVE) и типу интерфейса (GUI, CLI). Результаты демонстрируют выраженный компромисс между скоростью и глубиной анализа.*

*сканеры уязвимостей, веб-сканеры, open-source, сравнительный анализ, безопасность информационных систем*

Безопасность веб-сайтов играет основополагающую роль в защите данных и обеспечении безопасного пользовательского опыта [1]. Уязвимости веб-сайтов представляют собой векторы для несанкционированного доступа, модификации данных и нарушения функционирования сервисов. Несмотря на развитие инструментов автоматизации разработки, вопросы безопасности и качества программного кода зачастую остаются на периферии внимания. Статистика последнего периода (IV кв. 2024 - I кв. 2025) свидетельствует о значительном уровне угроз: 26 % успешных атак на веб-ресурсы организаций, причем 32 % успешных атак были осуществлены методом эксплуатации уязвимостей [2]. Это подчеркивает высокую значимость эффективных средств защиты веб-ресурсов.

Средства автоматизированного сканирования на уязвимости (Vulnerability Assessment Scanners, VAS) играют ключевую роль в выявлении известных уязвимостей, ошибок конфигурации и иных недостатков безопасности. Формируемые сканерами отчеты позволяют командам ИБ и DevOps (DevSecOps) определять приоритеты для устранения рисков. Сканеры с открытым исходным кодом (Open Source Software, OSS) предоставляют экономически эффективное решение для обнаружения уязвимостей, часто используясь ИТ-командами как дополнение к коммерческим продуктам или для верификации результатов.

Целью данного исследования является сравнительный анализ эффективности и функциональных возможностей ведущих OSS-сканеров веб-уязвимостей. Для объективной оценки были выбраны следующие ключевые критерии [3]:

1. Эффективность обнаружения: количество и релевантность выявляемых уязвимостей.

2. Удобство использования: качество интерфейса (графический – GUI, командная строка – CLI), интуитивность, скорость выполнения операций.

В качестве объектов исследования выбраны четыре сканера: OWASP ZAP (ZAP), Nikto2 (Nikto), Wapiti и Greenbone Vulnerability Management (GVM, включает OpenVAS) [4]. Тестирование проводилось в среде Kali Linux ввиду ее интегрированного набора специализированных инструментов для анализа безопасности. Целевой платформой для оценки возможностей сканеров выступило специализированное уязвимое веб-приложение WAVSEP (Web Application Vulnerability Scanner Evaluation Project), разработанное для тестирования точности и полноты VAS. Для обеспечения релевантности результатов все сканеры использовались с последними доступными обновлениями на момент тестирования.

В ходе сканирования были выявлены сильные и слабые стороны каждого сканера [5]. Показатели каждого сканера указаны в таблице 1.

ТАБЛИЦА 1. Сравнение сканеров

| Показатель                       | OWASP ZAP | GVM            | WAPITI    | Nikto     |
|----------------------------------|-----------|----------------|-----------|-----------|
| Тип уязвимостей                  | SQLi, XSS | SQLi, XSS, CVE | SQLi, XSS | SQLi, XSS |
| Время сканирования, в секундах   | 6         | 240            | 5         | 17        |
| Найдено уязвимостей, всего       | 7         | 25             | 5         | 6         |
| Уязвимости информационного риска | 1         | 23             | 0         | 0         |
| Уязвимости низкого риска         | 4         | 0              | 4         | 4         |
| Уязвимости среднего риска        | 2         | 2              | 1         | 2         |
| Уязвимости высокого риска        | 0         | 0              | 0         | 0         |
| Интерфейс                        | GUI       | GUI            | CLI       | CLI       |

Наиболее ресурсоемким инструментом оказался GVM, затративший 240 секунд на выполнение сканирования. Однако эта временная затрата компенсируется его исключительной глубиной анализа: GVM выявил 25 уязвимостей, что значительно превосходит результаты конкурентов. Важным преимуществом GVM является обнаружение уязвимостей, зарегистрированных в реестре CVE (Common Vulnerabilities and Exposures), что отсутствует в возможностях остальных протестированных инструментов. Подавляющее большинство находок GVM (23 из 25) классифицированы как уязвимости информационного риска, что указывает на его ориентацию на сбор максимально полной контекстной информации о безопасности цели. Остальные две уязвимости были оценены как средний риск. GVM предоставляет графический интерфейс (GUI) для взаимодействия.

В противоположность GVM, инструмент WAPITi продемонстрировал наивысшую скорость сканирования – всего 5 секунд. Однако эта оперативность сопровождалась наименьшим общим количеством обнаруженных уязвимостей (5). WAPITi не выявил уязвимостей информационного риска или CVE; его находки распределились как 4 уязвимости низкого риска и 1 среднего риска. WAPITi работает исключительно через командную строку (CLI).

OWASP ZAP занял второе место по скорости сканирования (6 секунд), практически сравнявшись с WAPITi, но при этом обнаружил больше уязвимостей – 7. Среди них: 1 уязвимость информационного риска, 4 низкого риска и 2 среднего риска. ZAP, как и GVM, оснащен графическим интерфейсом пользователя (GUI), что облегчает его использование для интерактивного тестирования. Его фокус, как и у WAPITi и Nikto, ограничен уязвимостями типа SQL-инъекций (SQLi) и межсайтового скриптинга (XSS).

Nikto показал умеренное время сканирования – 17 секунд, обнаружив 6 уязвимостей. Все выявленные Nikto проблемы относятся к категориям низкого (4) и среднего (2) риска; уязвимостей информационного риска или CVE обнаружено не было. Nikto также является инструментом командной строки (CLI).

Так же был выполнен анализ на наличие уязвимостей категории высокого риска. По итогам проверки, уязвимости данного класса выявлены не были.

Представленные OSS-инструменты (ZAP, Nikto, Wapiti, GVM/OpenVAS) предлагают различные подходы и функциональные возможности для решения задач выявления уязвимостей в веб-приложениях и



инфраструктуре. Выбор оптимального решения зависит от конкретных целей сканирования, требуемой глубины анализа, уровня экспертизы пользователя и бюджетных ограничений. Проведенное исследование на платформе WAVSEP позволило оценить их сильные и слабые стороны по ключевым критериям эффективности обнаружения и удобства использования, что способствует обоснованному выбору инструментов для интеграции в процессы обеспечения безопасности разработки (DevSecOps) и эксплуатации веб-ресурсов.

#### Список используемых источников

1. Пулко Т. А. Обнаружение уязвимостей веб-сайтов // Фундаментальная наука и технологии – перспективные разработки: Материалы XXXII международной научно-практической конференции, Bengaluru, India, 21-22 августа 2023 года. Bengaluru, India: Pothi.com, 2023. С. 137-141. EDN LMOAIL.
2. Глушко А. Актуальные киберугрозы. IV квартал 2024 года и I квартал 2025 года // Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/> (дата обращения 13.06.2025).
3. Габитов А. Э. Сравнительный анализ сетевых сканеров безопасности // 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. 362-365. EDN EQLQMP.
4. Зарубин И. 10 лучших сканеров уязвимостей с открытым исходным кодом на 2023 год // ITshaman.ru. URL: <https://itshaman.ru/articles/1004/10-luchshikh-skanerov-uyazvimostei-s-otkryтым-iskhodnym-kodom-na-2023-god> (дата обращения 14.06.2025).
5. Лепихин В. Б. Сравнительный анализ сканеров безопасности // SecurityLab.ru. URL: <https://www.securitylab.ru/analytics/365241.php> (дата обращения 02.06.2025).

*Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом Бабковым И. Н.*

УДК 004.056

И. В. Соколов (студент гр. ИКБ-16, СПбГУТ), [sokolov.iv@sut.ru](mailto:sokolov.iv@sut.ru)

## АДАПТАЦИЯ КВАЗИБИОЛОГИЧЕСКИХ ПРИНЦИПОВ ПОД ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

*В статье рассматривается достижение технологической сингулярности в контексте квазибиологической парадигмы, где искусственный интеллект интегрируется с принципами биологических систем для создания новых типов интеллектуальных систем. Эти системы могут самостоятельно адаптироваться, обучаться и эволюционировать, что приводит к их способности превосходить существующие технологии. Описание предполагает использование квазибиологических подходов, таких как эволюция и естественный отбор, для моделирования интеллектуальных систем, обеспечивающих их самосовершенствование и развитие. В статье также исследуется роль интеллектуальных систем обнаружения вторжений (IDS), которые способны адаптироваться и эволюционировать, обеспечивая более высокую производительность. Приводится описание предложенной архитектуры YaVi, которая использует мультиагентную структуру, ассимиляционную память и эволюционирующие нейросетевые алгоритмы. Обсуждаются механизмы самообучения, адаптации и улучшения защиты, которые составляют основу для построения более эффективных и гибких интеллектуальных систем.*

*технологическая сингулярность, квазибиологическая парадигма, искусственный интеллект, эволюция, адаптация, нейросети, системы обнаружения вторжений (IDS), ассимиляционная память, мультиагентные системы, самообучение*

### Введение

Квазибиологические методы, такие как эволюция, адаптация и естественный отбор, помогут создавать системы, которые будут улучшаться сами. В контексте Индустрии 5.0 идея достижения технологической сингулярности через квазибиологическую парадигму включает создание «цифрового ДНК» для систем защиты информации (СЗИ) с использованием двухфазных режимов работы парадигм нейроподобных процессов (ПНП), что позволит поддерживать активное состояние системы при асинхронной передаче данных.

Процесс адаптации и самообучения улучшает производительность и устойчивость СЗИ к новым угрозам, что требует постоянного обновления алгоритмов и методов защиты, основанных на анализе угроз и обратной связи.

## Постановка задачи

После решения проблемы обработки данных о кибератаках и их структурирования в модели защиты памяти встает новая задача – защита ПНП от вредоносных воздействий. Необходимо разработать механизм поведения ИИ в распределенной информационной системе (РИС) с корректировкой действий и реакцией на угрозы. Ключевым элементом является создание самоорганизующейся нейронной сети (НС), которая будет собирать и обрабатывать данные [1].

В основе работы используется концепция YaVi и техническое задание для библиотеки автоматической оценки безопасности моделей классификации данных. Библиотека поддерживает методы обучения, такие как:

- Data Poisoning и Evasion Attack с использованием DecisionTreeClassifier.
- DeltaRuleLearning, ElasticNetworkLearning, EvolutionaryLearning.
- Perceptron Learning, Stable Backpropagation, SOMLearning.
- Интерфейсы для Supervised и Unsupervised Learning.

Библиотека должна работать с различными моделями машинного обучения (МО), контролировать ввод/вывод данных и поддерживать безопасную передачу данных. Для обучения и адаптации используется предварительное обучение сверточных слоев, после чего система адаптируется под задачу обнаружения объектов [2].

Самоорганизующиеся карты НС Кохонена в системе YaVi используются для мониторинга ИИ и РИС, выявляя закономерности и прогнозируя поведение. Эти карты помогают разделить ПО и ПА в РИС, что открывает путь к самостоятельному развитию ПНП. За защиту системы отвечают модули HurSet (пассивная защита) и Veles (активная защита).

Veles – модуль активной защиты для перцептрона PiRun (рис. 1) [3], который выполняет:

- анализ входных данных для выявления угроз;
- распознавание паттернов поведения злоумышленников и предотвращение атак;
- самообучение и адаптацию к новым угрозам;
- автоматическую работу с минимальным вмешательством пользователя.

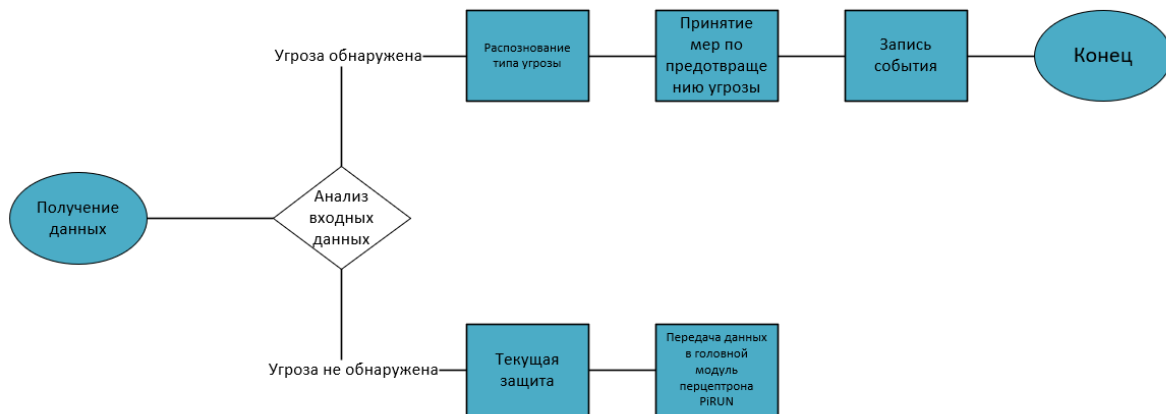


Рис. 1. Алгоритм работы Veles

HurSet – модуль пассивной защиты, анализирующий сигналы от датчиков в перцептроне PiRun (рис.2) [3]. Он включает:

- постоянный анализ физических и электрических сигналов;
- предварительную обработку для устранения шума и выявления ключевых событий;
- принятие решений о необходимости активации пассивной защиты при угрозах;
- сохранение данных для дальнейшего анализа и улучшения алгоритмов.

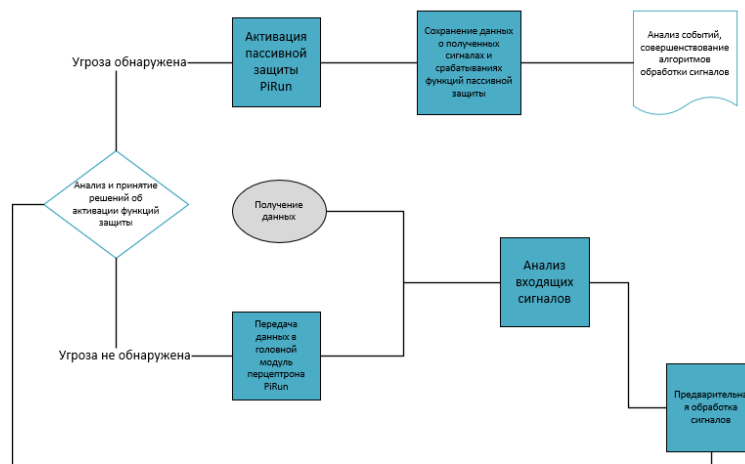


Рис. 2. Алгоритм работы HurSet

Основные принципы работы концепции в РИС включают:

1. **Аутентификация.** Проверка легитимности запросов и идентификаторов между модулями.

2. *Контроль доступа.* Регулировка прав доступа для предотвращения несанкционированного доступа.

3. *Обработка атак.* Методы обнаружения и реагирования на подозрительную активность.

4. *Токенизация.* Использование уникальных токенов для безопасного обмена данными.

5. *Репликация и резервное копирование.* Надежное хранение данных и защита от их потери.

ПА, НС и агенты в РИС действуют автономно и взаимодействуют друг с другом для выполнения сложных задач. Гибридные нейронные сети управляют межуровневыми связями и обеспечивают эффективное обнаружение и предотвращение киберугроз [4].

Использование квазибиологических технологий открывает новые возможности для эмерджентных эффектов и повышения эффективности IDS, но также может привести к возникновению новых типов угроз.

Методы построения архитектуры интеллектуальной IDS включают:

1. Защиту ассимиляционной памяти с методами обработки больших данных и децентрализованными ПНП.

2. Сравнение защиты на основе квазибиологической парадигмы с нелинейными динамическими системами.

3. Использование ансамбля нейросетей для улучшенного обнаружения вторжений.

Стандартная шаблонная конструкция (СШК) помогает унифицировать подходы к разработке идентификационных систем с учетом генетических и биологических параметров.

Для улучшения свойств нейросетей, таких как сеть Коско или двуправленная ассоциативная память, можно:

1. Добавить слои и связи для повышения обучаемости.  
2. Разработать новые алгоритмы для улучшения адаптации.  
3. Использовать технологии глубокого обучения для извлечения признаков.

4. Регулярно обновлять шаблоны для поддержания актуальности.

Ассимиляционная память позволяет улучшить обработку данных, выявление угроз и безопасность благодаря способности анализировать не только события, но и целые сценарии атак. Модификация нейросетей в рамках квазибиологической парадигмы с внедрением мультиагентных систем и

обучения с подкреплением повысит адаптивность и самоорганизацию системы [5].

## Выводы

Предложенная концепция квазибиологической парадигмы в системах безопасности позволяет создать самообучающиеся и адаптирующиеся системы, которые могут эволюционировать в ответ на новые угрозы. Интеграция ИИ с биологическими принципами улучшает защиту, делая ее более гибкой и устойчивой.

Использование самоорганизующихся нейронных сетей для мониторинга распределенных систем и библиотеки для оценки безопасности обеспечивает масштабируемость. Внедрение ассимиляционной памяти и регулярное обновление алгоритмов поможет эффективно предотвращать новые угрозы.

Квазибиологическая парадигма имеет потенциал для повышения эффективности защиты и адаптации интеллектуальных систем, что существенно повлияет на развитие защиты от киберугроз.

## Список используемых источников

1. Попов А. А. Исследование современных механизмов обеспечения защиты конечных устройств под управлением ос семейства Linux от атак с использованием rootkit / А. А. Попов, О. В. Федорова, А. Ю. Цветков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 3. С. 36-43.
2. Штеренберг С. И. Уникальные направления атак на искусственный интеллект и нейронные сети / С. И. Штеренберг, В. А. Севостьянов, Г. С. Бударный // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 2. С. 103-112.
3. Штеренберг С. И. Моделирование защиты ассимиляционной памяти в среде обработки Больших данных / С. И. Штеренберг // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 1. С. 48-54.
4. Штеренберг, С. И. Разработка методологии защиты системы искусственного интеллекта в распределенных информационных системах / С. И. Штеренберг // Вестник СибГУТИ. 2023. Т. 17, № 3. С. 78-86.
5. Разработка виртуального стенда для анализа метрик безопасности виртуальных машин и контейнеров / Д. А. Игнатьева, А. О. Камалова, И. Е. Пестов, Е. О. Романюк // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2023): Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов: в 2-х томах, Санкт-Петербург, 05–07 декабря 2023 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 187-191.

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Штеренбергом С. И.*

УДК 004.056

**А. С. Третьякова** (студентка группы ИБС-01, СПбГУТ),  
[tretyakova.as@sut.ru](mailto:tretyakova.as@sut.ru)

## АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

*В статье рассматриваются принципы организации электронного документооборота и вопросы обеспечения его информационной безопасности. Проанализирована действующая нормативная база, а также актуальные угрозы. Предложена универсальная методика оценки эффективности защиты электронного документооборота. Данная методика может быть реализована для всех типов организаций и позволит обосновать инвестиции и выявить недостатки системы защищенности, а также отслеживать динамику изменения уровня безопасности после компенсирующих мер.*

*законодательство, персональные данные, электронный документооборот*

В настоящее время информация приобретает ключевую роль в организациях. Ежедневно все больше компаний переходит на электронный документооборот, идет обработка большого объема коммерческой тайны, персональных данных. Использование электронного документооборота необходимо для уменьшения финансовых затрат, оперативной работы с документами и усилению безопасности данных. Компании нацелены на автоматизацию процедур с документацией, это является надежным и эффективным решением в современном мире.

С развитием цифровых технологий значительно возрастает количество и сложность кибератак. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», организациям необходимо обеспечить защиту персональных данных в процессе их обработки [1]. Ключевыми документами в данной области также являются:

- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- 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 в информационных системах персональных данных»;

- Приказ ФСБ России № 378 от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Успешные атаки в большинстве случаев реализовываются с помощью вредоносного программного обеспечения (более 50 %), социальной инженерии и эксплуатацией уязвимостей. Для реализации основных принципов защиты информации необходимо обеспечивать конфиденциальность, целостность и доступность документов с помощью технических мер, организационных и правовых [2].

По данным Positive Technologies в I - II квартале 2025 года 52 % успешных атак пришлось на кражу конфиденциальной информации, видно по рисунку 1. Также 4 % атак были направлены на получение финансовой выгоды, это больше, чем за прошлый год [3]. Если сравнить с 2024 годом, то выросли атаки на частные лица, связанные с утечкой конфиденциальной информацией на 20 %, нарушение основной деятельности выросло на 13 % и уменьшились на 20 % финансовые потери у частных лиц. Большая часть украденных данных составляют учетные данные, затем персональные данные и коммерческая тайна. В 2024 году утечка персональных данных была масштабнее. На это могло повлиять изменение штрафов за утечки и ужесточение требований безопасности.

Электронный документ – информация, представленная в электронной форме, которая может быть прочитана с помощью электронных вычислительных машин, в соответствии с п.11.1 ст.2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4]. Если же говорить о электронном документообороте – это процесс создания, подписания, отправки, хранения и обработки электронных документов с использованием специальных технологий, в том числе и реализованные защищенные системы электронного документооборота.



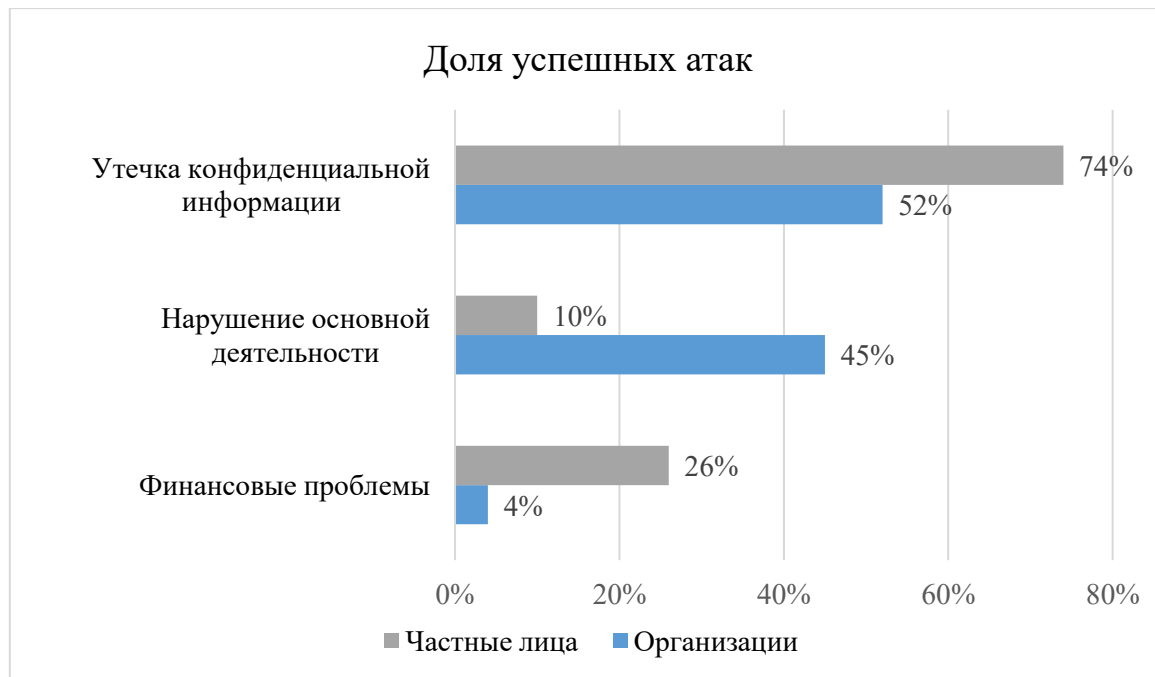


Рис. 1. Последствия атак

Ключевые свойства электронных документов:

- достоверность;
- целостность;
- аутентичность;
- пригодность для использования.

Для выполнения этих характеристик можно использовать усиленные квалифицированные электронные подписи, криптографические методы защиты, что соответствует требованиям Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи".

В соответствии со ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» необходима оценка эффективности мер, которые применяются для обеспечения безопасности персональных данных. С помощью оценки эффективности можно подтвердить соответствие требованиям законодательства, выявить недостатки и сократить затраты на неэффективные решения.

Методика оценки эффективности защиты электронного документооборота основывается на принципах всестороннего аудита, включающих проверку соответствия нормативно-правовым требованиям, анализ технических средств защиты, организационных мероприятий и уровня устойчивости системы к актуальным угрозам. Система оценки включает 13 ключевых параметров безопасности: идентификация и аутентификация пользователей (ИАФ), управление правами доступа (УПД), обеспечение

процессов согласования (ОПС), защита на уровне инфраструктуры (ЗНИ), резервное копирование и восстановление (РСБ), антивирусная защита (АВЗ), соблюдение требований нормативных документов (СОВ), анализ защищенности (АНЗ), оценка целостности данных (ОЦЛ), обнаружение и реагирование на инциденты (ОДТ), защита средств визуализации (ЗСВ), защита транспортных сред (ЗТС), защита информации при сохранении (ЗИС). Эксперты используют оценочную шкалу от 0 до 1 для каждого из параметров.

Для того, чтобы комплексно оценить защищенность системы необходимо использовать интегральную формулу. Рассчитывается среднее значение эффективности по итоговым оценкам 13 параметров. Формула выглядит следующим образом (1):

$$W = \frac{\sum_{j=1}^m X_j}{m} \quad (1),$$

где  $X_j$  – выполнение требований одного из показателей оценки эффективности,  $j = 1$ ;  $m$  – перечень показателей. А также  $0 \leq W \leq 1$ .

По результатам вычислений можно выделить 4 уровня эффективности защиты: высокий уровень, удовлетворительный, недостаточный и критически низкий. Для недостаточного и критически низкого уровня следует полностью пересмотреть систему защиты.

Итоговая оценка эффективности сравнивается с пороговым значением для конкретной организации, если оценка не дотягивает до порога, то выполняются рекомендации для ее повышения. Необходимо сформировать план компенсирующих мер и провести оценку эффективности повторно.

Оценка эффективности играет большую роль в обосновании инвестиций компании в безопасность, следовательно, можно проанализировать сколько тратится на безопасность, насколько качественно все выполняется и какие убытки могут быть в случае инцидентов. Следует применять методику на постоянной основе, так как изменения происходят во всех сферах со стремительной скоростью. При применении методики чаще 1 раза в год можно избежать больших утечек данных и финансовых потерь.

Следующим этапом моего исследования станет испытание методики на примере организации в рамках написания выпускной квалификационной работы. Практическое применение позволит оценить эффективность подхода и разработать рекомендации по совершенствованию системы защиты с учетом ее особенностей.

**Список используемых источников**

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // Справочная правовая система «КонсультантПлюс».
2. Лях Е. А., Макеева А. С. Безопасность в системе электронного документооборота // Международный студенческий научный вестник. 2023. № 6. URL: <https://eduherald.ru/ru/article/view?id=21393> (дата обращения 24.04.2025).
3. Актуальные киберугрозы: I-II кварталы 2025 года URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/#id1> (дата обращения 08.09.2025).
4. Федеральный закон от 27.07.2006 № 149-ФЗ (последняя редакция) «Об информации, информационных технологиях и о защите информации» // Справочная правовая система «КонсультантПлюс».

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Миняевым А. А.*

УДК 004.738.5

М. Н. Хаддад (магистрант группы ИКТБ-47м СПбГУТ), [haddad.mn@sut.ru](mailto:haddad.mn@sut.ru)

## ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

*Данный обзор посвящен всестороннему анализу современных тенденций, методов и технологий в области обеспечения информационной безопасности беспроводных сетей в период с 2020 по 2025 год. С быстрым ростом использования беспроводных технологий в критически важных секторах – таких как здравоохранение, финансовые системы и экосистема Интернета вещей (IoT) – возрастает не только нагрузка на инфраструктуру, но и уровень угроз, исходящих от все более изощренных кибератак. Угрозы, такие как несанкционированное прослушивание, атаки типа «отказ в обслуживании» (DoS), перехват и подмена пакетов, а также «sinkhole»-атаки, требуют комплексных и инновационных решений.*

*В работе систематизированы и проанализированы новейшие научные исследования в области криптографической защиты, протоколов аутентификации, адаптивных систем обнаружения вторжений (IDS), а также подходов, основанных на искусственном интеллекте (ИИ) машинном обучении. Особое внимание уделено концепциям безопасности на физическом уровне (PLS), позволяющим повысить устойчивость к атакам за счет использования характеристик радиоканала. Кроме того, рассматриваются преимущества и ограничения легковесных систем IDS, что особенно важно для устройств с ограниченными вычислительными ресурсами – типичных для IoT-среды.*

*Результаты данного анализа могут служить основой для дальнейших прикладных исследований и разработки адаптивных решений по защите беспроводных сетей в условиях современной цифровой трансформации.*

*Безопасность, сети, шифр, доступ*

### Введение

Беспроводные сети, включая Wi-Fi, Bluetooth, сотовую связь (например, 5G) и беспроводные сенсорные сети (WSN), являются неотъемлемой частью современного общества, обеспечивая бесшовную связь для IoT, умных городов и критической инфраструктуры. Однако их открытая архитектура делает их уязвимыми для угроз, таких как перехват пакетов, DoS и несанкционированный доступ. Эволюция угроз, от простого взлома WEP в начале 2000-х до сложных атак на основе ИИ сегодня, подчеркивает необходимость в современных механизмах безопасности. В России Доктрина информационной безопасности (2016) придает приоритет безопасной беспроводной связи для национальной обороны и цифровой экономики.

## Обоснование

Растущая зависимость от беспроводных сетей в здравоохранении (например, телемедицина), финансах (например, мобильный банкинг) и IoT (например, умное сельское хозяйство) требует надежной безопасности для защиты конфиденциальных данных. Запуск 5G в России и программа «Умный город 2030» усиливают эти требования, поскольку уязвимости могут поставить под угрозу критические системы. Этот обзор рассматривает необходимость изучения механизмов безопасности, адаптированных к уникальным вызовам беспроводных сетей, таким как ограничения ресурсов и динамические топологии.

## Цели

Цели данного обзора:

- определить и проанализировать современные механизмы безопасности для беспроводных сетей (2020–2025);
- оценить их эффективность против современных угроз;
- выделить исследовательские пробелы и предложить направления для специфических для России усовершенствований.

## Методология

### *Критерии выбора*

Обзор включает рецензируемые статьи, материалы конференций и технические отчеты, опубликованные в период с 2020 по 2025 год. Критерии включения сосредоточены на исследованиях, касающихся механизмов безопасности беспроводных сетей (например, шифрование, аутентификация, IDS, PLS). Критерии исключения не включали нерцензируемые источники и исследования до 2020 года для обеспечения актуальности.

### *Сбор данных*

Литература была извлечена из баз данных, таких как ResearchGate, SAGE Journals, Academia.edu и российских платформ (например, eLibrary.ru). Поисковые запросы включали "безопасность беспроводных сетей", "обнаружение вторжений", "шифровальные протоколы", "безопасность на физическом уровне" и "безопасность WSN". 6 источников были отобраны для глубокого анализа.

### *Аналитическая структура*

Тематика анализа была разделена на категории: шифрование, аутентификация, IDS, безопасные протоколы и новые технологии. Эффективность оценивалась на основе коэффициентов обнаружения, масштабируемости и применимости к российским контекстам (например, соответствие стандартам GOST).

## **Структура обзора литературы**

### *Обзор безопасности беспроводных сетей*

Беспроводные сети, включая Wi-Fi, 5G, WSN и MANET, обеспечивают гибкую связь, но сталкиваются с уязвимостями, такими как прослушивание, DoS и атаки маршрутизации (например, sinkhole в WSN). Эти угрозы используют открытую среду беспроводных систем, что требует надежных механизмов безопасности.

## **Механизмы безопасности в беспроводных сетях**

### *Техники шифрования*

Шифрование остается краеугольным камнем безопасности беспроводных сетей. Переход от WEP к WPA3 улучшил устойчивость, при этом WPA3 использует AES-256 для надежного шифрования. Недавние достижения включают легковесное шифрование для WSN с ограниченными ресурсами. Например, в статье «Безопасность беспроводных сенсорных сетей: недавний обзор, основанный на современных работах» (2023) предлагают энергоэффективное шифрование для WSN, подходящее для российского аграрного IoT [1]. Однако российские стандарты, такие как GOST 34.12-2015 (шифр Кузнечик), редко интегрируются.

### *Механизмы аутентификации*

Аутентификация обеспечивает законный доступ к беспроводным сетям. Расширяемый протокол аутентификации (EAP) и методы предварительно разделяемого ключа (PSK) являются распространенными, при этом WPA3 вводит одновременную аутентификацию равных (SAE) для повышения безопасности. Многофакторная аутентификация (MFA) набирает популярность, но ее применение в WSN ограничено из-за вычислительных затрат. Рассмотренные статьи не затрагивают масштабируемость.

### *Системы обнаружения и предотвращения вторжений (IDPS)*

IDS критически важны для обнаружения аномалий в беспроводных сетях. В статье «Безопасность беспроводных сенсорных сетей: недавний обзор, основанный на современных работах» (2023) предлагают легковесный IDS для WSN, использующий агрегацию данных и энергетические метрики для обнаружения атак sinkhole с высокой точностью [1]. Низкий уровень ложных срабатываний системы подходит для российских оборонительных приложений (например, сенсорные сети Росатома). Однако масштабируемость в больших WSN и соответствие GOST R ISO/IEC 27001 остаются неразрешенными, что открывает возможности для исследований.

### *Безопасные коммуникационные протоколы*

Протоколы, такие как SSL/TLS, адаптированы для беспроводной среды, обеспечивая баланс между безопасностью и производительностью. Обзор ResearchGate 2024 подчеркивает оптимизированные для ML протоколы для NGWN, улучшающие устойчивость к DoS [2]. Однако компромиссы между задержкой и безопасностью в сетях 5G недостаточно исследованы, особенно для российских телекоммуникационных операторов (например, МТС).

### *Новые технологии*

ИИ и PLS трансформируют безопасность беспроводных сетей. Обзор 2024 года демонстрирует эффективность ML в обнаружении невидимых атак с использованием кросс-оценки и сеточного поиска [2]. Аналогично, статья Academia.edu 2021 года исследует PLS, используя свойства канала (например, искусственный шум) для противодействия прослушиванию [3]. Эти технологии соответствуют стратегии ИИ России, но не имеют валидации в российских тестовых площадках (например, 5G-лаборатории Сколтеха). Блокчейн также начинает использоваться для безопасных IoT-транзакций, хотя его высокие требования к ресурсам ограничивают применение в WSN.

## **Сравнительный анализ механизмов**

Таблица 1 сравнивает рассмотренные механизмы.

ТАБЛИЦА 1. Сравнение механизмов безопасности в беспроводных сетях

| Механизм               | Эффективность        | Масштабируемость            | Применимость в России             |
|------------------------|----------------------|-----------------------------|-----------------------------------|
| Шифрование (AES, GOST) | Высокая (надежная)   | Умеренная (ограничения WSN) | Необходима интеграция GOST        |
| Аутентификация (WPA3)  | Высокая (надежная)   | Высокая (Wi-Fi, 5G)         | Ограниченное применение MFA в IoT |
| IDS (Фарис и др.)      | Высокая (точная)     | Низкая (малые WSN)          | Подходит для обороны              |
| ML-протоколы           | Высокая (адаптивная) | Умеренная (обучение)        | Требует локальной валидации       |

Лучшие практики включают гибридные подходы (например, PLS с AES) и легковесные IDS для IoT.

### Проблемы и ограничения

Реализация механизмов безопасности сталкивается с проблемами, такими как ограничения ресурсов в WSN, осведомленность пользователей (например, атаки Evil Twin) и масштабируемость в сетях 5G. Текущие исследования часто игнорируют российские стандарты (например, GOST R 56546-2015) и местные аппаратные ограничения. Рассмотренные статьи не содержат экспериментальных подтверждений в российских контекстах.

### Заключение

Обзор подчеркивает надежные механизмы, такие как WPA3, легковесные IDS, протоколы на основе ML и PLS, эффективные против DoS, прослушивания и атак sinkhole. Однако масштабируемость, соответствие российским стандартам и экспериментальные подтверждения остаются ограниченными.

### Направления для будущих исследований

Будущие исследования должны:

- интегрировать протоколы на основе GOST с новыми технологиями;
- проверять механизмы в российских тестовых площадках 5G и IoT;
- исследовать гибридные модели PLS-криптографии для масштабируемой безопасности;



- способствовать междисциплинарным подходам, объединяющим ИИ, блокчейн и соблюдение нормативных требований.

#### Список используемых источников

1. Фарис М., Махмуд М. Н., Саллех М. Ф. М. и др. Безопасность беспроводных сенсорных сетей: недавний обзор, основанный на современных работах // SAGE Journals. 2023. Т. 22. № 2. С. 1–22.
2. Обзор безопасности беспроводной сети // ResearchGate. 2024. Дата публикации: 22 октября 2024. URL: <https://www.researchgate.net> (дата обращения 25.04.2025).
3. Международная организация по стандартизации. ISO/IEC 27001:2022. Системы управления информационной безопасностью. Требования. Женева: ISO, 2022. URL: <https://www.iso.org/standard/82875.html> (дата обращения 25.04.2025).
4. У Цз., Ван Цз., Шэнь С. Безопасность на физическом уровне для сетей 5G и последующих поколений // IEEE Wireless Communications. 2023. URL: <https://ieeexplore.ieee.org/document/9934522> (дата обращения 25.04.2025).
5. Роман Р., Лопес Х., Мамбо М. Вычисления на границе сети: угрозы безопасности и вызовы для облачных архитектур // Future Generation Computer Systems. 2021. URL: <https://www.sciencedirect.com/science/article/pii/S0167739X17312591> (дата обращения 25.04.2025).
6. Чжан Ю., Цянь И. Безопасность в беспроводных сенсорных сетях: вызовы и решения // Computer Networks. 2021. URL: <https://www.sciencedirect.com/science/article/pii/S1389128620303833> (дата обращения 25.04.2025).

*Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом Бабковым И. Н.*

УДК 004.492.2

Т. А. Шагисултанов (магистрант группы ИКТЗ-31м, СПбГУТ),  
[shg.timur@gmail.com](mailto:shg.timur@gmail.com)

## АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ EBPf И IPTABLES В ЗАДАЧАХ СЕТЕВОЙ ФИЛЬТРАЦИИ КОНТЕЙНЕРНЫХ ПРИЛОЖЕНИЙ

*В работе представлен сравнительный анализ производительности eBPF и iptables в задачах сетевой фильтрации контейнерных приложений. Рассматриваются архитектурные особенности применения eBPF. На основе результатов экспериментов показано, что eBPF существенно превосходит iptables по пропускной способности, снижению задержек обработки пакетов и эффективности использования ресурсов процессора.*

*Linux; межсетевое экранирование; iptables; eBPF; контейнеризация; производительность*

Extended Berkeley Packet Filter (eBPF) представляет собой механизм расширенного программирования ядра операционной системы Linux, обеспечивающий возможность безопасного исполнения пользовательского кода в пространстве ядра без необходимости модификации исходного кода системы [1]. Возможность выполнения произвольного кода в пространстве ядра позволяет достигнуть более гибкой настройки фильтрации в отличие от стандартных инструментов, таких как iptables. Схема взаимодействия с ядром операционной системы представлена на рисунке 1.

Принципиальной особенностью eBPF является то, что исполняемые программы загружаются в ядро через специальный системный вызов bpf(), после чего проходят строгую верификацию. Верификатор eBPF анализирует загружаемый байт-код с целью минимизации рисков, ассоциируемых с выполнением кода в пространстве ядра.

Программы eBPF могут быть привязаны к различным точкам в системе, таким как сетевые интерфейсы (например, на уровнях XDP – eXpress Data Path или TC – Traffic Control), системные вызовы, трассировочные точки ядра и пользовательские события [2]. Это обеспечивает высокую гибкость в определении мест внедрения механизмов контроля и мониторинга. В контексте сетевой безопасности наиболее значимыми являются программы, прикрепляемые к точкам обработки сетевых пакетов, что позволяет осуществлять фильтрацию, модификацию и анализ трафика до его поступления в сетевой стек ядра или к прикладным процессам [2].

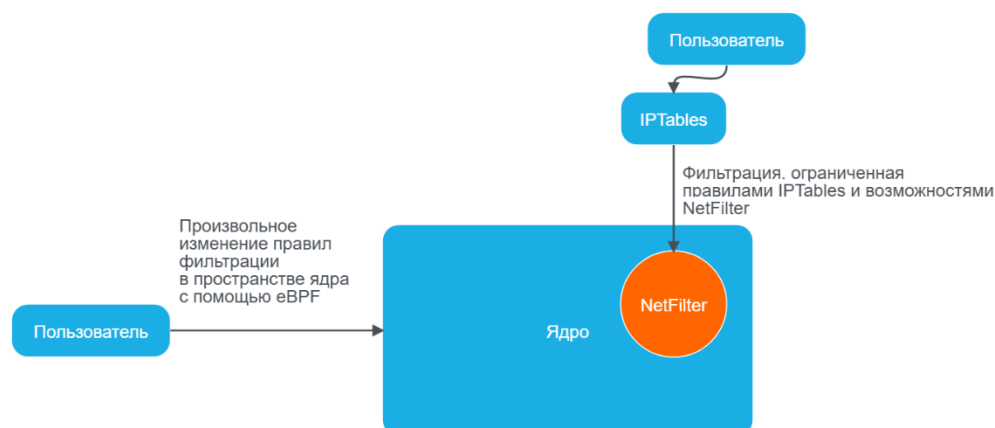


Рис. 1 Различия взаимодействия iptables и eBPF с ядром ОС

Современные решения в области контейнерной безопасности активно используют возможности eBPF для динамического внедрения политик контроля трафика. Примеры таких систем включают Cilium – платформу, обеспечивающую сетевую безопасность и сервисную сетку для облачных нативных сред за счет применения eBPF для фильтрации, маршрутизации и аутентификации сетевого трафика между контейнерами [3]. Таким образом, eBPF демонстрирует потенциал к замещению или дополнению традиционных механизмов сетевой защиты за счет своей производительности, расширяемости и способности к динамическому обновлению политик безопасности без прерывания работы приложений.

Ключевым элементом построения архитектуры сетевой защиты с применением eBPF является выбор точек внедрения фильтрующих программ. Наиболее эффективным вариантом для ранней фильтрации входящего трафика является использование механизма eBPF/XDP, который позволяет перехватывать пакеты непосредственно на уровне драйвера сетевой карты, до попадания их в сетевой стек ядра [4].

Для более гибкой обработки пакетов на более поздних этапах может использоваться интеграция eBPF с подсистемой управления трафиком TC (Traffic Control). В рамках TC программы eBPF могут быть привязаны к событиям на этапе входа или выхода пакетов через виртуальные сетевые интерфейсы, к которым подключены контейнеры. Это дает возможность реализовать тонкую настройку фильтрации, классификацию трафика, применение политик контроля полосы пропускания и мониторинг сетевых потоков [2].

Типичная архитектура сетевой защиты контейнеров с применением eBPF изображена на рисунке 2 и включает в себя следующие основные компоненты: контейнеры, подключенные к виртуальным сетевым интерфейсам (например, veth-парам), eBPF-программы, установленные на входных (ingress) и выходных (egress) точках сетевого стека, а также центральные компоненты управления политиками, которые обеспечивают динамическую загрузку, обновление и удаление eBPF-программ в зависимости от изменений в инфраструктуре или угроз безопасности. Архитектура использования eBPF для сетевой защиты контейнеров строится вокруг принципов ранней фильтрации трафика. В случае применения решений уровня сервисной сетки, таких как Cilium, архитектура дополнительно включает элементы шифрования трафика, сервис-дискавери и аутентификации между контейнерами посредством eBPF-программ [4].

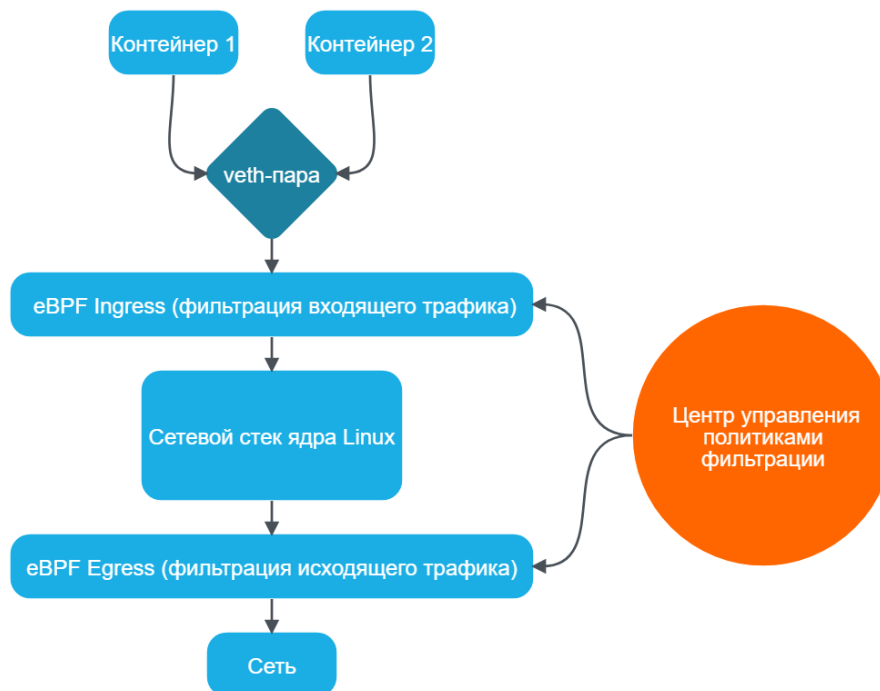


Рис. 2. Архитектура сетевой защиты контейнеров с применением eBPF

Особое внимание при проектировании архитектуры сетевой защиты контейнеров должно уделяться вопросам привязки eBPF-программ к соответствующим сетевым интерфейсам. Поскольку каждый контейнер в типичной среде виртуализации подключается к отдельному виртуальному интерфейсу, это позволяет устанавливать индивидуальные правила фильтрации и контроля для каждого экземпляра контейнера. Такой подход обеспечивает высокий уровень изоляции между приложениями и минимизирует риски горизонтального распространения атак внутри инфраструктуры.

Одним из ключевых преимуществ eBPF перед iptables является значительное увеличение пропускной способности при фильтрации сетевого трафика. XDP способен обрабатывать до 10 миллионов пакетов в секунду (Mpps) при наличии 1000 правил фильтрации, в то время как iptables достигает лишь 2 Mpps в аналогичных условиях [5], как изображено на рисунке 3. Это объясняется тем, что XDP работает на уровне драйвера сетевой карты, минимизируя количество этапов обработки пакетов в сетевом стеке ядра, тогда как iptables использует Netfilter, что приводит к дополнительным накладным расходам.

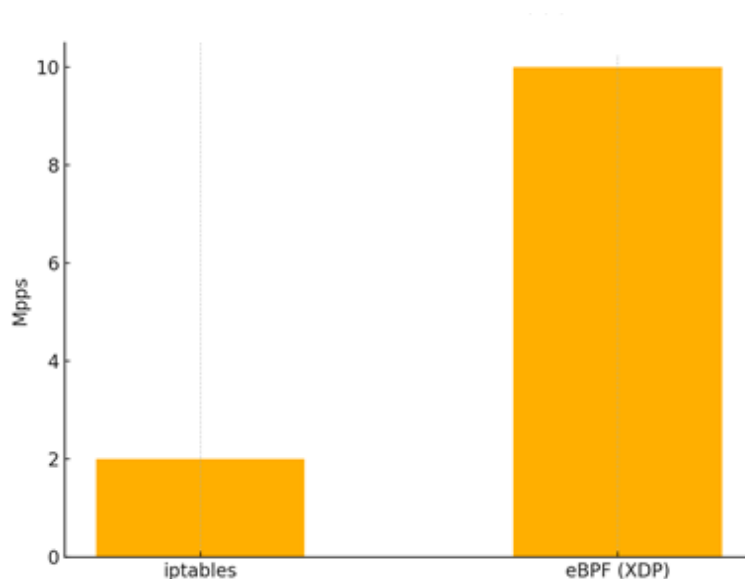


Рис. 3. Пропускная способность при 1000 правилах

При использовании eBPF (XDP) для фильтрации сетевого трафика с 5000 правил пропускная способность достигает 14 миллионов пакетов в секунду (Mpps), тогда как iptables в тех же условиях обрабатывает лишь 1.5 Mpps. На рисунке 4 также видно, что добавляемая задержка на пакет при применении XDP составляет 5-10 микросекунд, в то время как iptables увеличивает задержку на 50-100 микросекунд. В тестах с контейнерами на двух bare-metal узлах, соединенных 100 Гбит/с сетевым интерфейсом, максимальная пропускная способность одного TCP-соединения с использованием eBPF составила около 40 Гбит/с, а с iptables – 30 Гбит/с [5]. Для 32 параллельных TCP-соединений суммарная пропускная способность достигла 90 Гбит/с с eBPF и 70 Гбит/с с iptables, что близко к линейной скорости [6].

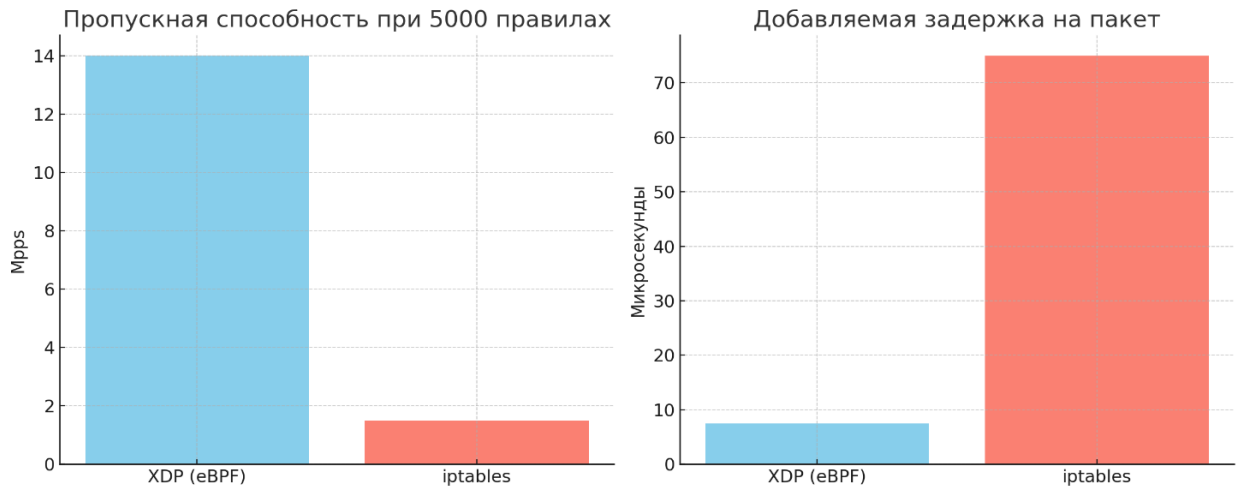


Рис. 4. Диаграммы пропускной способности и задержки на пакет при 5000 правил

На рисунке 5 изображено, как при фильтрации трафика с пропускной способностью 1 Mpps iptables нагружает CPU на 100 % одного ядра, тогда как eBPF (XDP) потребляет 30 % CPU при обработке 10 Mpps. Для достижения пропускной способности 40 Гбит/с с одним TCP-соединением eBPF использует около 50 % одного CPU-ядра, тогда как iptables требует почти 90 % ядра для достижения 30 Гбит/с [6].

Производительность iptables падает с ростом числа правил из-за линейного поиска (сложность  $O(n)$ ), тогда как eBPF, использующий хэш-таблицы (сложность  $O(1)$ ), сохраняет стабильную производительность. Тесты с 32 параллельными соединениями показывают, что eBPF способен поддерживать производительность, близкую к линейной скорости (100 Гбит/с), при достаточных CPU-ресурсах, что косвенно указывает на лучшую масштабируемость по сравнению с iptables.

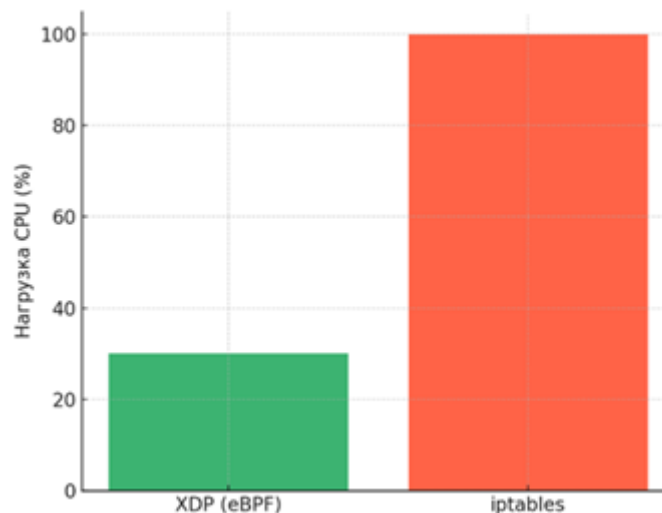


Рис. 5. Нагрузка на одно ядро CPU

В контексте контейнеризированных веб-приложений задержка HTTP-запросов является критическим параметром. При наличии 5000 правил фильтрации iptables увеличивает задержку HTTP-запросов на 15 %, тогда как XDP – всего на 2 %.

Результаты, приведенные в таблице 1 показывают, что eBPF существенно превосходит iptables по пропускной способности, снижению задержек обработки пакетов и эффективности использования ресурсов процессора, но сложнее в реализации и требует дополнительных навыков.

ТАБЛИЦА 1. Результаты тестов производительности

| Параметр                                    | eBPF (XDP)                                                   | iptables                                                        |
|---------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------|
| Уровень обработки пакетов                   | На уровне драйвера сетевой карты (до сетевого стека ядра)    | На уровне Netfilter в ядре (после прохождения сетевого стека)   |
| Пропускная способность (1000 правил)        | До 10 миллионов пакетов в секунду (Mpps)                     | Около 2 миллионов пакетов в секунду (Mpps)                      |
| Пропускная способность (5000 правил)        | До 14 Mpps                                                   | Около 1.5 Mpps                                                  |
| Добавляемая задержка на пакет               | 5–10 микросекунд                                             | 50–100 микросекунд                                              |
| Нагрузка на CPU при 1 Mpps                  | ~30 % одного ядра                                            | 100 % одного ядра                                               |
| Производительность при большом числе правил | Стабильная ( $O(1)$ благодаря хэш-таблицам)                  | Падает линейно ( $O(n)$ ) из-за линейного поиска                |
| Максимальная пропускная способность TCP     | До 90 Гбит/с при 32 соединениях                              | До 70 Гбит/с при 32 соединениях                                 |
| Гибкость обновления правил                  | Высокая: динамическая загрузка и обновление без перезагрузки | Низкая: изменение требует пересоздания или переустановки правил |
| Влияние на задержку HTTP-запросов           | Увеличение на 2 % при 5000 правилах                          | Увеличение на 15 % при 5000 правилах                            |
| Тип фильтрации                              | Программируемая, гибкая (можно писать свои логики)           | Жестко заданная фильтрация                                      |
| Сложность разработки и настройки            | Выше: требуется знание eBPF и особенностей ядра Linux        | Ниже: более стандартные подходы и широкая документация          |
| Поддержка контейнеризированных сред         | Отличная: легко интегрируется в динамическую инфраструктуру  | Ограниченная: сложнее масштабировать и обновлять                |

**Список используемых источников**

1. Benison Technologies. eBPF vs Traditional Packet Filtering Technologies: A Deep Dive. URL: <https://benisontech.com/ebpf-vs-traditional-packet-filtering-technologies-a-deep-dive/> (дата обращения 20.04.2025).
2. eBPF Foundation. What is eBPF? URL: <https://ebpf.io/what-is-ebpf/> (дата обращения 22.04.2025).
3. Benison Technologies. The Origins and Modern-Day Applications for eBPF Linux Development. URL: <https://benisontech.com/the-origins-and-modern-day-applications-for-ebpf-linux-development/> (дата обращения 23.04.2025).
4. Cilium. Cilium Documentation. URL: <https://docs.cilium.io/en/stable/> (дата обращения 23.04.2025).
5. Cloudflare. How to Drop 10 Million Packets. URL: <https://blog.cloudflare.com/how-to-drop-10-million-packets/> (дата обращения 24.04.2025).
6. Cilium. Benchmarking Cilium: Performance Benchmarks. URL: <https://docs.cilium.io/en/latest/operations/performance/benchmark/> (дата обращения 24.04.2025).

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ИБКС Кушниром Д. В.*



УДК 004.056.53

## ИССЛЕДОВАНИЕ СВОЙСТВ WAZUH ПРИ ПОСТРОЕНИИ ЗАЩИЩЕННОГО КОМПОНЕНТА ЛВС

**Р. Г. Шарифов** (студент группы ИКТЗ-15, СПбГУТ), [sharifov.rg@sut.ru](mailto:sharifov.rg@sut.ru)

*Современные SIEM-решения играют ключевую роль в защите локальных вычислительных сетей от разнообразных угроз. Цель настоящего исследования – оценить возможности платформы Wazuh при построении защищенного компонента ЛВС. Рассмотрены архитектурные особенности Wazuh Server, Indexer, Dashboard и агентов, а также механизмы мониторинга, корреляции событий и активного реагирования на инциденты. Эффективность систем продемонстрирована в лабораторных условиях через сценарии SSH-брутфорс, порт-сканирования и SQL-инъекций.*

*информационная безопасность, обнаружение вторжений, мониторинг сетей, кибербезопасность, Wazuh, SIEM*

### Введение

В условиях роста киберугроз [1] организации вынуждены усиливать мониторинг и анализ событий безопасности. Системы SIEM стали неотъемлемым инструментом для выявления атак и инцидентов. Поскольку SIEM-системы играют ключевую роль в обеспечении информационной безопасности, необходимо проводить тестирование их возможностей для оценки эффективности и выявления потенциальных ограничений [2]. Среди открытых решений особенно выделяется Wazuh – мощная и гибкая платформа, обеспечивающая сбор, корреляцию и активное реагирование на инциденты в локальных вычислительных сетях.

### Компоненты Wazuh

Центральные компоненты системы Wazuh SIEM [3] представлены подсистемами Wazuh Server, Wazuh Indexer и Wazuh Dashboard, выполняющими взаимосвязанные функции в рамках обеспечения комплексной безопасности локальной вычислительной сети (рис. 1).

### Wazuh Indexer

Wazuh Indexer является ключевым компонентом аналитической подсистемы платформы Wazuh, представляющий собой распределенный движок полнотекстового поиска на базе OpenSearch. Он принимает структурированные данные от сервера Wazuh и преобразует их в JSON-документы для быстрого поиска и анализа. Каждое событие хранится отдельно, с четкой

классификацией атрибутов по типам данных, что облегчает корреляцию и глубокий статистический анализ.

Хранение данных логически разделено на четыре специализированных индекса: `wazuh_alerts`, предназначенный для хранения важных уведомлений, `wazuh_archives`, содержащий полные журналы событий, `wazuh_monitoring`, собирающий телеметрические данные от агентов, и `wazuh_statistics`, фиксирующий метрики производительности. Это позволяет эффективно управлять жизненным циклом данных, включая автоматическое архивирование и резервирование важных оповещений.

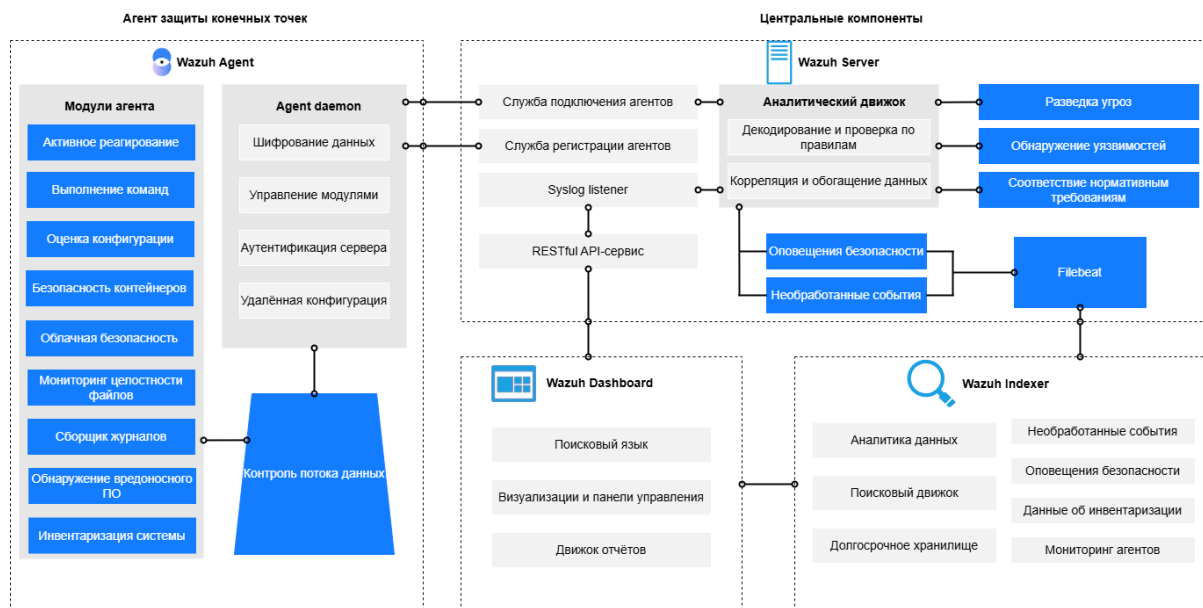


Рис. 1. Компоненты Wazuh

Физически данные распределяются по фрагментам на узлах вычислительного кластера, обеспечивая линейную масштабируемость и отказоустойчивость за счет репликации. Время задержки индексирования обычно не превышает одной секунды, что важно для оперативного реагирования.

## Wazuh Server

Wazuh Server обрабатывает события и централизованно управляет сетью сенсоров, получая телеметрию от агентов и по протоколу syslog. Данные обогащаются контекстом угроз и нормативными требованиями, затем передаются в Wazuh Indexer для хранения. Архитектура включает модули регистрации агентов, аутентификации, шифрования и управления настройками. Для систем без агентов предусмотрено преобразование syslog-сообщений. Интеллектуальное ядро – аналитический движок с модулями декодирования, корреляции событий и интеграцией баз данных MITRE

ATT&CK, уязвимостей и стандартов безопасности. Поддерживается масштабирование через кластеризацию и взаимодействие с внешними системами через RESTful API.

### **Wazuh Dashboard**

Wazuh Dashboard – веб-интерфейс платформы Wazuh, объединяющий аналитические и управляющие функции для интерактивного анализа событий и управления масштабируемой распределенной инфраструктурой мониторинга. Архитектура включает три уровня.

Первый, Wazuh Query Language, обеспечивает интуитивный отбор данных по атрибутам MITRE ATT&CK, правилам и показателям целостности через REST-API с высокой производительностью.

Второй уровень отвечает за визуализацию: с помощью гибкого конструктора пользовательских виджетов создаются гистограммы, тепловые карты и графики, адаптированные под особенности сети.

Третий уровень – движок отчетов, автоматизирующий периодическую генерацию PDF- и CSV-отчетов со сводными данными и деталями аномалий. Дополнительно реализованы разграничение доступа, настройка политик мониторинга, проверка состояния компонентов и встроенные инструменты отладки обнаружения.

### **Wazuh agent**

Агенты Wazuh разворачиваются на конечных устройствах – серверах, рабочих станциях, ноутбуках, облачных экземплярах и виртуальных машинах. Их задача заключается в постоянном сборе логов, метрик и иной эксплуатационной информации, способной указывать на потенциальные угрозы. Установленный агент не только агрегирует и передает данные, но и выполняет первичный анализ: осуществляет мониторинг логов в режиме реального времени, исследует поведение запущенных процессов и обнаруживает аномалии на уровне приложений. Это позволяет снизить нагрузку на центральные компоненты инфраструктуры и повысить общую производительность системы.

### **Мониторинг и реагирование на инциденты**

С целью оценки функциональных возможностей системы SIEM Wazuh в обеспечении безопасности локальной вычислительной сети (ЛВС) было

принято решение о проведении серии контролируемых атак. Данный подход позволил проанализировать эффективность механизмов мониторинга и реагирования, реализованных в SIEM Wazuh, в условиях моделируемых угроз для защищаемых компонентов ЛВС.

Для реализации контролируемых атак и анализа работы SIEM Wazuh была развернута лабораторная стендовая среда (рис. 2), включающая три узла: сервер с установленными центральными компонентами SIEM Wazuh, атакуемая машина, а также узел на базе Kali Linux, используемый в качестве источника атакующих воздействий.

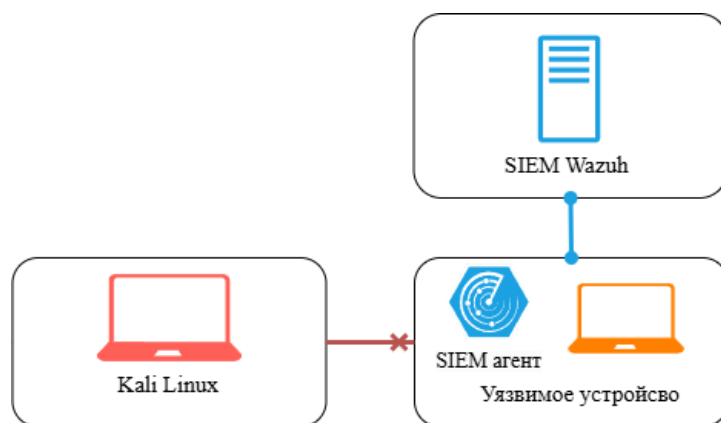


Рис. 2. Лабораторный стенд

Так, при проведении SSH-брутфорс атак – когда злоумышленник с помощью инструментов вроде Hydra осуществляет массовый перебор комбинаций логинов и паролей – Wazuh демонстрирует свою способность быстро выявлять и нейтрализовать угрозы. Система анализирует логи SSH-сервера и при обнаружении серии неудачных попыток входа, зафиксированных как событие 5763, с одного адреса инициирует модуль active-response. Этот модуль автоматически выполняет скрипт firewall-drop, добавляя IP-адрес источника атаки в блок-лист файрвола и тем самым предотвращая дальнейшие попытки несанкционированного доступа.

Кроме того, интеграция Wazuh с системой IDS/IPS Suricata позволяет эффективно обнаруживать порт-сканирование – предшествующий этап многих атак, при котором злоумышленник с помощью инструментов, например nmap, посылает серии SYN, FIN, XMAS или UDP-пакетов на разные порты для выявления открытых сервисов. Системы обнаружения и предотвращения вторжений [4] представляют собой решения для мониторинга сетевого трафика и системных событий с целью выявления подозрительной активности и предотвращения возможных угроз. Suricata анализирует сетевой трафик в реальном времени по сигнатурным правилам и

фиксирует аномальную частоту соединений или специфические шаблоны пакетов. Журналы Suricata поступают в Wazuh, где в конфигурации `ossec.conf` настроен локальный файл для их обработки. При срабатывании соответствующих правил Wazuh генерирует события о порт-сканировании и может дополнительно задействовать модуль активного реагирования для блокировки источника сканирования.

Наряду с обнаружением SSH-брутфорса и порт-сканирования, SIEM Wazuh эффективно выявляет SQL-инъекции через анализ веб-серверных логов, собираемых агентом системы. Правило ID 31164 нацелено на распознавание характерных признаков внедрения SQL-кода в запросы, модификации логических условий или добавления операторов. При срабатывании этого правила в интерфейсе SIEM появляется уведомление о потенциальном инциденте, что позволяет оперативно оценить источник атаки и принять меры.

Помимо обнаружения атак, в Wazuh можно настроить контроль целостности файлов [5], который регулярно сравнивает текущее состояние системных и пользовательских файлов с базовым снимком. При любом несанкционированном создании, изменении или удалении файлов система генерирует тревожные события. Эта функция полезна для своевременного выявления вторжений, несанкционированных изменений конфигурации и соблюдения нормативных требований по безопасности.

## Заключение

Таким образом, рассмотренные компоненты Wazuh: Server, Indexer, Dashboard и агенты во взаимодействии обеспечивают комплексный мониторинг, корреляцию событий и активное реагирование. На лабораторном стенде при моделировании SSH-брутфорса, порт-сканирования и SQL-инъекций платформа своевременно обнаруживала и блокировала атаки, включая автоматическое добавление вредоносных IP в черные списки. Результаты демонстрируют, что Wazuh обеспечивает надежную защиту компонентов ЛВС.

## Список используемых источников

1. Кибербезопасность на пике спроса: что движет отраслью в 2024–2025 годах // Anti-Malware URL: [https://www.anti-malware.ru/analytics/Technology\\_Analysis/Cybersecurity-market-trends-2024-2025](https://www.anti-malware.ru/analytics/Technology_Analysis/Cybersecurity-market-trends-2024-2025) (дата обращения 20.04.2025).
2. Штеренберг С. И. Разработка методики внедрения и выявления эффективности siem-системы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 40–45.

3. Wazuh. Getting started with Wazuh. Wazuh Documentation //Wazuh documentation. Wazuh Incorporation. URL: <https://documentation.wazuh.com/current/getting-started/index.html> (дата обращения 20.04.2025).

4. Штеренберг С. И. Метод построения архитектуры интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 1. С. 82-90.

5. Наргузина, Ж. К. Внедрение мониторинга целостности файлов на примере SIEM Wazuh с открытым исходным кодом // Молодой ученый. 2025. № 5 (556). С. 12-15. URL: <https://moluch.ru/archive/556/122274/> (дата обращения 24.04.2025).

*Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Штеренбергом С. И.*

## СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ И ЭКОНОМИКА ДАННЫХ

УДК 94(55)

Багери Н. А. (студент группы ИСТ-461, СПбГУТ), [bageri.na@sut.ru](mailto:bageri.na@sut.ru)

### ИРАН ВО ВТОРОЙ МИРОВОЙ ВОЙНЕ: ОТ НЕЙТРАЛИТЕТА ДО ТЕГЕРАНСКОЙ КОНФЕРЕНЦИИ

*Статья посвящена роли Ирана во Второй мировой войне, от политики нейтралитета до Тегеранской конференции 1943 года. Рассматриваются причины симпатий части иранского общества к нацистской Германии, включая идеологические, экономические и антиколониальные факторы. Анализируется деятельность протемецких групп (групп, поддерживающих Германию) и реакция религиозных лидеров на внешнеполитические изменения. Особое внимание уделено стратегическим причинам ввода войск союзников в 1941 году и их последствиям для Ирана. Исследуется значение Тегеранской конференции для послевоенного статуса страны. Рассмотрим, как война повлияла на внутреннюю политику и национальное самосознание.*

*Иран, Вторая мировая война, Тегеранская конференция, Персидский коридор, нацистская пропаганда, шиитское духовенство*

#### Введение

Вторая мировая война затронула практически все регионы мира, включая страны, которые официально объявляли нейтралитет. Иран, расположенный на стратегическом перекрестке между Европой и Азией, стал важным узлом в борьбе за контроль над ресурсами и логистическими маршрутами. Рассмотрим, как Иран оказался вовлечен в глобальный конфликт, почему его отношения с Германией сменились на сотрудничество с союзниками, и какие ключевые фигуры, помимо шаха, определяли судьбу страны в этот период. Особое внимание уделим восприятию Германии внутри Ирана, причинам ввода войск союзников и роли отдельных личностей в этом процессе [1, с. 45-48].

## Отношение иранского общества к Германии

В предвоенные годы и в начале 1940-х Германия вызывала заметные симпатии среди части иранского общества, особенно в образованных кругах. Это объяснялось сочетанием нескольких факторов. Во-первых, многие иранцы видели в Германии силу, способную противостоять традиционному британскому и советскому влиянию в регионе. Во-вторых, нацистская пропаганда успешно эксплуатировала идею «арийского родства» между немцами и персами, что находило отклик среди интеллектуальной элиты – немецкие дипломаты регулярно организовывали соответствующие культурные мероприятия в Тегеране. В-третьих, экономические связи играли важную роль: Германия была вторым по значимости торговым партнером Ирана после Великобритании, а многочисленные немецкие специалисты, работавшие в стране, способствовали укреплению двусторонних отношений [2, с. 18–25].

Однако эти симпатии не означали массовой поддержки нацистской идеологии. Большинство иранского населения оставалось равнодушным к политическим доктринам, сосредоточившись на насущных экономических проблемах. Шиитское духовенство, включая влиятельных аятолл, решительно осуждало антисемитскую и агрессивную политику нацистов как противоречащую исламским принципам. Левые силы, особенно коммунистическая партия Туде, активно выступали против фашизма, организуя протестные акции против немецкого влияния. Фактически, пронацистские настроения были распространены преимущественно среди политической элиты и части интеллигенции, но не в широких народных массах. Это подтверждается отсутствием значительного сопротивления со стороны населения после ввода войск союзников в 1941 году [3, с. 33–37].

Немецкое влияние в Иране поддерживалось через разветвленную сеть пропагандистской деятельности и подрывных операций. Германское посольство в Тегеране активно финансировало пронацистские публикации в местных СМИ, создавая благоприятный образ Третьего рейха. Ключевую роль в этом процессе играл министр внутренних дел Абдулхосейн Тайеб, который не только содействовал распространению пропагандистских материалов, но и поддерживал тесные контакты с немецкими дипломатами. Параллельно немецкие агенты проводили разведывательные операции против британских и советских интересов – в 1940 году была раскрыта группа, планировавшая диверсию на нефтяных месторождениях Хузестана с целью



нарушения поставок нефти союзникам. После ввода войск антигитлеровской коалиции пронацистские элементы подверглись масштабным репрессиям: британские и советские спецслужбы провели серию операций, в ходе которых были арестованы десятки иранских чиновников, подозреваемых в сотрудничестве с Германией [4, с. 89–92].

### **Поддержка Германии**

В предвоенные и военные годы иранская политическая элита разделилась на три основных лагеря по вопросу внешнеполитической ориентации. Наиболее активными сторонниками сотрудничества с Германией выступали министр внутренних дел Абдулхосейн Тайеб, который не только продвигал нацистскую идеологию, но и оказывал практическую помощь немецким агентам. Посол в Берлине Ахмад Матин-Дафари, также рассматривавший альянс с Третьим рейхом как средство ослабления британского и советского влияния в стране [1, с. 52–58].

Прозападная фракция, представленная послом в Лондоне Хоссейном Ала, делала ставку на союз с Великобританией как гарантию сохранения национального суверенитета. К этой позиции с оговорками присоединился и влиятельный аятолла Кашани, который, несмотря на принципиальное неприятие иностранного вмешательства, признавал необходимость временного сотрудничества с англичанами для противодействия нацистской угрозе [8, с. 104–107].

Левые силы, включая политика Таги Армани и активистку партии Туде Парвизи Каземи, видели в Советском Союзе не только защитника от немецкой агрессии, но и образец социально-экономического развития. Армани акцентировал внимание на необходимости советской поддержки для безопасности северных регионов, тогда как Каземи выступала за союз с СССР как средство защиты интересов трудящихся классов [7, с. 71–73].

### **Роль религиозных лидеров в политике Ирана военного периода**

В годы Второй мировой войны шиитское духовенство играло значительную, но неоднозначную роль в иранской политике. Два наиболее влиятельных религиозных деятеля – аятолла Абу-ль-Касим Кашани и аятолла Хоссейн Боруджерди – демонстрировали разные подходы к сложившейся ситуации.

Кашани, занимая принципиальную позицию против иностранного вмешательства, тем не менее решительно осуждал нацистскую идеологию как

противоречащую исламским ценностям. Его прагматизм проявился в 1941 году, когда после ввода войск союзников он призвал к сотрудничеству с антигитлеровской коалицией ради сохранения национальных интересов. В августе 1941 года Кашани активно выступал за поддержание общественного порядка и предотвращение конфронтации с войсками антигитлеровской коалиции [7, с. 88–91].

В отличие от Кашани, аятолла Боруджерди избрал стратегию сдержанного нейтралитета. Он сознательно избегал каких-либо публичных заявлений в поддержку или против воюющих сторон, что позволяло ему сохранять диалог как с союзниками, так и с местными властями. Боруджерди руководствовался опасениями, что открытая конфронтация может подорвать позиции религиозных институтов. Его осторожная позиция в конечном итоге способствовала сохранению автономии шиитского духовенства во время присутствия в Иране иностранных войск [8, с. 112–115].

Во время Тегеранской конференции 1943 года религиозные лидеры демонстрировали готовность к конструктивному взаимодействию с правительством, стремясь защитить интересы страны в условиях международного кризиса. Эта сбалансированная позиция духовенства позволила сохранить стабильность в религиозной сфере и избежать радикализации общества в военный период [4, с. 132–135].

### **Ввод войск союзников в Иран**

В июне 1941 года, после нападения Германии на СССР, Великобритания и Советский Союз начали тесную координацию своих действий, в результате чего Иран оказался перед реальной угрозой ввода иностранных войск. Это решение союзников было обусловлено тремя ключевыми факторами. Во-первых, активная немецкая разведывательная деятельность на территории Ирана вызывала серьезные опасения, что страна может превратиться в операционный плацдарм для действий Германии на Ближнем Востоке. Во-вторых, через Иран проходил стратегически важный Персидский коридор, который приобретал жизненно важное значение для обеспечения военных поставок союзникам. В-третьих, контроль над иранскими нефтяными ресурсами становился вопросом национальной безопасности – союзники не могли допустить, чтобы эти стратегические запасы оказались под контролем немецких войск [6, с. 50–55].

25 августа 1941 года началась совместная военная операция Великобритании и СССР под кодовым названием «Согласие». Британские войска

пересекли иранскую границу с юга, в то время как советские части вошли с северного направления. Военная кампания развивалась стремительно – уже к началу сентября союзнические силы установили полный контроль над ключевыми регионами страны. Эти события привели к важному политическому последствию: под давлением обстоятельств Реза-шах был вынужден отречься от престола, передав власть своему сыну Мохаммеду Резе Пехлеви, что ознаменовало начало нового этапа в современной истории Ирана [5, с. 77–82].

### **Тегеранская конференция 1943 года: символика места и исторические последствия**

Проведение первой встречи «Большой тройки» в Тегеране в конце ноября – начале декабря 1943 года не было случайным выбором. Этот город, оказавшийся на стыке советской и британской зон влияния, символизировал ту ключевую роль, которую Иран невольно играл в стратегических планах союзников. Расположенный на перекрестке транспортных маршрутов, Тегеран стал не просто удобным местом для встречи, но и живым воплощением «Персидского коридора» – той жизненно важной артерии, по которой шли военные поставки в Советский Союз. Мероприятие проходило в атмосфере строжайшей секретности и беспрецедентных мер безопасности. Как показывают рассекреченные архивные документы, советские и британские спецслужбы совместными усилиями нейтрализовали несколько серьезных угроз, включая подготовку покушения со стороны немецких диверсантов. Сама необходимость таких чрезвычайных мер безопасности красноречиво свидетельствовала о значении, которое придавали этому событию все воюющие стороны [7, с. 95–101].

Высказывания лидеров антигитлеровской коалиции об Иране носили в целом благожелательный, но достаточно общий характер. Рузвельт говорил о стране как о примере сотрудничества, Сталин подчеркивал принцип независимости, Черчилль выражал благодарность за вклад в общее дело. Однако за этими дипломатичными формулировками скрывалось сложное положение Ирана, формально сохранявшего суверенитет, но фактически находившегося под контролем стран антигитлеровской коалиции. Итоги конференции для иранского государства оказались противоречивыми. С одной стороны, была подтверждена территориальная целостность страны и обещана экономическая помощь. С другой – пребывание иностранных войск продолжалось еще несколько лет после окончания войны, что существенно

повлияло на внутривнутриполитическую ситуацию. Именно в этот период начинают формироваться те националистические настроения, которые впоследствии выльются в движение за национализацию нефтяной промышленности под руководством Мосаддыка [8, с. 118–124].

Историческая ирония заключается в том, что проведение конференции такого уровня в Тегеране, с одной стороны, подняло международный престиж Ирана, а с другой – наглядно продемонстрировало ограниченность его реального суверенитета в условиях военного времени. Это событие стало важной вехой не только в истории Второй мировой войны, но и в процессе формирования современного иранского национального самосознания, оказав влияние на последующее развитие страны в послевоенные десятилетия [1, с. 145–150].

## Заключение

Вторая мировая война стала переломным моментом в истории Ирана, поставив страну перед сложным выбором между нейтралитетом и вынужденным сотрудничеством с великими державами. Несмотря на симпатии части политической элиты и интеллигенции к нацистской Германии, обусловленные антиколониальными настроениями и идеологией «арийского братства», большинство иранского населения не поддержало фашистскую идеологию. Религиозные лидеры, особенно шиитское духовенство, открыто осуждали нацизм, а левые движения выступали за союз с СССР.

Ввод войск союзников в 1941 г. кардинально изменил положение Ирана, превратив его в ключевое звено системы военных поставок по «Персидскому коридору». Тегеранская конференция 1943 г. подтвердила стратегическую важность страны, но также заложила основы послевоенного кризиса, связанного с иностранным вмешательством. Война усилила националистические настроения, которые впоследствии вылились в движение за национализацию нефтяной промышленности.

Таким образом, несмотря на временное сотрудничество с Германией, Иран в целом сохранил антифашистскую позицию, а его общество, хотя и оказалось втянутым в глобальный конфликт, не приняло нацистскую идеологию. Война стала катализатором роста национального самосознания, определив дальнейшую борьбу Ирана за суверенитет и независимость.

**Список используемых источников**

1. Фазели Реза. Положение Ирана в ходе Второй мировой войны и отношения с нацистской Германией // Журнал истории Ирана. № 4. 2006. С. 45-58.
2. Гудерзи Махмуд. Мнение иранцев о нацистской Германии во время Второй мировой войны // Исследования современной истории. № 3. 2013. С. 12-32.
3. Голи-заде Аббас. Обзор внешней политики Ирана в период Второй мировой войны и отношения с нацистской Германией // Международный журнал политики. № 2. 2011. С. 33-47.
4. Сами Махмуд. Германия и Иран: политические и экономические отношения в период правления Пехлеви // Журнал исследований Ирана. № 1. 2012. С. 89-135.
5. Шаджаи Масуд. Политика нейтралитета Ирана во время Второй мировой войны и ее роль в отношениях с Германией // Исследования в области политики. № 5. 2008. С. 29-82.
5. Алипур Махмуд. Проблемы Ирана с союзниками и Германией во время Второй мировой войны // Журнал международных отношений. № 3. 2015. С. 44-55.
7. Ализаде Надер. Влияние Второй мировой войны на внутреннюю политику Ирана // Quarterly Journal of History and Politics, Vol. 12. № 2. 2009. С. 71-107.
8. Мусави Бнхнам. Роль и положение Ирана в мировой политике во время Второй мировой войны // Журнал иранской политической истории. № 4. 2014. С. 104-124.

*Статья представлена научным руководителем, доктором исторических наук, профессором Вороновым И. И.*

УДК 81.22

П. В. Баранова (студент группы ЗР-22, СПбГУТ), [baranova.pv@sut.ru](mailto:baranova.pv@sut.ru)

## ГОСУДАРСТВЕННАЯ РЕГУЛЯЦИЯ КИТАЙСКОГО ЖЕСТОВОГО ЯЗЫКА В КОНТЕКСТЕ АВТОРИТАРНОГО ПОЛИТИЧЕСКОГО РЕЖИМА

*В статье исследуется государственная регуляция китайского жестового языка (КЖЯ) как инструмента контроля и идеологического воздействия в условиях авторитарного политического режима КНР. Анализируются исторические этапы стандартизации КЖЯ, роль государственных институтов в его продвижении, а также использование жестового языка для пропаганды. Выявляется противоречие между декларируемой поддержкой языковых прав меньшинств и жесткой централизацией коммуникационных каналов.*

*Китай, жестовый язык, авторитаризм, стандартизация, идеология, языковая политика*

Китайская политическая система, характеризующаяся авторитарными методами управления, стремится к тотальному контролю над всеми сферами общественной жизни, включая коммуникационные практики. Жестовый язык, как основной инструмент общения глухих и слабослышащих граждан, не остается вне зоны государственного регулирования. Однако процесс его стандартизации имеет глубокие исторические корни и отражает двойственную природу государственной политики: с одной стороны, стремление к унификации, с другой – подавление культурного разнообразия. История китайского жестового языка (КЖЯ) насчитывает столетия. Первые упоминания о жестовом общении глухих встречаются в «Исторических записках» Сыма Цяня (II в. до н.э.), где отмечается использование спонтанных жестов, имитирующих предметы и действия [1]. Древний КЖЯ имел две основные формы:

1. Образные жесты, сочетающиеся с положением тела и мимикой (например, жест «спать» – наклон тела и руки, сложенные как подушка).
2. «Рисование» иероглифов на ладонях или в воздухе, что позже трансформировалось в современные практики [2].

До середины XIX века язык оставался фрагментированным из-за отсутствия централизованных школ. Переломным моментом стало открытие в 1887 году первой школы для глухих в провинции Шаньдун американскими миссионерами Чарльзом и Аннет Милле. Их деятельность, вдохновленная

решениями Миланского конгресса 1880 года, способствовала распространению устных методов обучения [3]. Однако уже к середине XX века сформировались два основных диалекта:

- Пекинский (северный), где доминировала устная традиция обучения;
- Шанхайский (южный), развивавшийся в условиях жестового преподавания глухими учителями [4].

Важным фактором стало влияние западных колониальных сил. Например, французская католическая школа в Шанхае (1892 г.) внедрила дактильный алфавит, что способствовало смешению местных и европейских жестовых традиций [5].

До принятия Закона о защите прав инвалидов (2008) процесс стандартизации носил фрагментарный характер. В 1947 году Министерство образования КНР инициировало первые попытки унификации жестов, направленные на сокращение диалектной разобщенности [2]. Однако отсутствие централизованной поддержки и ресурсов замедляло прогресс.

В 1950-х годах началась экспериментальная разработка «Схем и иллюстраций универсального языка жестов для глухих», завершившаяся публикацией четырехтомного сборника с 2000 жестов [6]. К 1988 году издательство Хуася выпустило обновленную версию словаря, включающую 3300 статей [7]. Эти издания, хотя и способствовали развитию КЖЯ, критиковались за игнорирование региональных особенностей. Например, в шанхайском диалекте 30 % лексики оставались уникальными, что создавало барьеры для коммуникации между носителями разных регионов [8].

С 2008 года в Китае действует Закон о защите прав инвалидов (中华人民共和国残疾人保障法), гарантирующий право на использование жестового языка [9]. Однако его реализация сопровождается жестким контролем. Образовательные программы и учебные материалы утверждаются Министерством образования и Китайской федерацией инвалидов (КФИ), что исключает альтернативные методики [3].

В 2018 году Министерство образования выпустило «Стандартный словарь китайского жестового языка», включающий 8000 жестов [10]. Унификация затронула даже идеологически значимые понятия:

- жест для «родины» заменен на символ, ассоциирующийся с патриотизмом и КПК;
- региональные диалекты (шанхайский, гуанчжоуский) объявляются «устаревшими», их использование в публичном пространстве ограничивается.

Внедрение систем ИИ для распознавания жестов позволяет мониторить коммуникацию в реальном времени. Например, платформы видеосвязи Tencent Meeting интегрированы с алгоритмами, анализирующими жесты на предмет «нежелательной» лексики [11]. В 2022 году такие системы выявили 12 000 «подозрительных» коммуникаций среди глухих пользователей [12].

Государство создает жесты для ключевых идеологических концепций:

- в 2022 году введен жест «социализм с китайской спецификой» – комбинация символов «Китай» и «прогресс» [12];

- учебники включают жестовые версии речей Си Цзиньпина и государственного гимна.

Процесс унификации КЖЯ имеет двойственные последствия:

Положительные аспекты:

1. Улучшение взаимопонимания между глухими из разных регионов. По данным исследования 2020 года, после введения стандарта уровень коммуникативной эффективности вырос на 45 %.

2. Доступность образования через единые программы. К 2020 году 80 % глухих учащихся получили доступ к стандартизированным учебным материалам [10].

3. Интеграция в общество: трудоустройство, доступ к государственным услугам.

Отрицательные аспекты:

1. Утрата культурного наследия локальных сообществ. Например, в Шанхае исчезли 200 уникальных жестов, связанных с местными традициями [8].

2. Ограничение свободы выражения через цензуру. В 2021 году 15 % глухих граждан сообщили о самоцензуре в публичных выступлениях.

3. Инструментализация языка для пропаганды.

Государственная регуляция КЖЯ отражает противоречия авторитарной модернизации: стремление к единству коммуникации сталкивается с подавлением культурного разнообразия. Стандартизация улучшает доступность услуг для глухих, но лишает их автономии. Для достижения подлинной инклюзии (процесс обеспечения равных возможностей для всех членов общества, включая людей с ограниченными возможностями, через устранение барьеров и создание условий для их полноценного участия в социальной, экономической и культурной жизни) необходим диалог между властью и носителями КЖЯ. Региональные диалекты не должны рассматриваться



как угроза единству, а скорее как культурное достояние, требующее сохранения. Опыт европейских стран, где стандартизация жестовых языков сочетается с поддержкой локальных вариантов (например, региональные жесты во Франции), демонстрирует возможность такого баланса [4]. В Китае это могло бы выражаться в создании гибридных образовательных программ, где общегосударственные нормы дополняются изучением местных жестов, или в учреждении советов при КФИ с участием глухих экспертов.

Таким образом, будущее КЖЯ зависит от способности государства преодолеть односторонность авторитарной модернизации. Только интеграция «снизу вверх», учитывающая мнение носителей и сохраняющая культурное наследие, позволит превратить жестовый язык из инструмента контроля в механизм подлинной социальной интеграции.

#### Список используемых источников

1. Цянь С. Исторические записки (Ши Цзи). Том 8. М.: Восточная литература, 2002.
2. 高宇翔. 中国手语的发展历史回顾 // 当代语言学. 2013. № 15. С. 94–100.
3. Lytle R. R. Deaf education in China: history, current issues, and emerging deaf voices // American Annals of the Deaf. 2005. № 150 (5). С. 457–469.
4. Fischer S. Variation in East Asian sign language structures // Sign Languages. Cambridge: Cambridge University Press, 2010. С. 499–518.
5. Hao L. Early Development of Chinese Sign Language in Shanghai Schools for the Deaf // Frontiers in Psychology. 2021. Т. 12. С. 702620.
6. 高宇翔. 中国手语的发展历史回顾 // 当代语言学. 2013. № 15. С. 94–100.
7. Su S-F. Lexical Comparison of Signs from Taiwan, Chinese, Japanese, and American Sign Languages: Taking Iconicity into Account // Taiwan Sign Language and Beyond. Taiwan, 2009. С. 149–176.
8. 赵晓驰. 中国手语标准化: 历程与审视 // 桂林航天工业学院学报. 2019. № 2. С. 304–310.
9. Закон КНР «О защите прав инвалидов» (2008). URL: <http://www.gov.cn> (дата обращения 29.04.2025).
10. 赵晓驰. 中国手语标准化: 历程与审视 // 桂林航天工业学院学报. 2019. № 2. С. 304–310.
11. Петров А. А. Китайская система тотального контроля за обществом // Chronos. 2020. № 9 (48). С. 25–36.
12. Маслов Д., Яновский К. Авторитаризм и передовой китайский опыт // Экономическая политика. 2009. № 6. С. 147–163.

*Статья представлена научным руководителем, доцентом кафедры ИиРВ СПбГУТ, кандидатом исторических наук Молчановой Т. В.*

УДК 336.71

Е. Ф. Бармин (студент группы ЭМ-41, СПбГУТ), [barmin.ef@sut.ru](mailto:barmin.ef@sut.ru)**КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА БАНКА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ НА ПРИМЕРЕ ВТБ**

*В условиях стремительного развития цифровых технологий и экономики данных банки сталкиваются с необходимостью изменения традиционных бизнес-моделей. Рассмотрен опыт цифровой трансформации ПАО «ВТБ» как одного из крупнейших российских банков. Анализируются ключевые направления использования данных: технологии Big Data, искусственный интеллект, автоматизация процессов, а также системы обеспечения кибербезопасности. Подчеркивается роль данных как стратегического ресурса, обеспечивающего повышение эффективности и снижение издержек, так и формирование устойчивых конкурентных преимуществ банка в условиях цифровой экономики.*

*ВТБ, цифровая трансформация, IT-инвестиции, ИИ, Big Data, омниканальность, экосистема, автоматизация процессов*

Конкуренция в банковском секторе и стремительное развитие цифровых технологий требуют от финансовых организаций гибкости, инновационности и технологической устойчивости. Внешторгбанк (ВТБ) демонстрирует системный подход к цифровой трансформации, сочетающий масштабные инвестиции, импортозамещение и внедрение передовых IT-решений. Банк активно развивает розничное и цифровое направления, интегрирует искусственный интеллект, модернизирует инфраструктуру и выстраивает собственную технологическую платформу, что позволяет ему усиливать позиции на рынке и адаптироваться к новым экономическим и технологическим вызовам.

Внешторгбанк – второй по активам банк России с широкой клиентской базой. По итогам 2023 г. его чистая прибыль составила рекордные 432,3 млрд руб., что существенно превышает результаты 2021 г. (327 млрд руб.) [1]. ВТБ больше всего представлен в корпоративном сегменте. Обладает международной сетью филиалов, широкой клиентской базой, различными моделями работы с клиентами. В то же время в последние годы ВТБ активно развивает розничный и цифровой бизнес, используя преимущества государственного статуса.

С 2020 по 2022 гг. банк проводил масштабную программу цифровой трансформации: глубокую модернизацию инфраструктуры, переработку бизнес-процессов и создание нового операционного цикла. Банк инвестировал в сферу ИТ 291,3 млрд руб., а экономический эффект от этого уже превысил 300 млрд руб. [2].

В соответствии с новой стратегией ВТБ ключевыми направлениями цифрового развития стали масштабирование розничного направления и омниканальность, решения на основе ИИ и полное достижение технологического суверенитета. По мнению руководства, в приоритете «сквозное обслуживание клиентов между блоками» и «технологическая независимость». Это означает, что в критической ИТ-инфраструктуре ВТБ планирует полностью перейти на отечественное оборудование.

ВТБ почти полностью отказался от применения зарубежных технологий – более 90 % используемых систем переведены на отечественный ИТ-стек. К началу 2024 г. в банке было импортозамещено 760 систем и 850 тыс. ИТ-компонентов [3]. Это защищает от внешних перебоев и санкций, а также уменьшает затраты.

Активно модернизируя ИТ-инфраструктуру, ВТБ построил частное облако на базе микросервисной архитектуры – 167 сервисов покрывают все продукты и каналы банка. К 2023 году компания вывела 5 из 7 устаревших центров обработки данных, использует домашние средства виртуализации и контейнеризации, полностью «выстраивает ИТ-ландшафт на отечественных решениях». Это дает крайне высокую надежность – доступность сервисов 99,99 %, многократное резервирование (каждая критическая система размножена 3–6 раз) и быстрое аварийное переключение составляет примерно 3 минуты [3].

Главная выгода – высокая надежность и гибкость. Например, скорость выхода новых продуктов на рынок упала с 240 до 30 суток (целью банка является 21 день), расчет клиентских предложений сократился с 16 до 6 дней. Автоматизация позволила уменьшить фронт-офис и бэк-офис на 40 %, а производительность оставшихся сотрудников выросла на 40 % [2].

После трансформации компания использует единое мобильное/интернет-приложение «ВТБ Онлайн». Каналы самообслуживания сейчас полностью охватывают клиентов всех сегментов. В таблице 1 перечислены все основные платформы и сервисы для взаимодействия с клиентами.

ТАБЛИЦА 1. Структура цифровых сервисов ВТБ по клиентским сегментам и технологиям (составлено автором по [3, 4])

| Направление/<br>технология                     | Целевая<br>аудитория/<br>пользователи        | Основные<br>платформы<br>и сервисы                                                      | Ключевые показатели и<br>факты                                                                                                                                          |
|------------------------------------------------|----------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ОБСУЖИВАНИЕ КЛИЕНТОВ</b>                    |                                              |                                                                                         |                                                                                                                                                                         |
| Розничные<br>клиенты                           | 11,5 млн<br>физических лиц                   | ВТБ онлайн                                                                              | 50 млн переводов и<br>платежей ежемесячно.<br>«ВТБ Онлайн» получило<br>среднюю оценку в RuStore<br>4,7 из 5 баллов.<br>Функции: СБП, VTB Pay,<br>FaceID, робот-советник |
| Малый<br>и средний<br>бизнес                   | 1 млн компаний                               | Интернет-банк «Мой<br>бизнес»                                                           | 7 млн цифровых операций<br>в месяц.<br>Функции: анализ<br>платежей, зарплатные<br>проекты, электронные<br>счета                                                         |
| Крупный<br>бизнес                              | 19 тыс. корпора-<br>тивных клиентов          | Система ДБО 2.0                                                                         | 1 млн операций в месяц                                                                                                                                                  |
| Сотрудники<br>банка<br>(внутренние<br>системы) | 12 тыс.<br>розничных<br>менеджеров           | VTB Pro<br>(омниканальный<br>фронт-офис).<br>Единая CRM<br>и платформа<br>микросервисов | Обслуживание 410 тыс.<br>клиентов в неделю в 1270<br>отделениях.<br>Омниканальный подход<br>(мобайл, веб, отделение,<br>колл-центр)                                     |
| <b>ВНЕДРЕНИЕ ТЕХНОЛОГИЙ</b>                    |                                              |                                                                                         |                                                                                                                                                                         |
| ИИ-<br>ассистенты                              | Клиенты и<br>сотрудники                      | Голосовой<br>помощник «Тамара»,<br>Робот-консультант в<br>«ВТБ Мои<br>Инвестиции»       | Цель к 2026 г. - у каждого<br>клиента и сотрудника<br>будет цифровой советник                                                                                           |
| Big Data и<br>аналитика                        | Банк (для<br>маркетинга и<br>персонализации) | Собственная Big<br>Data-платформа                                                       | Реферальная программа: +<br>200 тыс. клиентов и + 300<br>тыс. продуктов за 1-е<br>полугодие 2024 г. без<br>затрат на маркетинг                                          |
| Биометрия<br>и<br>безопасность                 | Клиенты                                      | Биометрическая аутен-<br>тификация, СБП (QR-<br>платежи), цифровой<br>рубль и токены    | Используется для входа в<br>приложение и сервисы.                                                                                                                       |

ВТБ делает ИИ одним из краеугольных камней своей цифровой стратегии. Запущенный в 2024 г. «Цифровой помощник» объединяет разработки на основе больших языковых моделей, компьютерного зрения и распознавания речи. Банк интегрирует ИИ-алгоритмы во все продукты: скоринг кредитов, риск-менеджмент, антифрод, контактный центр и др. Например, автоматизированы маршрутизация запросов и оценка кредитоспособности, а в аналитике используется платформа Mirion (графовую ML-систему для выявления мошенничества, проверки контрагентов и конфликтов интересов).

Банк развивает собственные технологии через R&D-проекты с ведущими вузами (МФТИ, Сколтех) и активно занимается импортозамещением AI-инструментов, создавая отечественные IT-решения. При этом компания использует искусственный интеллект, опираясь на массив транзакционных данных 22 млн клиентов. Это позволяет создавать высокоперсонализированные предложения, прогнозировать активность и укреплять конкурентные позиции банка.

В повышении конкурентоспособности особую роль играет кибербезопасность. Переход на российские ПО и аппаратные средства снижает риски уязвимостей и санкционного давления. ВТБ реализует «принцип минимум прав»: защищенное облако (ФЗ-152), многоуровневую аутентификацию и мониторинг аномалий во всех системах. Банк сертифицирует критические решения в рамках национальной программы импортозамещения, обеспечивая соответствие требованиям Центробанка и регулятора.

Кроме того, ВТБ уделяет внимание отказоустойчивости: резервирование дата-центра, регулярные учения по восстановлению работы, сегментирование сети и др. Важную роль играет высокая доступность инфраструктуры и оперативное обновление (190 релизов ПО в сутки), что также является конкурентным преимуществом.

Для понимания конкурентных преимуществ ВТБ важно сравнить с лидерами рынка:

- Сбербанк – абсолютный лидер (активы примерно 50 трлн руб., а чистая прибыль 1,262 трлн руб. за 2023 год [5]). Он превзошел ВТБ в масштабах и экосистеме сервисов. ВТБ уступает ему по рознице, но сильнее представлен в корпоративном и международном бизнесе.
- Альфа-Банк – крупнейший частный банк (активы 8,411 трлн руб., а чистая прибыль за 2023 составила год 94,2 млрд руб. [5]), фокусируется на цифровом опыте. Банк активно строит «фиджитал» модель: сотни новых

офисов и отличное цифровое окружение. ВТБ при этом сосредоточен на более консервативной модели с упором на безопасность и госсектор.

- Т-банк – полностью цифровой (активы 1,818 трлн руб., чистая прибыль за 2023 составила год 37,1 млрд руб. [5]). Отличается быстрым ростом и инновациями (FinTech-платформа, кешбэк, брокер). ВТБ не может конкурировать по скорости инноваций с Т-банк, но выигрывает за счет надежности и доверия корпоративных клиентов.

Опыт ВТБ демонстрирует, что цифровая трансформация – это не только модернизация ИТ-инфраструктуры, но и глубокое переосмысление бизнес-процессов, подходов к клиентскому сервису и стратегическому управлению. Переход к отечественным технологиям, развитие омниканальности, интеграция ИИ и Big Data в банковские продукты позволили ВТБ существенно повысить эффективность, надежность и конкурентоспособность. Несмотря на конкуренцию со стороны технологичных частных банков и лидера рынка – Сбербанка, ВТБ успешно формирует собственную экосистему и укрепляет статус одного из ведущих игроков в цифровой экономике России.

#### Список используемых источников

1. ВТБ обновил рекорд по чистой прибыли в 2023 году // ГК «РосБизнесКонсалтинг». URL: <https://www.rbc.ru/finances/20/02/2024/65d3ab519a79477a0d1181ea> (дата обращения 03.05.2025).
2. ВТБ инвестировал 291,3 млрд рублей в цифровую трансформацию // Сетевое издание «CNews». URL: [https://www.cnews.ru/news/top/2023-06-08\\_vtb\\_idealnaya\\_tsifrovaya?erid=Kra23nkVc](https://www.cnews.ru/news/top/2023-06-08_vtb_idealnaya_tsifrovaya?erid=Kra23nkVc) (дата обращения 03.05.2025).
3. Официальный сайт ПАО «ВТБ». URL: <https://www.vtb.ru/> (дата обращения 03.05.2025).
4. ВТБ: искусственный интеллект станет частью всех технологий и сервисов // Сетевое издание «CNews». URL: [https://banks.cnews.ru/news/line/2024-02-27\\_vtb\\_iskusstvennyj\\_intellekt](https://banks.cnews.ru/news/line/2024-02-27_vtb_iskusstvennyj_intellekt) (дата обращения 03.05.2025).
5. Официальный сайт Банки.ру. URL: <https://www.banki.ru/> (дата обращения 03.05.2025).

*Статья представлена научным руководителем, старшим преподавателем кафедры ЭД СПбГУТ, кандидатом экономических наук Ююкиной Т. И.*

УДК 330.47

**О. В. Волчик** (ст. преподаватель кафедры ЭД, СПбГУТ), [volchik.ov@sut.ru](mailto:volchik.ov@sut.ru)  
**С. А. Федорова** (студент группы ЭМ-01в, СПбГУТ)

## РАЗРАБОТКА АЛГОРИТМА СОЗДАНИЯ ПРОЦЕССНОЙ МОДЕЛИ ИСПОЛНИТЕЛЬНОГО ОРГАНА ГОСУДАРСТВЕННОЙ ВЛАСТИ

*В статье рассматривается важность эффективного функционирования исполнительных органов государственной власти (ИОГВ) в условиях цифровой трансформации, с акцентом на Комитет по информатизации и связи Санкт-Петербурга (КИС СПб). Обсуждаются проблемы, с которыми сталкиваются эти органы при внедрении процессного управления, включая законодательные ограничения и бюрократические барьеры. Работа освещает этапы разработки модели бизнес-процессов, начиная с подготовительного этапа и заканчивая внедрением изменений, подчеркивая необходимость уделять внимание не только формализации бизнес-процессов, но и выбору подходящих методологий моделирования, таких как BPMN, IDEF0 и EPC. Также подчеркивается важность взаимодействия команды проекта с различными подразделениями для достижения успешных результатов в оптимизации государственных услуг.*

*цифровая трансформация, бизнес-процессы, исполнительные органы государственной власти, Комитет по информатизации и связи, процессное управление, BPMN, IDEF0, EPC, оптимизация, государственные услуги*

В современном мире, когда происходит активная цифровая трансформация важно уделять особое внимание эффективному функционированию исполнительных органов государственной власти (ИОГВ), которая напрямую зависит от готовности вовремя адаптироваться к современным технологиям, оптимизировать внутренние процессы под скорость современного мира и повышать качество предоставляемых государственных услуг. Ключевой орган, который отвечает за формирование и реализацию государственной политики в сфере информационных технологий и связи, играющий главную роль в обеспечении цифровой зрелости региона – Комитет по информатизации и связи Санкт-Петербурга (КИС СПб).

Отметим некоторые проблемы, возникающие в КИС СПб, при решении выполняемых задач [1]:

- неукоснительное исполнение требований законодательства, наличие дополнительного законодательного регулирования госструктур;
- выраженные «вертикальные колодцы» управления;
- деятельность, ориентированная на полномочия исполнителя, а не на потребителя;

- присутствует формализм и бюрократия;
- невысокая скорость изменений по причине необходимости глубокого (а значит, длительного) изучения действующего законодательства с целью внесения в него необходимых изменений;
- при интервьюировании систематически звучит «исторически сложилось» и делается «отсылка» к действующему законодательству.

Изложенные проблемы связаны с тем, что функциональная структура управления КИС СПб не обеспечивает достаточный уровень взаимодействия структурных подразделений для достижения удовлетворенности, как внешних, так и внутренних потребителей. Следовательно, есть необходимость в реализации иных более эффективных подходов, одним из которых является процессный подход.

Разработка процессной модели начинается с подготовительного этапа, который включает в себя: формирование команды проекта, определение рамок проекта, выбор методологии моделирования, выбор инструмента моделирования, изучение нормативной базы и обучение команды [2].

Команда проекта должна состоять из представителей КИС СПб, конкретнее, руководителей подразделений и экспертов в различных областях. Так же команда должна содержать специалистов бизнес-моделированию и анализу проекта [2].

При определении рамок проекта должны подниматься такие вопросы как: «Какие процессы будут моделироваться?», «Будет ли охватываться весь функционал КИС СПб или только определенные направления?». Также необходимо определить границы моделирования [3].

Далее необходимо выбрать методологию моделирования. Наиболее распространенные методологии представлены на рисунках 1-3.

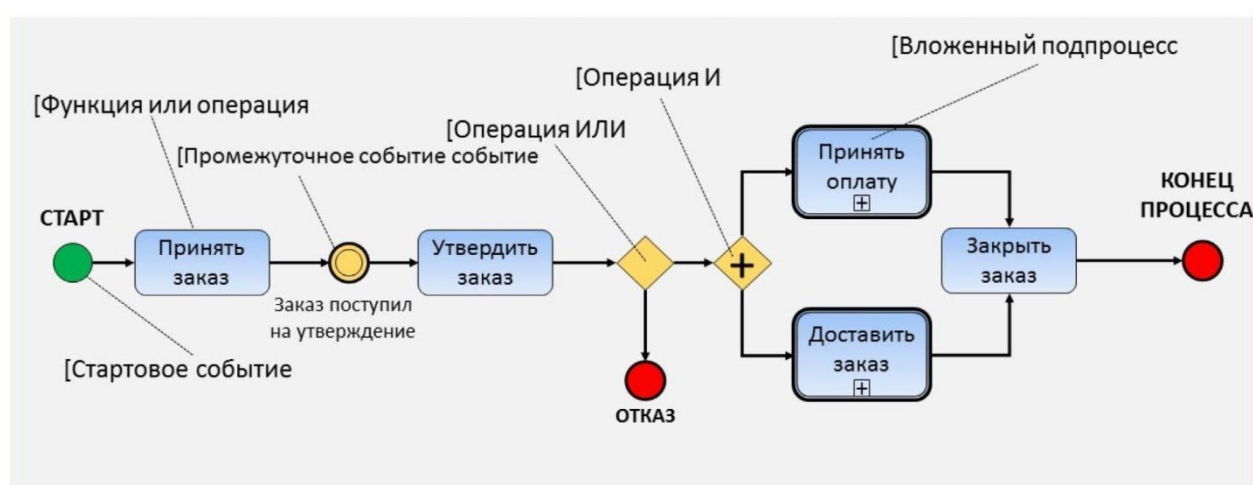


Рис. 1. Методология BPMN (Business Process Model and Notation)



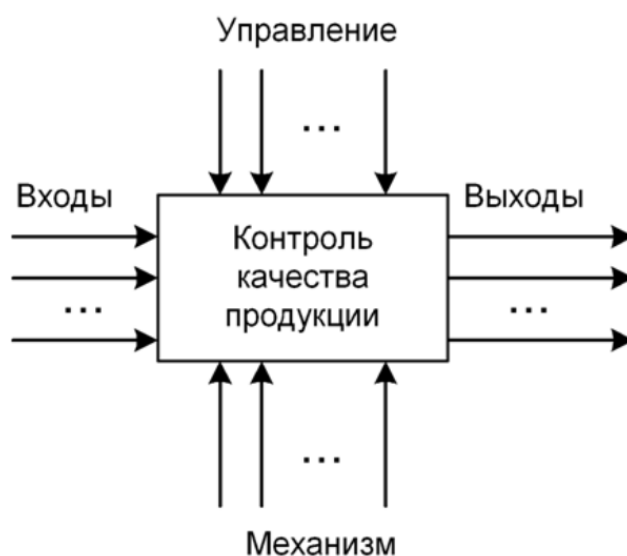


Рис. 2. Методология IDEF0

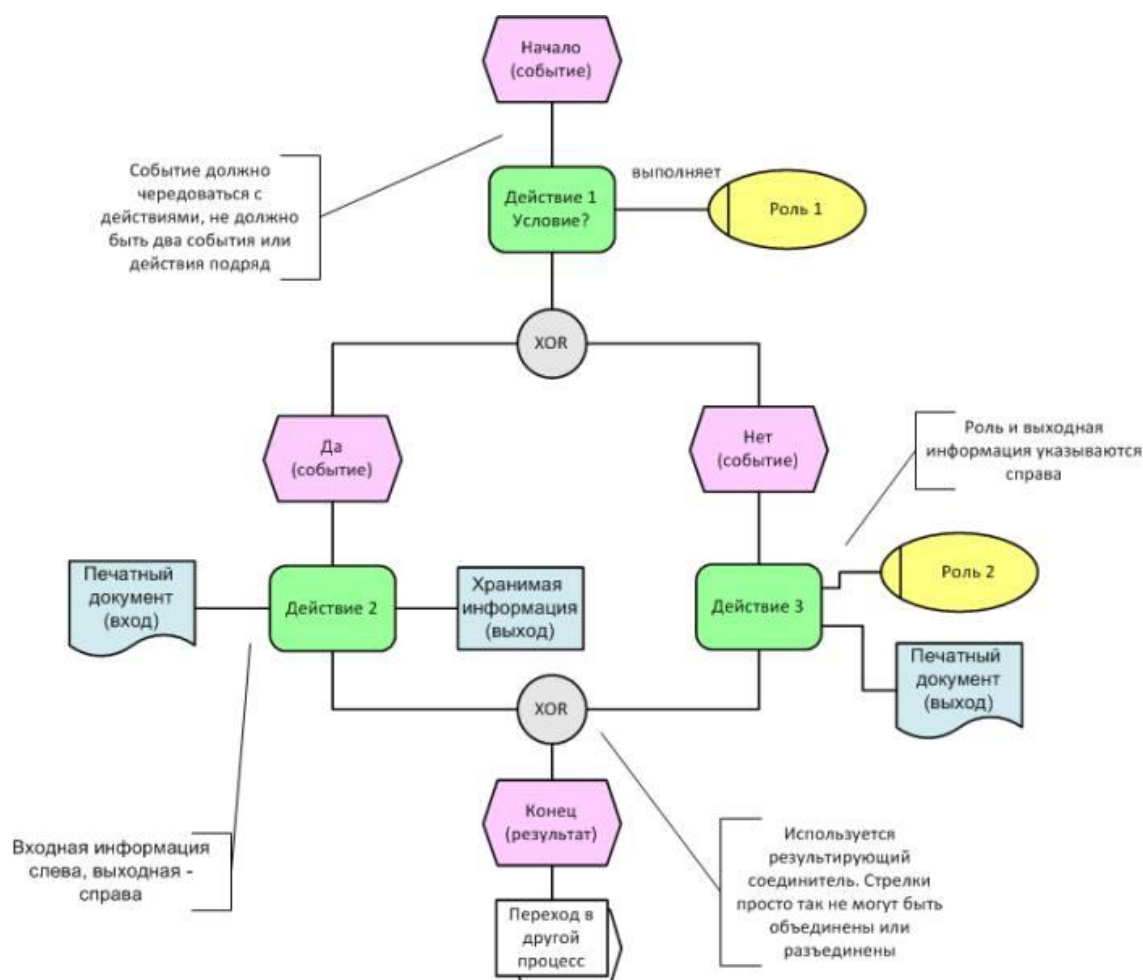


Рис. 2. Методология EPC (Event-driven Process Chain)

Кратко опишем приведенные на рисунках методологии описания процессов [4]:

- BPMN (Business Process Model and Notation). Широко распространенный стандарт для моделирования бизнес-процессов, поддерживает визуальное представление, гибкость и возможность автоматизации;
- IDEF0. Более ориентирована на функциональное моделирование, показывает «что» делается, а не «как». Может быть полезна для верхнего уровня моделирования;
- EPC (Event-driven Process Chain). Подходит для описания последовательности событий и функций.

После выбора методологии планирования необходимо изучить нормативную базу [5], регламентирующую КИС СПб, в том числе:

- Положение о Комитете по информатизации и связи.
- Регламенты предоставления государственных услуг.
- Стандарты и политики в области информационных технологий.
- Федеральные законы и нормативные акты в сфере информации и связи.

Для завершения подготовительного этапа необходимо обеспечить постоянное обучение команды работе с выбранной методологией моделирования [5].

Следующим этапом разработки процессной модели является сбор информации. Для начала необходимо провести интервью с руководителями и сотрудниками различных подразделений КИС СПб, чтобы получить достоверную информацию о выполнении бизнес-процессов в настоящее время [1].

Далее необходимо провести анализ документации, изучить соответствующие регламенты, инструкции и другие материалы, которые относятся к моделируемым процессам, а также по возможности понаблюдать за тем, как действительно выполняются процессы [5].

На основе собранных данных необходимо разработать модели бизнес-процессов «как есть», используя выбранную нотацию и инструмент моделирования, чтобы детально отразить текущую ситуацию, включая все ключевые этапы, участников, информационные системы, документы, и недостатки, обеспечив достаточную детальность для последующего анализа и выявления проблемных областей [1].

Потом следует провести всестороннюю оценку разработанных моделей «как есть» с привлечением экспертов КИС СПб и специалистов по бизнес-моделированию, используя методы анализа времени выполнения, стоимости, рисков и соответствия нормативным требованиям, чтобы выявить узкие

места, дублирование, неэффективные участки и другие проблемы в бизнес-процессах [5].

Основываясь на результатах анализа моделей «как есть», следует разработать модели бизнес-процессов «как должно быть», отражающие оптимизированные и улучшенные процессы, включая предложения по реинжинирингу, автоматизации, оптимизации использования информационных систем и улучшению взаимодействия между подразделениями с учетом требований нормативных правовых актов и передовых практик [3].

Затем нужно представить разработанные модели «как есть» и «как должно быть» руководству КИС СПб и заинтересованным сторонам для получения обратной связи, внести необходимые корректировки, обеспечить согласование и утверждение моделей для дальнейшей реализации [2].

Последним этапом создания процессной модели является разработка и реализация плана внедрения изменений в бизнес-процессы, включая обучение сотрудников, внедрение необходимых информационных систем и инструментов, организацию мониторинга выполнения процессов и оценку эффективности внедренных изменений, а также регулярный пересмотр и обновление моделей бизнес-процессов для поддержания их актуальности и эффективности [2].

Анализ современного состояния и путей совершенствования бизнес-процессов в рамках ИОГВ, в частности КИС СПб, демонстрирует необходимость комплексного подхода к внедрению процессного управления. Разработка моделей «как есть» и «как должно быть» позволяет не только выявить недостатки в существующих процессах, но и сформировать эффективные предложения по их оптимизации. Важно, что успешное внедрение предложенных изменений возможно лишь при постоянном обучении сотрудников и постоянном мониторинге процессов. Таким образом, подход к процессному управлению в государственных структурах должен учитывать как требования законодательства, так и потребности граждан, что повысит качество предоставляемых государственных услуг и сделает взаимодействие с гражданами более эффективным.

#### **Список использованных источников**

1. Панкратова С. Н. Внедрение системы процессного управления в комитете по информатизации и связи опыт проекта в 2023 году. Внедрение системы процессного управления в комитете по информатизации и связи опыт проекта в 2023 году / Панкратова С. Н. // Business Studio. URL: <https://www.businessstudio.ru/files/pankratova.pdf> (дата обращения 25.04.2025).

2. Тимохин А. Ликбез для руководителей: моделирование бизнес-процессов на раз-два-три / Тимохин А. // Business Studio. URL: [https://www.businessstudio.ru/articles/article/likbez\\_dlya\\_rukovoditeley\\_modelirovanie\\_biznes\\_pro/](https://www.businessstudio.ru/articles/article/likbez_dlya_rukovoditeley_modelirovanie_biznes_pro/) (дата обращения 25.04.2025).

3. Копцюх Е. С. Основные задачи этапа обследования в рамках проектов автоматизации / Копцюх Е. С. // cyberleninka. URL: <https://cyberleninka.ru/article/n/osnovnye-zadachi-etapa-obsledovaniya-v-ramkah-proektov-avtomatizatsii> (дата обращения 25.04.2025).

4. Моделирование бизнес-процессов: методика, нотация, инструмент. URL: [https://emirs.miet.ru/oroks-miet/upload/ftp/pub/2015/11\\_0/563778e6738ac/Lecture2.pdf](https://emirs.miet.ru/oroks-miet/upload/ftp/pub/2015/11_0/563778e6738ac/Lecture2.pdf) (дата обращения 25.04.2025).

5. Кузнецов И. В. Эффективность управления бизнес-процессами в государственных органах власти / Кузнецов И. В. // Молодой ученый. URL: <https://moluch.ru/archive/542/118610/> (дата обращения 25.04.2025).

УДК 659

А. С. Кривенко (студент группы РСО-13, СПбГУТ), [krivenko.as@sut.ru](mailto:krivenko.as@sut.ru)

## ОСОБЕННОСТИ ПРОДВИЖЕНИЯ ИСТОРИКО-ПРОСВЕТИТЕЛЬСКИХ ПРОЕКТОВ (НА ПРИМЕРЕ "ИСТОРИЯ РОССИЙСКОГО ПРЕДПРИНИМАТЕЛЬСТВА")

*В статье рассматриваются особенности продвижения историко-просветительских проектов в современных условиях на примере проекта «История российского предпринимательства». Анализируются используемые форматы коммуникации, роль цифровых технологий, медиастратегии и взаимодействие с образовательными и культурными учреждениями. Особое внимание уделено проблемам популяризации исторических знаний и формированию положительного образа предпринимательства в общественном сознании. Проект представлен как успешная модель комплексного подхода к просветительской деятельности, объединяющая научную достоверность и современные методы вовлечения аудитории.*

*историко-просветительский проект, продвижение, цифровые медиа, предпринимательство, история, маркетинг в культуре*

Историко-просветительские проекты играют важную роль в формировании исторической памяти, гражданской идентичности и развитии интереса к культурному наследию. В условиях цифровизации и возрастающей конкуренции за внимание аудитории продвижение подобных инициатив требует инновационного подхода, адаптированного к реалиям цифровой коммуникации.

Проект «История российского предпринимательства» представляет собой комплексную инициативу, направленную на исследование, систематизацию и популяризацию информации о развитии предпринимательской деятельности в России с XVIII века до наших дней.

Современные подходы к продвижению культурных и просветительских проектов основываются на междисциплинарных моделях, сочетающих элементы культурного маркетинга, цифровых коммуникаций, сторителлинга и бренд-менеджмента. Одним из ключевых принципов продвижения историко-просветительских инициатив является необходимость создания устойчивого интереса аудитории через эмоциональную, визуально привлекательную и при этом содержательно достоверную подачу материала. Исто-

рический контент должен быть не только информативным, но и интерактивным, чтобы соответствовать ожиданиям цифровой аудитории, привыкшей к динамичному потреблению информации [1].

Теоретическая база продвижения просветительских проектов включает понятия «медиаистории», «культурной репрезентации» и «публичной истории», подчеркивающие важность адаптации исторических знаний к формату массовой коммуникации. Кроме того, важным является учет целевой аудитории и сегментация контента в зависимости от уровня подготовленности и интересов потребителей – от школьников до специалистов [2].

Эффективная коммуникация требует вовлечения через личные истории, биографии, визуализацию данных, а также использование современных платформ (социальные сети, подкасты, YouTube и др.), что позволяет достигать широкой аудитории и формировать устойчивый просветительский эффект.

Таким образом, продвижение историко-просветительских проектов требует сочетания научного подхода, направленный на трансформацию исторического знания в доступный, интересный и актуальный культурный продукт.

Сам проект «История российского предпринимательства» представляет собой масштабную историко-просветительскую инициативу, направленную на популяризацию знаний об экономической истории России и формирование положительного образа предпринимателя в общественном сознании. Основной целью проекта является демонстрация значимости предпринимательской деятельности в историческом развитии страны, а также преодоление негативных стереотипов, связанных с частным бизнесом. Проект охватывает широкий хронологический диапазон – от XVIII века до современности – и акцентирует внимание на биографиях выдающихся предпринимателей, чьи судьбы и достижения стали неотъемлемой частью отечественной истории.

Одной из ключевых особенностей проекта является его мультимедийный формат. Для охвата широкой аудитории используются различные каналы распространения контента: официальный сайт, социальные сети (VK, Telegram, YouTube), специализированные подкасты, документальные фильмы и анимационные видеоролики. Такой подход позволяет адаптировать сложный исторический материал под разные группы пользователей – от школьников до специалистов в области экономики и истории. Проект активно применяет элементы сторителлинга, предлагая аудитории не просто

сухие факты, а эмоционально насыщенные, визуально оформленные истории, которые делают исторический материал живым и вовлекающим.

Важную роль в продвижении играет сотрудничество с культурными и образовательными институтами: музеями, университетами, библиотеками. Проводятся лекции, семинары, выставки, организуются публичные дискуссии и просветительские мероприятия. Отдельное внимание уделяется образовательной составляющей: проект включает разработку методических пособий и учебных программ для школ и вузов, что способствует включению темы истории предпринимательства в систему формального образования.

Особое внимание в рамках проекта уделяется персоналиям – выдающимся предпринимателям прошлого, среди которых Савва Мамонтов, Павел Третьяков, Николай Второв, Алексей Алафузов и другие. Такой подход позволяет не только сделать исторический нарратив более персонализированным и эмоционально насыщенным, но и актуализировать тему социальной ответственности, культурного меценатства и инновационной инициативы как неотъемлемых черт российского бизнеса.

Таким образом, проект «История российского предпринимательства» демонстрирует эффективную модель просветительской работы в цифровую эпоху. Он сочетает научную достоверность с привлекательной подачей, активно использует цифровые инструменты и формирует устойчивый интерес к теме истории отечественного бизнеса как важной части национального наследия.

Несмотря на очевидные успехи проекта «История российского предпринимательства», его реализация сталкивается с рядом проблем и вызовов, характерных для историко-просветительских инициатив в целом.

Во-первых, одной из основных проблем является недостаточная узнаваемость исторических фигур российского предпринимательства. В общественном сознании доминируют образы политических и культурных деятелей, тогда как представители делового сообщества остаются в тени. Отсутствие четко сформированной и поддерживаемой государственной политики по популяризации экономической истории также затрудняет продвижение темы.

Во-вторых, существует проблема стереотипного восприятия предпринимательства, особенно в контексте дореволюционной и советской эпох. Часто бизнес ассоциируется исключительно с наживой или эксплуатацией,

а не с созидательной деятельностью, вкладом в культуру, благотворительностью и техническим прогрессом. Преодоление этих искаженных представлений требует комплексной работы с аудиторией и времени.

Кроме того, определенные сложности возникают при адаптации научного материала для широкой публики. Необходимо находить баланс между содержательной точностью и доступностью подачи. Это требует не только высокого уровня профессиональной подготовки авторов, но и вовлечения специалистов в области медиа, дизайна и образования.

Еще один вызов связан с конкуренцией за внимание в информационном пространстве. Историко-просветительские проекты зачастую проигрывают более «легкому» и развлекательному контенту. Это требует постоянного обновления форматов, интерактивности, использования трендовых подходов (например, геймификации, коротких видео, инфографики).

Наконец, устойчивое развитие проекта во многом зависит от финансирования и институциональной поддержки. Без долгосрочной стратегии, вовлечения партнерских организаций и поддержки со стороны государства и бизнеса проект рискует остаться временным явлением, несмотря на его значимость для культурного и образовательного пространства страны.

Таким образом, проект «История российского предпринимательства» представляет собой яркий пример того, как историко-просветительская инициатива может эффективно работать в условиях современной цифровой среды. Его реализация демонстрирует возможности комплексного подхода к популяризации исторических знаний, включающего мультимедийные форматы, образовательные программы, культурные мероприятия и активную работу в социальных сетях.

В то же время проект наглядно выявляет ряд вызовов, с которыми сталкиваются подобные инициативы: необходимость борьбы с историческими стереотипами, сложность адаптации академических знаний для широкой публики, конкуренция с развлекательным контентом и зависимость от внешней поддержки. Эти проблемы требуют системного подхода и взаимодействия разных сфер – науки, образования, культуры, бизнеса и медиа.

Данный проект может рассматриваться как модель успешного историко-просветительского проекта, сочетающего научную глубину и современную форму подачи. Его опыт представляет ценность для разработки и реализации аналогичных инициатив в других областях истории и культуры, способствуя формированию культурной идентичности и исторического самосознания общества.



### **Список используемых источников**

1. Веселова М. Н. Основы проектной деятельности для социально-экономических и гуманитарных специальностей. Учебное пособие Санкт-Петербург.: КноРус, 2024. 192 с.

2. Ковалевой Н. Б., Ковалева Ф. А. Инновационное проектирование гуманитарных технологий. Москва: Литрес, 2018. 65 с.

*Статья представлена научным руководителем, деканом факультета СТЭД СПбГУТ, кандидатом политических наук, доцентом Шутманом Д. В.*

УДК 659.4  
ГРНТИ 19.21.91

Е. Н. Лапшина, М. Р. Мустафаев (студенты группы РСО-43, СПбГУТ),  
[lizalap5072@gmail.com](mailto:lizalap5072@gmail.com), [makaryalta@mail.ru](mailto:makaryalta@mail.ru)

## ЭФФЕКТИВНЫЙ КОРПОРАТИВНЫЙ КОНТЕНТ: СТРАТЕГИИ, КРЕАТИВ И АНАЛИТИКА

*Данная статья рассматривает, как применение эффективных стратегий создания и распространения корпоративного контента может повлиять на деятельность и благосостояние фирмы (организации). На примере деятельности крупных компаний («Google» и «Газпром») демонстрируется, как использование качественных технологий корпоративного контента позволяет не только удерживать сотрудников компании на рабочих местах, но и вовлекать их в процесс двусторонней коммуникации, что способствует развитию долгосрочных доверительных отношений между организацией и ее общественностью и продвижению фирмы на рынке.*

*корпоративный контент, лояльность сотрудников, коммуникация, привлечение клиентов, эффективный подход*

Корпоративный контент, под которым понимаются все данные и документы, которые генерируются и используются в работе компании [1], является важным элементом функционирования любой организации. Это могут быть отчеты, договоры, презентации, заявки клиентов, электронные письма, видео-контент и многое другое. Такой контент позволяет удерживать сотрудников, адаптировать новых членов команды, вовлекать сотрудников в коммуникацию, а также помогает сплотить команду в период стресса и кризиса.

Специалист по контент-маркетингу Валерия Ласкова подчеркивает, что создание корпоративного контента служит во благо нынешних и потенциальных клиентов [2]. Качественный корпоративный контент – это хороший способ для привлечения внимания к деятельности фирмы, а также для формирования экспертного образа организации и доверия со стороны целевой аудитории. Например, интервью со специалистом команды формирует из него лидера мнений в конкретной сфере. Аудитория видит, что в компании работают профессионалы, что в конечном счете ведет к увеличению количества клиентов, привлечению ценных сотрудников и партнеров, и продвижению организации на рынке.

Управление корпоративным контентом требует системного подхода. Ведь каждый сотрудник должен иметь возможность быстро найти необходимую информацию, а клиенты и соискатели через непрерывный поток контента будут знакомиться с различными аспектами функционирования компании. Это говорит о необходимости стратегического планирования корпоративного контента и о важности применения эффективных технологий его создания. Фомина Е.А., чьи работы упоминались выше [1], выделяет следующие аспекты эффективного корпоративного контента:

- формирование коммуникативных сетей. То есть соединение участников коммуникационного процесса с помощью информационных потоков;
- формирование, развитие и продвижение положительного внутреннего и внешнего имиджа организации;
- формирование и реализация стратегии продвижения бренда;
- вовлечение сотрудников в управление. Иными словами, оптимизация опыта сотрудника через экспертный контент.

Чтобы избежать задержек и ошибок в производстве и использовании корпоративного контента используются специальные системы управления контентом. Они могут отличаться функционалом и, соответственно, применяться в разных областях. К примеру, системы электронного документооборота (СЭД), являясь наиболее узким классом инструментов, фокусируются на том, чтобы настроить работу с документами согласно нормам и требованиям законодательства, а также регламентам компании. Сюда можно отнести регистрацию договоров, подписание кадровых документов электронной подписью для удаленных сотрудников. Существуют также системы управления корпоративным контентом ECM (Enterprise Content Management), которые появились как решение для упорядочивания и управления информацией в организации. Такие системы предназначены для работы с различными типами контента – от документов до мультимедийных файлов. Также ECM-системы позволяют работать как со структурированными, так и с неструктурированными данными, что делает их очень удобными для решения задач, возникающих при разработке и распространении корпоративного контента. Такая многофункциональность позволяет назвать ECM не просто хранилищами, а полноценными сложными платформами. Таким образом, можно говорить о том, что специальные системы управления контентом играют важную роль в процессе корпоративной коммуникации, поскольку системы электронного документооборота и платформы управления

корпоративным контентом помогают систематизировать информацию, делают ее доступной для сотрудников и защищают от потерь.

Корпоративный контент помогает продвигать компанию, привлекать клиентов и управлять мотивацией и вовлеченностью сотрудников. Именно поэтому в создании такого контента важно обращать внимание на креативность. Алиса Петрова, креативный директор агентства видеопродакшна «Moskva Production», рассуждает о ценности и допустимых границах креатива в корпоративном контенте [3]. Она говорит о том, что прямой задачей креатора, занимающегося созданием корпоративного контента является расширение представления клиентов, в роли которых в данном контексте выступают сами фирмы и организации, о возможных вариантах решения запроса. При этом важно учитывать, что любой контент должен быть в первую очередь эффективным для решения той задачи, которая была изначально поставлена. И порой, некоторые организации делают выбор в пользу проверенных временем технологий, которые не отличаются какой-то особой креативностью. В тоже время следование новым форматам и идеям помогает сформировать позитивный имидж, повысить лояльность клиентов и сотрудников, выстроить более глубокую коммуникацию. Следовательно, для достижения наибольшей эффективности, необходимо очертить допустимые для бренда рамки креатива. В этом случае идеи не будут слишком радикальными, но при этом не повторяют то, что уже сделано другими компаниями.

Говоря о корпоративном контенте, как о части целостной системы функционирования организации, стоит упомянуть о важности постоянной оценки эффективности корпоративного контента. В данном контексте необходимо отталкиваться от тех задач, которые изначально ставились при разработке контента. Если приоритетной задачей было поднятие заинтересованности аудитории и получение обратной связи, то нужно отслеживать реакцию в социальных сетях: комментарии, лайки, репосты, участие в обсуждениях и т.д. Если внимание акцентируется на определенных продуктах или услугах, то необходимо отслеживать, насколько увеличилось количество покупок или заявок. Важной метрикой также будет являться трафик из поисковых систем, по которому можно оценить, например, какие статьи приводят больше посетителей, или какие материалы находят больший отклик у аудитории. Опираясь на данные по трафику, можно определить актуальные для целевой аудитории темы, приоритетный формат подачи контента, и выделить определенные закономерности. Немаловажными, и при этом весьма эффективными, инструментами аналитики могут выступать

различные опросы, как среди сотрудников, так и среди потребителей. Опросы позволяют напрямую выяснять у аудитории мотивы поведения, отношение к бренду, к конкретным товарам или аспектам деятельности. Структурированная информация, полученная в ходе таких опросов, может полноценно отражать мнение общественности по каким-либо вопросам, проявлять сильные и слабые стороны действующей стратегии корпоративного контента и способствовать развитию эффективной коммуникации.

Далее представлен ряд примеров эффективного использования корпоративного контента известными организациями.

Транснациональная корпорация «Google», специализирующаяся на широком спектре IT-продуктов и интернет-сервисов, активно генерирует и использует корпоративный контент для достижения эффективной коммуникации с сотрудниками, клиентами и партнерами. Корпоративный контент играет важную роль во внутренней коммуникации, обучении сотрудников и поддержке инновационной культуры в данной компании. «Google» создает разнообразные материалы: внутренние блоги и новости для информирования команд о событиях и проектах, обучающие курсы и видео для повышения квалификации сотрудников, а также техническую документацию для разработки и поддержки продуктов. Стоит отметить, что сам процесс работы сотрудников компании осуществляется зачастую через сервисы, выпускаемые Google. Примером может служить «Google workspace», который является универсальной платформой для работы, включающей множество функций и инструментов, и формирующей единую экосистему. Это способствует повышению лояльности к бренду со стороны сотрудников и формированию экспертного образа компании, которая не боится использовать собственный продукт для внутреннего рабочего процесса. Данный аспект может привлекать и потенциальных ценных сотрудников, которые, будут заинтересованы в том, чтобы стать частью крупной команды профессионалов-единомышленников. Также Google активно использует корпоративный контент для обмена знаниями между отделами и стимулирования сотрудничества. Это помогает сохранять прозрачность, развивать двустороннюю коммуникацию и поддерживать единую корпоративную культуру в крупной организации [4].

Таким образом, на примере транснациональной корпорации «Google» мы видим, что планомерные действия компании, включающие разработку уникального корпоративного контента, постоянный анализ и оптимизацию такого контента и поощрение нестандартного подхода к решению задач,

способствуют не только выстраиванию доверительной коммуникации между организацией и ее общественностью, но и продвижению компании на рынке.

Наглядным примером эффективного использования корпоративного контента является российская компания «Газпром». С января 2004 г. выходит корпоративный журнал «Газпром» [5], тираж которого составляет 10 150 экземпляров. Аудиторией данного корпоративного журнала является менеджмент и топ-менеджмент ПАО «Газпром» и дочерних обществ, Правительство РФ и Администрация Президента РФ, зарубежные партнеры ПАО «Газпром» и независимые производители газа, СМИ, инвестиционные компании и экспертное сообщество. Корпоративный журнал «Газпром» создается для информирования сотрудников и партнеров компании о новостях и достижениях. В журнале публикуются статьи о новых проектах, уникальные аналитические материалы о деятельности, стратегии, планах крупнейшей российской компании, интервью ее топ-менеджеров и руководителей дочерних предприятий, заметки о благотворительных и спонсорских проектах Группы «Газпром» в сфере культуры, духовности и спорта. Особое внимание уделяется вопросам повышения эффективности и безопасности на производстве, что способствует росту доверия к организации со стороны сотрудников и позволяет удерживать на рабочих местах ценных специалистов. На официальном сайте доступен архив номеров данного журнала, с которым может ознакомиться любой желающий. Такая открытость компании способствует формированию доверия к бренду со стороны потребителей, потенциальных сотрудников и партнеров. Журнал способствует формированию единого корпоративного духа и обмену опытом между подразделениями, а регулярные публикации помогают поддерживать прозрачность и открытость внутри компании.

На примере корпоративного журнала «Газпром» мы видим, как открытость и доступность информации способствует росту авторитета компании как внутри организации, так и за ее пределами. Уникальный корпоративный контент привлекает внимание, формирует образ экспертного бренда, и способствует налаживанию эффективной коммуникации, что в совокупности с эффективными маркетинговыми решениями, выводит предприятие на лидирующие позиции на рынке.

Таким образом, использование эффективных технологий корпоративного контента, включающих стратегический подход, креативные решения и

постоянную аналитику, способствует выстраиванию долгосрочных доверительных отношений между компанией и ее сотрудниками, потребителями и партнерами. Грамотный процесс формирования и распространения такого контента требует от фирмы (организации) непрерывного поиска наиболее эффективных инструментов распространения информации, налаживания сервисов для внутреннего документооборота компании и исследования аналитических данных. Корпоративный контент, являясь неотъемлемой частью функционирования фирмы, способствует формированию целостной корпоративной культуры, налаживанию открытой коммуникации между организацией, ее партнерами, реальными и потенциальными сотрудниками и клиентами, а также росту доверия к бренду, и, соответственно, его продвижению на рынке. Поэтому, в условиях постоянной конкуренции, организации должны обращать особое внимание на использование эффективных технологий корпоративного контента, который должен быть не только информативным, но и привлекающим внимание к бренду в положительном ключе.

#### Список используемых источников

1. Фомина Е. Управление корпоративными коммуникациями. С.: СКФУ, 2022. 93 с.
2. Каким должен быть корпоративный контент, чтобы привлечь клиентов. URL: <https://probusiness.io/marketing/4694-vam-est-o-chem-rasskazat-kakim-dolzhen-byt-korporativnyy-kontent-chtoby-privlech-klientov.html> (дата обращения 25.04.2025)
3. Между креативом и рутиной: каким должен быть корпоративный контент. URL: <https://adindex.ru/publication/opinion/creative/2024/10/17/326549.phtml> (дата обращения 25.04.2025)
4. Google Workspace | Бизнес-приложения и инструменты для совместной работы/ URL: <https://workspace.google.com/intl/ru/> (дата обращения 25.04.2025)
5. Корпоративный журнал ПАО «Газпром». URL: <https://www.gazprom.ru/press/journal/journal-gazprom/?ysclid=m9y1ihvjb846430087> (дата обращения 25.04.2025)

*Статья представлена научным руководителем, деканом факультета СТЭД СПбГУТ, кандидатом политических наук, доцентом Шутманом Д. В.*

## УДК 338.1

**В. В. Макаров** (д.э.н., профессор, профессор кафедры ЭД СПбГУТ)

**А. А. Фокичев** (магистрант группы БИ-41м, СПбГУТ), [fokichev.aa@sut.ru](mailto:fokichev.aa@sut.ru)

## **ВЛИЯНИЕ ТЕХНОЛОГИИ 5G НА РАЗВИТИЕ УСЛУГ ДЛЯ БИЗНЕСА В ТЕЛЕКОММУНИКАЦИЯХ**

*В современных условиях цифровизации экономики и стремительного развития цифровых технологий особое значение приобретает внедрение новых поколений телекоммуникационных сетей. Технология 5G представляет собой революционный шаг в развитии мобильной связи, открывая принципиально новые возможности для бизнеса и корпоративных пользователей. Внедрение связи нового поколения способно затронуть бизнес-процессы в таких областях как промышленное производство, облачные сервисы, здравоохранение, финансовые услуги и транспорт, создавая ряд положительных эффектов и открывая новые инвестиционные перспективы.*

*телекоммуникации, технология 5G, экономика, бизнес-модели, услуги для бизнеса*

В современных условиях цифровизации экономики и стремительного развития цифровых технологий особое значение приобретает внедрение новых поколений телекоммуникационных сетей. Технология 5G представляет собой революционный шаг в развитии мобильной связи, открывая принципиально новые возможности для бизнеса и корпоративных пользователей.

Телекоммуникационные технологии являются одним из ключевых факторов развития современной экономики. Эволюция поколений мобильной связи от 1G до 4G демонстрирует постоянное увеличение скорости передачи данных, снижение задержки сигнала и расширение спектра предоставляемых услуг. Существующие сети LTE, хоть и остаются эффективными, не могут адекватно поддерживать экспоненциальный рост трафика данных и потребность в обработке данных в режиме реального времени. Технология 5G представляет собой инновационный уровень развития телекоммуникаций, отличающийся следующими ключевыми характеристиками [1]: высокая скорость передачи данных до 20 Гбит/с, минимальная задержка сигнала (менее 1 мс), увеличенная плотность подключения до 1 миллиона устройств на квадратный километр и повышенная энергоэффективность (в среднем на 90 % выше, чем у предыдущего поколения). Анализ текущего состояния 5G показывает, что эта технология ак-



тивно внедряется в крупнейших городах мира. Ведущие телекоммуникационные компании проводят пилотные проекты и создают коммерческие сети нового поколения.

Инфраструктура 5G состоит из базовых станций нового поколения, представляющих собой мощные и компактные устройства, способные обеспечивать стабильную связь в зонах с большой плотностью устройств, центров обработки данных, являющихся ключевым элементом инфраструктуры 5G, так как они обрабатывают информацию, передаваемую между устройствами в структуре сети, и оптических проводных (оптоволоконные линии) и беспроводных (лазерные системы связи) линий коммуникаций, используемых для передачи данных на большие расстояния между элементами инфраструктуры связи с минимальными потерями и задержкой. Оборудование абонентского доступа позволяет пользователям подключаться к сети 5G через различные устройства, такие как смартфоны, планшеты, ноутбуки и умные дома. Системы управления сетью обеспечивают автоматизацию процессов, мониторинг состояния сети и быстрое реагирование на возможные сбои.

Внедрение технологии 5G открывает новые возможности развития для следующих направлений бизнес-услуг [2]:

1. Новый стандарт беспроводной связи расширяет горизонты для развития IoT, позволяя создавать масштабные сети с поддержкой миллионов устройств в реальном времени. Это особенно важно для промышленного интернета вещей (IIoT), где требуется высокая надежность и минимальная задержка сигнала. В условиях производства преимуществом использования беспроводной сети является возможность мгновенного ввода в эксплуатацию оборудования без необходимости создания кабельной инфраструктуры, а также поддержка стабильной связи подвижных производственных объектов. На практике 5G может применяться в межмашинной коммуникации, создавая бесшовную интеграцию различных устройств и систем в производственной линии, а также в оперативных задачах, таких как система предиктивного обслуживания станков, отслеживая состояние оборудования в режиме реального времени, или система контроля, мгновенно передавая показатели датчиков и изображения камер.

2. Технология 5G создает новые возможности для развития облачных сервисов, таких как высокопроизводительные вычисления, распределенные системы хранения данных и виртуальные рабочие места, что позволяет ком-

паниям гибко масштабировать свои ресурсы и снижать затраты на инфраструктуру. В качестве примера можно привести облачные платформы для работы с большими данными. Пользователи этих платформ в рамках нового поколения связи смогут значительно быстрее загружать большие объемы данных через беспроводную сеть и получать результаты.

2. Внедрение технологии 5G создает новые условия для развития здравоохранения, включая телемедицину, дистанционный мониторинг пациентов в реальном времени, роботизированную хирургию, персонализированную медицину и медицинские носимые устройства. Благодаря минимальной задержке сигнала возможно появление мобильных диагностических комплексов, позволяющих проводить диагностику здоровья пациентов на дому или отдаленных районах и мгновенно получать информацию об изменении их состояния, а также проведение телехирургических операций с использованием роботов-хирургов, в процессе которых команды в режиме реального времени передаются по беспроводной связи в труднодоступные районы.

4. В сфере финансовых услуг пятое поколение связи позволит совершать быстрые транзакции, безопасные платежи и развивать блокчейн-технологий. Расширенные возможности подключения и высокая скорость сетей 5G способствуют эффективной высокочастотной торговле и обработке транзакций в реальном времени, что улучшает работу финансовых рынков. Кроме того, передовые технологии искусственного интеллекта и машинного обучения, поддерживаемые 5G, позволят точнее оценивать риски, выявлять мошенничество и обеспечивать кибербезопасность, защищая финансовые данные и транзакции.

5. Развитие технологии 5G даст скачок в развитии транспорта, в том числе внедрение беспилотных транспортных средств, умные логистические системы и автоматизацию складского хозяйства. Беспилотные автомобили и грузовики, подключенные к сети 5G, смогут перемещаться по дорогам, следуя заданным маршрутам и избегая препятствий, что позволит оптимизировать логистические процессы и снизить затраты на транспортировку, а автоматизированные грузовые терминалы в портах, подключенные к быстрой беспроводной сети, ускорят работу и снизят расходы, автоматизировав обработку грузов.

Распространение пятого поколения беспроводной связи окажет значительное влияние на экономику, создавая ряд положительных эффектов и открывая новые инвестиционные перспективы [3]. Рост капиталовложений в

инфраструктуру 5G простимулирует развитие телекоммуникационной отрасли и смежных секторов, таких как производство оборудования, строительство базовых станций и разработка программного обеспечения, а развертывание новой сети потребует привлечения специалистов в области строительства, инженерии, программирования и управления проектами, что поспособствует созданию более 100 тысяч новых рабочих мест в сфере телекоммуникаций. По различным оценкам экспертов, внедрение 5G может добавить до 1–2 % к ежегодному росту ВВП России, что подчеркивает его значимость для экономики страны [4].

В свою очередь, благодаря повышению эффективности сетей и снижению затрат на их обслуживание, операторы связи смогут сократить операционные расходы, что положительно скажется на их финансовых показателях. Новые технологии позволят автоматизировать процессы управления сетью, что снизит необходимость в ручном вмешательстве и, соответственно, затраты на обслуживание, а ускорение передачи данных и снижение задержки сигнала позволят компаниям быстрее обрабатывать информацию, принимать решения и выполнять операции, что повышает общую эффективность бизнес-процессов.

Несмотря на многочисленные преимущества, внедрение 5G сопряжено с рядом проблем и вызовов. Высокая стоимость оборудования, сложность создания новой инфраструктуры и проблемы выделения частотного диапазона в купе с необходимостью значительных инвестиций в строительство базовых станций и сложностью их размещения, обуславливают необходимость разработки эффективных стратегий развертывания сети. С другой стороны, вопросы распределения радиочастотного спектра, стандарты совместимости и лицензирование услуг требуют четкого регулирования со стороны государственных органов. Пути решения технологических проблем включают модульное построение сети, использование существующих инфраструктур, разработку защищенных протоколов передачи данных и создание резервных каналов связи [2].

Развертывание сетей нового поколения в России осложняется тем фактом, что используемый в Европейских странах для этой цели band 78 (диапазон частот 3,3–3,8 ГГц) оказался уже занят «Фиксированной спутниковой службой». Правительство приняло ряд мер для решения этой проблемы, включая установление срока освобождения этого частотного диапазона для мобильной связи. Кроме того, ГКРЧ предложила использовать свободные частоты в диапазоне 4,4–4,99 ГГц (band 79) для создания новых сетей [4].

В основе развития 5G для бизнеса лежит необходимость в разработке сервисов и решений, отвечающих специфическим потребностям различных отраслей, таких как промышленность, здравоохранение, транспорт. Внедрение 5G будет способствовать созданию гибких и масштабируемых решений, которые могут адаптироваться к растущему объему данных и возрастающему количеству устройств, обеспечивать совместимость новых сервисов с существующими системами и инфраструктурой для минимизации затрат на внедрение, способствовать разработке бизнес-моделей, обеспечивающих высокую рентабельность инвестиций и быструю окупаемость затрат на внедрение новой технологии.

Бизнес-модели могут включать событийные услуги, специализированные сети, виртуальные частные сети, управляемые сервисы и платформенные решения. Ожидается рост спроса на персонализированные решения, увеличение доли автоматизированных процессов, развитие гибридных облачных решений и расширение спектра IoT-приложений. Стратегические направления развития включают интеграцию с искусственным интеллектом, развитие квантовых коммуникаций и внедрение технологий машинного обучения для создания экосистем цифровых сервисов. Эти направления позволят бизнесу максимально использовать потенциал 5G и обеспечить устойчивое развитие в условиях цифровой трансформации экономики [5-9].

В заключение можно отметить, что технология 5G – это значительное изменение в телекоммуникациях, которое открывает новые перспективы для развития бизнеса. Успешное внедрение 5G требует комплексного подхода, учитывающего технические, экономические и регуляторные аспекты. Развитие 5G связано с углублением цифровизации экономики, появлением новых бизнес-моделей, формированием новых рынков, созданием экосистем цифровых сервисов и интеграцией с другими технологиями. Дальнейшее развитие сетей 5G будет зависеть от способности операторов связи и бизнеса эффективно использовать ее потенциал для создания инновационных решений и повышения конкурентоспособности.

#### **Список используемых источников**

1. Портал о современных технологиях мобильной и беспроводной связи. <https://1234g.ru/> (дата обращения 20.04.25).
2. Artikel «5G ist nicht nur einfach eine weitere Mobilfunktechnik, sondern wird die Wirtschaft radikal beeinflussen». <https://de.nttdata.com/insights/artikel/neue-business-chancen-durch-5g> (дата обращения 05.04.25).

3. Чачис Д. Ю. Как технология 5G повлияет на маркетинг и бизнес // Вестник науки. 2023. Т. 5. №7 (64) С. 51-54.
4. Отчет ассоциации GSMA «5G в России: Влияние спектра на перспективы развития» <https://d-russia.ru/wp-content/uploads/2020/11/5g-spectrum-in-russia.pdf> (дата обращения 05.04.25).
5. Макаров В. В., Слуцкий М. Г., Устриков Н. К. Проблемы и задачи цифровой трансформации экономики России // Международный журнал гуманитарных и естественных наук. 2020. № 4-1 (43). С. 174-177.
6. Слуцкий М. Г., Сеница С. А., Макаров В. В. Анализ состояния и тенденции развития рынка инфокоммуникаций // Международный журнал гуманитарных и естественных наук. 2022. № 1-3 (64). С.152-155.
7. Филиппов И. Ф., Нефедов А. С. Анализ бизнес-моделей и услуг в сетях мобильной связи пятого поколения // Современные проблемы радиоэлектроники и телекоммуникаций. 2021. №4. С.78.
8. Цифровая экономика: тренды и перспективы трансформации бизнеса // Материалы VIII Межфакультетской научно-практической конференции молодых ученых / Москва. 2024.
9. Shafi M., Molisch A.F., Smith P.J., Haustein T., Zhu P., De Silva P., Tufvesson F., Benjebbour A., Wunder G. 5G: A tutorial overview of standards, trials, challenges, deployment, and practice // IEEE journal on selected areas in communications. 2017. Vol. 35. № 6. P. 1201-1221.

УДК 339.138

**С. Б. Макарова** (студентка группы РСМ-31з, СПбГУТ),  
[makarova.sb@sut.ru](mailto:makarova.sb@sut.ru)

## ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ И РЕКОМЕНДАЦИИ ПО ПРОДВИЖЕНИЮ СОБЫТИЙНЫХ МЕРОПРИЯТИЙ

*В статье рассмотрены теоретико-методологические подходы к анализу событийных мероприятий как инструмента продвижения брендов и повышения их узнаваемости. Раскрываются ключевые принципы событийного маркетинга, его классификация и основные методологические направления исследования. Представлены успешные кейсы бренд-участия в массовых мероприятиях, таких как спортивные шоу, культурные фестивали и городские акции. Особое внимание уделено рекомендациям по разработке и реализации событий, включая медиапланирование, подбор каналов коммуникации и оценку эффективности. Статья адресована специалистам в области маркетинга, PR, event-менеджмента и брендинга.*

*событийный маркетинг, продвижение, бренд, мероприятие, аудитория, эффективность, медиаплан*

Событийный маркетинг в условиях глобальной медиатизации и информационной насыщенности приобретает особую значимость как инструмент формирования устойчивых связей между брендом и целевой аудиторией. Согласно наблюдениям А. А. Вершинкиной, развитие нишевых форм событийного туризма, таких как свадебный туризм, демонстрирует высокую эффективность с точки зрения привлечения платежеспособной аудитории и мультипликативного эффекта на смежные сектора экономики [1].

С. А. Гуров, исследуя географию рок-фестивалей, подчеркивает, что данные мероприятия выступают в роли катализаторов территориального брендинга, создавая устойчивую ассоциативную идентификацию местности в массовом сознании [2]. Т. А. Кравчук и Д. М. Асланова в своей работе предлагают структурно-функциональную модель организации событийных мероприятий, где продвижение рассматривается как последовательный процесс, включающий анализ целевых аудиторий, разработку сценарных решений, медиапланирование и постивент-оценку эффективности на основе показателей KPI [3].

Таким образом, на современном этапе событийный маркетинг выступает не только как механизм коммуникации, но и как важный элемент территориального и бренд-ориентированного развития [4].

События классифицируются по совокупности критериев, каждый из которых предопределяет целевое содержание, масштаб и формат интеграции заинтересованных сторон [5]. Научное изучение событийных мероприятий опирается на комплекс методологических подходов, каждый из которых акцентирует внимание на определенном аспекте феномена.

- инструментальный подход исходит из того, что событие является совокупностью функциональных механизмов воздействия на потребительское поведение и лояльность. Здесь акцент делается на эффективности, измеримости и управляемости коммуникационных практик;
- коммуникативный подход трактует событие как особую форму социального взаимодействия, сосредоточенную на создании публичного смысла, формировании символических структур и расширении медиаприсутствия;
- креативный подход выстраивает анализ вокруг концептуальной оригинальности, образной насыщенности и эмоционального резонанса, возникающего в процессе контакта между брендом и участником события;
- проектный подход предлагает рассматривать мероприятие как управляемую совокупность этапов (инициация, планирование, реализация, постанализ), каждый из которых подлежит количественной и качественной оценке на основе четко установленных целевых индикаторов [3].

Далее отметим, что встраивание бренда в структуру события может осуществляться посредством следующих механизмов:

- сценарное включение, при котором бренд становится частью основного содержания (например, тематическая зона или авторская мастерская);
- продуктивное внедрение, когда в рамках мероприятия осуществляется демонстрация, пробное использование или эксклюзивное распространение товаров или услуг;
- партнерские взаимодействия, предполагающие совместную организацию события несколькими субъектами с общими целевыми интересами;
- пространственная экспансия, выражающаяся в брендировании пространства, архитектурных объектах, выставочных форматах;
- технологическое вовлечение, связанное с применением интерактивных и цифровых решений, способствующих углублению опыта взаимодействия с брендом.

Построение эффективной системы взаимодействия с основными заинтересованными сторонами требует детальной предварительной проработки.

В работе с аудиторией важнейшим этапом является построение поведенческих моделей на основе мотивационно-психологических установок, что позволяет формировать адекватные формы вовлечения и сценарии реакций. С партнерскими структурами взаимодействие должно строиться на принципах

ценностной комплементарности и взаимной репутационной выгоды, а также предусматривать совместное производство контента и координацию медийных активностей. Со средствами массовой информации следует выстраивать стабильные рабочие отношения, предполагающие наличие цифрового пресс-центра, подготовку аналитических и визуальных информационных материалов и проведение предварительных пресс-показов.

Одним из наиболее устойчивых примеров стратегического продвижения посредством событийной активности выступает маркетинговая модель компании Red Bull, базирующаяся на создании и организации собственных экстремальных соревнований. В данном случае бренд не только выступает инициатором мероприятий, но и формирует вокруг них полноценное информационное пространство. Наиболее яркими примерами являются соревнования Red Bull Air Race в Будапеште, которые привлекли около 650 тысяч зрителей, а также проект Red Bull Stratos, получивший всемирную известность благодаря трансляции космического прыжка, которую одновременно наблюдали более 9,5 миллиона пользователей. Videоконтент, созданный в рамках данных мероприятий, в дальнейшем активно тиражировался в цифровой среде, усиливая узнаваемость бренда. По итогам года реализации проекта продажи продукции Red Bull увеличились на 11 %, что позволяет говорить о высокой эффективности данного формата [6].

Примером успешной коллаборации культурных инициатив и коммерческих структур является акция «Ночь музеев», ежегодно проводимая в большинстве субъектов Российской Федерации. Только в 2023 году общее число участников мероприятия составило более 2,1 миллиона человек, из которых около 550 тысяч посетили музеи в Москве. По данным организаторов, партнерское участие таких компаний, как «Сбер», МТС и «Яндекс Афиша», обеспечило технологическую поддержку мероприятия, улучшило навигационные возможности и предоставило дополнительные сервисы. В результате общее среднее время пребывания гостей на площадках возросло до 3,4 часов, что существенно превышает показатели стандартного режима работы учреждений. Также было зафиксировано увеличение выручки от реализации сопутствующих товаров на 18 %, что подтверждает взаимовыгодный характер партнерства [7].

На региональном уровне событийные мероприятия становятся действенным инструментом формирования локальной идентичности и стимулирования социально-экономической активности. Так, ежегодная Сырная ярмарка в Костроме в 2024 году привлекла свыше 60 тысяч участников и более 80 производителей. Общий объем реализованной продукции составил



порядка семи тонн. Проведение мероприятия стало важным фактором в развитии туристического потенциала региона, где наблюдался прирост турпотока до 1,8 миллиона посещений. Аналогичную функцию выполняет музыкальный фестиваль «Дикая мята» в Тульской области, посещаемость которого составила около 20 тысяч человек, из которых более 30 % прибыли из других регионов, что, в конечном итоге, обеспечило загрузку гостиничного фонда на уровне 92 процентов. Бренды-партнеры, в числе которых были «Тинькофф» и «Азбука вкуса», активно использовали фестиваль как площадку для представления продукции и сбора обратной связи от аудитории [8].

Практическая реализация подобных мероприятий требует четко выстроенной организационной структуры и соблюдения логической последовательности действий. Процесс подготовки событийного проекта включает ряд этапов, обеспечивающих его согласованность и эффективность. В первую очередь осуществляется постановка целей, а также определяются параметры целевой аудитории и ее поведенческие особенности. Далее проводится комплексный анализ внешних условий, включая сезонные факторы, инфраструктурные ограничения и правовую регламентацию. На следующем этапе разрабатываются сценарный план, партнерская модель и визуальная концепция мероприятия.

После утверждения содержания проекта осуществляется ресурсное и финансовое планирование: формируется бюджет, определяются источники финансирования, устанавливаются приоритеты по расходам. Этап непосредственной организации включает в себя формирование команды, заключение договоров с подрядчиками, распределение ролей и выстраивание логистических решений. Реализация проекта сопровождается техническим обеспечением, координацией исполнителей и контролем за соблюдением временных и содержательных рамок. Завершающая стадия включает анализ достигнутых результатов, сбор обратной связи от участников и расчет ключевых показателей эффективности, на основании которых формируется итоговый отчет и разрабатываются рекомендации для последующих мероприятий.

Медиаплан структурирует каналы, сроки и объемы информационных сообщений. К ключевым показателям эффективности относятся охват, посещаемость, доля новой аудитории и товарооборот. Рассчитывается коэффициент возврата инвестиций как отношение прибыли к затратам. Полученные данные позволяют оптимизировать последующие мероприятия и обосновывать инвестиционную привлекательность проекта для партнеров.

Оценка результативности строится на анализе как внутренних данных (опросы, трафик, продажи), так и внешнего резонанса (медиапубликации,

обсуждение в сети). Косвенные индикаторы включают рост туристического потока и повторные визиты. Комплексная диагностика позволяет объективно оценить влияние события и его коммуникативную ценность.

Подводя итоги исследования, стоит сказать, что событийный маркетинг на современном этапе приобретает статус одного из ключевых инструментов построения устойчивых и эмоционально насыщенных коммуникаций между брендом и целевой аудиторией. Проведенный анализ показал, что грамотно организованное мероприятие позволяет не только транслировать ценности и смыслы, заложенные в бренд, но и формировать долговременную привязанность потребителя, способствуя усилению его лояльности. В условиях информационного перенасыщения и снижения доверия к традиционным рекламным форматам события становятся средой, в которой происходит подлинное вовлечение, а бренд выходит за рамки товарного знака и превращается в элемент личного опыта участника.

#### Список используемых источников

1. Вершинкина А. А. Свадебный туризм // Туристско-рекреационный потенциал и особенности развития туризма и сервиса. 2021. С. 59–62.
2. Гуров С. А., Евдокимов В. В. Событийный туризм: бизнес-модель фестиваля // Бизнес и дизайн ревю. 2017. Т. 1. № 4 (8). С. 2.
3. Асланова Д. М., Кравчук М. А. Развитие событийного туризма на российском туристическом рынке // Актуальные проблемы современного образования. 2019. № 1 (26). С. 256–260.
4. Киреева Ю. А., Охотников И. В., Сибирко И. В. Событийный туризм как драйвер развития туристского рынка в регионах России // Московский экономический журнал. 2020. № 9. С. 61.
5. Власова Т. И., Алейников А. В. Событийный туризм – эффективный антикризисный инструмент привлечения туристских потоков в регион // Вестник НАТ. 2015. № 1. С. 38–40.
6. Red Bull Air Race – Hungary // Red Bull. URL: <https://www.redbull.com/us-en/events/red-bull-air-race-hungary> (дата обращения 02.06.2025).
7. «Ночь музеев» 2023: более 2 млн участников по всей России // ТАСС. URL: <https://tass.ru/kultura/17830483> (дата обращения 26.05.2025).
8. Сырная ярмарка стала крупнейшим событийным мероприятием Костромской области // БезФормата. URL: <https://vohma.bezformata.com/listnews/sobitiynim-meropriyatiem-kostromskoy/133578556/> (дата обращения 12.05.2025).

*Статья представлена научным руководителем, кандидатом политических наук, доцентом Кульназаровой А. В.*

УДК 39

В. С. Михайлюк (студент группы ЗР-21, СПбГУТ), [mikhailuk.vs@sut.ru](mailto:mikhailuk.vs@sut.ru)

## ПОЗИЦИЯ ГОСУДАРСТВА ПО ОТНОШЕНИЮ К ЦЕРКВИ В СОВРЕМЕННОЙ ФИНЛЯНДИИ

*В статье анализируются религиозные процессы в современной Финляндии, особенности взаимоотношений государства и церкви, рассматриваются особенности религиозной жизни Финляндии, ее позиция в государстве, причины потери прихожан у церкви Финляндии, и почему, несмотря на это, церкви все еще крепко держатся в обществе. Особое внимание уделяется структуре церковных организаций и роли религии в жизни финского населения и тому, как религию влияет на жизнь финнов и какое культурное значение имеет церковь.*

*Финляндия, религия, церковь, вера, финны, мировоззрение*

Как известно, большинство финнов придерживаются лютеранства. Лютеранская церковь возникла вследствие реформационного движения протестантов под руководством Лютера в 1517 г. Финляндия приняла лютеранство в 1526 г., когда в Швеции, в состав которой она входила, была проведена официальная реформация в масштабе страны. Реформация дала финскому народу собственную письменность и содействовала развитию его национальной культуры. В XVI веке был переведен на финский язык Новый Завет, ставший для финнов одновременно и первым букварем. Его перевел Микаэль Агрикола – финский гуманист и деятель Реформации. Он был первым лютеранским епископом Финляндии, просветителем и первым переводчиком Библии на финский язык. Лютеранская церковь сыграла важную роль в распространении грамотности среди финнов [1].

Финляндия в настоящее время является преимущественно христианской страной: 63,6 % финского населения являются членами Евангелическо-лютеранской церкви Финляндии (протестанты), 33,6 % не принадлежат ни к какой церкви, 1,0 % – православные христиане, 0,9 % – другие христиане и 0,9 % исповедуют другие религии [2]. Эта информация находится в открытом доступе на официальном веб-сайте статистики Финляндии («StatFin»), предоставляемый *Statistikeskus* («Statistics Finland»), центральным статистическим бюро страны.

Евангелическо-лютеранской церкви Финляндии является самой многочисленной: она насчитывает около 3,6 миллиона прихожан [3] из общей численности населения в 5,6 миллиона человек, Евангелическо-лютеранская

церковь Финляндии остается одной из крупнейших лютеранских церквей в мире, хотя ее число сокращается.

На начало 2025 года к Евангелическо-лютеранской церкви принадлежало 62,2 % финнов [4-7], однако согласно последнему четырехлетнему докладу Церкви (2016-2019), вера финнов в Бога за 20 лет почти вдвое сократилась. В 1999 году почти половина (47 %) финнов верила в Бога, но в 2019 году только каждый четвертый верил в Бога.

В частности, в 2023 году веб-сайт «*Eroakirkosta.fi*», предлагающий электронную услугу по выходу из национальных церквей Финляндии, сообщил, что более 850 000 человек отказались от членства в церквях с момента открытия веб-сайта в 2003 году.

Религиозность финской молодежи в настоящее время падает, что объясняется атеистическими и прагматичными взглядами на мир [8]. Другие причины отказа от веры, включают, в первую очередь, дебаты об однополых браках и то, как они повлияют на лютеранскую церковь. Законопроект, легализующий однополые браки, был одобрен в 2014 году, и, следовательно, лютеранская церковь должна была прояснить свою позицию по этому вопросу: если она не распространит браки на однополые пары, ей будет труднее оправдать свою роль «народной церкви», имеющей тесные связи с государством, и если она это сделает, ей придется изменить свои учения и практику. Хотя и некоторые епископы открыто поддерживали законопроект, общий консервативный имидж лютеранской церкви также привел к отставкам. За последние пять лет этот вопрос стал одной из самых популярных причин отказа от членства в лютеранской церкви.

Несмотря на явное снижение веры в Бога среди людей, это не означает снижения значимости Лютеранской церкви. Ее статус по-прежнему гарантирован законом, и она может рассчитывать на относительно сильную общественную поддержку [9].

Православная церковь Финляндии разделена на три епархии («*hiippakunta*»), каждая из которых состоит из приходов («*seurakunta*»). Приход в Финляндии – это сообщество православных верующих, собирающихся для совместной молитвы и участия в таинствах в особый храм с причтом. Всего насчитывается 21 приход, 140 священников и 57 613 прихожан, из которых 54 895 проживают в Финляндии [5]. Центральным законодательным органом церкви является центральный синод, в состав которого входят:

- епископы и епископы-коадьюторы;
- одиннадцать священников;

- три кантора;
- восемнадцать мирян и мирянок.

Приходами управляют настоятель и приходской совет, который избирается тайным голосованием.

В Финляндии регистрация прихожан обязательна. Связано это с тем, что в Финляндии за Православной церковью законодательно закреплён особый статус, выражающийся в т.ч. в праве сбора налогов с целью финансирования своей деятельности, но и предполагающий некоторую ответственность церкви перед обществом, например, в ведении учета актов гражданского состояния прихожан. В соответствии с законодательством, только постоянно проживающие в стране лица могут регистрировать свою вероисповедную принадлежность. Вне зависимости от своего места проживания и приходской принадлежности все прихожане заносятся в особый государственный регистр. Такая традиционная, фиксированная форма членства в приходе имела место и в дореволюционной России [10].

Прихожанин ежемесячно отчисляет 1-2 % от своего дохода в форме т.н. церковного налога («kirkollisvero»). Из собранных именно таким образом налоговых средств осуществляется финансирование приходской деятельности на местах. Так, каждый прихожанин оказывает посильную материальную помощь своему приходу и всей Православной Церкви в Финляндии [10].

Также и деятельность Евангелическо-лютеранской церкви Финляндии финансируется государством за счет специального церковного налога, взимаемого как с физических, так и юридических лиц.

Вместе с таким сильным влиянием религии – Финляндия имеет большой опыт преподавания религии в общеобразовательных школах в качестве обязательного предмета. Этот опыт постоянно развивается, поскольку современность ставит новые вопросы в духовном воспитании детей.

С 2003 года преподается предмет «Обучение своему вероисповеданию» (или «Свое вероисповедание»). В школах изучают не только лютеранское и православное вероисповедание, но и католицизм, ислам, буддизм и кришнаизм.

Также для детей из семей, исповедующих нерелигиозное мировоззрение и официально не принадлежащих ни к какой религиозной конфессии или религиозному объединению, в школьную программу введен предмет «Мировоззрение».

Занятия по этим предметам проводят с 1-го по 9-й класс основной школы, а также в гимназиях, в среднем по 1 часу в неделю в течение каждого года обучения.

В системе высшего образования Финляндии существуют теологические факультеты. Они являются частью университетов и предлагают обучение по различным направлениям теологии.

Основные университеты с теологическими факультетами:

- Хельсинкский университет («University of Helsinki»): Факультет теологии («Teologinen tiedekunta») является одним из ведущих в стране. Здесь изучают различные направления теологии, включая систематическую теологию, библейские науки, церковную историю, практическую теологию и религиоведение;

- Университет Або Академи («Åbo Akademi University»): Этот университет является шведскоязычным университетом в Турку. Здесь также есть факультет теологии, предлагающий обучение на шведском языке.

За последние годы, влияние веры и церкви отходит на второй план для финнов. С каждым годом, количество неверующих становится все больше. Но несмотря на это, финнов интересует церковь, религия и духовность, и они все также присоединяются к церкви, хоть и менее активно.

Вера и церковь для финнов играют важную роль в их жизни – даже если они не являются прихожанами, то крещения, венчания и похороны по-прежнему зачастую проводятся в церквях. Это связано с традициями и культурным значением этих обрядов.

Особенности церковного кода Финляндии тесно связаны с финским менталитетом. Здесь традиционно большое внимание уделяется частной жизни, тут главное – человек, а не государство. Свою миссию Евангелическо-лютеранская церковь видит в духовном пробуждении паствы. Кроме того: Евангелическо-лютеранская церковь ведет обширную волонтерскую работу с детьми, одинокими стариками, с семьями, попавшими в кризисную ситуацию [11]. Именно поэтому государство поддерживает Церковь: она стала слишком важным культурным фактором в жизни финнов.

#### Список используемых источников

1. Религиозные традиции в жизни финских переселенцев // Cyberleninka. URL: <https://cyberleninka.ru/article/n/religioznyie-traditsii-v-zhizni-finskih-pereselentsev-75> (дата обращения 16.04.2025).

2. StatFin / Statistics Finland. URL: [https://pxdata.stat.fi/PxWeb/pxweb/en/StatFin/StatFin\\_\\_vaerak/](https://pxdata.stat.fi/PxWeb/pxweb/en/StatFin/StatFin__vaerak/) (дата обращения 16.04.2025).

3. SUOMEN EVANKELIS-LUTERILAINEN KIRKKO // evl.fi. URL: <https://evl.fi/> (дата обращения 16.04.2025).
4. Kirkontilastot.fi. URL: <https://www.kirkontilastot.fi/> (дата обращения 16.04.2025).
5. Ort.fi. URL: <https://ort.fi/> (дата обращения 16.04.2025).
6. Практические аспекты организации преподавания религии в светских школах Финляндии // Cyberleninka. URL: <https://cyberleninka.ru/article/n/prakticheskie-aspekty-organizatsii-prepodavaniya-religii-v-svetskih-shkolah-finlyandii> (дата обращения 16.04.2025).
7. Teologinen tiedekunta // helsinki.fi. URL: <https://www.helsinki.fi/fi/teologinen-tiedekunta> (дата обращения 16.04.2025).
8. From Finland: Are we witnessing a historic change in religiosity // cne.news. URL: <https://cne.news/article/4033-column-from-finland-are-we-witnessing-a-historic-change-in-religiosity> (дата обращения 18.04.2025).
9. Finland: recent trends and patterns in religion, secularism and atheism // o-re-la.ulb.be. URL: <https://o-re-la.ulb.be/analyses/item/1424-finland-recent-trends-and-patterns-in-religion-secularism-and-atheism.html> (дата обращения 18.04.2025).
10. Быть прихожанином // ort.fi. URL: <https://www.ort.fi/ru/%D0%B1%D1%8B%D1%82%D1%8C-%D0%BF%D1%80%D0%B8%D1%85%D0%BE%D0%B6%D0%B0%D0%BD%D0%B8%D0%BD%D0%BE%D0%BC/> (дата обращения 18.04.2025).
11. Финское общество и церковь – пять веков // finland.fi. URL: <https://finland.fi/ru/zhizn-i-obshhestvo/finskoe-obshhestvo-i-tserkov-pyat-vekov/> (дата обращения 18.04.2025).

*Статья представлена научным руководителем, доцентом кафедры ИиРВ СПбГУТ, кандидатом исторических наук Молчановой Т. В.*

УДК 328

Д. Н. Постникова (студент группы ЗР-22, СПбГУТ), [postnikova.dn@sut.ru](mailto:postnikova.dn@sut.ru)

## ОСОБЕННОСТИ ОРГАНИЗАЦИИ МЕСТНОЙ ВЛАСТИ В КИТАЕ НА ПРИМЕРЕ СУАР

*В статье рассматриваются особенности реализации модели местного самоуправления в Китайской Народной Республике на примере Синьцзян-Уйгурского автономного района. Особое внимание уделено взаимодействию формальной автономии и централизованного управления, роли Конституции КНР и особенностям административной практики в СУАР. Отмечается противоречие между провозглашенными в законодательстве правами автономии и реальным функционированием регионального управления.*

*Китай, СУАР, местное управление, автономия, этнополитика.*

Вопрос организации местной власти в Китайской Народной Республике (КНР) представляет собой не только управленческую, но и этнополитическую проблему, особенно в многонациональных регионах. Одним из наиболее показательных примеров взаимодействия центра и периферии выступает Синьцзян-Уйгурский автономный район (СУАР) – крупнейшая автономная единица в составе КНР, обладающая формально широкими полномочиями, но находящаяся под жестким контролем центральной власти. Анализ структуры местного управления в Китае через призму СУАР позволяет понять, как в условиях унитарного государства реализуется модель автономии, ориентированная на управление этнически неоднородными территориями.

Исторически формирование системы автономий в КНР связано с идеологической эволюцией взглядов Коммунистической партии Китая на вопрос самоопределения. В первые десятилетия XX века, под влиянием марксистской теории и советского опыта, партия декларировала право народов на отделение. Однако уже в процессе создания КНР в 1949 году было принято решение отказаться от федерализма в пользу унитарной модели с элементами автономии. Как подчеркивают исследователи, автономия рассматривалась не как уступка, а как инструмент управляемой интеграции нацменьшинств в единую государственную систему. Так, в 1952 году была принята «Программа осуществления национального территориального самоуправления», а в 1984 году – специальный Закон КНР об автономиях, подтвержденный поправками 2001 года. Именно на этих правовых основаниях строится статус СУАР и других автономных образований [3].

Вопрос о предоставлении автономий национальным меньшинствам в первые годы существования КНР был предметом внутреннего компромисса



и идеологической переоценки. В теории, Коммунистическая партия Китая, особенно в период 1930-х годов, следовала советской модели, признавая право народов на самоопределение, включая отделение. Однако уже к моменту провозглашения КНР в 1949 году стало ясно, что руководство страны не готово к федерализму или подлинной децентрализации. Унитарное государство с четко централизованной партийной вертикалью стало основной моделью государственного строительства.

В то время, несмотря на декларативную поддержку права национальных меньшинств на развитие собственной культуры и языка, в партийных кругах преобладала убежденность в необходимости жесткой интеграции всех этносов в единую китайскую нацию. Идея автономий была скорее инструментом политической стабилизации и контроля над окраинами, чем выражением реальной готовности к этнокультурному многообразию [3]. Именно в этом контексте Синьцзян, как потенциально нестабильный и геополитически чувствительный регион, был включен в административную схему КНР под видом автономии, но с фактическим доминированием центра.

Уже в 1952 году в КНР была разработана «Программа осуществления национального территориального самоуправления», в которой были зафиксированы три уровня автономных единиц: район, округ и уезд. Однако в ней подчеркивалось, что автономия возможна только в рамках единства государства, при безусловном подчинении центра. Даже при создании СУАР в 1955 году модель была сконструирована таким образом, чтобы избежать возникновения реальной политической самостоятельности: высшие должности распределялись в соответствии с партийной иерархией, а любые формы этнической мобилизации подавлялись как угроза национальному единству. Таким образом, уже на этапе становления республики идея автономии рассматривалась как политическая форма лояльности, а не как инструмент этнического самоуправления.

Современная система местного управления в КНР во многом опирается на положения Конституции 1982 года, особенно ее шестого раздела, посвященного организации местных органов власти. Согласно основному закону страны, Китай делится на административно-территориальные единицы различного уровня: провинции, автономные районы, города центрального подчинения, а также уезды и поселковые образования. На каждом уровне создаются народные собрания и исполнительные органы, формируемые и подотчетные этим представительным структурам. В автономных образованиях, таких как СУАР, предусматривается особый режим: местные органы власти формируются преимущественно из представителей титульных

нацменьшинств, допускается использование национальных языков в делопроизводстве, а также право принимать собственные нормативные акты, адаптированные к культурным и религиозным особенностям населения [2].

Важно отметить, что такие акты касаются, как правило, вопросов культурной политики, образования, языковой практики, традиционной медицины, регулирования религиозной деятельности и сохранения самобытности. Например, в СУАР разрабатываются меры по использованию уйгурского языка в образовательных учреждениях, а также документы, регулирующие работу исламских организаций и мечетей. Однако реализация таких актов часто зависит от политической обстановки, и при усилении контроля со стороны центра автономные нормы могут быть приостановлены или ограничены [3].

Однако, несмотря на провозглашенные механизмы самоуправления, автономия в китайском контексте не эквивалентна федерализму. Районная национальная автономия в КНР – это не форма самоопределения, а способ интеграции этнических меньшинств в централизованную систему управления. Законодательные акты КНР в сфере этнополитики сконструированы таким образом, чтобы формально предоставить автономным районам широкие права, но фактически сохранить контроль за ними в руках центральных властей [3]. Например, акты, принимаемые на уровне автономного района, требуют одобрения вышестоящих инстанций, а все ключевые кадровые назначения происходят под контролем Коммунистической партии Китая. Таким образом, речь идет скорее о культурно-административной автономии, чем о полноценной политической самостоятельности.

СУАР в этом контексте представляет особый интерес как регион, где сочетаются геополитическая значимость, экономическая стратегия и этническая напряженность. Будучи крупнейшим по площади регионом Китая, СУАР граничит с восемью государствами и служит важным звеном в инициативе «Один пояс – один путь». При этом население района неоднородно: помимо ханьцев здесь проживает значительное число уйгуров, казахов, киргизов и других народов, традиционно исповедующих ислам. Официально регион наделен правом развивать национальные школы, религиозные учреждения и культурные организации. Однако, как показывают исследования, реальная практика отличается от декларируемых норм: с начала XXI века усиливаются меры по контролю за религиозной и этнической сферой, ограничивается преподавание на уйгурском языке, а участие представителей нацменьшинств в управлении все чаще носит формальный характер [1].

Особым инструментом управления в СУАР выступает Синьцзянский производственно-строительный корпус – уникальная административно-хозяйственная структура, сочетающая функции сельскохозяйственного освоения, охраны общественного порядка и идеологического воздействия. Корпус обладает автономной системой управления, включающей собственные суды, школы и органы безопасности, и подчиняется непосредственно центральному правительству. Такая модель позволяет Пекину укреплять присутствие ханьского населения и контролировать стратегически важные районы, минуя формальные автономные институты [1].

В конечном счете, организация местной власти в КНР, особенно на примере СУАР, демонстрирует двойственность китайского подхода к управлению этническими регионами. С одной стороны, конституционные и законодательные нормы декларируют уважение к культурной самобытности и автономии национальных меньшинств, с другой – централизованная партийно-государственная вертикаль фактически нейтрализует потенциал этих институтов. Местная власть в Китае, таким образом, оказывается инструментом не только администрирования, но и обеспечения политической лояльности, где этнокультурное разнообразие подчинено задаче внутренней стабильности и территориальной целостности государства [3].

#### Список используемых источников

1. Капицын В. М., Ван Яо. Синьцзян-Уйгурский автономный район Китая: территориальное самоуправление и национальная политика. *Ars Administrandi* (Искусство управления). 2013. №1. С. 78–83. URL: [https://elibrary.ru/download/elibrary\\_20363312\\_86029183.pdf](https://elibrary.ru/download/elibrary_20363312_86029183.pdf) (дата обращения 27.03. 2025).
2. Конституция Китайской Народной Республики: офиц. текст. Принята Всекитайским собранием народных представителей 4 декабря 1982 г. (в ред. от 2018 г.). URL: <https://legalns.com/download/books/cons/china.pdf> (дата обращения 25.03.2025).
3. Ставров И. В. Законодательная реализация этнополитики и районной национальной автономии в КНР // *Актуальные проблемы права: теория и практика*. 2023. № 2. С. 131–135.

*Статья представлена научным руководителем, доцентом кафедры ИиРВ СПбГУТ, кандидатом исторических наук Молчановой Т. В.*

УДК 659.442

**К. А. Скрынченко** (студент группы РСО-11 СПбГУТ),  
[skrynchenko.ka@sut.ru](mailto:skrynchenko.ka@sut.ru)

## **СВЯЗИ С ОБЩЕСТВЕННОСТЬЮ В ТЕАТРАЛЬНОЙ СФЕРЕ: УСПЕШНЫЕ ПРАКТИКИ РАБОТЫ С МОЛОДЕЖНОЙ АУДИТОРИЕЙ**

*Статья посвящена рассмотрению методов привлечения молодежной аудитории к театру в современной России. Рассматриваются эффективные практики: образовательные проекты, цифровые коммуникации, молодежные инициативы. Подчеркивается роль репертуарной политики и адаптации форматов и важность комплексного подхода для привлечения молодежи.*

*театр, коммуникации в театральной сфере, молодежная аудитория, связи с общественностью в театре*

Согласно наблюдениям, театральный ландшафт современной России отличается высокой степенью разнородности, что связано как с разнообразием площадок и форматов, так и с неоднородностью культурного запроса самих зрителей. Это порождает двойственное отношение публики к театру как к виду досуга. Для части аудитории театр остается значимым, эмоционально насыщенным культурным опытом, обладающим почти сакральным значением. Однако для других – для молодых людей – он воспринимается как неактуальное, скучное искусство, не отвечающее современным ожиданиям.

Особенно остро эта проблема проявляется в регионах, где молодежь редко находит театральный формат, способный ее увлечь. Зрители ждут от театра яркого и запоминающегося события, но сталкиваются с репертуаром, в котором доминируют школьная классика и традиционные формы постановки. В результате возникает барьер восприятия театра как «неподходящего» для молодого зрителя.

В качестве одного из решений исследователи предлагают обновление репертуарной политики, акцент на современную проблематику, новые интерпретации классики, а также активную работу театров с образом собственной аудитории. Демонстрация живой, разнообразной публики, создание информационных и навигационных материалов для «новичков» может способствовать разрушению стереотипов и расширению зрительской базы. Особенно важную роль в этом могут сыграть молодежные театры, способные обращаться к актуальным форматам и языку, близкому их целевой аудитории [1].

С учетом этих данных становится очевидной необходимость целенаправленной работы с молодежной аудиторией и создания привлекательных форм театральной коммуникации. Далее рассмотрим наиболее успешные практики взаимодействия театров с молодежью.

Среди наиболее значимых федеральных программ стоит выделить инициативу «Пушкинская карта», реализуемую в соответствии с постановлением Правительства Российской Федерации от 08.09.2021 № 1521 [2]. Программа направлена на расширение культурной доступности для молодежи в возрасте от 14 до 22 лет, предоставляя им возможность ежегодно использовать специальную банковскую карту с лимитом в 5 000 рублей для посещения учреждений культуры.

Наряду с государственными мерами значительную роль играют и собственные инициативы театров. Многие театральные учреждения осознают необходимость активной коммуникации с молодой аудиторией и стремятся к тому, чтобы не только сохранять традиции, но и переосмысливать формы взаимодействия, адаптируясь к интересам и привычкам нового поколения.

В России стали появляются независимые проекты, ориентированные исключительно на молодежную аудиторию. Яркий пример – «Театральный проект 27» из Санкт-Петербурга, полностью сосредоточенный на создании спектаклей, отражающих проблемы, чувства и внутренний мир молодых людей. Проект появился в 2019 году и за шесть лет команда молодых режиссеров, актеров и художников создала 20 спектаклей, которые затрагивают важные для молодежи темы и говорят с ними на понятном языке. Проект собрал 55 тысяч зрителей офлайн, полмиллиона в онлайн-просмотрах, и выступил в 30 городах России [3]. Этот опыт показывает, что театр, ориентированный на молодежь, может быть глубоким, актуальным и востребованным.

Крупные театры по всей стране внедряют специальные молодежные предложения. Это долгосрочные программы, которые позволяют молодежи и студентам регулярно посещать спектакли по доступным ценам, участвовать в образовательных мероприятиях и быть ближе к театральному процессу. Почти все театры России уделяют внимание молодежной аудитории и студентам, предоставляя значительные скидки и специальные условия, поэтому важно регулярно просматривать официальные сайты театров и узнавать актуальную информацию о действующих программах и возможностях приобретения билетов на льготных условиях.

Последние десятилетия театры все активнее развивают образовательные инициативы: лекции, мастер-классы, открытые репетиции и творческие встречи становятся важными элементами работы с молодежной аудиторией.

Так, в театре «Сатирикон» имени Аркадия Райкина студенты принимают участие в мастер-классах, организуемых в рамках программы Высшей школы сценических искусств. Эти занятия дают возможность лично поработать с педагогами, артистами и режиссерами, осваивая азы актерского мастерства, сценической речи и пластики. Молодежь вовлечена в процесс не как пассивные слушатели, а как активные участники. Одним из таких мастер-классов стал урок Ирины Турсуновой, посвященный развитию речи и ораторского мастерства. В рамках занятия «Я могу говорить!» участники улучшали дикцию и уверенность при публичных выступлениях, что особенно важно для будущих профессионалов театра [4].

В рамках образовательных инициатив театр имени Ленсовета проводит лекции и дискуссии по актуальным темам театрального искусства, истории и современной драматургии, адаптированные для молодой аудитории. Так недавно прошел лекционный блок проекта «Опыт русской духовности. Естественный рубеж», реализуемого Фондом поддержки Театра имени Ленсовета. Лекции были направлены на изучение и популяризацию вопросов русской духовности, культуры и философии через призму искусства и истории. В рамках блока прошли встречи с экспертами, которые раскрыли темы, связанные с развитием духовных и культурных традиций России [5].

Театральные лаборатории являются еще одним из форматов взаимодействия с молодыми людьми в театральной среде. Эти площадки становятся мостом между театром и новым поколением, предоставляя возможность для непосредственного участия в творческом процессе. Особое внимание стоит уделить опыту Большого драматического театра имени Г. А. Товстоногова (БДТ), их лаборатории предоставляют молодым режиссерам возможность разрабатывать эскизы спектаклей в сотрудничестве с профессиональными актерами труппы, что позволяет участникам получить ценный практический опыт. В рамках проекта «To stage» осуществлялось формирование и тестирование нового языка современного театра, который объединял такие направления, как литература и паблик-арт, хореография и архитектура, поэзия и саунд-арт, уличное искусство и кино. В БДТ существует множество лабораторий: «Педагогическая лаборатория БДТ», инклюзивная лаборатория «Не зря», посвященная взаимодействию людей с инвалидностью по зрению и слуху и молодых профессионалов в области искусства и многие другие.

Несомненно, сегодня театры осознают необходимость активного присутствия в цифровом пространстве и уделяют особое внимание ведению официальных страниц в социальных сетях. Яркий пример этого: театр «Мастерская» под руководством Григория Козлова, который активно реализует «Театр вне театра», направленный на расширение форм взаимодействия с

аудиторией за пределами традиционной сцены. В рамках проекта театр ведет рубрику «Театральный альбом», публикуя интервью с актерами, режиссерами и участниками творческого процесса, тем самым раскрывая внутреннюю жизнь театра для широкой публики. Использование визуальных и мультимедийных средств позволяет сделать театральный процесс более открытым и привлекательным для молодого поколения, социальные сети становятся не только инструментом продвижения, но и самостоятельной площадкой для формирования новой культурной среды вокруг театра.

Ведущие театры страны реализуют разнообразные технологии по связям с общественностью для привлечения молодежи: через образовательные инициативы, мастер-классы, театральные лаборатории, лекции и открытые репетиции, широко практикуются льготные программы. Особое внимание уделяется цифровому взаимодействию – театры развивают активное присутствие в социальных сетях, создавая разнообразный контент, способный расширить аудиторию и сформировать новое поколение зрителей. Все это способствует формированию устойчивого интереса к театру, развитию зрительской культуры и культурной самореализации молодого поколения.

#### Список используемых источников

1. Коллектив авторов Театральный зритель и продвижение спектаклей. Результаты качественного исследования. М: Российский институт театрального искусства-ГИТИС, 2021. С.13-17.
2. Постановление Правительства Российской Федерации от 08.09.2021 г. № 1521 // Правительство России URL: <http://government.ru/docs/all/136439/> (дата обращения 15.04.2025).
3. О проекте // Театральный проект 27. URL: <https://theatre27.ru/#about> (дата обращения 22.04.2025).
4. Приглашаем на мастер-класс по культуре речи и ораторскому искусству «Я могу говорить!» // Высшая школа сценических искусств URL: <https://www.raikin-school.com/news/kultrechi23/> (дата обращения 25.04.2025).
5. Фонд поддержки Театра им. Ленсовета // ВКонтакте URL: [https://vk.com/wall-219467611\\_19](https://vk.com/wall-219467611_19) (дата обращения 25.04.2025).

*Статья представлена научным руководителем, доцентом кафедры СПН СПбГУТ, кандидатом философских наук Астафьевой-Румянцевой И. Е.*

УДК 659.127.8

П. В. Соколов (студент группы РСО-43, СПбГУТ), [sokolov.pv@sut.ru](mailto:sokolov.pv@sut.ru)

## РОЛЬ СОЦИАЛЬНЫХ СЕТЕЙ В ФОРМИРОВАНИИ ИМИДЖА БРЕНДА И ЕГО ВЛИЯНИИ НА ПОТРЕБИТЕЛЕЙ

*Современные социальные сети играют ключевую роль в процессе формирования имиджа брендов. Платформы, такие как ВКонтакте, TikTok, Telegram и другие, позволяют компаниям строить прямую коммуникацию с аудиторией, усиливать узнаваемость бренда и влиять на потребительские предпочтения. Благодаря уникальным механизмам вовлечения пользователей, социальные сети становятся важнейшими каналами для развития лояльности и продвижения продукции на рынке.*

*имидж бренда, социальные сети, маркетинг, потребительское поведение, вовлеченность*

В условиях высокой конкуренции компании активно используют социальные сети для формирования положительного восприятия бренда. Создание качественного контента, проведение интерактивных кампаний и работа с отзывами пользователей способствуют укреплению репутации бренда и формированию долгосрочной эмоциональной связи с потребителями [1, 2].

### Основные стратегии формирования имиджа бренда в социальных сетях

- создание уникального контента, отражающего ценности и миссию бренда;
- постоянная вовлеченность – регулярное взаимодействие с аудиторией через комментарии, лайки, прямые эфиры;
- персонализация сообщений – адаптация контента под разные группы пользователей;
- использование визуальной идентичности – единый стиль оформления публикаций (цвета, логотипы, типографика).

Контент в социальных сетях должен не только информировать, но и вызывать эмоциональный отклик, побуждая к участию в жизни бренда.

### Роль инфлюенсеров в формировании имиджа бренда

Инфлюенсеры стали важнейшими посредниками между брендами и потребителями. Согласно исследованию Influencer Marketing Hub (2024), более 72 % потребителей доверяют рекомендациям блогеров так же, как и советам друзей [3, 4].

Сотрудничество с микро- и макроинфлюенсерами помогает:



- повысить доверие к бренду;
- расширить охват целевой аудитории;
- адаптировать имидж компании к различным культурным и социальным группам.

### **Негативное влияние социальных сетей на имидж бренда**

Несмотря на преимущества, социальные сети могут нанести вред бренду в случае:

- распространения негативных отзывов;
- ошибок в маркетинговых кампаниях (например, неудачные рекламные акции);
- кризисов репутации, вызванных некорректными публикациями.

### **Методы оценки эффективности социальных медиакампаний**

Эффективность формируемого имиджа можно оценить с помощью следующих показателей:

- Engagement Rate (ER) – отношение взаимодействий к количеству подписчиков.
- Sentiment Analysis – анализ тональности отзывов о бренде.
- Reach and Impressions – количество охваченных пользователей и количество просмотров публикаций.
- Conversion Rate – отношение числа пользователей, совершивших целевое действие, к общему числу посетителей.

Одним из ключевых факторов успешного формирования имиджа в социальных сетях является вовлеченность аудитории. Показатели лайков, комментариев, репостов и времени взаимодействия с контентом напрямую отражают уровень интереса пользователей и их отношение к бренду.

Известно, что эффективность работы в социальных сетях можно измерить различными метриками, в том числе уровнем вовлеченности (ER, Engagement Rate), который рассчитывается по формуле [3]:

$$ER = (\text{Лайки} + \text{Комментарии} + \text{Репосты}) / \text{Количество подписчиков} \times 100 \%$$

На рисунке 1 показана зависимость уровня вовлеченности от типа контента.

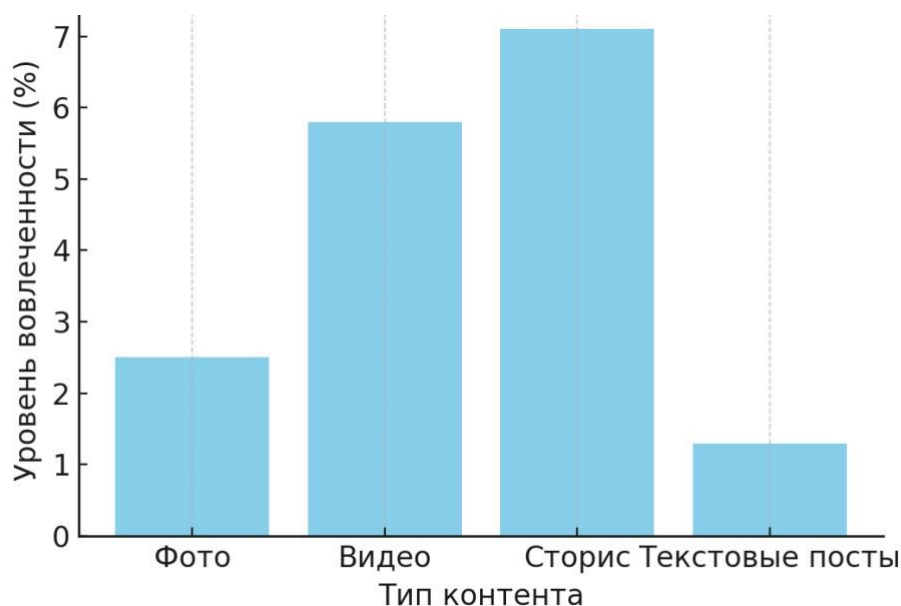


Рис. 1. Зависимость уровня вовлеченности от типа контента

ТАБЛИЦА 1. Показатели вовлеченности на различных типах контента

| Тип контента    | Уровень вовлеченности ( %) |
|-----------------|----------------------------|
| Фото            | 2,5                        |
| Видео           | 5,8                        |
| Сторис          | 7,1                        |
| Текстовые посты | 1,3                        |

Социальные сети предоставляют брендам уникальные возможности для создания, поддержания и укрепления своего имиджа. Компании, которые эффективно используют контент, вовлекают аудиторию и сотрудничают с инфлюенсерами, получают значительные конкурентные преимущества. Однако при этом важно учитывать возможные риски и уделять особое внимание управлению репутацией. Формирование устойчивого позитивного имиджа в социальных сетях становится важнейшей задачей современного брендинга.

#### Список используемых источников

1. Котлер Ф., Келлер К. Л. Маркетинг менеджмент. 15-е изд. СПб.: Питер, 2016. 832 с. ISBN 978-5-496-02120-3.
2. Соловьев А. В. Социальные сети как инструмент формирования имиджа компании // Маркетинг в России и за рубежом. 2018. № 3. С. 45–50.

3. Ильина Е. В. Инструменты продвижения бренда в социальных сетях // Маркетинг и маркетинговые исследования. 2023. № 2. С. 18–23.
4. Петрова Н. С. Социальные медиа как фактор формирования имиджа бренда // Экономика и управление. 2022. № 6 (178). С. 97–102.
5. Васильев К. И. Маркетинговые коммуникации в цифровую эпоху: социальные сети и их роль // Журнал «Маркетинг в России и за рубежом». 2021. № 5. С. 30–34.

*Статья представлена научным руководителем, деканом факультета СТЭД СПбГУТ, кандидатом политических наук, доцентом Шутманом Д. В.*

УДК 004.032.6

Н. С. Соловьев (студент группы БИМ-41з, СПбГУТ), [solovev.ns@sut.ru](mailto:solovev.ns@sut.ru)

## ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДИАГНОСТИКЕ СУРДОЛОГИЧЕСКИХ ЗАБОЛЕВАНИЙ

*Внедрение искусственного интеллекта в процесс диагностики сурдологических заболеваний, связанных с анализом медицинских снимков, набирает все большую популярность благодаря тому, что позволяет сократить долю человеческого труда и временные затраты. Благодаря этому возрастает точность получаемых результатов, сокращаются временные затраты, а также уменьшается вероятность совершения ошибок, возникающих из-за человеческого фактора.*

*анализ, медицинские данные, искусственный интеллект, нейронные сети.*

Сурдология – узкое направление в оториноларингологии, посвященное изучению возникновения, диагностики и лечения различных заболеваний, связанных со слухом [1].

Возможности искусственного интеллекта разнообразны и если говорить о них в контексте сурдологии, то они могут применяться в анализе медицинских изображений. Под медицинскими изображениями подразумеваются снимки компьютерной томографии и магнитно-резонансной томографии, анализируя которые, врачи получают необходимую информацию о текущем состоянии пациента. Однако, просмотр сотен снимков на предмет выявления патологий – это трудоемкий процесс, требующий высокой квалификации специалиста, который помимо прочего может осложняться низким качеством предоставляемых данных. Автоматизировать процесс обработки медицинских изображений и их последующий анализ можно при помощи нейронных сетей. Чтобы сеть могла выполнять поставленные перед ней задачи ее необходимо обучить. Компьютерная программа обучается по мере накопления опыта относительно некоторого класса задач и целевой функции, если качество решения этих задач улучшается с полученным опытом [2].

В таблице 1 представлены способы применения нейронных сетей для обработки и анализа медицинских данных.

ТАБЛИЦА 1. Способы применения нейронной сети

| Способ применения              | Описание                                                       |
|--------------------------------|----------------------------------------------------------------|
| Классификация изображений      | Разделение изображения на категории или классификация объектов |
| Детектирование объектов        | CNN может выявлять и выделять объекты на изображении           |
| Повышение качества изображения | Всевозможные виды обработки изображения                        |
| Сегментация                    | Разделение изображения на области, соответствующие объекту     |
| Анализ видео                   | Комплекс инструментов для обработки видео файлов               |

Благодаря широкому функционалу, которым обладают нейронные сети в вопросах обработки и анализа изображений, возможно сократить долю человеческого труда, а также временные затраты, путем передачи рутинных задач на машину. Для работы с медицинскими изображениями предполагается использовать Сверточную нейронную сеть (СНС) или Трансформер (СТ). Каждая из представленных моделей, способна обработать и проанализировать изображения, но при этом обладает рядом преимуществ и недостатков, влияющих на выполнение поставленных задач.

СНС – предназначены для работы со входами, имеющими сетчатую структуру и характеризующимися сильными пространственными зависимостями в локальных областях сетки. Наиболее показательным примером данных, имеющих такую структуру, является двухмерное изображение [2]. Особенностью является высокий уровень проникновения в контекст в тех случаях, когда информация в пространстве непрерывна, а именно, когда носители информации расположены рядом. Благодаря тому, что любое изображение состоит из пикселей, которые находятся в непосредственной близости друг от друга и содержат в себе визуальные данные, такого рода сети могут распознать связь между ними. После загрузки снимка в такую модель она будет рассматривать каждый пиксель представленного изображения и классифицировать его. Если в одном пикселе будет опознано лицо, то и в соседних тоже.

Сверточная сеть состоит из следующих элементов:

1. Сверточные слои: каждая плоскость в сверточном слое – это один нейрон, которые реализует операцию свертки и одновременно с этим является матричным фильтром;

2. Слои субдискретизации – отвечают за уменьшение размера изображения;

3. Полносвязные слои – используются для классификации данных и находятся перед выходом;

На рисунке 1 представлен процесс работы сверточной нейронной сети.

Каждое измерение включает в себя направления консолидации данных, которые состоят из уровней иерархии, где каждый вышестоящий уровень соответствует большей степени агрегации данных по конкретному признаку. Благодаря этому возможно получить произвольный уровень детализации информации по каждому измерению. В процессе свертки одно или несколько подчиненных значений измерений заменяются теми значениями, которым они подчинены, при этом уровень обобщения данных уменьшается. Задача, которая стоит перед сверточным слоем, сводится к поиску весов, а именно к поиску матрицы свертки, которая эквивалентна весам в нейронах.

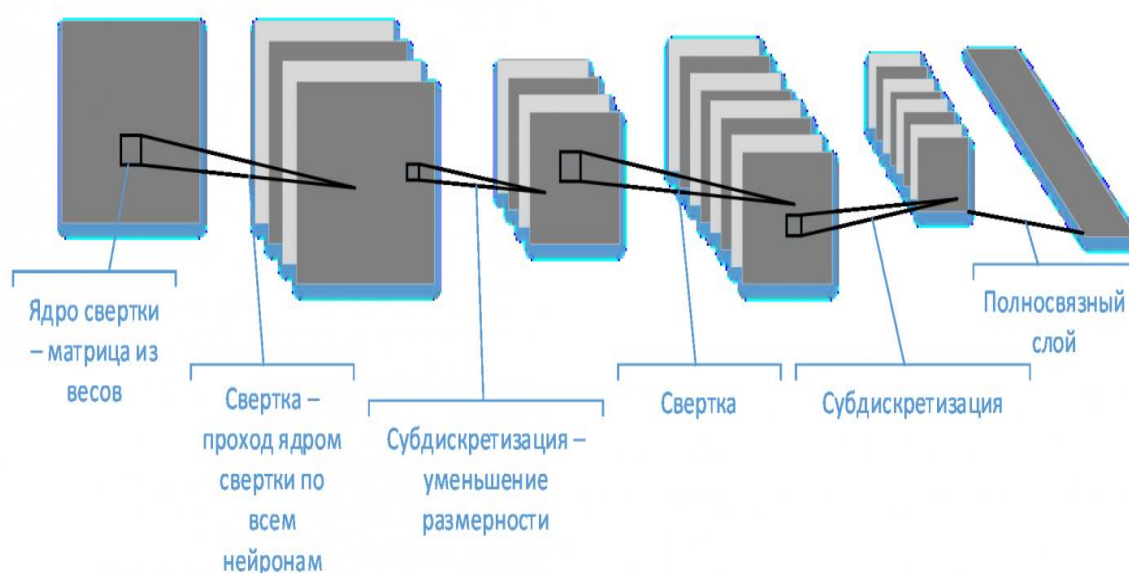


Рис. 1. Сверточная нейронная сеть

Нейроны занимаются поисками неких признаков на том участке изображения, который им доступен, а когда поиск заканчивается, они передают информацию об этом дальше формируя таким образом абстрактную карту.

Однако, когда подобных карт ставится слишком много, система начинает уплотнять их, что называется операцией объединения. В рассматриваемой архитектуре принято ставить акцент на поиск признаков, а не выявление их точно места расположения, поэтому из соседних нейронов выбирается карта того, который имеет максимальное или среднее значение искомого признака, а нейроны в последующем воспринимаются как некий уплотненный нейрон, то есть объединяются, тем самым теряя размерность.

С математической точки зрения операция свертки выглядит следующим образом:

$$Y_{(i,j)} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} X(i+m, j+n) * K(m, n) + b$$

где  $Y_{(i,j)}$  – выходное значение после применения фильтра,  $M, N$  – размеры ядра свертки,  $X(i, j)$  – входное изображение,  $K(m, n)$  – фильтр (ядро свертки),

$m, n$  – координаты элементов ядра свертки,  $b$  – смещение.

Преимущества данной модели в сравнении с Трансформерами, заключаются в том, что ее необходимо меньше вычислительных мощностей, а также она быстрее обучается, требуя меньший набор данных. Что в свою очередь, чревато такими недостатками как ограничения в захвате долгосрочных зависимостей, потому что акцент стоит на локальных признаках и не приспособленности к работе с большими изображениями ввиду того, что не будет хватать вычислительных мощностей.

Трансформер – разновидность нейронных сетей, призванная обрабатывать последовательные данные. Таким сетям необязательно соблюдать порядок при работе с последовательными данными, они могут акцентировать свое внимание на определенных элементах. Архитектура такой сети состоит из:

- «кодировщика» – слоя, который получает на вход векторизованную последовательность с информацией;
- «декодировщика» – слоя, который получает на вход часть векторизованной последовательности и выход кодировщика;

На рисунке 2 представлено устройство сети Трансформер.

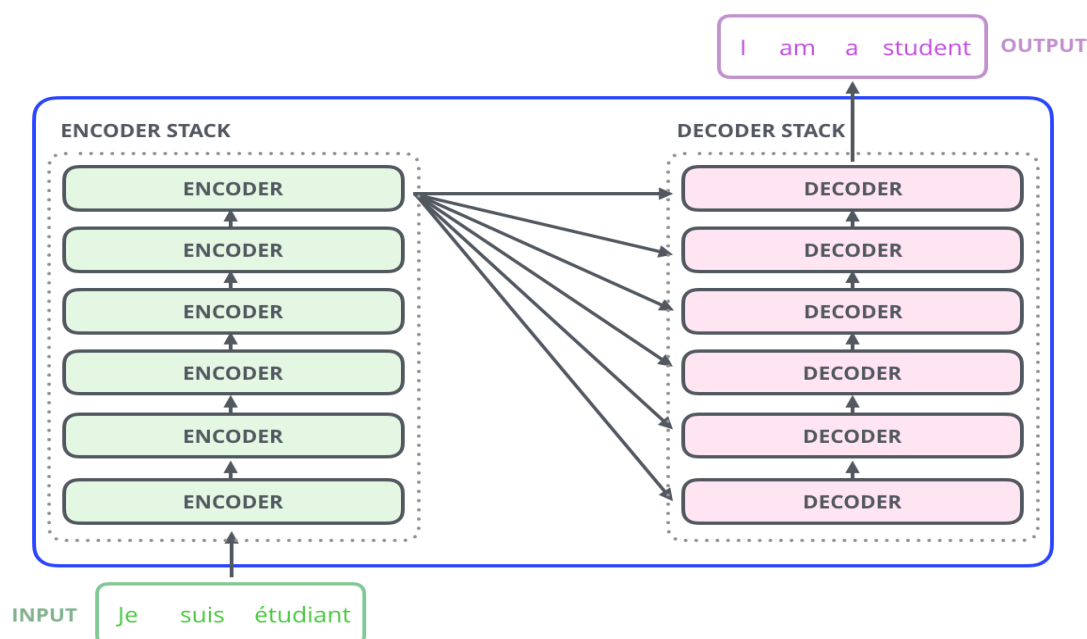


Рис. 2. Нейронная сеть Трансформер

ТС создают цифровое представление каждого элемента последовательности, инкапсулируют важную информацию вместе с окружающим ее контекстом. Получившийся результат можно загрузить в другие сети, которые в свою очередь используют полученную информацию для решения поставленных перед ними задач, например, классификация или синтез. Таким образом получается добиться лучшего понимания скрытых паттернов и взаимосвязи между входными данными [3].

С математической точки зрения механизм внимания, используемый в этой разновидности нейронной сети, выглядит следующим образом:

$$Attention(Q, K, V) = softmax(\frac{QK^T}{\sqrt{d_k}})V$$

$Q$  – запросы (векторные представления, которые определяют на, что обратить внимание),  $K$  – ключи (векторы определяющие наиболее релевантные части данных),  $V$  – значения (данные, которые будут извлечены в результате),  $softmax$  – функция, сортирующая входные данные по степени важности,  $\sqrt{d_k}$  – размерность ключа.

Преимущества ЕС в сравнении с СНС заключаются в том, что они способна обрабатывать более объемные наборы данных, что позволяет им выявлять глобальные зависимости, что полезно при работе с сложными снимками, которые включают много элементов. В свою очередь для работы им



необходимо больше вычислительных ресурсов и входных данных, чтобы обучиться на них, что является недостатком

В настоящее время перспективным для использования нейронных сетей представляются следующие практические медицинские задачи сурдологии:

- классификация состояния внутреннего уха;
- сегментация слухового нерва, улитки, овального окна и т.д.;
- оценка патологий на поперечных срезах КТ/МРТ.

Сверточные сети, как показывает опыт их использования для обработки рентгеновских и томографических изображений [4, 5] демонстрируют лучшие результаты при использовании ограниченных по размеру датасетов и хорошо «улавливают» локальные особенности, (например, очаги воспаления, опухоли, аномалии во внутреннем ухе и т.д.). В отличие от трансформеров, СНС требуют меньше ресурсов для обучения. Хорошо отлаженные архитектуры СНС широко используются и доступны в виде готовых фреймворков.

Таким образом на данном – начальном – этапе применения нейронных сетей в сурдологии представляется целесообразным использовать сверточные нейронные сети, и по мере накопления материалов и появления уверенности в положительных результатах их использования проводить сравнительный анализ СНС и СТ сетей.

#### Список используемых источников

1. Бобошко М. Ю., Савенко И. В., Гарбарук Е. С., Журавский С. Г., Мальцева Н. В., Бердникова И. П. Практическая сурдология. СПб.: Диалог, 2021. 79 с.
2. Николенко С. И., Кадуринов А. А., Архангельская Е. О. Глубокое обучение. Погружение в мир нейронных сетей / СПб.: Питер, 2020. 17 с.
3. Аггавал Чару. Нейронные сети и глубокое обучение: учебный курс.: Пер. с англ. СПб.: ООО "Диалектика", 2020. - 486 с.
4. A comprehensive review of deep neural networks for medical image processing: Recent developments and future opportunities, Healthcare Analytics, Volume 4, December 2023, 100216.
5. Medical image analysis using deep learning algorithms" Front. Public Health, 07 November 2023 Sec. Digital Public Health. Volume 11. 2023. URL:| <https://doi.org/10.3389/fpubh.2023.1273253> (дата обращения 25.04.2025).

*Статья представлена научным руководителем,  
доктором технических наук, профессором Сотниковым А. Д.*

## СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

УДК 351.858

**Ю. Д. Вилкова** (магистрант группы РСО-41м, СПбГУТ), [vilkova.yd@sut.ru](mailto:vilkova.yd@sut.ru)  
**А. Ю. Цыгоняева** (к.т.н., доцент кафедры истории и регионоведения, СПбГУТ)

### ОСОБЕННОСТИ ПРОДВИЖЕНИЯ ГОСОРГАНИЗАЦИЙ ПОСРЕДСТВОМ СОЦИАЛЬНЫХ СЕТЕЙ

*В статье рассмотрены особенности продвижения госорганizations в соцсетях на примере анализа деятельности Агентства занятости населения и Центра развития и поддержки предпринимательства. Исследование основывается на контент-анализе публикаций и оценке визуальных стратегий. А также присутствуют выводы и рекомендации по продвижению для каждой организации, что поможет повысить эффективность коммуникации между государством и гражданами.*

*продвижение, социальные сети, государственные организации, контент, вовлеченность аудитории*

Социальные сети стали неотъемлемой частью нашей жизни. Они стали не просто удобным способом общения между людьми, а также местом для продвижения своего бренда, товара или услуг. Это касается не только коммерческих организаций, но и государственных. Через соцсети можно рассказать достаточно большой аудитории о своих услугах, поделиться новостями или событиями и укрепить связи с общественностью.

По распоряжению Правительства РФ, государственные структуры обязали создать и вести официальные аккаунты в таких социальных сетях как ВКонтакте и Одноклассники. Но в продвижении и ведении этих страниц значительно отличается от частных предприятий, в них есть свои нюансы. Ниже рассмотрим специфику:

1. **Согласование.** Необходимость согласовывать каждый шаг. Нужно информировать руководство об абсолютно каждом решении. Полученные правки могут быть необычными, такими как заменить союз «но», на «зато».

2. **KPI.** Сложно определить KPI в государственных пабликах. Там может и не быть системы оценивания результатов или в ней могут сравнивать несравнимые вещи

3. **Социальные сети.** Появились ограничения на некоторые соцсети, которые являются запрещенными в Российской Федерации организациями.

4. **Бюджет.** Так как государственные структуры являются бюджетными организациями, деньги, выделяемые на продвижение, ведение и создание контента могут быть ограниченны.

5. **Поручение начальства.** Могут быть ситуации, когда руководитель даст информацию, которая может не вписываться в запланированный план. Возникают трудности в обыгрывании новости и вписании ее в общий контент [1].

Учитывая все сказанное выше, можно заметить, что ведение аккаунтов государственных организаций имеет строгие правила, под которые нужно подстроиться. Важно также не забывать и про основные цели ведения таких пабликов. Ниже приведены основные аспекты, на которые нужно ориентироваться при составлении плана продвижения государственных организаций:

1. **Информирование.** Нужно предоставлять важную и свежую информацию о работе организации. Публиковать новости, услуги, мероприятия и информацию на которых специализируется госорган.

2. **Отчетность и видимость.** Публиковать отчеты о проделанной работе, информировать о своих планах на будущее. А также освещать работу внутри структуры, для повышения доверия среди населения.

3. **Повышение заинтересованности.** Мотивировать граждан к участию в различных государственных мероприятиях, повысить интерес к деятельности организации и его программам.

4. **Лояльность.** Формирование лояльного комьюнити, одобрение деятельности и повышение доверия среди граждан.

5. **Обратная связь.** Сбор обращений, сообщений и комментариев для обработки и дальнейшего анализа целевой аудитории. Именно их жалобы и предложения помогут составить планы ведения соцсетей в будущем. А также оперативно реагировать на них.

Далее рассмотрим на конкретном примере Агентство занятости населения и Центр развития и поддержки предпринимательства.

Агентство занятости населения в Санкт-Петербурге имеет страницы в таких социальных сетях как «ВКонтакте» и «Одноклассники». Через сообщества они распространяет информацию об открытых вакансиях в различные организации, самых актуальных и востребованных профессиях, полезные статьи, которые помогут при поиске работы, информацию о программах переквалификации и обучения и предоставляет консультации по вопросам трудоустройства [2].

Их целевой аудиторией являются жители Санкт-Петербурга, которые ищут работу или просто интересуются новостями в сфере занятости населения. А также есть удобные гиперссылки для перехода между необходимыми сегментами основного сообщества, направленные на различные категории граждан.

Рассмотрим внешнее оформление страницы. Из рис. 1 видим, что все оформлено в единой цветовой гамме. В качестве основного цвета они взяли белый и синий, что достаточно часто встречается в госорганизациях.

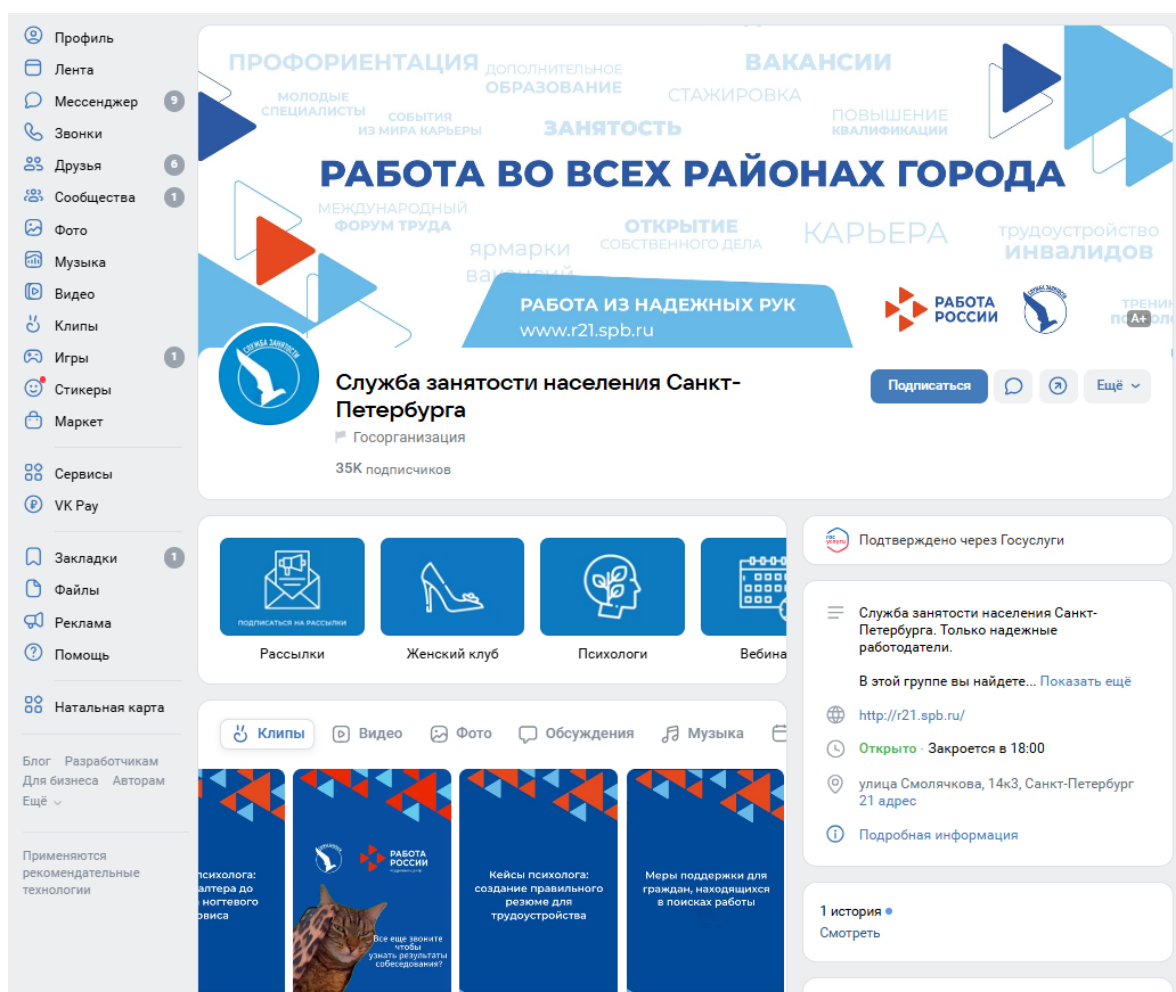


Рис. 1. Официальная страница Службы занятости населения Санкт-Петербурга в социальной сети ВКонтакте

Информация в сообществе представлена не только в текстовом формате (Посты), но и посредством видеоконтента (Клипы).

Проведя анализ публикаций в сообществе Агентства занятости населения, можно выделить несколько основных особенностей продвижения:

1. Полезная информация. Публикуются вакансии, важные изменения в законах, аналитические статьи о рынке труда.

2. Мероприятия. Периодически проводятся полезные прямые эфиры с экспертами. А также анонсы мероприятий, таких как «Ярмарка вакансий», «Дни карьеры», «Всероссийская ярмарка трудоустройства» и т.п.

3. Обратная связь. Кураторы сообщества отвечают на вопросы в комментариях и личных сообщениях, но не всегда оперативно.

4. Интерактив. Очень редко проводят опросы среди подписчиков, практически нет развлекательных постов с конкурсами или примерами успешного трудоустройства.

5. Периодичность публикаций. 2-3 поста в день (нет подбора времени публикации, когда аудитория активна).

6. Хештеги. Активно используются под каждым постом хештеги (например: [#мероприятия@czn\\_spb](#), [#вакансии@czn\\_spb](#), [#новости@czn\\_spb](#)).

7. Другие платформы. На сайте сложно найти ссылку на ВК или Одноклассники. Мессенджеры WhatsApp и Viber доступны исключительно для сообщений [3].

Особенности ведения социальных сетей «Службы занятости населения» несут просветительский характер их деятельности. Их группа не в полной мере использует методы вовлечения аудитории.

Рекомендации:

1. Внедрить чат-бот для автоматизации ответов на часто задаваемые вопросы.

2. Увеличить количество опрос и различных взаимодействий с аудиторией.

3. Добавить неформальный и развлекательный контент.

Проанализируем еще одну госорганизацию – «Центр развития и поддержки предпринимательства» (СПб ГБУ «ЦРПП»). На сайте есть ссылки на такие соцсети как «ВКонтакте», «Одноклассники», «Telegram» и «WhatsApp». Последние две используются для индивидуальной консультации, а их сообщество ВК рассмотрим подробнее.

Официальная группа называется «Мой бизнес | Санкт-Петербург». Основная аудитория состоит из начинающих предпринимателей, самозанятых или людей, интересующихся бизнесом [4].

Графический дизайн страницы оформлен в оттенках черного и желтого цвета, в целях привлечения внимания (рис. 2). Регулярность выкладывания контента варьируется от 2 до 5 постов в день, динамика публикаций происходит в течении всего дня.

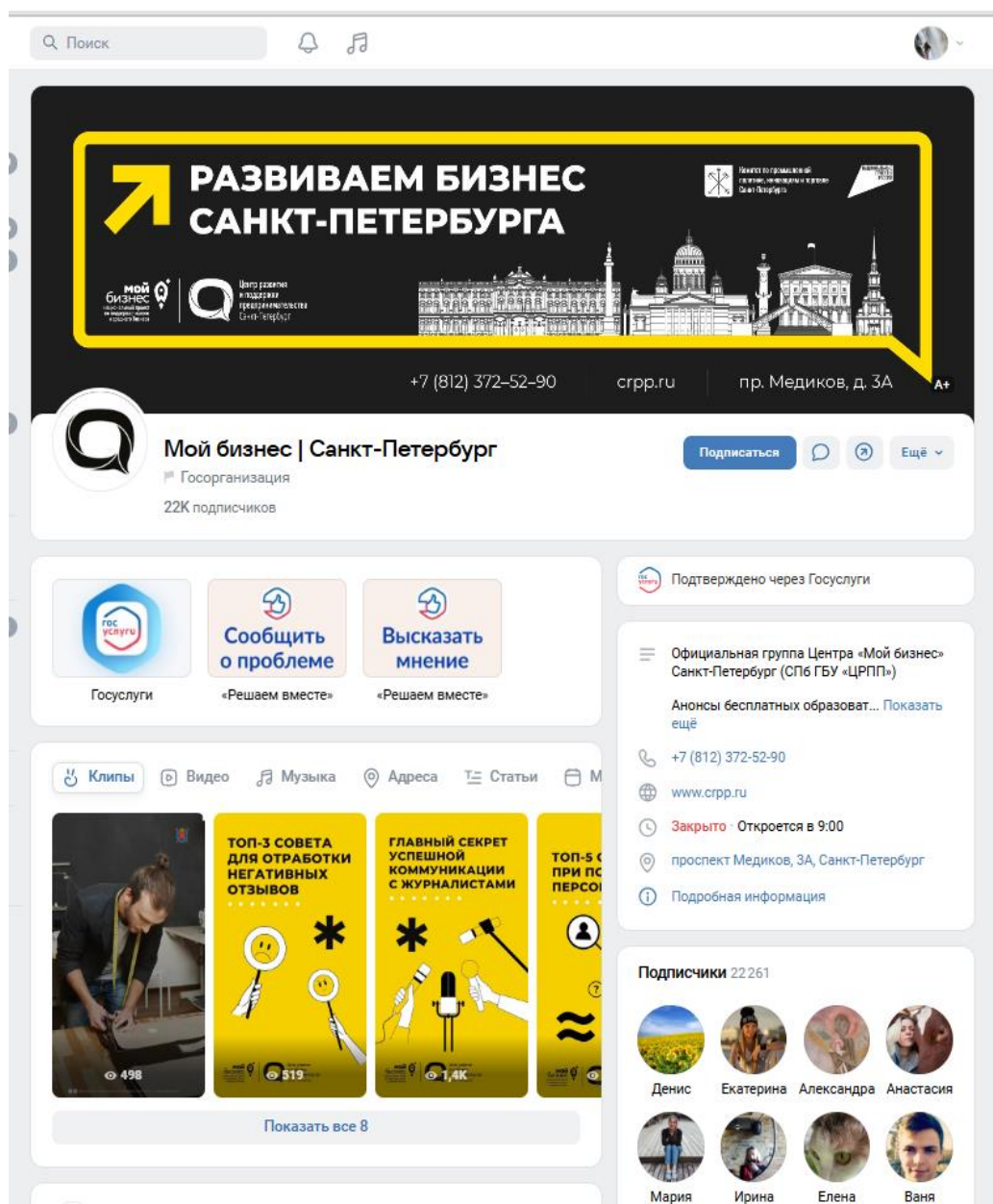


Рис. 2. Официальный аккаунт «Центр развития и поддержки предпринимательства» в социальной сети ВКонтакте

Проанализировав публикации в сообществе «Мой бизнес», были выявлены основные особенности продвижения:

1. Уклон на образование. Публикуются гайды по открытию бизнеса, игровые бизнес-тренинги, онлайн-семинары и т.п.
2. Истории успеха. Истории, интервью и полезные советы от успешных предпринимателей повышают доверие аудитории.

3. Конкурсы. Проводятся конкурсы по различным направлениям бизнеса для малых и средних компаний, что повышает вовлеченность аудитории.

4. Нерегулярность контента. После периода высокой активности в публикации материала наступает затишье, что негативно сказывается на удержании аудитории.

5. Обратная связь. Администраторы сообщества оперативно отвечают в комментариях и личных сообщениях.

6. Хештеги. Хештеги помогают в поиске материала на странице, но в данном сообществе они не используются, что достаточно неудобно.

Рекомендации:

- разработать график публикации материалов, это поможет избежать спадов активности;
- создание большего количества коротких видео с советами от экспертов;
- начать использовать хештеги для удобства и большего охвата пользователей;
- увеличить количество новостей о нововведениях и изменениях в сфере предпринимательства.

Проведя исследование социальных сетей двух государственных организаций (Агентство занятости населения и Центр развития и поддержки предпринимательства) были выявлены не только особенности продвижения, но и составлены рекомендации по улучшению сообществ. А также, анализ показал, что госструктуры могут быть достаточно гибкими в соцсетях, если будут взаимодействовать и прислушиваться к потребностям своей целевой аудитории.

#### **Список используемых источников:**

1. Как вести соцсети госорганизаций: специфика и контент. URL: <https://blog.tochkadostupa.pro/kak-vesti-sotsseti-gosorganizatsij-spetsifika-i-kontent/> (дата обращения 17.04.2025).
2. Официальная группа Центра занятости населения Санкт-Петербурга // ВКонтакте. URL: [https://vk.com/czn\\_spb](https://vk.com/czn_spb) (дата обращения 19.04.2025).
3. Официальный сайт Регионального центра размещения заказов Санкт-Петербурга. URL: <https://r21.spb.ru/main.htm> (дата обращения 23.04.2025).
4. Официальная группа Центра развития поставщиков // ВКонтакте. URL: [https://vk.com/crpp\\_ru](https://vk.com/crpp_ru) (дата обращения 25.04.2025).

*Статья представлена научным руководителем, кандидатом философских наук, доцентом кафедры Истории и регионоведения СПбГУТ Цыгоняевой А. Ю.*



УДК 621.396.673

И. А. Власов, И. А. Скрыков (студенты группы ИКТВ-21, СПбГУТ),  
[vlasov.ia@sut.ru](mailto:vlasov.ia@sut.ru)

## РАСЧЕТ И КОМПЕНСАЦИЯ РЕАКТИВНОЙ СОСТАВЛЯЮЩЕЙ ПРОВОЛОЧНЫХ АНТЕНН ДИАПАЗОНА 200 МЕТРОВ

*В статье рассматриваются методы расчета и компенсации реактивной составляющей проволочных антенн диапазона 200 метров (1,5 МГц). Проведен анализ влияния реактивного сопротивления на согласование антенны с фидерной линией и КПД системы. Представлены графики зависимостей сопротивлений от длин антенн и методики расчета индуктивной и емкостной составляющих для различных типов антенн. Исследуется зависимость сопротивлений от формы и размеров антенн, а также от их ориентации и положения в пространстве.*

*связь, радиосвязь, антенны, антенны диапазона 200 метров, излучатели*

Существует несколько вариантов проволочных антенн диапазона 200 м [1-3]. Для эффективного излучения антенны выполняются удлиненными относительно  $\lambda/4$ , и имеют индуктивный характер входного сопротивления. Для антенн такого типа достаточным условием согласования является компенсация реактивного сопротивления.

Сопротивление излучения антенн лежит в пределах от 10 до 300  $\Omega$ , а реактивная составляющая в районе 300  $\Omega$ .

Определим границы компенсируемых реактивностей. Сделаем запас на 10 %, тогда для компенсации емкостной составляющей на нижней частоте 1,449 МГц потребуется индуктивность:

$$L = \frac{X_L}{2\pi f_H} = \frac{330}{2\pi \cdot 1,449} = 36 \text{ мкГн}$$

Для компенсации индуктивной составляющей на верхней частоте 1,62 МГц потребуется емкость:

$$C = \frac{1}{2\pi f_H X_C} = \frac{1}{2\pi \cdot 1,62 \cdot 330} = 298 \text{ пФ}$$

Для компенсации малого количества реактивного сопротивления требуется большое количество емкости. Например, для компенсации 10  $\Omega$  требуется почти 10 нФ.



Для дальнейшего определения КПД надо определить соотношение активного  $R_a$  и реактивного  $X_a$  сопротивления антенны, что является добротностью антенны:

$$Q_a = \frac{X_a}{R_a}$$

Из этого следует, что худший вариант при малом активном сопротивлении, тогда полоса пропускания антенны будет узкая, значит потребует тонкой настройки (рис. 1).

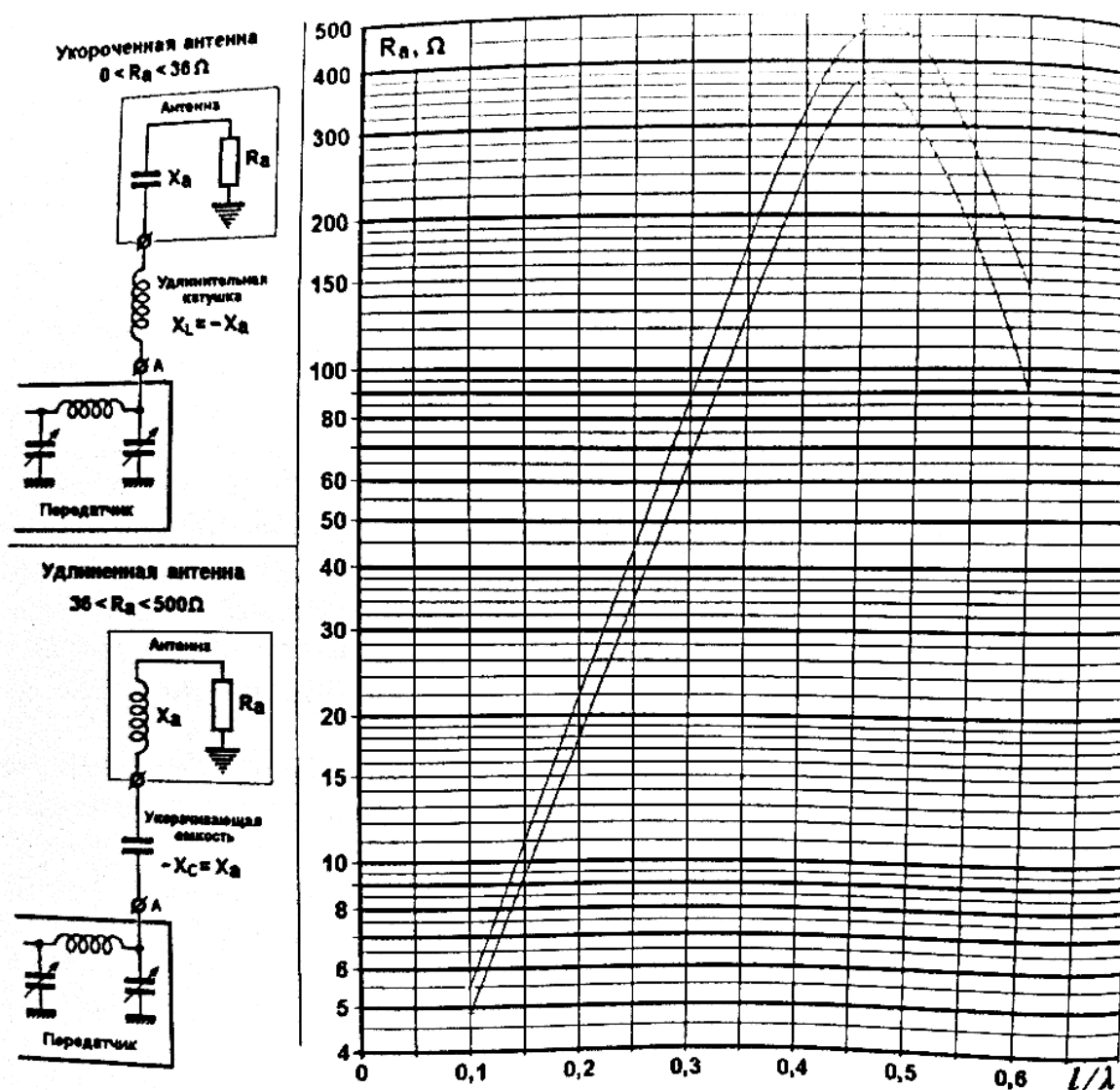


Рис. 1. Сопротивление антенн

Рассчитаем КПД и добротность проволочной антенны с активным сопротивлением 10 Ω. По графику из рисунка 1 видно, что сопротивление 10

$\Omega$  соответствует антенна с длиной  $0,15 \lambda$  или 30 м. Реактивная составляющая такой антенны носит емкостной характер и может быть рассчитана по формуле:

$$X_a = \rho \cdot \operatorname{ctg} \left( \frac{2\pi \cdot l}{\lambda} \right),$$

где  $\rho$  – волновое сопротивление проводника и может быть рассчитано по формуле:

$$\rho = 138 \cdot \lg \left( \frac{4h}{D} \right),$$

где  $h$  – высота проводника над землей,  $D$  – диаметр проводника.

Зависимость  $\rho$  приведена на рисунке 2.

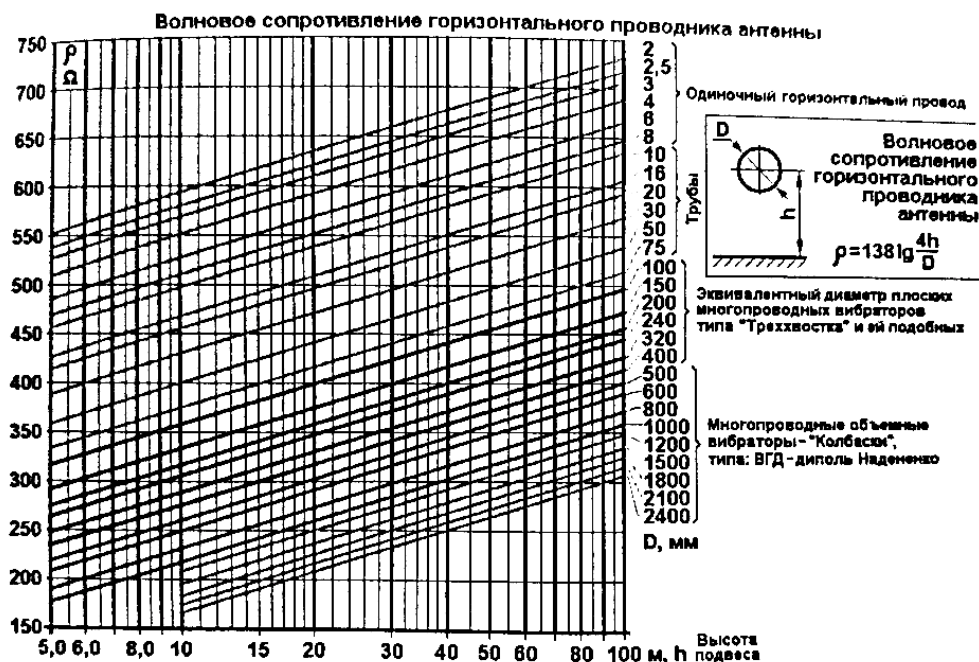


Рис. 2. Волновое сопротивление горизонтального проводника антенны

Если брать за антенну подвешенный проводник на высоте 12 м, то значение  $\rho$  будет лежать в районе 600  $\Omega$ , тогда реактивное сопротивление:

$$X_a = 600 \cdot \operatorname{ctg}(2\pi \cdot 0,15) = 440 \Omega$$

Добротность контура:

$$Q_a = \frac{X_a}{R_a} = \frac{440}{10} = 44$$

Что потребует точной настройки.

КПД антенного контура при собственной добротности катушки  $Q_{xx} = 200$ :

$$\eta = \frac{1}{1 + \frac{Q_a}{Q_{xx}}} = \frac{1}{1 + \frac{44}{200}} = 0,82$$

При такой добротности полоса пропускания по уровню половины мощности составит:

$$2\Delta f = \frac{f_p}{Q} = \frac{1532}{44} = 35 \text{ кГц.}$$

При полосе АМ сигнала 16 кГц, на высших модулирующих частотах будут наблюдаться потери уровня, что приведет к снижению отношения сигнал/шум, как следствие, увеличение ВЧ шумов на приемной стороне.

Из графика на рисунке 2 видно, что лучше использовать многопроволочные антенны. Такие антенны имеют низкое значение реактивного сопротивления, которое в последствии проще компенсировать, а также обеспечивают высокую стабильность  $R_a$  и  $X_a$  при изменении погодных условий. Следует обратить внимание на рисунок 3 из которого следует что волновое сопротивление вертикального проводника меньше на 50  $\Omega$ . Волновое сопротивление наклонных антенн будет средним между этими графиками.

Эквивалентные диаметры многопроволочных антенн представлены на рисунке 4.

Рассчитаем параметры многопроволочной цилиндрической антенны диаметром 1 м. с количеством проводников  $n = 6$  толщиной 1 см., высотой подвеса 12 м. и длиной 31 м. Тогда эквивалентный диаметр составит:

$$D = 2 \cdot 0,5 \cdot \sqrt[6]{\frac{6 \cdot 0,01}{2 \cdot 0,5}} = 0,63 \text{ м.}$$

Волновое сопротивление определяем по рисунку 2  $\rho = 260 \Omega$ .

Рассчитаем сопротивления:

$$X_a = 260 \cdot \text{ctg}(2\pi \cdot 0,15) = 189 \Omega$$

$$R_a = 10 \Omega$$

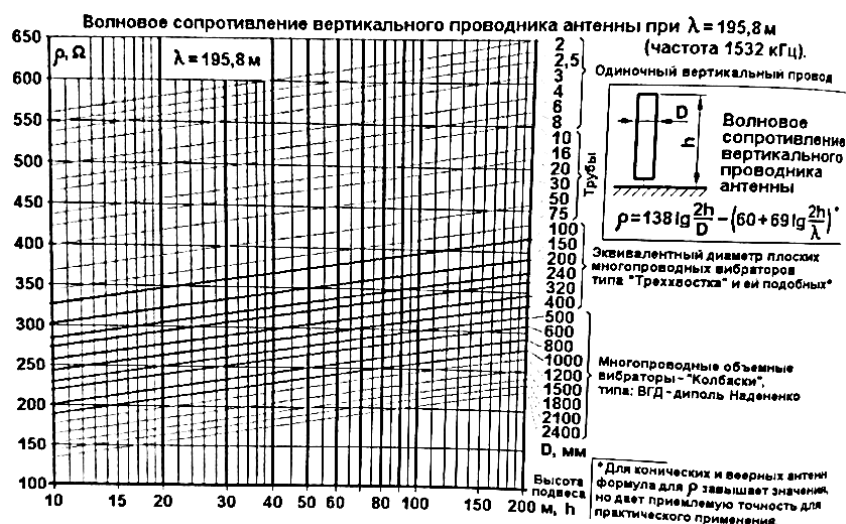


Рисунок 3. Волновое сопротивление вертикального проводника антенны

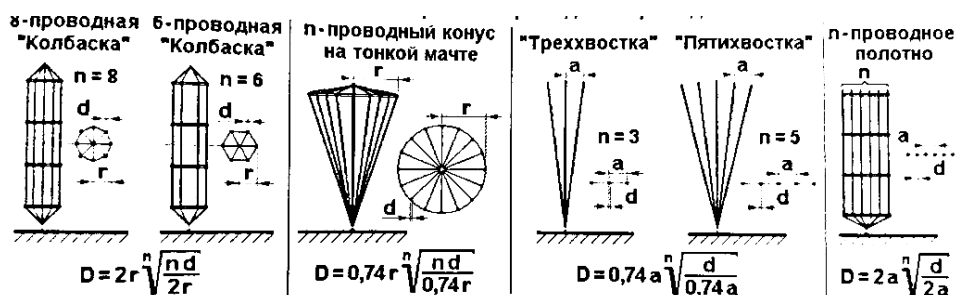


Рисунок 4. Эквивалентные диаметры многопроводных антенн

Добротность антенного контура:

$$Q_a = \frac{X_a}{R_a} = \frac{189}{10} = 18,9$$

Требуемая индуктивность для компенсации реактивной составляющей сопротивления:

$$L = \frac{X_L}{2\pi f_H} = \frac{189}{2\pi \cdot 1,449} = 20,8 \text{ мкГн}$$

КПД антенный составит:

$$\eta = \frac{1}{1 + \frac{Q_a}{Q_{xx}}} = \frac{1}{1 + \frac{18,9}{200}} = 0,91$$

Теперь рассчитаем трех проволочную антенну длиной до 70 м. и высотой подвеса 25 м. При такой длине  $R_a = 220 \Omega$ . Возьмем диаметр проволоки 2.5 мм. Эквивалентный диаметр составит:

$$D = 0,74 \cdot 5 \cdot \sqrt[3]{\frac{0,0025}{0,74 \cdot 5}} = 0,32 \text{ м.}$$

Тогда  $\rho = 330 \Omega$ . Удлиненная антенна будет иметь индуктивный характер сопротивления:

$$X_a = 330 \cdot \operatorname{ctg}\left(2\pi \cdot \frac{70}{185,2}\right) = 351 \Omega$$

Если подвесить антенну с наклоном  $45^\circ$ , то  $X_a$  составит  $325 \Omega$ . Емкость конденсатора составит:

$$C = \frac{1}{2\pi f_n X_C} = \frac{1}{2\pi \cdot 1,62 \cdot 325} = 302 \text{ пФ}$$

КПД антенного контура возможно рассчитать только лишь учитывая омические потери в проводнике антенны. Соответственно, чем больше проводников в антенне, тем выше будет КПД.

Таким образом расчеты показывают, что для диапазона 200 метров рациональный разброс длин многопроволочных антенн от  $0,15 \lambda$  до  $0,38 \lambda$ . Реактивное сопротивление лежит от  $X_C = 190 \Omega$  до  $X_L = 350 \Omega$ .

#### Список используемых источников

1. Комаров С. Н. / Индивидуальное радиовещание: практическое руководство для руководителей и членов конструкторских радиокружков и радиостанций Индивидуального радиовещания / Москва: Медиа Паблишер, 2017. [www.cgf.su](http://www.cgf.su). 1: Самодельные передающие антенны диапазона 200 метров. 2017. 150 с. ISBN 978-5-903650-56;
2. Ротхаммель К., Кришке А. / Антенны. Том 1.: Пер. с нем. М.: ДМК Пресс. 416 с.: ил. ISBN 5-85648-715-X;
3. Гавеля Н. П., Истрашкин А. Д., Муравьев Ю. К., Серков В. П. / Антенны. Часть 1 / Санкт-Петербург: Военная краснознаменная академия связи, 1963.

*Статья представлена научным руководителем,  
кандидатом технических наук, доцентом Сагдеевым А. К.*

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

**СТУДЕНЧЕСКАЯ ВЕСНА**

13-15 мая 2025

**Сборник научных статей  
Специальный выпуск**

*Научное издание*

Верстка

М. О. Мотыгина

Корректурa

Д. Н. Яшугин

Дизайн логотипа Г. И. Юрьев

Подписано в печать 19.11.2025

Объем 35,56 усл.-печ. л.

Объединенная редакция рецензируемых научных изданий СПбГУТ  
193232 СПб., пр. Большевиков, 22, корп. 1

