2025

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

СТУДЕНЧЕСКАЯ ВЕСНА

СБОРНИК НАУЧНЫХ СТАТЕЙ

СПЕЦИАЛЬНЫЙ ВЫПУСК

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
Специальный выпуск

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., специальный выпуск / Под ред. А. В. Рабина; сост. А. А. Дзюбаненко, И. М. Татарникова. СПб.: СПбГУТ, 2025. 304 с.

Рецензент – заведующий кафедрой конструирования и производства радиоаппаратуры Пензенского государственного университета, доктор технических наук, профессор **Юрков Н. К.**

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.

ISBN 978-5-89160-383-7

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 621.373.8

И. Д. Акимова (студент группы ИКТО-18, СПбГУТ), akimova.id@sut.ru

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ПЕРЕСТРАИВАЕМОГО ОДНОМОДОВОГО ЛАЗЕРА DBR

В системах связи, использующих технологию плотного спектрального мультиплексирования DWDM, востребованы лазеры с перестраиваемой длиной волны. Известно, что лазеры DBR могут перестраиваться в широком диапазоне длин волн. В работе проведено моделирование и исследование одномодового лазера DBR с двумя перестраиваемыми током брэгговскими зеркалами.

лазерный диод, лазер с распределенными брэгговскими отражателями, лазер DBR, перестройка длины волны

MODELING AND STUDYING A TUNABLE SINGLE-MODE DBR LASER

Akimova I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Tunable wavelength lasers are in demand in communication systems using dense wavelength division multiplexing (DWDM) technology. DBR lasers are known to be tunable over a wide wavelength range. This paper models and studies a single-mode DBR laser with two current-tunable Bragg mirrors.

Key words: *laser diode, distributed Bragg reflector laser, DBR laser, wavelength tuning*

Перестраиваемые лазеры находят свое наибольшее применение в реконфигурируемых DWDM-сетях, обеспечивая возможность динамического управления спектральными каналами, что важно для реконфигурируемых сетей и сложных сетевых топологий, где требуется гибкость управления каналами и оперативное реагирование на изменения нагрузки. В таких сетях

один универсальный модуль может заменить десятки фиксированных передатчиков, что упрощает эксплуатацию и снижает затраты.

Перестройка длины волны может осуществляться следующими методами: термический (для DFB лазеров), механический (для лазеров с внешней резонаторной полостью) и токовый для лазеров DBR [1].

Ниже, на рисунке 1, приведена схема моделируемого лазера, которая состоит из активной среды и двух брэгговских зеркал, по обе стороны от активной области, образующие резонатор.

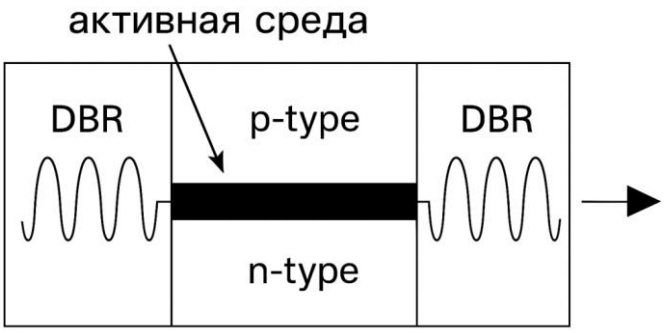


Рис. 1. Схема моделируемого лазера

Зеркала настроены на отражение длины волны Брэгга (1):

$$\lambda_B = 2n_{\text{eff}}\Lambda, \tag{1}$$

где λ_B – длина волны максимального отражения, n_{eff} – эффективный показатель преломления волноводной моды, Λ – пространственный период решетки.

Амплитуды волн по прохождении через зеркало связываются матрицей передачи F, которая связывает амплитуды напряженности поля в падающих и отраженных волнах на его входе и выходе. Лазер DBR можно представить системой, состоящей из трех последовательно включенных компонентов: двух брэгговских зеркал и активной среды между ними.

Матрица передачи брэгговского зеркала имеет вид (2):

$$F_m = \begin{bmatrix} s \cdot \cosh(s \cdot L) - i \cdot \Delta\beta \cdot \sinh(s \cdot L) & -i \cdot K \cdot \sinh(s \cdot L) \\ i \cdot K \cdot \sinh(s \cdot L) & s\cosh(s \cdot L) + i \cdot \Delta\beta \cdot \sinh(s \cdot L) \end{bmatrix}, \tag{2}$$

где L – длина зеркала, i – мнимая единица, а коэффициент связи K, фазовое рассогласование $\Delta\beta$ и параметр s определяются выражениями:

$$K = \frac{1}{\lambda} \cdot \sqrt{\frac{2[(n+\Delta n)^2 - n^2]}{(n+\Delta n)^2 + n^2}}, \tag{3}$$

$$\Delta\beta = k - \frac{\pi}{\Lambda}, \tag{4}$$

$$s = \sqrt{K^2 - \Delta\beta^2}. \tag{5}$$

В выражениях (3–5) Δn – параметр модуляции показателя преломления, Λ – период решетки, k – волновое число в области зеркала (6):

$$k = \frac{2\pi}{\lambda} \cdot \sqrt{\frac{(n+\Delta n)^2 + n^2}{2}}. \tag{6}$$

Для слоя активной среды матрица передачи F_a имеет вид (7):

$$F_a = \begin{bmatrix} \exp(i \cdot k_0 \cdot n_a \cdot L_a) & 0 \\ 0 & \exp(-i \cdot k_0(\lambda) \cdot n_a \cdot L_a) \end{bmatrix}, \tag{7}$$

где L_a, n_a – длина и показатель преломления активного слоя, k_0 – волновое число в активном слое:

$$k_0 = \frac{2\pi \cdot n_a}{\lambda}, \tag{8}$$

Если оба зеркала одинаковы, общая матрица передачи DBR может быть рассчитана следующим образом:

$$FF = F_m \cdot F_a \cdot F_m. \tag{9}$$

Для коэффициента отражения от такой структуры справедливо выражение (10):

$$R_1(\lambda) = \left| \frac{FF_{1,0}}{FF_{0,0}} \right|^2. \tag{10}$$

Токовая перестройка зеркал позволяет нам изменять показатель преломления примерно в пределах двух процентов [2]. Перестраивать длину волны предлагается в диапазоне 1530–1550 нм. На рис. 2 представлен график зависимости коэффициента отражения от длины волны при различных показателях преломления. Разница между показателями преломления – четверть процента от исходного показателя преломления, что составляет 0,0085.

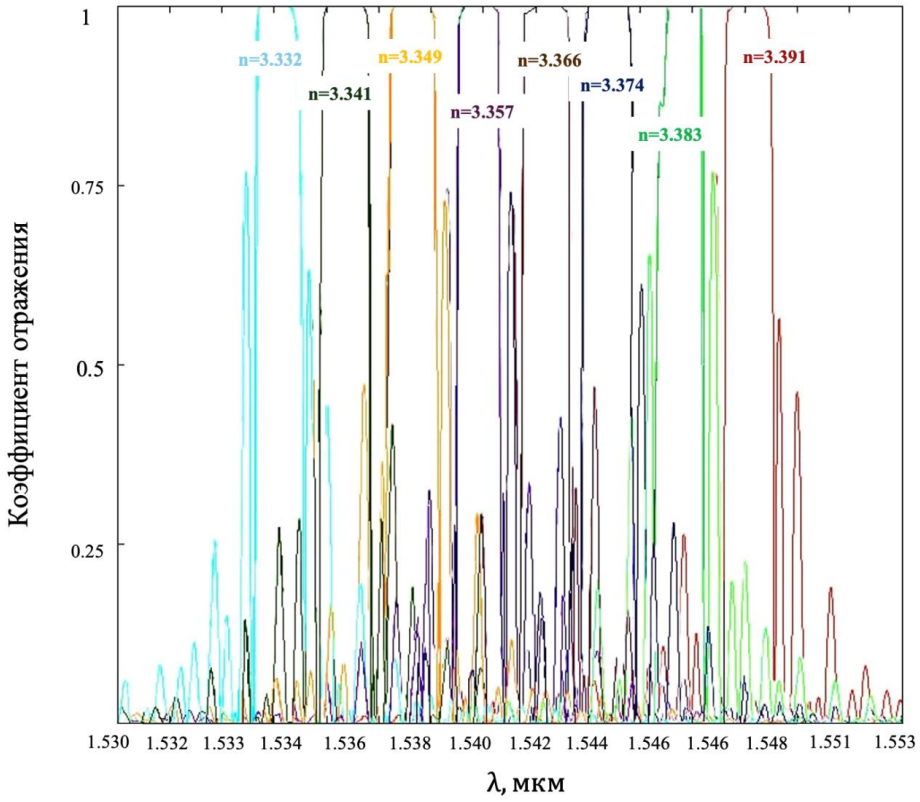


Рис. 2. График зависимости коэффициента отражения от длины волны при изменении показателя преломления основного материала

Ниже в таблице 1 представлены результаты расчета центральной длины волны в спектре отражения от показателя преломления. Показатель преломления изменялся с шагом 0,25 %. Диапазон перестройки составляет около 16 нм.

ТАБЛИЦА 1. Значения t_β при различных β

Δ, %	n-Δn	λB1, мкм	λ (R), мкм	Δλ, нм
0,00	3,400	1,550	1,550	0
-0,25	3,391	1,546	1,548	2
-0,50	3,383	1,542	1,546	4
-0,75	3,374	1,538	1,544	6
-1,00	3,366	1,535	1,542	7
-1,25	3,357	1,531	1,540	9
-1,50	3,349	1,527	1,539	12
-1,75	3,341	1,523	1,537	14
-2,00	3,332	1,519	1,534	15

На рис. 3 представлен график, по которому можно определить показатель преломления, требуемый для перестройки на определенную длину волны. Видно, что эта зависимость носит практически линейный характер.

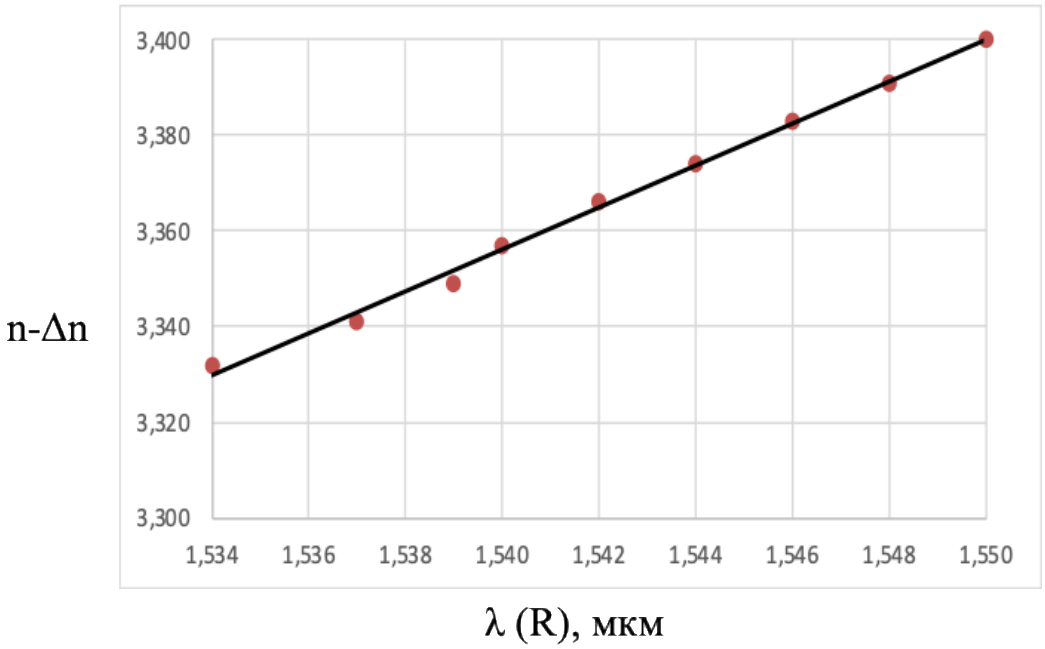


Рис. 3. График зависимости изменения длины волны отражения от изменения показателя преломления

В работе проведено моделирование спектра отражения трехслойной структуры DBR лазера путем изменения эффективного показателя преломления. Получена зависимость изменения длины волны отражения от изменения показателя преломления. Модель будет использована в дальнейших исследованиях токовой перестройки DBR лазера.

Список используемых источников

1. Jens Buus. Tunable laser sources for (D)WDM. Materials, Active Devices, and Optical Amplifiers, edited by Connie J. Chang-Hasnain, Dexiu Huang, Yoshiaki Nakano, Xiaomin Ren // Proceedings of SPIE. 2004. Vol. 5280. 0277-786X/04/$15. DOI:10.1117/12.529498.

2. Vijaysekhar Jayaraman, Zuon-Min Chuang, and Larry A. Coldren. Theory, Design, and Performance of Extended Tuning Range Semiconductor Lasers with Sampled Gratings // IEEE Journal Of Quantum Electronics. 1993. Vol. 29. № 6.

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

УДК 004.032.26

Э. В. Ашурова (студент группы ИКТК-12, СПбГУТ), ashurova.ev@sut.ru

РАЗРАБОТКА АЛГОРИТМА ОБУЧЕНИЯ НЕЙРОННОЙ СЕТИ ДЛЯ СНИЖЕНИЯ ЗАТРАЧЕННЫХ ВРЕМЕННЫХ РЕСУРСОВ НА АНАЛИЗ И ВЫЯВЛЕНИЕ ПРИЧИН АВАРИЙ В ПРОЦЕССЕ ОБМЕНА КОРОТКИМИ СООБЩЕНИЯМИ

Несмотря на стремительное развитие телекоммуникационных технологий, SMS до сих пор являются важным элементом системы информирования абонентов операторами или приложениями и не теряют актуальность с течением времени. Нейронные сети являются отличным решением для оптимизации процесса выявления аварий во время обмена короткими сообщениями и минимизации участия инженера в проверке CDR-файлов. Алгоритм, описанный в данной статье, предназначен для уменьшения затраченного рабочего времени на анализ причин аварийных ситуаций в мобильной сети и их последующего устранения.

нейронные сети, искусственный интеллект, архитектура нейронной сети, мобильные сети, CDR-файлы

DEVELOPMENT OF A NEURAL NETWORK TRAINING ALGORITHM TO REDUCE THE TIME SPENT ON ANALYZING AND IDENTIFYING THE CAUSES OF ACCIDENTS DURING THE EXCHANGE OF SHORT MESSAGES

Ashurova E.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Despite the rapid development of telecommunications technologies, SMS messages remain an important element of subscriber notification systems by operators or applications and remain relevant over time. Neural networks are an excellent solution for optimizing the process of identifying incidents during SMS exchanges and minimizing engineer involvement in checking CDR files. The algorithm described in this report is designed to reduce the time spent on analyzing the causes of incidents in a mobile network and their subsequent resolution.

Key words: *neural networks, artificial intelligence, neural network architecture, mobile networks, CDR files*

SMS – это аббревиатура от английского словосочетания «short message service», то есть сервис коротких сообщений. Он позволяет обмениваться текстовыми сообщениями через мобильный телефон или другое коммуникационное устройство. Вместо осуществления длинных вызовов, пользователи могут использовать короткие сообщения для быстрой и удобной коммуникации. Эти сообщения доставляются посредством мобильной сети провайдера связи и могут быть получены практически мгновенно. Сегодня надежность SMS сервиса обуславливается их активным применением в работе банковских сервисов и других бизнес-критичных отраслей.

Для анализа аварийных ситуаций, возникших в процессе передачи SMS, используются CDR-файлы – записи детализации вызовов, которые включают в себя сигнализационную информацию о каждой транзакции. Call Detail Record представляет собой структурированную запись, которая создается телекоммуникационным оборудованием. CDR-файлы фиксируют попытку пересылки короткого сообщения, содержат все ключевые параметры за время отправки и доставки сообщения в точку назначения [1].

Нейронная сеть является упрощенной имитацией биологических нейронных сетей, представленной в виде математической модели. Она состоит из взаимосвязанных элементов – искусственных нейронов, сгруппированных в слои, которые анализируют поступающую информацию путем линейных и нелинейных преобразований для выявления закономерностей в данных. Обучение нейронной сети заключается в настройке весов связей между нейронами с целью минимизации возможных ошибок в результатах обработки.

В данной статье приводится пример использования алгоритма нейронной сети прямого распространения для автоматизации процессов траблшутинга (от англ. troubleshooting) аварий, возникающих при передаче пользовательских и системных сообщений в мобильной сети различных операторов.

Функционирование алгоритма оптимизации выглядит следующим образом (рис. 1):

1. Абонент или операторский сервис (ESME) отправляет короткое сообщение в мобильную сеть (GSM).

2. SMS регистрируется в центре обработки коротких сообщений (SMSC), используемом для передачи и временного хранения сигнализационных сообщений в сетях подвижной связи как от абонента – MO-плечо (от англ. Mobile Oriented), так и к нему – MT-плечо (от англ. Mobile Terminated).

3. На всех этапах доставки сообщения SMSC формирует CDR-файлы, которые собираются и маркируются в отдельном каталоге на сервере. После чего, в соответствии с настройками журнала crontab, файлы, записанные за определенный промежуток времени, например, за 24 часа, передаются по протоколу sftp в базу данных. Сотрудник активирует скрипт, который используется для поиска нужных записей CDR, их сбор в общий файл и форматирование для удобства обработки нейросетью, и передает эти данные на вход нейронной сети. При необходимости у сотрудников будет возможность подгружать требуемые для анализа файлы вручную.

4. На вход нейронной сети поступают текстовые данные, необходимые сотруднику, после чего транзакции последовательно анализируются по каждому значению с разделителем «;» для выявления кода ошибки.

5. В качестве результата анализа сотруднику будет предоставлен текстовый вывод, содержащий основную информацию о транзакции: MSISDN входящего и исходящего абонентов, план и тип нумерации (TON и NPI), идентификатор сообщения (для случаев проблем с конкатенированным сообщением), статус сообщения, информация об ошибке и ее возможные причины [2].

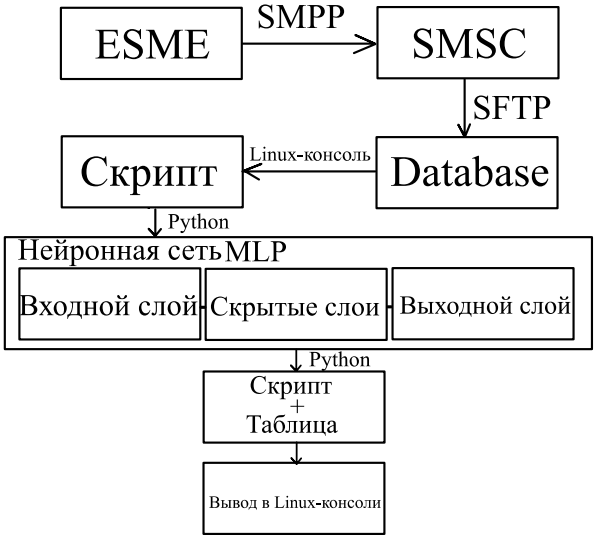


Рис. 1. Алгоритм оптимизации анализа аварий при помощи нейронной сети

Выполнение поставленной задачи наиболее оптимизировано при использовании для обучения модели многоуровневого перцептрона (MLP). Она содержит несколько скрытых слоев (рис. 2). Каждый нейрон в одном слое имеет направленные связи с нейронами последующего слоя. Число слоев зависит от степени сложности задачи, поставленной перед нейронной сетью. На выходе нейронная сеть будет выдавать в качестве результата обработки CDR ошибку, из-за которой сообщение не было доставлено [3].

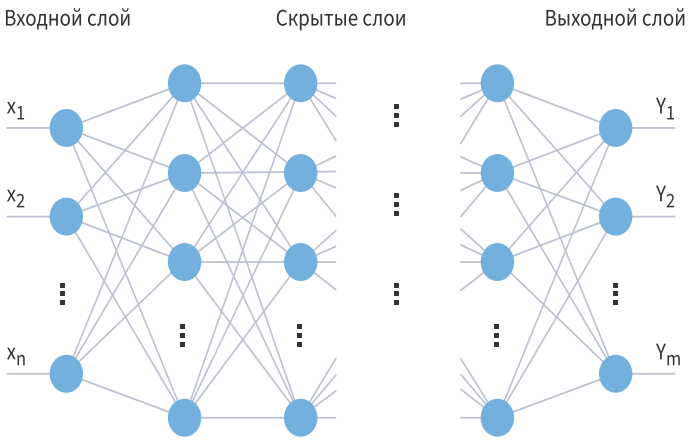


Рис. 2. Архитектура многослойного перцептрона

Так как MLP не является генеративной нейронной сетью, она не способна предоставлять развернутые текстовые ответы в соответствии с обнаруженной ошибкой. Для этого можно создать таблицу или словарь в формате «ключ-значение», где каждому коду ошибки будет соответствовать конкретный текст-шаблон. После обработки нейросетью CDR-файла, специализированный скрипт будет сопоставлять полученную ошибку с готовым шаблоном и подставлять в него необходимые данные об абонентах.

Рассмотрим, какая техническая реализация может быть у предложенного алгоритма, который будет использоваться сотрудником, отвечающим за траблшутинг аварий, связанных с короткими сообщениями. Инженеру поступает обращение, в котором указано, что в операторской сети произошел сбой, и в течение определенного времени, допустим, одного часа, на абонента с конкретным MSISDN не поступают A2P SMS от служб-рассыльщиков.

Сотрудник, которому необходимо выяснить причину аварии, загружает в нейронную сеть CDR-файл (или использует скрипт для оптимизации времени, затраченного на поиск и форматирование нужных данных за конкретный промежуток времени), который представляет собой текстовый файл, динамически заполняемый центром обработки кротких сообщений за определенный промежуток времени. Чаще транзакции записываются в один файл формата.csv в течение часа, после чего создается новый файл. В сети крупного оператора CDR-файл, записанный за один час, может содержать несколько миллионов транзакций, имеющих формат, представленный на рисунке 3 (конфиденциальные данные пользователей были изменены в целях соблюдения законов о безопасности персональных данных):

```
send_mt.log.gz:2025-02-05 09:49:38.718;SendMT;data;0;5;1;operator;
1;1;2222222222;3333333333;4444444444;5555555555;0;;;;1/1;0;0;0;-1;0;;-1;0;0;-1;-1;1;2222
222222_66666;0;77777;2222222222;;;;-1;4;4444444444;2222222222;;-1;-1;-1;12107;
```

Рис. 3. Пример одной транзакции в CDR-файле

Нейронная сеть получает на входной слой файл в формате csv, содержащий сигнализационную информацию о транзакциях, совершенных в течение одного часа, анализирует полученные данные, передавая на выходной слой ошибку, получаемую во время передачи коротких сообщений и протокол, по которому она пришла. Пример вывода нейросети может иметь следующий вид: MAP 27 [4]. После чего срабатывает скрипт, который ищет соответствия по имеющимся у него в таблице кодам ошибки и подходящим

к ним шаблонам (Таблица 1). В выбранный шаблон скрипт подставляет персональные данные из CDR-файла, такие как IMSI и MSISDN отправителя и получателя, также он будет содержать рекомендации о причинах аварий и рекомендации по их устранению. Этот шаблон и выводится сотруднику в качестве результата обработки (рис. 4).

ТАБЛИЦА 1. Пример табличного сопоставления кода ошибки и текстового шаблона

Код ошибки	Текстовый шаблон
MAP 13	Для абонента < IMSI > вызов запрещен. Вероятно, на счете абонента недостаточно средств или проблемы с Billing-сервером или с маршрутизацией на MSC
MAP 27	Доставка SMS до абонента < MSISDN > невозможна, так как абонент не зарегистрирован в сети или отключен

```
Доставка SMS до абонента 2222222222 невозможна, так как абонент не зарегистрирован в сети или отключен
```

Рис. 4. Итоговый результат обработки для сотрудника

Предложенный в данной статье алгоритм анализа CDR-файлов с использованием нейронной сети позволит инженеру технической поддержки избежать длительного поиска необходимых параметров, а также упростить первичный анализ причины неисправности. Благодаря практической реализации данного алгоритма станет возможно существенно оптимизировать процесс выявления проблемы и минимизировать участие инженера в анализе CDR-файлов для более продуктивного распределения рабочего времени на решение более трудных задач.

Список используемых источников

1. 3GPP TS 23.040 V16.0.0 (2019-06). Technical Specification Group Core Network and Terminals; Technical realization of the Short Message Service (SMS); Stage 2. URL: https://www.3gpp.org/ftp/Specs/archive/23_series/23.040/ (дата обращения 28.04.2025).

2. SMPP Developers Forum. Short Message Peer-to-Peer Protocol Specification v3.4. 1999. URL: https://smpp.org/SMPP_v3_4_Issue1_2.pdf (дата обращения 28.04.2025).

3. Хайкин С. Нейронные сети: полный курс / Саймон Хайкин; пер. с англ. – 2-е изд. М.: ООО «И.Д. Вильямс», 2006. 1104 с.

4. Бишоп К. Распознавание образов и машинное обучение / Кристофер М. Бишоп; пер. с англ. М.: Издательский дом «Вильямс», 2011. 738 с.

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

УДК 621.39

Н. С. Васильев (студент группы ИКФ-11 СПбГУТ)
В. Г. Нестеров (студент группы ИКТФ-46м СПбГУТ), nesterov.vg@sut.ru

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ ПРЕДВАРИТЕЛЬНОГО ОПТИЧЕСКОГО УСИЛИТЕЛЯ EDFA

Работа посвящена практической оптимизации параметров предварительных оптических эрбиевых усилителей (EDFA), предназначенных для одновременного усиления большого количества каналов в современных волоконно-оптических систем связи (ВОСС) с технологией плотного мультиплексирования в волновой области (DWDM). Целью оптимизации является увеличение длины регенерационного участка ВОСС при минимизация технических и экономических ресурсов. К оптимизируемым параметрам предварительных оптических эрбиевых усилителей (ПОУ) относятся: коэффициент усиления, уровень накачки, частотная характеристика выравнивающего фильтра и шум-фактор. Оптимизация проводится для параметров конкретных ВОСС и ее компонентов, таких, как количество каналов, интервал между каналами, затухание в демультиплексорах (DMUX), пороговая чувствительность фотоприемного устройства (ФПУ), требуемое оптическое отношение сигнала к шуму (OSNR) и энергетический запас. В работе проведены: теоретическое обоснование оптимизации, имитационное моделирование ПОУ отдельно и в составе ВОСС, а также анализ полученных результатов.

волоконно-оптическая система связи (ВОСС), предварительный оптический усилитель (ПОУ), выравнивающий оптический фильтр (ОФ), одномодовое оптическое волокно (ОВ)

OPTIMIZATION OF EDFA OPTICAL PRE-AMPLIFIER PARAMETERS

Vasiliev N., Nesterov V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper is devoted to the practical optimization of erbium-doped optical pre-amplifier (EDFA) parameters designed for simultaneous amplification of a large number of channels in modern fiber-optic communication systems (FOCS) using dense wave-domain multiplexing (DWDM) technology. The goal of the optimization is to increase the length of the FOCS regeneration section while minimizing technical and economic resources. The parameters of the erbium-doped optical pre-amplifier (EDFA) to be optimized include gain, pump level, equalization filter frequency response, and noise figure. Optimization is performed for parameters of specific fiber-optic communication systems (FOCS) and their components, such as the number of channels, channel spacing, demultiplexer attenuation (DMUX), photodetector threshold sensitivity (PDT), required optical signal-to-noise ratio (OSNR), and power margin. The paper includes a theoretical justification for the optimization, simulation modeling of the PDT separately and as part of the FOCS, and an analysis of the obtained results.

Fiber-optic communication system (FOCS), optical preamplifier (OPA), optical equalization filter (OF), single-mode optical fiber (SMF)

Оптимизируемые элементы ПОУ и их параметры

Оптимизация предварительного оптического усилителя (ПОУ) является многовариантной задачей, и требует обоснованного выбора элементов и их параметров.

- эрбиевое волокно, его тип и длина l_{ob};
- источник накачки, длина волны λ_p и уровень мощности p_p;
- коэффициент усиления ПОУ g, дБ;
- диапазон равномерно усиливаемых длин волн $\Delta\lambda$.

Критериями оптимизации являются минимизация: стоимости, расхода материалов и комплектующих, энергопотребления и т.п. при безусловном достижении требуемого качества связи в ВОСС, в которой будет использоваться ПОУ.

Описание схемы исследования

На рис. 1 показана схема исследования однокаскадного ОУ EDFA с попутной накачкой в моделирующей программе (GainMaster) [1]. В предварительном исследовании использован источник излучения накачки (Pump) с уровнем мощности p_p = 20 дБм (100 мВт) на длине волны 980 нм. Выбираем из [1] эрбиевое оптическое волокно (ОВ) Generic *I*-4 с рекомендуемой длиной l_{ob} = 10 м. В программе используется многоканальный источник оптического излучения (Multiple Source), перекрывающий весь *C* диапазон длин волн от λ = 1520 до 1560 нм с интервалом $\Delta\lambda$ = 0.4 нм ($\Delta\nu$ = 50 ГГц), с уровнем входного сигнала p = -30 дБм (1 мкВт).

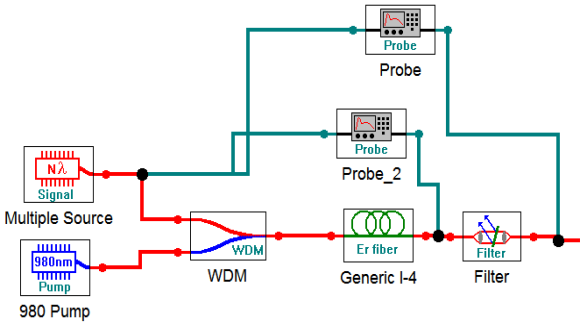


Рис. 1. Схема ПОУ EDFA с попутной накачкой

В схему входит мультиплексор WDM для объединения излучений сигнала и накачки, выравнивающий фильтр (GFF Filter) и измерительные приборы Probe.

На рис. 2 показана зависимость уровня мощности на выходе эрбиевого ОВ, исходя из которой можно определить оптимальные интервалы длин волн для различного количества каналов DWDM.

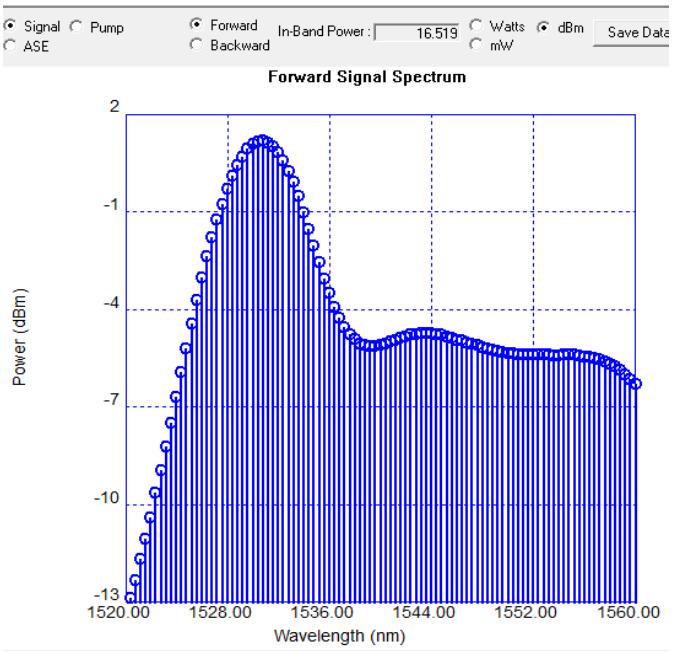


Рис. 2. Зависимость уровня мощности сигнала на выходе ОУ EDFA от длины волны для M = 100 каналов с интервалом $\Delta\nu_c$ = 50 ГГц

Рассчитаем диапазон усиливаемых ОУ длин волн для n = 1, 8, 16, 40 и 80 каналов с интервалом между каналами $\Delta\nu_c$ = 50 ГГц ($\Delta\lambda_c$ = 0.4 нм)

$$\Delta\nu = n\Delta\nu_c \quad \Delta\lambda = n\Delta\lambda_c \tag{1}$$

Проведем выбор оптимальных значений минимальной λ_{min} и максимальной λ_{max} длин волн для рассчитанного значения $\Delta\lambda = \lambda_{max} - \lambda_{min} + \Delta\lambda_c$. Критерием выбора является минимальная разница Δp в дБ между максимальным p_{max} и минимальным p_{min} сигналами на выходе эрбиевого ОВ. Результаты приведены в таблице 1.

ТАБЛИЦА 1. Результаты выбора диапазонов усиливаемых ПОУ длин волн

n	1	8	16	40	80
$\Delta\lambda$, нм	-	3.2	6.4	16	32
λ_{min}, нм	1530.8	1529.6	1527.2	1524.8	1524.4
λ_{max}, нм	1530.8	1532.4	1533.2	1540.4	1556.0
p_{max}, дБм	12.6	8.08	5.9	4.0	2.3
Δp, дБ	0	0.71	2.5	6.3	6.8

Теоретическое описание сигналов, шумов и параметров ПОУ

Определим минимальный уровень канального сигнала на выходе ВОЛТ с технологией DWDM (на входе демультиплексора) p_{s_min} и максимально допустимый уровень усиленного спонтанного излучения (УСИ) p_{sp_max}, при котором ПОУ не нужен. Задаемся параметрами транспондера: пороговым уровнем p_{pr} и требуемым оптическим отношением сигнала к шуму $osnr_T$, а также энергетическим запасом a_3 и потерями в демультиплексоре $a_{DMUX.}$

$$p_{s\_min} = p_{pr} + a_3 + a_{DMUX}, \qquad p_{sp\_max} = p_{s\_min} - osnr_T \tag{2}$$

Для ВОСС со скоростью передачи B = 10 Гбит/с типичные значения параметров p_{pr} = –25 дБм, a_3 = 5 дБ, a_{DMUX} = 5 дБ, требуемое оптическое отношение сигнала к шуму $osnr_T$ > 12.2 дБ [2]. Примем коэффициент шума ПОУ nf = *5* дБ. Тогда из (2) получим p_{s_min} = -15 дБм и p_{sp_max} = –27.2 дБ.

Определим необходимый коэффициент усиления g и получаемое при этом $osnr_{out}$ на выходе ПОУ, если входной сигнал p_s меньше p_{s_min}, а $osnr_{in} > osnr_T + nf$ = 17.2 дБ.

$$g = p_{s\_min} - p_s = p_{pr} + a_3 + a_{DMUX} - p_s \qquad osnr_{out} = osnr_{in} + nf \tag{3}$$

Рассмотрим однопролетную ВОСС, в которой уровень сигнала УСИ на входе ФПУ определяется только ПОУ (накопленным от предыдущих пролетов УСИ пренебрегаем). Определим уровни сигнала $p_{sФ}$ и УСИ $p_{spФ}$, а также $osnr_Ф$ на входе ФПУ и укажем ограничения на величины $p_{sФ}$ и $osnr_Ф$.

$$p_{sФ} = p_s + g - a_{DMUX} > p_{pr} + a_3 \quad p_{spФ} = -58 + nf + g - a_{DMUX} \tag{4}$$

$$osnr_Ф = p_{sФ} - p_{spФ} = p_s + 58 - nf > osnr_T \tag{5}$$

Из неравенства (5) выразим минимальную величину сигнала на выходе однопролетного ВОЛТ p_{s1} (входе демультиплексора) и необходимую для этого сигнала величину коэффициента усиления по (3)

$$p_{s1\_min} = -58 + nf + osnr_T \qquad g_{1max} = p_{pr} + a_3 + a_{DMUX} + 58 - nf - osnr_T \tag{6}$$

Тогда из (6) получим p_{s1_min} = –40.8 дБм и g_{1max} = 25.8 дБ.

Исследование ПОУ для ВОСС со скоростью передачи B_c = 10 Гбит/с

В программе GainMaster исследованы схемы ПОУ для ВОСС с количеством каналов M = 1, 8, 16, 40 и 80. Был выбран входной сигнал p_s = –30 дБм. Для каждого ПОУ индивидуально подбирались параметры выравнивающего фильтра GFF. Подбором уровня накачки на длине волны λ_p = 980 нм добивались уровня выходного сигнала ПОУ примерно p_{out} = –5.5…– 6.5 дБм и коэффициента усиления ПОУ g = 23.4…24.4 (при M > 1). Результаты исследования ПОУ приведены в таблице 2.

ТАБЛИЦА 2. Результаты исследований ПОУ для ВОСС с B_c = 10 Гбит/с

Кол-во каналов, M	Уровень накачки, p_p, дБм	Мощн. накач., мВт/ на 1 канал	Вых. уров. сигн., p_{s_out}, дБм	Сум. вых. уров. сигн. p_{s_Σ}, дБм	Коэф. усил. g, дБ	Коэф. шума, nf, дБ
1	8	6.3	– 8	– 8	22.0	4.3
8	10	1.25	– 6.6	2	23.4	4
16	13	1.25	– 5.5	6.6	24.4	3.7
40	17	1.25	– 6.5	9.5	23.4	3.5
80	20	1.25	– 5.6	13.4	24.4	3.4

Из таблицы 2 видно, что при увеличении количества каналов в ВОСС в ПОУ с примерно одинаковыми коэффициентами усиления g и шум-факторами nf необходимо увеличивать мощность накачки p_p прямо пропорционально количеству каналов.

Исследование 8-канальной ВОСС со скоростью B_c = 10 Гбит/с

Для проверки правильности проведенных расчетов ПОУ проведено моделирование ВОСС (рис. 3) в программе OptiSystem [3]. Схема включает 8 передатчиков (Transmitter), терминальный мультиплексор (WDM Mux), ВОЛТ, включающий стандартное (SF) и компенсирующее (DCF) ОВ, ПОУ с g = 30 дБ, демультиплексор (WDM Demux) и ФПУ с p-i-n ФД. Интервал между каналами $\Delta\nu_c$ = 50 ГГц, Длина ОВ SF l_{ov} = 150 км. Целью исследований является определение зависимости качества связи от уровня входного сигнала ПОУ p_{s_in} и его коэффициента усиления g.

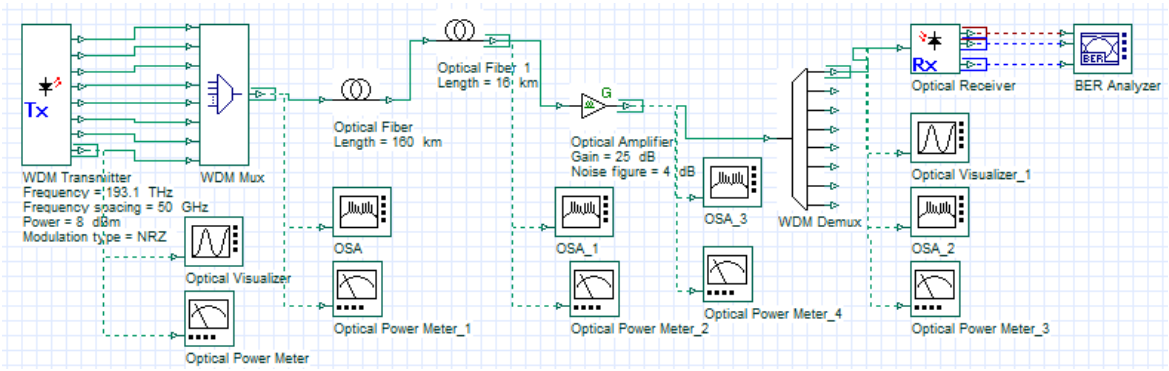


Рис. 3. Схема 8-канальной ВОСС со скоростью 10 Гбит/с и протяженностью 150 км

ТАБЛИЦА 3. Результаты исследования ВОСС (все параметры приведены ко входу и выходу ПОУ).

p_{s_in}, дБм	$osnr_{in}$, дБ	g, дБ	p_{s_out}, дБм	$osnr_{out}$, дБ	$p_{s\_ф}$, дБм	Q
– 30.5	29.5	25	– 5.5	23	– 11	15
– 30.5	29.5	20	– 10.5	23.5	– 15.5	13
– 30.5	29.5	30	– 0.5	23.5	– 5.5	17
– 34.0	29.5	25	– 7.5	21.5	– 13.5	11
– 36.5	29.5	25	– 11.5	17.5	– 16.5	8
– 38.5	29.5	25	– 13.5	15.5	– 18.5	7
– 38.5	29.5	30	– 8.5	15.5	– 13.5	6.5

Исследования показали, что использование ПОУ очень эффективный способ повышения качества связи для ВОСС с последним пролетом большой протяженности при слабых сигналах. Результаты моделирования в основном подтверждают правильность теоретических расчетов. Например, минимальный сигнал на входе ПОУ составил $p_{s\_min} = –38.5$ дБм оказался немного больше теоретического –40.8 дБм.

Список используемых источников

1. Gainmastertm Amplifier design software manual revision 1.1, 2004

2. Трещиков В. Н., Листвин В. Н. DWDM-системы, Четвертое издание, Москва: Техносфера. 2021. 29 с.

3. OptiSystem User Guide and Reference Manual. Optical Communication System Design Software. Version 19. Optiwave Systems Inc. 2022.

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

УДК 004.7:504.75

А. Н. Волков (д.т.н., доцент кафедры СС и ПД, СПбГУТ), volkov.an@sut.ru
Д. В. Маршев (студент группы ИКТУ-13, СПбГУТ), marshev.dv@sut.ru

ПРОБЛЕМАТИКА ИНТЕГРАЦИИ ЗЕЛЕНЫХ ИКТ В ПЕРСПЕКТИВНЫЕ СЕТИ СВЯЗИ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Статья посвящена проблемам интеграции зеленых ИКТ в перспективные сети связи. Рассматриваются ключевые вызовы, такие как высокое энергопотребление, углеродный след и парадокс Джевонса, а также анализируются современные методы и стандарты для повышения экологической устойчивости телекоммуникационной инфраструктуры. Особое внимание уделяется роли Международного союза электросвязи (МСЭ) в разработке стандартов и рекомендаций для зеленых ИКТ. Статья предлагает комплексный подход к решению экологических и экономических задач, стоящих перед отраслью связи.

ИКТ, зеленые ИКТ, сети 6G/IMT-2030, сети нового поколения, энергоэффективность, устойчивое развитие, стандарты связи

INTEGRATION CHALLENGES AND PERSPECTIVES OF GREEN ICT IN NEXT-GENERATION COMMUNICATION NETWORKS

Volkov A., Marhsev D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article focuses on the challenges of integrating Green ICT into next-generation communication networks. It examines key issues such as high energy consumption, carbon footprint, and the Jevons Paradox, while analyzing modern methods and standards for enhancing the environmental sustainability of telecommunication infrastructure. Special attention is given to the role of the International Telecommunication Union (ITU) in developing Green ICT standards and guidelines. The paper proposes a comprehensive approach to addressing the ecological and economic challenges facing the telecommunications industry.

Key words: *ICT, Green ICT, 6G/IMT-2030, next-generation networks, energy efficiency, sustainability, telecommunication standards*

Введение

Переход к экологически чистым (зеленым) телекоммуникациям является комплексной задачей, находящейся в поле внимания как ученых-исследователей, так и органов, регулирующих отрасль телекоммуникаций, различных правительственных структур и организаций, занимающихся вопросами устойчивого развития и изменения климата. За последнее десятилетие объем

создаваемых, копируемых и потребляемых данных в мире демонстрирует экспоненциальный рост – от единиц в 2010 году до сотен зеттабайт в 2025 [1], что обусловлено распространением Интернета вещей, развитием искусственного интеллекта (ИИ), расширением облачных сервисов, стриминговых платформ и социальных сетей. Эти технологии требуют огромных вычислительных ресурсов, что, в свою очередь, ведет к увеличению энергопотребления. Стабильный рост пользователей услуг мобильной связи и подключенных устройств (Интернет вещей), а также возросшее потребление энергоресурсов сетевой инфраструктурой (базовые станции, маршрутизаторы, ЦОДы) привело к увеличению эксплуатационных расходов и росту выбросов CO_2. Согласно ряду исследований на долю сектора ИКТ приходится 1.5-4 % глобальных выбросов CO_2 [2], а на центры обработки данных (ЦОД) и коммуникационные сети приходится 2-3 % мирового потребления электроэнергии [1]. Решением данных экологических и экономических вызовов может стать использование более экологичных телекоммуникационных технологий, что позволит отрасли связи решить проблемы не только негативного воздействия на окружающую среду, но и способствовать созданию более устойчивого энергетического будущего.

Концепция зеленых ИКТ

Зеленые технологии представляют собой практики и методы, направленные на минимизацию негативного воздействия на окружающую среду, связанного с использованием технологий. Концепция зеленых информационно-коммуникационных технологий (ИКТ) рассматривается в узком и широком смысле. Узкое понимание ставит целью развитие технологий, направленных на снижение энергопотребления и углеродного следа телекоммуникационной инфраструктуры. Широкое понимание базируется на принципе системной устойчивости и является наиболее распространенным в современных исследованиях. Современное определение зеленых ИКТ сформировалось в 2020-е годы.

Концепция зеленых ИКТ (англ. Green ICT) получила широкое признание в научной и отраслевой среде, что подтверждается многочисленными исследованиями и международными стандартами [3], и демонстрирует консенсус в научном сообществе относительно базовых принципов устойчивого развития телекоммуникационных систем. Под «зелеными ИКТ» понимается экологически устойчивый подход к проектированию, производству, эксплуатации и утилизации ИКТ-оборудования и инфраструктуры, направленный на минимизацию их воздействия на окружающую среду. Ключевые аспекты включают повышение энергоэффективности, сокращение углеродного следа, внедрение принципов циркулярной экономики, а также применение возобновляемых источников энергии.

Как свидетельствует анализ научных публикаций, современные исследования в области зеленых ИКТ консолидируются вокруг ключевых направлений, представленных в Таблице 1.

ТАБЛИЦА 1. Основные направления исследований в области зеленых ИК

Направление исследований	Ключевые технологии / методы	Вызовы
Энергоэффективность ИКТ-инфраструктур	Динамическое управление нагрузкой ЦОД. Жидкостное охлаждение серверов Оптимизация алгоритмов облачных вычислений	Высокие капитальные затраты
Утилизация и переработка оборудования	Биоразложение плат Модульный дизайн устройств	Недостаток стандартизированных метрик
Оптимизация ресурсов	Виртуализация сетевых функций Контейнеризация микросервисов ИИ-балансировка нагрузки	Компромисс производительность / энергопотребление
Сертификация и стандартизация	Эко-маркировка	Региональные различия в стандартах
Устойчивый ИВ (IoT)	Энергосбор Сетевые протоколы с низким энергопотреблением Саморазлагающиеся датчики	Ограниченный срок службы устройств
Просветительские инициативы	Цифровые углеродные калькуляторы Геймификация экопрактик	Низкая осведомленность пользователей

Активное развитие и внедрение зеленых ИКТ ограничивается рядом сложностей, таких как необходимость высоких первоначальных затрат на внедрение зеленых ИКТ, отсутствие стандартизированных показателей для оценки энергоэффективности, а также ограниченная осведомленность и принятие практик зеленых ИКТ и Интернета вещей [3].

Более того, развитие энергоэффективных (зеленых) ИКТ сталкивается с фундаментальным противоречием – технологическая оптимизация не приводит к снижению общего энергопотребления, а зачастую стимулирует его рост. Этот эффект, известный как парадокс Джевонса (Jevons Paradox), особенно ярко проявляется в сфере облачных вычислений и искусственного ин-

теллекта [4]. В контексте ИКТ это означает, что оптимизация энергопотребления процессоров, ЦОДов и сетей может стимулировать еще больший спрос на вычисления, а не приносить экономические выгоды. Можно предположить, что зеленые ИКТ требуют не только инженерных решений, но и системного пересмотра подходов к цифровизации.

Роль МСЭ в разработке стандартов 6G/IMT-2030

Международный союз электросвязи (МСЭ) играет ключевую роль в формировании экологических стандартов для телекоммуникаций. Важным шагом является инициатива МСЭ 6G/IMT-2030 (International Mobile Telecommunications-2030), направленная на разработку стандартов и требований для будущих поколений беспроводных коммуникационных технологий, включая шестое поколение мобильной связи (6G), что предполагает создание универсальной и надежной экосистемы связи, способной удовлетворять потребности цифрового мира будущего. Особое внимание уделяется созданию сетей, которые способны эффективно управлять ресурсами и минимизировать свое воздействие на окружающую среду. Использование возобновляемых источников энергии и экологически чистых технологий позволит сделать телекоммуникационную инфраструктуру более устойчивой и снизить углеродный след. В сетях связи 2030 года (6G/IMT-2030) ключевыми технологиями для обеспечения более высокой производительности и новых типов услуг в сетях следующего поколения будут являться искусственный интеллект и машинное обучение, применяемые для интеллектуального управления потоками трафика и оптимизации сетевых процессов, квантовые компьютеры, нанотехнологии, сверхплотные сети (англ. UDN, Ultra-Dense Networks) и сети с ультрамалыми задержками (англ. ULLC, Ultra-Low Latency Communications) [5, 6, 7].

Стандартизация сетей 5G/IMT-2020 и 6G/IMT-2030 является критическим важным для обеспечения надежной, эффективной и безопасной связи. Она позволит не только интегрировать существующие технологии, но и подготовить инфраструктуру для будущих инноваций, способствующих появлению новых услуг и приложений в сфере телекоммуникаций.

Международная стандартизация зеленых ИКТ

Основу для сертификации зеленых решений закладывает МСЭ (англ. ITU-T, International Telecommunication Union – Telecommunication Standardization Sector). Он разрабатывает рекомендации по устойчивым телекоммуникациям в рамках рабочей группы по экологической эффективности (англ. FG-EE, Focus Group on Environmental Efficiency) и серии стандартов L.1400

[8]. Серия L.1400 охватывает такие направления, как методики оценки воздействия ИКТ на окружающую среду (L.1400), оценку энергопотребления сетей (L.1410), измерение углеродного следа ИКТ (L.1420) и повышение энергоэффективности центров обработки данных (L.1430). В рамках исследовательской группы ITU-T Study Group 5 (SG5) «Окружающая среда, изменение климата и экономика замкнутого цикла» разрабатываются рекомендации по зеленым ИКТ и исследуется воздействие систем типа «Интеллектуальные здания» на энергозатраты.

Заключение

Таким образом, внедрение зеленых ИКТ в перспективные сети связи требует комплексного подхода, направленного на развитие новых технологических решений, унификацию зеленых стандартов и поиск путей преодоления парадокса Джевонса. Зеленые ИКТ могут стать одним из стратегических факторов конкурентоспособности телекоммуникационной отрасли в эпоху цифровой трансформации.

Список используемых источников

1. World Economic Forum. Data growth drives ICT energy innovation. 22.05.2024. URL: https://www.weforum.org/stories/2024/05/data-growth-drives-ict-energy-innovation/ (дата обращения 02.05.2025).

2. World Bank, International Telecommunication Union. Measuring the Emissions and Energy Footprint of the ICT Sector: Implications for Climate Action. 2024. URL: http://hdl.handle.net/10986/41238 (дата обращения 02.05.2025).

3. Ghansawant V. Green Computing: Current Research Trends // International Journal of Science and Research (IJSR). 2021. Vol. 10. № 7. P. 1-3. DOI: 10.21275/MR21709173309.

4. Luccioni A., Strubell E., Crawford K. From Efficiency Gains to Rebound Effects: The Problem of Jevons' Paradox in AI's Polarized Environmental Debate // ArXiv. 2025. URL: https://doi.org/10.48550/arXiv.2501.16548 (дата обращения 02.05.2025).

5. Волков, А. Н. Сети связи пятого поколения: на пути к сетям 2030 / А. Н. Волков, А. С. А. Мутханна, А. Е. Кучерявый // Информационные технологии и телекоммуникации. 2020. Т. 8, № 2. С. 32–43. DOI:10.31854/2307-1303-2020-8-2-32-43. EDN:ZWNTDB.

6. Искусственный интеллект в сетях связи пятого и последующих поколений / А. С. Бородин, А. Н. Волков, А. С. А. Мутханна, А. Е. Кучерявый // Электросвязь. 2021. № 1. С. 17-22. DOI:10.34832/ELSV.2021.14.1.001. EDN:JDHISS.

7. Abdellah Ali R., Koucheryavy A.: Artificial Intelligence Driven 5G and Beyond Networks // Telecom IT. 2022. Vol. 10. № 2. PP. 1-13. DOI:610.31854/2307-1303-2022-10-2-1-13. EDN:VAFXSU.

8. ITU-T Recommendation L.1400: Methods for evaluating environmental impact of ICTs. Geneva: International Telecommunication Union, 2023. URL: https://www.itu.int/rec/T-REC-L.1400-2023/en (дата обращения 02.05.2025).

УДК 654.739

Р. Р. Зайдуллин (студент группы ИКТС-33м, СПбГУТ), zaidullin@sut.ru

МОДЕЛЬ РАСПРЕДЕЛЕННОГО УПРАВЛЕНИЯ СЕТЕВОЙ НАГРУЗКОЙ С ПРИМЕНЕНИЕМ ПРИНЦИПОВ ТЕОРИИ ХАОСА

Управление распределенными сетями в условиях нестабильной нагрузки остается одной из ключевых задач современной телекоммуникационной инфраструктуры. Статические алгоритмы и централизованные методы не всегда справляются с быстрыми изменениями трафика. В этой связи растет интерес к самоорганизующимся моделям, основанным на теории хаоса, которая позволяет строить адаптивные стратегии управления за счет высокой чувствительности системы к начальному состоянию.

управление сетью, теория хаоса, логистическая модель, адаптивные системы

A DISTRIBUTED NETWORK LOAD MANAGEMENT MODEL USING CHAOS THEORY PRINCIPLES

Zaydullin R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Managing distributed networks under unstable loads remains a key challenge for modern telecommunications infrastructure. Static algorithms and centralized methods cannot always cope with rapid traffic changes. Therefore, there is growing interest in self-organizing models based on chaos theory, which enables the development of adaptive control strategies due to the system's high sensitivity to the initial state.

Key words: *network management, chaos theory, logistic model, adaptive systems.*

Для практической реализации подхода управления сетью на основе теории хаоса предлагается рассмотреть сеть как совокупность взаимодействующих узлов, в каждом из которых происходит изменение нагрузки во времени. Под нагрузкой будем понимать относительный объем трафика, обрабатываемого узлом, нормированный на диапазон от 0 до 1. Поведение каждого узла зависит от текущего состояния и управляющего параметра, который корректируется в ответ на изменение условий – например, рост локального трафика, снижение пропускной способности, изменения в маршрутизации.

Основная идея заключается в том, чтобы вместо фиксированных или линейных правил управления использовать нелинейную динамику – хаотическую модель, способную к самоорганизации [1]. Для этого применяется логистическое отображение, о котором говорилось в предыдущем разделе. Оно позволяет формировать динамическое поведение узлов: при определенных параметрах система входит в устойчивое или колебательное состояние, а при других – демонстрирует хаотическую активность, благоприятную для адаптации и равномерного распределения нагрузки.

Чтобы проанализировать поведение такой системы, смоделируем сеть из пяти узлов, каждый из которых управляется на основе хаотической модели. Начальная нагрузка узлов устанавливается случайным образом в диапазоне от 0.1 до 0.9. Управляющий параметр r выбирается в диапазоне, соответствующем области хаотического режима (в частности, $r = 3.7$). Система моделируется на 50 шагов времени. Для сравнения проводится параллельный эксперимент: вторая модель использует те же начальные условия, но без какого-либо управления – нагрузка на узлы снижается линейно, имитируя пассивную деградацию [2].

На рисунке 1 изображен график (логистическая карта) – классическое представление зависимости устойчивости системы от параметра r (рис. 1). Данная карта позволяет выбрать режимы работы сети: при $r < 3.57$ система ведет себя устойчиво или периодически, а при $r > 3.57$ – переходит в хаотическое поведение [3]. Эта граница (обозначена вертикальной линией) критична для настройки модели, поскольку хаос, в данном контексте, означает повышенную чувствительность к текущему состоянию узла, что и требуется для гибкого управления.

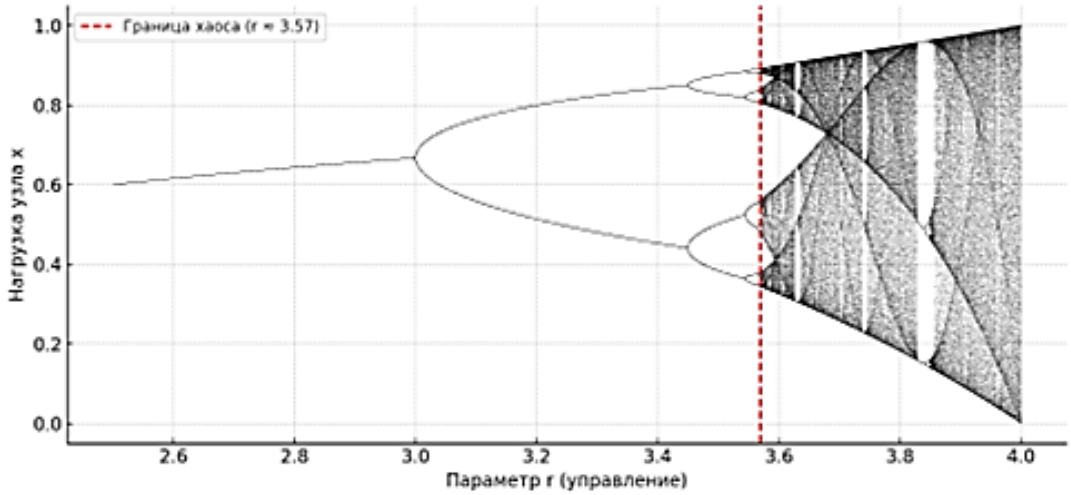


Рис. 1. Логическая карта: устойчивое и хаотическое поведение узла в зависимости от параметра r

На рисунке 2 представлен график динамики изменения нагрузки узлов в течение времени в двух моделях: с использованием хаотического управления (сплошные линии) и без него (пунктирные линии).

Видно, что хаотическая модель поддерживает активность узлов, обеспечивая постоянное перераспределение нагрузки и предотвращая резкое снижение (рис. 2). В отличие от нее, система без управления демонстрирует затухание, что может привести к снижению эффективности передачи данных [4].

Описанная модель позволяет реализовать адаптивную систему управления, в которой каждый узел реагирует на изменения в сети на основе внутренней логики, заложенной в хаотическом отображении. Это делает возможным повышение устойчивости всей сети без необходимости в централизованном контроле или заранее заданных правилах поведения.

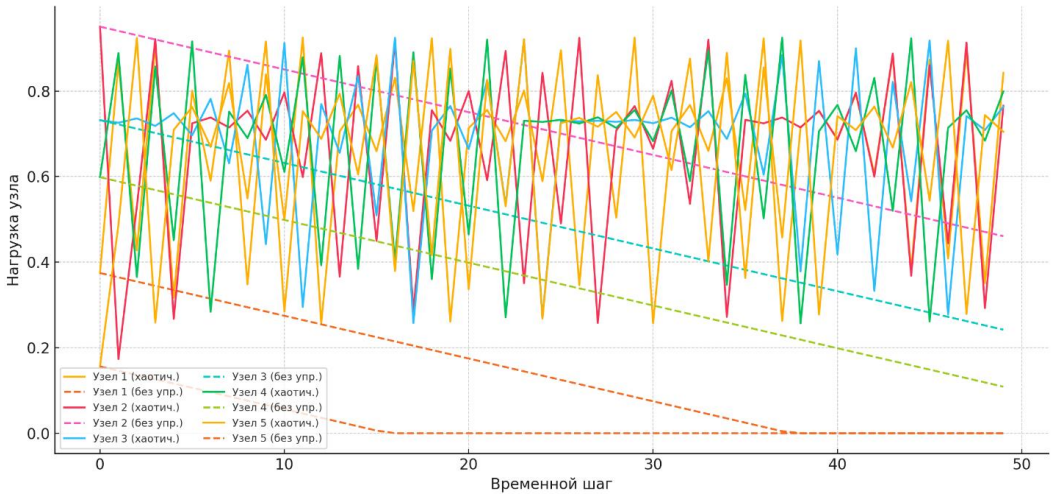


Рис. 2. График динамики нагрузки: хаотическое управление против статического

Для проверки эффективности предложенной модели управления сетью на основе хаотической динамики были проведены имитационные эксперименты. Основной задачей являлось оценить способность системы к восстановлению после перегрузки, а также ее поведение в условиях изменяющейся нагрузки.

Как было сказано ранее, сеть представлялась в виде множества узлов, каждый из которых управлялся локально, на основе логистического отображения. Начальные условия моделировали реальную сетевую ситуацию: часть узлов (в данном случае три из пяти) начинала с высокой степени загрузки – выше 85 %, в то время как остальные находились в стабильном состоянии.

Система моделировалась на 60 шагов времени. Управляющий параметр r поддерживался на уровне 3.7, что соответствует режиму хаотического поведения согласно логистической карте, изображенной на рисунке 1 ранее. Это позволяло каждому узлу адаптивно реагировать на собственную загрузку, изменяя поведение без централизованного вмешательства.

На рисунке 3 показан график динамики восстановления нагрузки узлов после перегрузки.

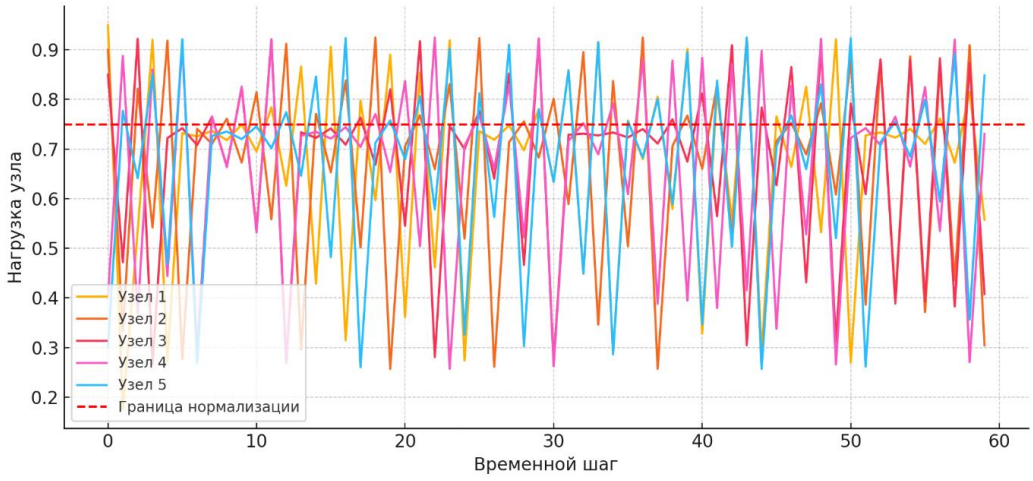


Рис. 3. График восстановления нагрузки узлов после перегрузки при хаотическом управлении

Видно, что система в целом демонстрирует стремление к нормализации: перегруженные узлы постепенно снижают свою нагрузку, а менее нагруженные входят в активный режим, перераспределяя трафик (рис. 3). Красная пунктирная линия обозначает условную границу "нормализации", за которую система выходит уже на 20–25 шаге. Характерные колебания нагрузки вблизи этой границы указывают на наличие внутренней регуляции, обусловленной хаотической природой управления.

Важное преимущество хаотического управления заключается в том, что при отсутствии жестких правил или централизованного контроля, система способна адаптироваться и выходить из критических состояний, используя только локальные параметры и поведение каждого узла. Это подтверждается наблюдаемым эффектом восстановления: узлы синхронно адаптируются, уменьшая разброс по нагрузке и повышая общую устойчивость.

Таким образом, экспериментально-теоретическая модель продемонстрировала ключевое свойство: способность к самоорганизующемуся поведению, при котором система стабилизируется не в результате внешнего вмешательства, а благодаря заложенной в нее внутренней динамике. Это делает предложенный подход перспективным для применения в реальных распределенных сетях, особенно в условиях непредсказуемых нагрузок или отказов.

Список используемых источников

1. Тюрин Ю. Н. Теория хаоса и фракталы. М.: Наука, 2006. 272 с.

2. Завьялов В. В. Математическое моделирование процессов управления в распределенных системах. СПб.: Лань, 2015. 312 с.

3. Николаев С. Ю. Логистическая карта как инструмент анализа поведения телекоммуникационных систем // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2019. Т. 19. № 4. С. 55–62.

4. Фролов В. А. Хаотические процессы и их применение в информационных системах // Информационные технологии. 2020. № 3. С. 45–50.

Статья представлена научным руководителем, доцентом кафедры ИКС СПбГУТ, кандидатом технических наук Кисляковым С. В.

УДК 654.739

Захаров Е. С. (студент группы ИКТК-11, СПбГУТ) zakharov@niuitmo.ru

ПРИМЕНЕНИЕ LSTM ДЛЯ АНАЛИЗА И ПРОГНОЗИРОВАНИЯ В РАСПРЕДЕЛЕННЫХ СЕТЯХ

Современные телекоммуникационные сети, включая 5G/6G, IoT и облачные сервисы, требуют инновационных подходов к мониторингу. Традиционные методы, такие как SNMP и NetFlow, демонстрируют ограниченность в прогнозировании инцидентов. Внедрение LSTM-сетей (Long Short-Term Memory) открывает возможности для предиктивного анализа и автоматизации через SDN (Software-Defined Networking). Цель работы – разработка архитектуры системы мониторинга, сочетающей LSTM для прогнозирования и SDN для автоматического реагирования.

LSTM, SDN, предиктивный мониторинг, сетевые технологии, машинное обучение

APPLYING LSTM TO ANALYSIS AND FORECASTING IN DISTRIBUTED NETWORKS

Zakharov E.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Modern telecommunications networks, including 5G/6G, IoT, and cloud services, require innovative monitoring approaches. Traditional methods such as SNMP and NetFlow have demonstrated limitations in predicting incidents. The introduction of LSTM (Long Short-Term Memory) networks opens up opportunities for predictive analysis and automation via SDN (Software-Defined Networking). The goal of this work is to develop a monitoring system architecture that combines LSTM for prediction and SDN for automated response.

***Key words**: LSTM, SDN, predictive monitoring, network technologies, machine learning*

Проблемы традиционного мониторинга

Традиционные системы мониторинга, такие как SNMP и NetFlow, остаются реактивными, что создает значительные трудности для управления современными сетями. Например, SNMP использует статические пороговые значения для обнаружения проблем, что приводит к генерации большого числа ложных оповещений. Это особенно критично в крупных сетях с сотнями или тысячами устройств, где циклические нагрузки и временные пики могут быть ошибочно интерпретированы как аномалии [1]. Кроме того, NetFlow фокусируется на анализе сетевого трафика, но его эффективность снижается при высокой частоте дискретизации данных. Например, при дискретизации 1:1000 пакетов система может пропустить до 20 % низкоинтенсивных DDoS-атак, что увеличивает время реакции на инциденты до 10–15 минут [2].

Другой важной проблемой является отсутствие комплексного анализа разнородных данных. Метрики устройств (CPU, RAM), сетевой трафик и логи часто анализируются изолированно, что снижает точность прогнозирования [3]. Таким образом, традиционные методы не способны обеспечить предиктивный подход, необходимый для современных распределенных сетей.

Как LSTM решают эти проблемы

LSTM-сети относятся к модифицированным рекуррентным нейронным сетям (RNN), архитектура которых оптимизирована для обработки временных последовательностей. Ключевое отличие от базовых RNN заключается в наличии специализированной структуры, обеспечивающей устойчивое хранение информации в течение длительных временных промежутков. Это позволяет моделям глубоко анализировать динамику временных рядов и выявлять скрытые взаимосвязи в данных, недоступные для традиционных алгоритмов. Подобные возможности делают LSTM перспективным инструментом для прогнозирования критических ситуаций в распределенных сетях – от перегрузок коммутаторов и DDoS-атак до внезапных аппаратных сбоев [4].

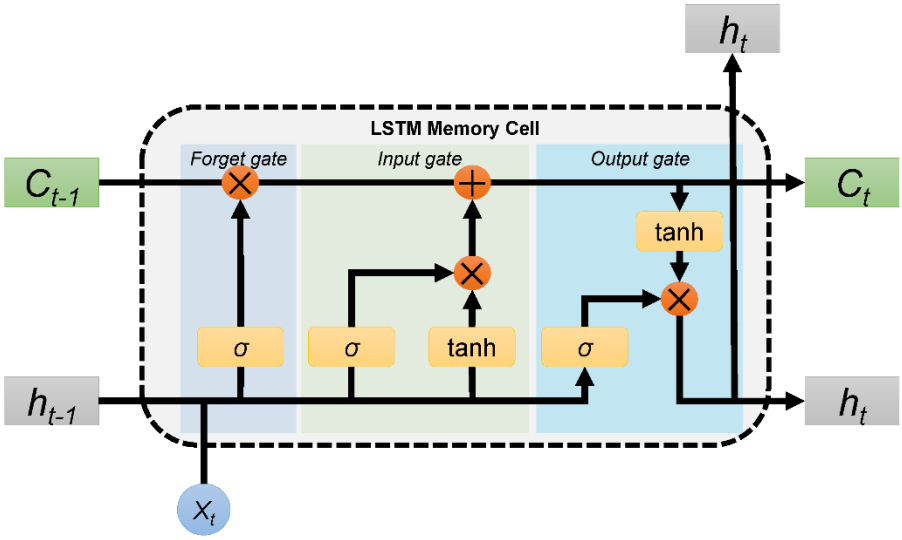


Рисунок 1. Структура LSTM-ячейки [Источник: https://dida.do/what-is-an-lstm-neural-network]
Примечание: Forget gate определяет, какие данные из предыдущего состояния сохраняются;
Input gate контролирует добавление новой информации в память;
Output gate формирует выходное значение

Среди принципиальных достоинств LSTM-архитектур выделяется возможность обработки зависимостей на значительных временных отрезках. Например, модель способна исследовать динамику нагрузки в сетевых узлах за трехдневный период, выявляя критические аномалии: резкий скачок запросов к ресурсам или синхронные колебания в работе смежных узлов. Такой подход обеспечивает точность прогнозирования перегрузок на уровне 92 %, демонстрируя превосходство над устаревшими методами анализа [5].

Интеграция LSTM с сетями с программно-определяемой архитектурой (SDN) создает основу для автоматизации мер реагирования. При обнаружении риска перегрузки коммутационного оборудования за 10 минут до предполагаемого события система SDN динамически перераспределяет до трети трафика по альтернативным каналам, снижая задержку реакции до 1–3 секунд [6]. Эта стратегия превращает сетевую инфраструктуру из системы реагирования на возникшие сбои в систему, способную предотвращать инциденты на докритической стадии. Такой подход становится обязательным условием для функционирования высоконадежных сервисов – удаленной диагностики пациентов или систем управления автономным транспортом, где каждая миллисекунда имеет стратегическое значение.

Результаты и примеры применения

Практическая эффективность LSTM-моделей многократно подтверждена в условиях реальных сетевых инфраструктур. В ходе тестирования на сетях 5G алгоритм продемонстрировал высокую точность прогнозирования сбоев в коммутационных узлах, обрабатывая хронологические данные о трафике за многодневный период. Модель выявила повторяющиеся аномалии нагрузки, связанные с циклами массового подключения пользователей в рабочие часы (с 9:00 до 18:00), включая характерные суточные всплески трафика. Экспериментальные измерения показали точность прогноза в 92 % при среднеквадратичной ошибке 0,08, что напрямую привело к сокращению продолжительности простоев и оптимизации временных параметров реакции системы – задержка снизилась до 5–8 секунд.

Другим примером является использование LSTM для обнаружения DDoS-атак. Модель анализировала пространственную плотность сетевых запросов и выявляла аномальные кластеры, такие как 1000+ запросов в секунду с одного IP-адреса. При этом LSTM подтверждала атаку, сравнивая текущие паттерны трафика с историческими данными о ранее зафиксированных атаках. Время обнаружения составило всего 5 секунд, а время реакции – 8 секунд, что значительно лучше, чем у традиционных методов.

Перспективы развития

Разработка и внедрение LSTM-сетей открывают новые горизонты для мониторинга распределенных сетей. Одним из перспективных направлений является интеграция LSTM с технологиями 6G и edge-вычислениями. Например, перенос обработки данных на edge-устройства (маршрутизаторы, шлюзы) позволит сократить задержки до 5–10 мс и уменьшить

нагрузку на центральные серверы. Локальное выполнение легковесных LSTM-моделей обеспечит фильтрацию трафика и прогнозирование сбоев непосредственно на устройстве, что критично для приложений реального времени, таких как беспилотный транспорт или AR/VR [6].

Кроме того, использование квантовых вычислений может радикально повысить эффективность обучения LSTM-моделей. Квантовые алгоритмы оптимизации способны ускорить обучение в 50–100 раз, что позволит обрабатывать экзабайты данных в реальном времени. Это особенно важно для умных городов и промышленного IoT, где требуется анализ больших объемов данных с минимальными задержками.

Заключение

Использование LSTM-сетей в мониторинге распределенных сетей демонстрирует значительный потенциал для преобразования управления современными телекоммуникационными сетями. Объединение LSTM с программно-определяемыми сетями (SDN) обеспечивает переход от реактивного к предиктивному подходу, что подтверждается теоретическим анализом и модельными сценариями.

Список использованных источников

1. Листровой С. В., Минухин С. В., Листровая Е. С. Разработка метода мониторинга распределенной вычислительной системы на основе определения кратчайших путей и кратчайших гамильтоновых циклов в графе. М.: Научтехиздат, 2015. 14 с.

2. Исаева А. С., Денисенко М. А., Коц И. Н. Testing the layout of the rail condition monitoring system using LSTM recurrent neural networks // St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 2022. Vol. 15, № S3.2. PP. 51–55.

3. Кузнецов А. А., Ковалев С. П. Тестирование и мониторинг в распределенных автоматизированных системах технологического управления / Известия Российской академии наук. Теория и системы управления. 2009. № 5. С. 57–68.

4. Довгаль В. А., Довгаль Д. В. Облако вещей: анализ проблем обеспечения конфиденциальности и безопасности // Информационные системы и технологии в моделировании и управлении: сборник трудов VI Международной научно-практической конференции, Ялта, 24–26 мая 2021 года / Симферополь: ИТ «Ариал», 2021. С. 222–232.

5. Каретников В. В., Будко Н. П., Аллакин В. В. Синтез подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети ведомственного ситуационного центра Электротехника, электронная техника, информационные технологии: сборник научных трудов. 2021. Вып. 7. С. 64–80

6. Сторожук М. Использование систем мониторинга сетей для обеспечения работы критически важных приложений // Первая миля. 2021. № 1. С. 40–44.

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

УДК 004.051

Г. С. Зозуля (студент группы ИКТС-43м, СПбГУТ), zozulya.gs@sut.ru

РАЗРАБОТКА МЕТОДОВ ПРИНЯТИЯ РЕШЕНИЯ ПО МИГРАЦИИ МИКРОСЕРВИСОВ НА СЕТЯХ СВЯЗИ

В связи с активным развитием подходов к созданию сетей связи и инфраструктуры приложений, сфера сетевых технологий претерпела значительные изменения. Одним из главных изменений можно выделить переход от монолитных систем к микросервисной архитектуре. Параллельно с этим, концепция граничных или туманных вычислений приобрела значительную роль, предоставляя возможность снижения задержки и улучшения производительности, особенно для Интернета вещей (IoT) и сервисов реального времени. Данная работа носит обзорный характер и направлена на сравнение существующих алгоритмов принятия решений по миграции микросервисов и их анализ.

микросервисы, миграция, туманные вычисления, алгоритмы миграции, балансировщик нагрузки

DEVELOPMENT OF DECISION-MAKING METHODS FOR MIGRATION OF MICROSERVICES IN COMMUNICATION NETWORKS

Zozulya G.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Due to the rapid development of approaches to creating communication networks and application infrastructure, the field of network technologies has undergone significant changes. One of the key changes is the transition from monolithic systems to microservice architectures. At the same time, the concept of edge or fog computing has gained significant importance, offering the opportunity to reduce latency and improve performance, especially for the Internet of Things (IoT) and real-time services. This paper is a review and aims to compare and analyze existing decision-making algorithms for microservice migration.

Key words: *microservices, migration, fog computing, migration algorithms, load balancer*

Туманные вычисления (Fog computing) – это горизонтальная архитектура системного уровня (рис 1), которая распределяет функции вычислений, хранения, управления и сетевого взаимодействия ближе к пользователям по принципу «облако – вещь» [1]. Структура Fog-сети показана на рис. 1.

При внедрении микросервисной архитектуры на основе туманных вычислений возникает потребность в эффективных методах принятия решений для миграции микросервисов между ядром сети и ее периферией. Эти

методы позволяют поддерживать минимальные потери и низкий уровня задержки, что заявлено одним из приоритетов международных мобильных телекоммуникаций [2]. Но также должны учитывать такие факторы, как состояние сети, доступность ресурсов и требования к приложениям.

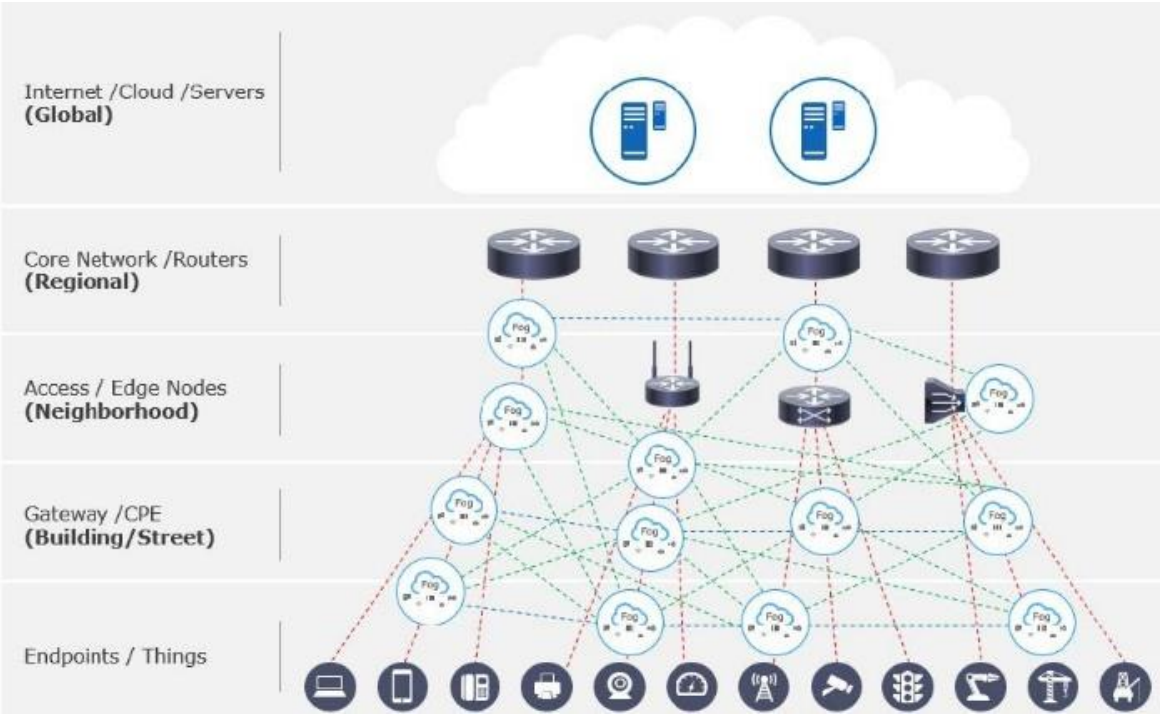


Рис. 1. Структура Fog-сети

Рассмотрим основные мотивы миграции внутри сетей:

1. Масштабирование. Микросервисная архитектура позволяет быстро масштабировать и развертывать новые копии без потери качества при большой нагрузке на систему.

2. Оптимизация задержек. Достигается путем использования ресурсов на периферии с последующим мониторингом.

Однако отсюда вытекают основные проблемы, с которыми сталкиваются разработчики при попытках миграции:

1. Сложность зависимостей между микросервисами, особенно в динамичных средах. Системы и приложения часто имеют сложные многоуровневые или цепочечные зависимости, что затрудняет процесс миграции. Динамичный характер периферийных сред с мобильностью пользователей и изменяющимися условиями сети усугубляет сложность управления зависимостями.

2. Обеспечение высокого уровня QoS. Обеспечение непрерывности обслуживания и минимизация сбоев для пользователей является критически

важной задачей во время миграции. Особенно в мобильных сетях связи, когда пользователь постоянно перемещается, при этом требуя сохранить качество услуг.

3. Угрозы безопасности в распределенной среде. Основные риски для микросервисной архитектуры в Fog сетях связаны с наличием многочисленных независимых сервисов, поэтому важно обеспечить шифрование и защиту при их подключении и миграции [1].

Для учета особенностей и решения основных проблем миграции разработано несколько алгоритмов принятия решений.

1. Алгоритмы, которые учитывают метрики производительности [3]. Основными метриками являются задержка, пропускная способность и использование ресурсов, для координации решения о миграции. Целью координации является минимизация общей задержки (состоящей из задержки вычислений, задержки передачи и задержки миграции) и стоимости миграции. Достигается созданием архитектуры граничных облаков, где в каждом из них находится некоторое количество вычислительных узлов, каждый узел принадлежит только одному облаку. При перемещении объекта, проверяется есть ли на соседнем узле развернутый микросервис, какая задержка до узла и после происходит переключение объекта.

2. Алгоритмы, для оценки производительности микросервисов на основе тестирования в потенциальных средах назначения [4]. В рамках данного подхода используется контроллер для оркестровки запущенных микросервисов, который также имеет доступ к макетной версии каждого из них. Макетная версия создается разработчиком и включает в себя стресс-тесты. Когда оркестратор получает запрос на миграцию, то направляет макет на каждый хост назначения и выполняет привязку макетов. Каждый тест собирает свои результаты и отправляет их обратно на хост исходного микросервиса. На основе полученных результатов микросервис решает, какой из возможных пунктов назначения лучше соответствует его политике.

3. Алгоритмы миграции с учетом зависимостей [5]. В этом подходе создается контролируемая и реалистичная среда для миграции микросервисов между ядром и периферией. Фреймворк iDynamics позволяет моделировать и эмулировать динамические условия графа вызовов и изменчивости межсетевого взаимодействия между узлами. Модульная архитектура фреймворка, включает: анализатор динамики графа, менеджер динамики изменения сети и расширитель политики планирования.

4. Алгоритм с децентрализованной структурой (DMSA) [6]. Цель алгоритма – создать децентрализованную архитектуру для эффективного управления микросервисами на пограничных узлах. В ней переработаны стандартные модули обнаружения и мониторинга, а функции планирования делегированы распределенным агентам микросервисов. Основные функции выполняются динамическую взвешенную многоуровневую балансировку нагрузки, учитывающий надежность, приоритет и задержку ответа. Балансировщик прослушивает несколько портов и пересылает запросы с нулевым копированием для повышения эффективности.

Также стоит отметить алгоритмы принятия решений на основе искусственного интеллекта и машинного обучения, например метод распределения вознаграждений (RSDQL) и алгоритм мягкой критики (ASAC).

ТАБЛИЦА 1. Сравнение алгоритмов

Название	Сильные стороны	Ограничения
Координация микросервисов	фокус на минимизации всевозможных задержек; наличие онлайн и офлайн алгоритмов	сложность внедрения в системы с отличающимся сценарием
Фреймворк	легковесность; не нужен дополнительный узел для тестирования	дополнительное время на тестирование среды назначения
iDynamics	разнообразие инструментов; возможность регулировать пропускную способность и задержки при тестировании	поддержка сложной системы; необходимо знать всю топологию заранее, для учета зависимостей
DMSA	прерывание соединения с плоскостью управления не приводит к прекращению миграции	необходимость агентов для каждой группы микросервисов; использование только TCP

В большинстве алгоритмов используются дополнительные наборы инструментов для принятия решений, что создает единую точку отказа и усложняет систему, а из-за отсутствия стандартизации возникают трудности в интеграции алгоритма для различных сценариев. Также стоит отметить создание дополнительных тестовых сред, что безусловно является преимуществом, но влечет замедление принятия решений в реальной сети.

Все это позволяет определить цель для дальнейших исследований, слабые места представленных алгоритмов предполагают разработку гибридного метода, основанного на группе легковесных образов, которые будут

осуществлять контроль в каждом краевом облаке, а общее взаимодействие будет построено на принципах хореографии. Данное решение не будет перегружать систему дополнительным программным обеспечением, следить за микросервисами в реальном времени и собирать данные с нескольких независимых точек. А переход от оркестровки к хореографии исключит единые точки отказа, так как узлы будут реагировать только на случившиеся события, что устранит необходимость установления соединения. Гибридный метод будет разработан для внедрения напрямую в работающую систему и будет отвечать основным принципам концепции IMT-2030.

Список используемых источников

1. OpenFog Reference Architecture for Fog Computing // OpenFog Consortium. 2017. 162 p.

2. ITU'S IMT-2030 Vision: navigating towards 6G in the Americas // A 5G AMERICAS. 2024. 20 p.

3. Wang S. Delay-Aware Microservice Coordination in Mobile Edge Computing: A Reinforcement Learning Approach // IEEE Transactions on Mobile Computing. 2020. PP. 939-951.

4. Rubio-Drosdov E. A Framework for Microservice Migration and Performance Assesment / E. Rubio-Drosdov, D. Diaz-Sanchez, A. Marin-Lopez, F. Almenares // Department of Telematics Engineering, University Carlos III of Madrid. 2020. 11 p.

5. Chen M. A Controllable and Realistic Framework for Evaluating Microservice Scheduling in Cloud-Edge Continuum / M. Chen, M.T. Islam, M.R. Read, R. Buyya // The University of Melbourne. 2025.14 p.

6. Chen Y. DMSA: A Decentralized Microservice Architecture for Edge Networks / Y. Chen, C. Lu, Y. Huang, C. Wu, F. Guo, H. Lu, C. W. Chen // University of Science and Technology of China. 2025. 12 p.

Статья представлена научным руководителем, доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом Редругиной Н. М.

УДК 621.396

М. В. Никитин (студент группы ИКТР-22, СПбГУТ), nikitin1.mv@sut.ru

ОБЗОР НОВЫХ ПОКОЛЕНИЙ БЕСПРОВОДНОЙ СВЯЗИ

В статье раскрывается роль нового поколения беспроводной связи, рассматривается разница технических характеристик систем 5G и 6G, а также влияние фактора искусственного интеллекта (ИИ). Определены преимущества и недостатки системы 5G, сервисы и услуги после внедрения 6G, раскрыта значимость интеллектуальной собственности в развитии телекоммуникации и этапы подготовки к внедрению технологии 6G в России.

5G, 6G, искусственный интеллект, интеллектуальная собственность

OVERVIEW OF NEW GENERATIONS OF WIRELESS COMMUNICATIONS

Nikitin M.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article reveals the role of the new generation of wireless communications, examines the difference in the technical characteristics of 5G and 6G systems, as well as the influence of artificial intelligence (AI). The advantages and disadvantages of the 5G system, services and services after the introduction of 6G are identified, the importance of intellectual property in the development of telecommunications and the stages of preparation for the introduction of 6G technology in Russia are revealed.

***Key words**: 5G, 6G, artificial intelligence, intellectual property*

Создание научно-технического задела и необходимой нормативной базы для развития прогрессивных технологий беспроводной связи 5G и последующих поколений предопределяет развитие новых технологических прогрессов в рамках страны [1].

Мобильные сети каждое десятилетие совершают революционный скачок, открывая все больше и больше новых возможностей для пользователей. В современном мире, когда 5G становится все более глобальным стандартом, а ученые уже тестируют прототипы 6G, происходит новый технологический прогресс.

Каждое поколение беспроводных технологий меняет и привносит новые захватывающие функции. Если 4G совершил техническую революцию, подарив пользователем быстрый мобильный интернет и возможность цифровизации, то 5G подарит новые возможности в общении, работе, развлечениях и даже в медицине.

В свою очередь система беспроводной связи 6G будет внедрена для преодоления ограничений и улучшения возможностей 5G [2].

Технологии 5-го поколения мобильных сетей имеет ряд преимуществ и недостатков. Среди преимуществ 5G технологий можно отнести: сверхвысокая передача данных, минимальная задержка сигнала, энергоэффективность, надежность соединения.

Одни из ключевых проблем 5G является массовое подключение, что и в предыдущих поколениях, при высоком количестве подключенных устройств происходит перегрузка сети и проблемы совместимости, не все девайсы поддерживают сети следующего поколения. Так же одним из минусов ограниченная зона покрытия, высокочастотные волны имеют малый радиус действия (до 300 м).

В 2019 году произошел старт новых коммерческих сетей 5G. Внедрение новой сети поспособствовало ведущим странам мира через некоторое время начать создание следующего шестого поколения, с созданием специализированных центров научно-технических институтов в области разработки 6G.

Лидирующими странами по патентам в области разработок 5G являются Китай (Huawei Technologies, ZTE Corporation), США (Qualcomm, Intel Corporation), Южная Корея (Samsung Electronics, LG Electronics), Швеция (Ericsson), Финляндия (Nokia). У России на сегодняшний день патенты отсутствуют. Вышеуказанные компании считаются ведущими производителями микросхем, чипов, оборудования для сетей мобильной связи.

Ключевой особенностью в различии 6G от 5G является расширенный сектор услуг для всех абонентов. Главными качествами 6G, относительно сетей связи 5G, будут считаться социально-ориентированными: создание новых ИКТ определит в получении большого массива информации, виртуальных ресурсов, а также физических из любой точки земли [5]. Развитие медицины в сфере человеко-центричных услуг, а именно взаимодействия человека с «машиной» обеспечит своевременное обследование и диагностирование заболевания дистанционно в любом месте при использовании специальных датчиков.

Это только некоторые из сервисов, которые появятся с внедрением 6G. ФГУП НИИР создала уникальную матрицу сервисов и услуг, основываясь на сетях 6G – «мир будущего» для экономики, а также других отраслей (рис. 1). Именно по заказу Минцифры России специалистами ФГУП НИИР был разработан данный материал, согласно план-графику развития и внедрения сетей 6G в Российской Федерации.

Концепция создания и облик сетей мобильной связи 6G будут определять будущую архитектуру сети, которая должна реализовывать принцип обеспечения соединения и оказания услуг связи «для любого абонента в любом месте в любое время». Обеспечение принципа соединения в любом месте с любым абонентом подразумевает наличие воздушно-космического сегмента в архитектуре сети в дополнение к традиционной наземной сети мобильной связи, что соответственно будет расширять и дополнять наземную архитектуру новыми элементами воздушных и спутниковых сетей [3].

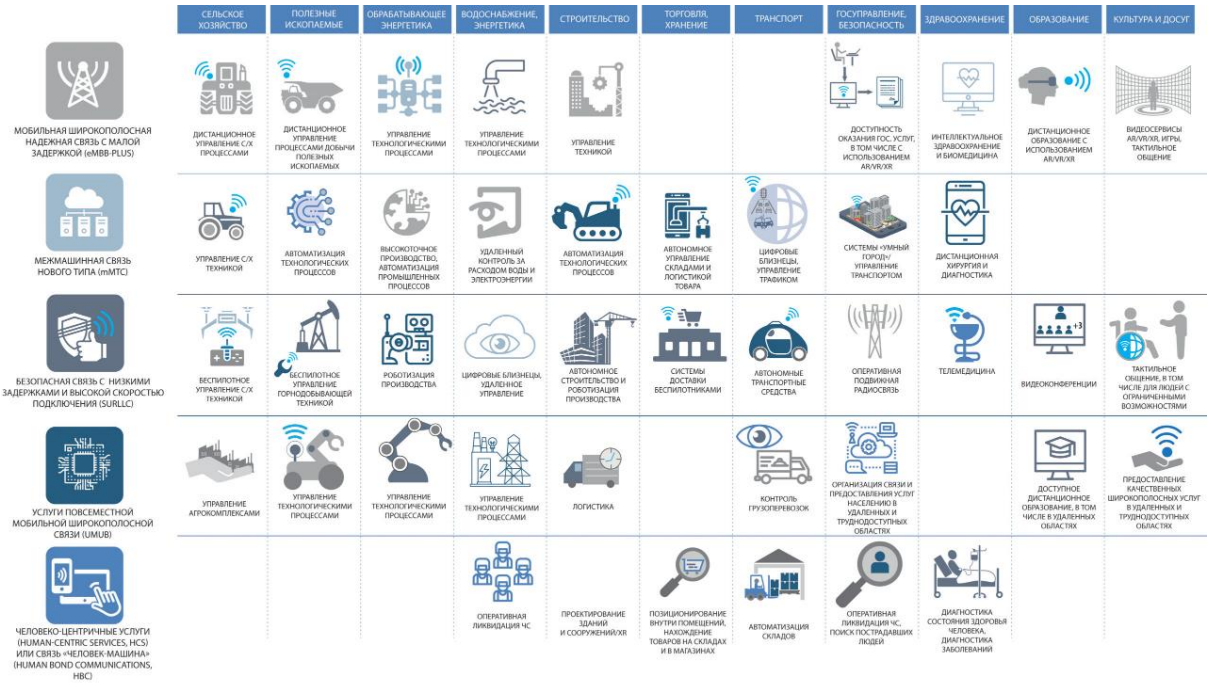


Рис. 1. Матрица сервисов и услуг, предоставляемых на сетях 6G (разработчик ФГУП НИИР)

С 2020-го года и по настоящее время в Российской Федерации активно разрабатывают технологии 6G, являющие неотъемлемой частью в Министерстве цифрового развития, связи и массовых коммуникаций (Минцифры). Развитие технологических систем запланирована до 2030-го года. Высокоскоростная пропускная способность, используемая в 5G, сегодня является главной задачей для специалистов, которая уже в будущем будет считаться фундаментом и стандартом для мобильных сетей 6G.

Предполагается, что технология 6G будет обеспечивать скорость до 1 Тбит/с, в то время как 5G может обеспечить скорость до 1 Гбит/с и немного выше. В табл.1 приведено сравнение характеристик 5G и 6G.

ТАБЛИЦА 1. Сравнение характеристик 5G и 6G

Характеристики	5G	6G
Индивидуальная скорость передачи данных	1 Гбит/с	1 Тбит/с
Скорость загрузки данных	20 Гбит/с	> 1000 Гбит/с
Задержка в U-плоскости	0,5мс	< 0,1мс
Задержка в C-плоскости	10мс	< 1мс
Подвижность	500 км/ч	1000 км/ч
	30 бит/с/Гц	100 бит/с/Гц
Рабочая частота	3-300 ГГц	1000 ГГц

Так же из ключевых особенностей 6G будут являться терагерцовый и миллиметровый диапазоны, которые, в свою очередь, будут расширять область действия на высоте, под водой и даже в космическом пространстве. Нужно еще обратить внимание на требования использование новых коммуникационных инфраструктур. К ним непосредственно относятся каналы, имеющие высокую скорость передачи данных, которые используют ТГц, а также новые архитектуры и 3D-соединения (многоуровневая сетевая инфраструктура, объединяющая: наземные, воздушные и космические станции).

Беспроводная связь шестого поколения будет тесно связана с такими областями, как искусственный интеллект (ИИ), virtual reality (виртуальная реальность), а также additional reality (дополнительная реальность).

Искусственный интеллект (ИИ) будет включать в себя особенности машинного обучения на конечных узлах сети [4]. Сеть 6G и модели на основе ИИ совместно создадут «симбиотический организм», обеспечивающий работу для всей системы. Совместная работа ИИ сервисов 6G в будущем будет внедряется в повседневные гаджеты, в военно-промышленные комплексы (беспилотные летательные аппараты, военная техника и др.), робототехнику и автомобили.

Любое нововведение и разработка является интеллектуальной собственностью в создании нового продукта 6G. Жесткая конкуренция среди разработчиков телекоммуникаций вынуждает вносить свою лепту в стандарты 6G, а также запатентовывать результаты научно-технических разработок как в технологии, так и в конструкции.

По разработанному план-графику развития мобильных сетей 2020 г. специалистами ФГУП НИИР, в России планируется переход на 6G в 2030-му году. Подготовка к внедрению технологии ведется поэтапно. В ходе развития высокоскоростных сетей с 2023 года начались разработки санитарно-эпидемиологических требований к оборудованиям 6G с электромагнитными полями. Однако, уже в 2024 году началось формирование технический условий и требований непосредственно к самому оборудованию сетей 6G, на основании уже полученного опыта предшествующих исследований. Важно отметить, что с 2024 года поступают предложения по переходу сетей связи от стандартов 5G к 6G.

Российские специалисты активно работают с разработками беспроводных сетей, которые в будущем будут входить в международные фундамен-

тальные стандарты 6G. Новейшее слово в мобильной связи 6G своими особенными характеристиками будет катализатором развития любой отрасли государства.

На основании вышеизложенного следует отметить, что огромную роль играют как возможности беспроводной связи новых поколений, так и интеллектуальная собственность. При условии получении патентов на технологии 5G и 6G последует высокотехнологический прорыв российского производства электроники и средств связи как внутри страны, так и на международном рынке.

Научное развитие на сегодняшний день зависит в достаточном финансировании научно-исследовательских центров, обучении специалистов в области технологии сетей и связи, что должно обеспечивать научный задел. Беспроводные сети новых поколений откроют новые возможности не только для обычных пользователей, но и в разных сферах таких как: медицина, промышленность и производство, логистика и др. Успешное внедрение этих направлений позволит России занять одно из лидирующих позиций на мировой арене.

Список используемых источников

1. Девяткин Е. Е., Иванкович М. В. Сети мобильной связи 6G. План действий для России // Электросвязь. 2022.

2. Тихвинский В. О., Девяткин Е. Е., Бочечка Г. С., Бородин А. С. Старт развитию нового поколения мобильной связи 6G // Электросвязь. 2020. № 1. С. 54-59.

3. Катеринкина Е. Н. Интеллектуальные отражающие поверхности как один из сценариев создания сетей 6G // Проблемы техники и технологий телекоммуникаций ПТиТТ-2020: XXII Международная научно-техническая конференция, IV научный форум телекоммуникации: теория и технологии ТТТ-2020, Самара, 17-20 ноября 2020 года. Самара: Поволжский государственный университет телекоммуникаций и информатики, 2020. С. 172-173.

4. Исобоев Ш. И., Халматов Б. М., Коптев В. А. Оценка перспектив развития и применения искусственного интеллекта в мобильной связи 5-го и 6-го поколений // Экономика и качество систем связи. 2022. № 1. С. 20-25.

5. Девяткин Е. Е., Иванкович М. В. Сети мобильной связи 6G. План действий для России // Электросвязь. 2022.

Статья представлена заведующим кафедрой БТС СПбГУТ, доктором технических наук, доцентом Фокиным Г. А.

УДК 621.396

В. П. Подсветова (студент группы РМ-22, СПбГУТ), podsvetova.vp@sut.ru

КАНАЛ СВЯЗИ С НАЗЕМНЫМ БПА

В данной работе рассматриваются ключевые аспекты организации канала связи с беспилотными наземными объектами (БНО), представляющими собой автономные или дистанционно управляемые платформы для выполнения задач на поверхности земли. Основное внимание уделено параметрам канала связи: допустимой вероятности битовой ошибки (BER – Bit Error Rate), пропускной способности, задержке и надежности передачи данных. Проанализированы особенности распространения радиоволн в различных условиях, включая влияние земной поверхности и городской застройки. Выполнен сравнительный обзор технологий беспроводной связи, таких как радиочастотная связь (RF – Radio Frequency), беспроводная локальная сеть (Wi-Fi – Wireless Fidelity), сотовая связь четвертого поколения (LTE – Long-Term Evolution), энергоэффективная дальнодействующая связь (LoRa – Long Range), а также спутниковая связь. Особое внимание уделено устойчивости сигнала и применению адаптивных методов в условиях внешних радиопомех. Отмечается важность выбора соответствующей технологии связи в зависимости от задач, условий эксплуатации и требований к надежности и скорости передачи данных.

беспилотные наземные объекты, канал связи, радиоволны, задержка, пропускная способность, устойчивость к помехам, RF, Wi-Fi, LTE, LoRa, спутниковая связь, дифракция, городская застройка

COMMUNICATION CHANNEL WITH UGV

Podsvetova V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper explores the essential aspects of establishing a communication channel with unmanned ground vehicles (UGVs), which operate either autonomously or via remote control on land. The focus is placed on the key communication parameters such as bit error rate (BER), bandwidth, latency, and transmission reliability. The study discusses radio wave propagation characteristics in various environments, including terrain-related effects and urban clutter. A comparative analysis of communication technologies–RF, Wi-Fi, LTE, LoRa, and satellite–is presented, evaluating their suitability for different UGV applications. Special attention is given to signal robustness and adaptive techniques in the presence of interference. The work emphasizes the importance of selecting an appropriate communication method based on mission requirements and operational conditions.

Key words: *unmanned ground vehicles, communication channel, radio waves, latency, bandwidth, interference resistance, RF, Wi-Fi, LTE, LoRa, satellite communication, diffraction, urban propagation*

Беспилотные наземные объекты (БНО) представляют собой автоматизированные транспортные средства, функционирующие без присутствия человека на борту. Эти устройства применяются в разнообразных отраслях – от сельского хозяйства и охраны до оборонной сферы. Эффективное выполнение их задач невозможно без устойчивого канала связи, обеспечивающего передачу управляющих сигналов, данных с сенсоров, а также мониторинг технического состояния БНО.

Основные характеристики канала связи

Основные характеристики канала связи представлены в таблице 1.

ТАБЛИЦА 1. Значение параметров связи до БНО и от БНО [1, 2]

Параметр	Направление связи	
	До БНО (команды)	От БНО (высокочувствительные данные)
BER	Менее 10^{-5}…10^{-6}	Менее 10^{-6}…10^{-8}
Скорость передачи данных	10-100 кбит/с	10 кбит/с – единицы Мбит/с
Пропускная способность	До 100 кбит/с	От 100 кбит/с
Задержка	Минимально возможная	
Устойчивость к помехам	Зависит от протоколов и технологий связи	
Дальность связи	Зависит от выбранной технологии, оптимальной для выполнения задач	

Особенности распространения радиосигналов

Передача сигналов в наземной среде имеет ряд особенностей:

- влияние рельефа и поверхности – когда антенны находятся близко к земле, возникают эффекты дифракции, ослабляющие сигнал. Если антенны подняты выше, возможно прямое распространение волн без существенных помех.
- городская застройка – в условиях плотной застройки сигнал претерпевает многочисленные отражения и ослабляется. Потери определяются по статистическим моделям распространения, рекомендованным ITU-R P.1411-9 [3].

Технологии связи

Существуют различные беспроводные технологии, применяемые в зависимости от условий эксплуатации.

ТАБЛИЦА 2. Технологии беспроводной связи с БНО [4].

Технология связи	Диапазон частот	Пропускная способность	Задержка и время отклика
RF	400-900 МГц	10-1000 кбит/с	5-100 мс
Wi-Fi	2.4/5 ГГц	54 Мбит/с – 1 Гбит/с	1-50 мс

Технология связи	Диапазон частот	Пропускная способность	Задержка и время отклика
LTE	700-2600 МГц	100 Мбит/с – 1 Гбит/с	20-50 мс
LoRa	433/868/915 МГц	0.3 – 50 кбит/с	1-10 с
Satellite	1-30 ГГц	1-10 Мбит/с	500 мс – 2 с

По данным из таблицы 2 можно сделать следующие заключения:

● RF (Радиосвязь) лучше всего подходит для простых систем с низкой скоростью передачи данных, работающих на небольших расстояниях, где критична умеренная задержка и средняя помехоустойчивость (простое дистанционное управление, мониторинг в сельской местности);

● Wi-Fi лучше всего подходит для высокоскоростной передачи данных на относительно коротких расстояниях, где важна минимальная задержка, но возможны помехи (передача видеопотока, контроль и телеметрия в закрытых помещениях или на промышленных объектах);

● LTE (мобильная/сотовая связь) лучше всего подходит для мобильных БНО, которым требуется высокая скорость передачи данных и умеренные задержки, с возможностью широкого охвата территории (городская среда, где возможны перемещения на большие расстояния, например, доставка или патрулирование);

● LoRa лучше всего подходит для систем, где важны энергоэффективность, большая дальность связи и высокая устойчивость к помехам, но допустима низкая скорость передачи информации и большая задержка (длительный мониторинг окружающей среды, сельское хозяйство, системы оповещения на больших территориях);

● Satellite (спутниковая связь) лучше всего подходит для связи на очень больших расстояниях, в труднодоступных или удаленных районах, где другие технологии невозможны, несмотря на высокую задержку и подверженность помехам (контроль за БНО в отдаленных регионах, на полюсах, в пустынях).

Практические рекомендации

Для повышения надежности и эффективности связи с БНП рекомендуется:

1. Использовать гибридные схемы, совмещающие, например, LTE и Wi-Fi;
2. Применять ретрансляторы и Mesh-сети для расширения покрытия;
3. Настраивать адаптивное модулирование для повышения помехоустойчивости [1, 2];
4. Интегрировать при ухудшении параметров систему мониторинга состояния связи с автоматическим переключением каналов [2].

Выводы

Организация надежного канала связи – основа для полноценного функционирования наземных беспилотных систем. Выбор технологии должен учитывать не только пропускную способность и помехоустойчивость, но и условия местности, характер задач и требуемую автономность.

Улучшение канала связи для беспилотных наземных объектов (БНО) является ключевым аспектом для повышения их эффективности и надежности в различных приложениях.

Поэтому для улучшения качества связи с БНО следует:

1. Использовать надежные современные протоколы связи в зависимости от требований к расстоянию и к скорости передачи данных;

2. Рассмотреть возможность использования ретрансляторов или Mesh-сетей для расширения покрытия связи;

3. Исследовать возможность использования антенн с повышенной эффективностью или специализированных антенн для конкретных условий эксплуатации;

4. Использовать адаптивные методики кодирования и модуляции для повышения устойчивости канала связи в динамических условиях;

5. Реализовать системы мониторинга состояния канала связи, чтобы оперативно выявлять и устранять проблемы, собирать и анализируйте данные о качестве связи, чтобы в перспективе улучшать инфраструктуру.

Каждая технология связи имеет свои особенности, и выбор наиболее подходящей зависит от конкретных целей и условий эксплуатации. Так, например, для городских условий и высокой скорости – Wi-Fi, LTE; для энергоэффективных и дальнодействующих систем – LoRa; для глобального охвата и связи в труднодоступных местах – спутниковая связь; а для простых и локальных систем – RF.

Список используемых источников

1. Rappaport T. S. Wireless Communications: Principles and Practice. Prentice Hall, 2002.

2. Molisch A. F. Wireless Communications. Wiley, 2011.

3. ITU-R P.1411-9. Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency-range 300 MHz to 100 GHz, 2017.

4. ETSI TR 103 257. Electromagnetic compatibility and Radio spectrum Matters…, 2019.

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

УДК 621.391

С. В. Пономарев (студ. группы ИКТО-17, СПБГУТ),
Dudkin.Valentin@sut.ru

ПРИМЕНЕНИЕ ДИНАМИЧЕСКОГО ХАОСА В ОПТОВОЛОКОННОЙ СВЯЗИ: СОВРЕМЕННЫЕ ПОДХОДЫ, ПАТЕНТНЫЕ РЕШЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

В статье анализируются современные подходы к использованию динамического хаоса в оптоволоконных системах связи с акцентом на повышение пропускной способности и уровня защиты передаваемой информации. Рассмотрены методы широкополосного спектрального уплотнения на основе хаотических источников, позволяющие снизить зависимость от набора когерентных лазеров и обеспечить гибкость архитектуры. Уделено внимание интеграции хаотической оптики с квантовыми протоколами распределения ключей (QKD), формирующими основу для многоуровневой защиты, а также рассмотрены перспективные направления исследований, включая гибридные схемы хаотико-квантовой модуляции. Показано, что совмещение хаотических и квантовых технологий может стать фундаментом для нового класса систем защищенных коммуникаций.

динамический хаос, оптоволоконная связь, спектральное уплотнение, квантовая криптография, физическая защита информации

APPLICATION OF DYNAMIC CHAOS IN FIBER-OPTIC COMMUNICATIONS: MODERN APPROACHES, PATENT SOLUTIONS, AND DEVELOPMENT PROSPECTS

Ponomarev S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper analyzes modern approaches to the application of dynamic chaos in fiber-optic communication systems, with a focus on enhancing both data throughput and transmission security. Methods of broadband spectral multiplexing based on chaotic sources are discussed, highlighting their ability to reduce dependence on sets of coherent lasers and to improve system flexibility. Special attention is given to the integration of chaotic optics with quantum key distribution (QKD) protocols, enabling multilayered security architectures. Mathematical models of chaotic signal multiplexing are presented, along with prospective research directions involving hybrid chaotic–quantum modulation schemes. It is demonstrated that the convergence of chaotic and quantum technologies may form the foundation for a new class of secure communication systems.

Key words: *dynamic chaos, fiber-optic communication, spectral multiplexing, quantum cryptography, physical layer security*

Современные оптоволоконные системы связи сталкиваются с двойной задачей: необходимостью увеличения пропускной способности каналов и

обеспечением высокой степени защиты передаваемой информации [1]. Традиционные методы спектрального уплотнения, такие как WDM, демонстрируют высокую эффективность, однако требуют применения сложной и дорогостоящей элементной базы. В этой связи все большее внимание уделяется динамическому хаосу, который, обладая широкополосными шумоподобными свойствами, открывает новые возможности для мультиплексирования и маскировки данных [2]. Одновременно усиливается интерес к интеграции хаотических сигналов с квантовой криптографией [5], обеспечивающей принципиально новый уровень безопасности. Такой синтез формирует перспективное направление исследований, способное задать основу будущего развития технологий защищенных инфокоммуникаций.

Современные подходы к спектральному уплотнению на базе динамического хаоса в оптоволоконных системах

Широкополосное спектральное уплотнение, реализуемое на основе хаотических источников излучения, в настоящее время рассматривается как одно из перспективных направлений развития фотонных телекоммуникационных систем [2]. В отличие от традиционной технологии WDM (Wavelength Division Multiplexing), предполагающей использование набора узкополосных когерентных лазеров для формирования индивидуальных каналов, динамический хаос позволяет генерировать широкий непрерывный спектр, из которого посредством спектральной селекции выделяются поддиапазоны для передачи информации. Подобный подход позволяет отказаться от применения большого числа стабилизированных источников, что приводит к снижению совокупной стоимости системы и повышает ее архитектурную гибкость.

Ключевая концепция метода заключается в генерации широкополосного хаотического сигнала, например с использованием полупроводникового лазера с оптической обратной связью. Получаемый спектр характеризуется шумоподобным распределением мощности в диапазоне десятков гигагерц, что обеспечивает возможность сегментации спектра на совокупность ортогональных подканалов. Селекция каналов реализуется с помощью широкополосных фильтров, включая растянутые волоконные решетки Брэгга (CFBG – chirped fiber Bragg grating) и тонкопленочные фильтры с регулируемой полосой пропускания. Каждый выделенный спектральный сегмент подвергается модуляции информационным сигналом и далее объединяется в общий оптический тракт.

Математическая модель процесса [6] может быть представлена на основе спектрального разложения исходного хаотического сигнала S(ω). Пусть $H_k(\omega)$ обозначает передаточную функцию фильтра, выделяющего k-й канал. Тогда временной сигнал в выбранном канале определяется выражением:

$$x_k(t) = F^{-1}\{S(\omega) \cdot H_k(\omega)\}, \quad (1)$$

а результирующий мультиплексированный сигнал может быть записан в виде:

$$X(t) = \sum_{k=1}^{N} x_k(t), \quad (2)$$

где F^{-1} – соответствует операции обратного преобразования Фурье.

На следующем этапе формируется информационный поток, который модулирует выделенный сигнал. Если обозначить информационную последовательность в k-м канале как $m_k(t)$, то результирующий промодулированный сигнал примет вид:

$$x_k^m od(t) = m_k(t) \cdot x_k(t) \quad (3)$$

После индивидуальной модуляции всех спектральных сегментов производится их обратное объединение в общий оптический тракт. Математически итоговый мультиплексированный сигнал можно выразить как:

$$X(t) = \sum_{k=1}^{N} x_k^m\, od(t) = \sum_{k=1}^{N} m_k(t) \cdot F^{-1}S(\omega) \cdot H_k(\omega), \quad (4)$$

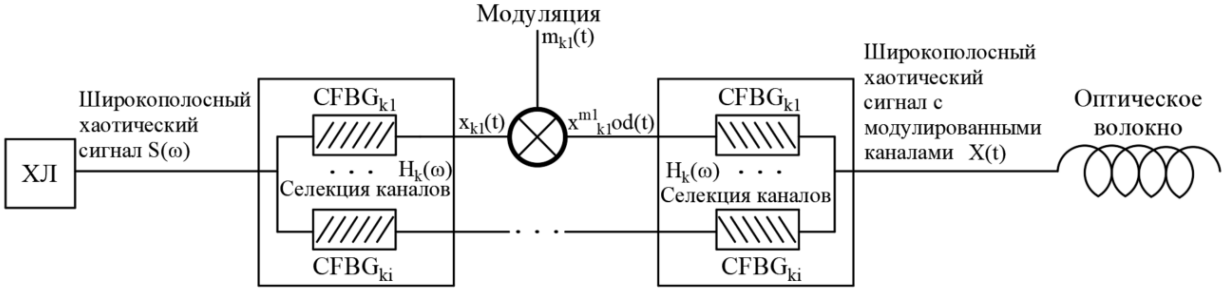


Рис. 1. Структурная схема спектрального мультиплексирования при применении технологии динамического хаоса

Использование хаотических источников в системах спектрального уплотнения характеризуется рядом преимуществ. Во-первых, за счет шумоподобной структуры спектра достигается повышенный уровень скрытности

передачи [3], что имеет особое значение для защищенных систем связи. Во-вторых, широкая полоса генерации хаоса одним источником позволяет существенно уменьшить себестоимость мультиплексирования за счет снижения количества излучателей в сравнении с дискретными лазерами классических WDM-систем. Вместе с тем практическая реализация сопряжена с рядом вызовов, среди которых ключевыми являются обеспечение синхронизации передающих и приемных модулей [4], а также разработка элементной базы с достаточной полосой пропускания. Указанные вопросы составляют предмет активных исследований и определяют направления дальнейшего развития технологии.

Перспективы совмещения хаотической оптики и квантовой криптографии

Одним из наиболее примечательных направлений развития является интеграция хаотических методов модуляции с квантовой криптографией. Современные исследования и патентные разработки (например, [5]) показывают возможность построения гибридных систем, где хаотический оптический носитель сочетается с фазовым кодированием, основанным на квантовых случайных процессах. Такой подход открывает путь к созданию многоуровневой защиты, в которой хаотический спектр выполняет роль физической маскировки, а квантовые протоколы распределения ключей (QKD) обеспечивают стойкость к атакам на фундаментальном уровне.

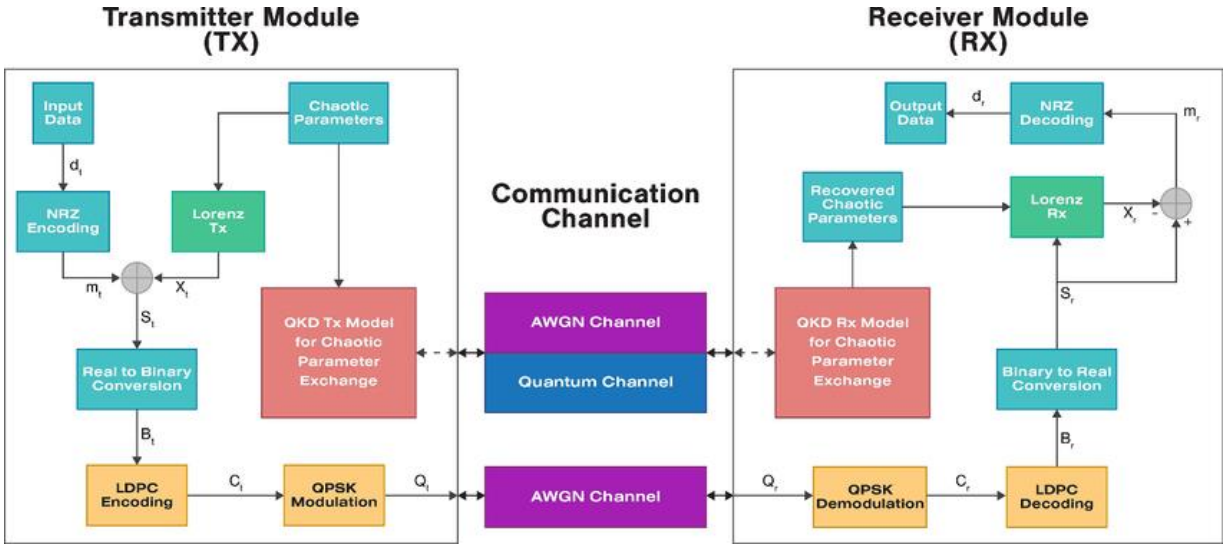


Рис. 2. Структурная хаотической оптики и квантовой криптографии

Суть идеи заключается в формировании световых импульсов, на которые накладываются одновременно два типа фазовых флуктуаций: хаотические, генерируемые оптической системой с обратной связью, и квантовые, возникающие на основе случайных процессов фотонного шума. В результате создается двойной уровень кодирования, где информация защищена как за счет непредсказуемости хаоса, так и благодаря принципиальной невозможности клонирования квантовых состояний.

Перспективность данного направления заключается в том, что оно формирует основу для нового класса коммуникационных систем, способных удовлетворять возрастающие требования к безопасности в государственных, финансовых и оборонных сетях. В отличие от традиционных решений, где хаос или квантовая криптография применяются изолированно, объединение этих подходов позволяет получить качественно новый уровень защищенности, что делает подобные разработки особенно актуальными в контексте будущего развития инфокоммуникационных технологий.

Проведенный анализ показывает, что использование динамического хаоса в оптоволоконных системах связи открывает новые перспективы как в области повышения пропускной способности, так и в обеспечении безопасности информации. Широкополосное спектральное уплотнение на основе хаотических источников позволяет отказаться от множества стабилизированных лазеров, снижая стоимость и сложность архитектуры. Дополнительные преимущества связаны с шумоподобной природой спектра, обеспечивающей маскировку передачи. В то же время ключевые вызовы касаются синхронизации приемопередатчиков и разработки элементной базы с расширенной полосой. Перспективным направлением является совмещение хаотической оптики и квантовой криптографии, формирующее многоуровневую систему защиты на физическом уровне. Такое объединение позволяет создать качественно новый класс защищенных коммуникаций, ориентированных на государственные, финансовые и оборонные сети.

Список используемых источников

1. Argyris A., Hamacher M., Chlouverakis K. E., Bogris A., Syvridis D. Chaos-based communications at high bit rates using commercial fibre-optic links // Nature. 2005. Vol. 438. № 7066. PP. 343–346. DOI:10.1038/nature04275.

2. Chen H., Zhang Y., Li X., Tang S. Optical Chaos Generation and Applications // Advanced Photonics Research. 2025. Vol. 4. № 2. PP. 123–135. DOI:10.1002/adpr.202500123.

3. Wu J., Xiang S., Pan W., Xu Z. Analog–Digital Combined High-Secure Chaotic Optical Communication System // Photonics. 2024. Vol. 11. №. 9. PP. 1144. DOI:10.3390/photonics11091144.

4. Uchida A., Rogister F., Garcia-Ojalvo J., Roy R. Synchronization of chaotic oscillators: Focus on laser diodes with time-delayed feedback // Progress in Optics. 2005. Vol. 48. P. 203–341. DOI:10.1016/S0079-6638(05)48004-6.

5. Optical chaotic communication system combined with quantum key distribution: пат. CN111314048A Китай. № CN111314048A; заявл. 2020.

6. Slim I. H. Signal Processing for Optical Communication Systems / Institute for Circuit Theory and Signal Processing, Technical University of Munich. 2017. P. 64–69.

Статья представлена научным руководителем, профессором кафедры ОКСС СПбГУТ, доктором технических наук, профессором Дудкиным В. И.

УДК 004.732
ГРНТИ 49.43.29

А. В. Светова (аспирант кафедры ССиПД, СПбГУТ), svetova.av@sut.ru

ОБЗОР РЫНКА УСТРОЙСТВ С ПОДДЕРЖКОЙ НОВОГО СТАНДАРТА IEEE 802.11BE

В статье приводится обзор седьмого поколения Wi-Fi, сравниваются характеристики предыдущих поколений Wi-Fi 6 и Wi-Fi 6E с новым Wi-Fi 7, рассматриваются появившиеся революционные технологии, а также проводится обзор рынка устройств с поддержкой стандарта IEEE 802.11be.

IEEE 802.11be, Wi-Fi 7, Wi-Fi роутер, Wi-Fi адаптер, точка доступа

AN OVERVIEW OF THE MARKET OF DEVICES SUPPORTING THE NEW IEEE 802.11BE STANDARD

Svetova A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper provides an overview of the seventh generation of Wi-Fi, compares characteristics of the previous generations of Wi-Fi 6 and Wi-Fi 6E with the new Wi-Fi 7, examines revolutionary technologies that have emerged, and also reviews the market of devices supporting the IEEE 802.11be standard.

Key words: *IEEE 802.11be, Wi-Fi 7, Wi-Fi router, Wi-Fi adapter, access point*

В современном, стремительно цифровизирующемся мире, беспроводные локальные сети (Wireless Local Area Network, WLAN) стали неотъемлемой частью нашей повседневной жизни. Они обеспечивают не только мобильность и удобство доступа к информации, но и являются ключевой технологией, поддерживающей широкий спектр приложений, от домашних развлечений и офисной работы до критически важных промышленных систем и инновационных концепций Интернета вещей (Internet of Things, IoT). В основе подавляющего большинства современных беспроводных сетей лежит стандарт IEEE 802.11, более известный как Wi-Fi (от англ. Wireless Fidelity – «высокая точность беспроводной передачи данных»).

Стандарт IEEE 802.11 – это не просто набор технических спецификаций, это комплексная и динамично развивающаяся экосистема протоколов,

технологий и решений, определяющая принципы функционирования беспроводных локальных сетей. Появившись в 1997 году, каждое новое поколение стандарта приносило значительные улучшения в пропускной способности, эффективности использования радиочастотного спектра, безопасности и управлении энергопотреблением. От первых, относительно медленных и небезопасных версий, до современных гигабитных решений, IEEE 802.11 прошел долгий путь эволюции, став ключевым фактором развития мобильной связи и Интернета.

На данный момент самым передовым решением является появившийся в 2024 году стандарт IEEE 802.11be [1] (так называемое седьмое поколение Wi-Fi – Wi-Fi 7), который объединяет все преимущества Wi-Fi 6/6E и расширяет их до совершенно нового уровня. В отличие от своих предшественников, Wi-Fi 7 предлагает не просто эволюционные улучшения, а включает в себя ряд революционных технологий, нацеленных на удовлетворение потребностей в высокоскоростной и надежной беспроводной связи для таких требовательных приложений, как VR/AR, облачные игры, потоковое видео в разрешении 8K [2]. Теоретическая максимальная скорость передачи данных Wi-Fi 7 достигает 46 Гбит/с, что примерно в 4.8 раза превышает возможности Wi-Fi 6/6E (9.6 Гбит/с). Это достигается за счет комбинации нескольких факторов, включая более широкие каналы до 320 МГц (что вдвое превышает максимальную ширину канала в Wi-Fi 6/6E), более высокую плотность модуляции и новые технологии. Одна из таких технологий – это Multi-Link Operation (MLO), которая позволяет устройствам одновременно использовать несколько частотных диапазонов (2.4, 5 и 6 ГГц) и обеспечивает агрегацию каналов для увеличения пропускной способности, а также отказоустойчивости, так как устройство может переключаться между каналами в случае помех. Следующая прогрессивная технология – это Multi-Resource Units (MRU), позволяющая более гибко и эффективно распределять ресурсы канала между пользователями. Вместо выделения целых Resource Units (RU) одному пользователю, MRU позволяет назначать несколько небольших RU разным пользователям одновременно, что повышает эффективность использования спектра [3]. Ниже представлена таблица 1, демонстрирующая улучшения нового поколения Wi-Fi [4].

ТАБЛИЦА 1. Сравнение функций в спецификациях IEEE 802.11ax и IEEE 802.11be

Стандарт	802.11ax (Wi-Fi 6)	802.11ax (Wi-Fi 6E)	802.11be (Wi-Fi 7)
Год выхода	2021	2021	2024
Максимальная скорость, Гбит/с	9.6	9.6	46
Диапазоны, ГГц	2.4, 5	2.4, 5, 6	2.4, 5, 6
Ширина каналов, МГц	20, 40, 80, 160	20, 40, 80, 160	20, 40, 80, 160, 320
Модуляция до	1024-QAM	1024-QAM	4096-QAM
MIMO	8×8 UL/DL MU-MIMO	8×8 UL/DL MU-MIMO	16×16 UL/DL MU-MIMO
Протокол защиты	WPA3	WPA3	WPA3

Таким образом, новый стандарт предлагает экспоненциальный скачок в скорости, высокую эффективность и исключительную надежность, открывая все новые возможности для развлечений, работы и других сфер жизни [5]. Внедрение Wi-Fi 7 потребует новых устройств, поддерживающих данный стандарт, чтобы полностью раскрыть его потенциал. Далее представлены данные, которые позволяют оценить, насколько много устройств у различных производителей поддерживает современный стандарт. Анализ данных из таблицы 2 показывает, что Wi-Fi роутеры с поддержкой IEEE 802.11be только начинают появляться на рынке. Их доля пока невелика – менее 10 %, а некоторые производители пока и вовсе не имеют моделей с поддержкой этого стандарта.

ТАБЛИЦА 2. Доля Wi-Fi роутеров с поддержкой IEEE 802.11be

Тип устройства	Производитель	Название модели с поддержкой Wi-Fi 7	Доля от моделей этого типа от общего кол-ва устройств
Wi-Fi роутер	TP-Link	BE3600	3 из 47 (6.4 %)
		BE5100	
		BE6500	

Тип устройства	Производитель	Название модели с поддержкой Wi-Fi 7	Доля от моделей этого типа от общего кол-ва устройств
Wi-Fi роутер	ASUS	RT-BE88U, BE7200	4 из 37 (10.8 %)
	ASUS D-Link	RT-BE86U, BE6800	4 из 37 (10.8 %) 1 из 34 (2.9 %)
		TUF-BE3600, BE3600	
		RT-BE58U, BE3600	
		DIR-X8970	
	Xiaomi Mi	BE3600	4 из 16 (25.0 %)
	Xiaomi Mi NETGEAR	BE7000	4 из 16 (25.0 %) 1 из 24 (4.1 %)
		BE6500 PRO	
		BE5000	
		Nighthawk RS770S	

Ситуация с Wi-Fi адаптерами с поддержкой IEEE 802.11be еще сложнее. Как демонстрирует таблица 3, на рынке практически отсутствуют подобные устройства.

ТАБЛИЦА 3. Доля Wi-Fi адаптеров с поддержкой IEEE 802.11be

Тип устройства	Производитель	Название модели с поддержкой Wi-Fi 7	Доля от моделей этого типа от общего кол-ва устройств
Wi-Fi адаптер	TP-Link	Archer TXE75E	1 из 18 (5.6 %)
	COMFAST	CF-977A	1 из 12 (8.3 %)
	ASUS	PCE-BE92BT	1 из 5 (20.0 %)

Рынок точек доступа также находится на начальной стадии, но уже есть несколько моделей, которые можно приобрести (таблица 4). В отличие от Wi-Fi роутеров, точки доступа обычно предназначены для бизнеса и предприятий, поэтому производители больше нацелены на быструю интеграцию новых технологий.

ТАБЛИЦА 4. Доля точек доступа с поддержкой IEEE 802.11be

Тип устройства	Производитель	Название модели с поддержкой Wi-Fi 7	Доля от моделей этого типа от общего кол-ва устройств
Точка доступа	Aruba	730 Series (AP-734)	1 из 21 (4.8 %)
	TP-Link	Omada EAP772	2 из 38 (5.3 %)
		EAP773	
	Ruckus Networks	R770	1 из 26 (3.8 %)
Точка доступа	Cambium Net-works	XV3-8	1 из 22 (4.2 %)
	Ubiquiti	UniFi U7 Pro Max	7 из 139 (5.0 %)
		UniFi U7 Pro	
		UniFi E7	
		UniFi U7 Outdoor	
		UniFi U7 Pro XGS	
		UniFi U7 Pro XG	
		UniFi U7 Lite	
	Zyxel	NWA130BE	2 из 18 (11.2 %)
		NebulaFlex WBE660S	
	MikroTik	wAP LTE kit (2024)	1 из 23 (4.3 %)

Таким образом, стандарт IEEE 802.11be имеет огромный потенциал для бизнеса и предприятий. Несмотря на то, что стандарт вышел совсем недавно, уже появляются устройства, поддерживающие Wi-Fi 7. На данный момент таких устройств пока мало, но мы можем ожидать множество предложений в будущем.

Список используемых источников

1. IEEE Std 802.11be-2024 – IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Enhancements for Extremely High Throughput (EHT) // IEEE. June 22, 2025.

2. Технические спецификации Wi-Fi 7. Введение. URL: https://www.asus.com/ru/support/faq/1051272/ (дата обращения 01.05.2025).

3. IEEE 802.11be – Wi-Fi 7: новые вызовы и возможности. Часть 1. URL: https://wireless-e.ru /standarty/wi-fi-7-chast-1/ (дата обращения 01.05.2025).

4. Почему Wi-Fi 7 – маркетинговая гонка, бесполезная в России. URL: https://zoom.cnews.ru/publication/item/65078 (дата обращения 01.05.2025).

5. Выпущены первые устройства с Wi-Fi 7: на подходе смартфоны и ноутбуки. URL: https://dzen.ru/a/ZZ1OT6uw2QMFAJoH (дата обращения 01.05.2025).

Статья представлена научным руководителем, доцентом кафедры ССиПД СПбГУТ, кандидатом технических наук Дунайцевым Р. А.

УДК 654.739

А. Д. Стерликов (магистрант группы ИКТС-43м, СПбГУТ),
sterlikov.ad@sut.ru

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНЦЕПЦИИ «УМНЫЙ» ДОМ

Современная жизнь становится все более динамичной и насыщенной, что создает потребность в автоматизации рутинных задач. ИИ позволяет «умным» домам выполнять множество функций автоматически, освобождая время жильцов для более важных дел.

искусственный интеллект, интернет вещей, умный дом

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN THE SMART HOME CONCEPT

Sterlikov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Modern life is becoming increasingly dynamic and busy, creating a need to automate routine tasks. AI allows smart homes to perform many functions automatically, freeing up residents' time for more important activities.

Key words: *artificial intelligence, internet of things, smart home*

Основная цель ИИ заключается в разработке машин, которые могут имитировать когнитивные функции человека и взаимодействовать с окружающей средой на интеллектуальном уровне [1].

Автоматизация управления бытовыми приборами с использованием методов искусственного интеллекта (ИИ) в системах "умного" дома представляет собой ключевую область, которая значительно повышает уровень комфорта и эффективности. Реализация системы автоматизации домашнего быта с использованием графовых нейронных сетей (GNN) начинается с представления всех данных о пользователе в виде графа, где узлы (nodes) отражают различные объекты или события – например, устройства умного дома, действия пользователя, состояния систем, задачи и т.д. А ребра (edges) обозначают связи и взаимодействия между ними, будь то временные зависимости, логические связи или физические взаимодействия. Например, граф может включать узлы, представляющие пользователя, его календарь, быто-

вые приборы, и ребра между ними могут указывать на частоту использования устройства, привязку к определенному времени суток или зависимость одних действий от других.

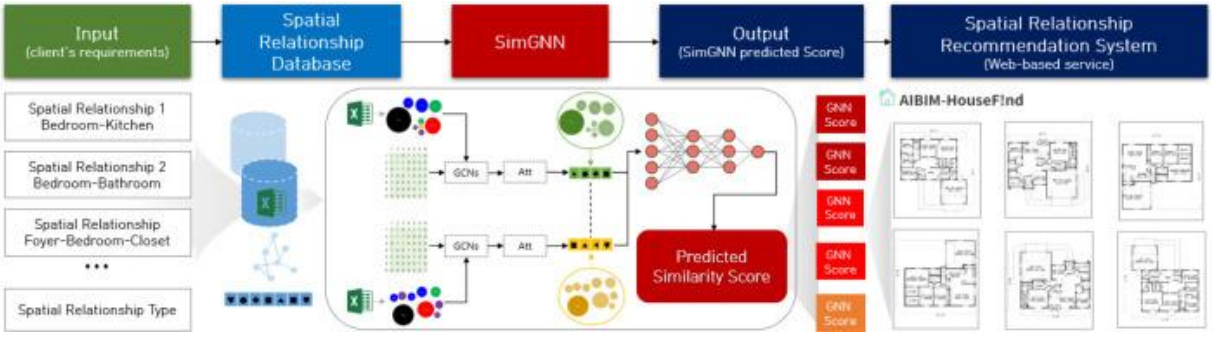


Рис. 1. Архитектура GNN

Весь ключ к применению GNN заключается в том, чтобы улавливать сложные паттерны и взаимозависимости между этими объектами на основе их связей, а не просто обрабатывать данные как плоские или временные ряды. Архитектура GNN позволяет на каждом слое обновлять представление узлов на основе их соседей и передавать информацию по ребрам, что по сути является агрегированием контекстной информации. Например, в случае задачи рекомендации по бытовым задачам, GNN может «узнать», что, если пользователь включает кофеварку каждое утро перед 8:00, это действие связано с началом дня, после которого следуют определенные рутинные задачи. Сначала происходит первичное обучение на больших массивах данных – это могут быть лог-файлы устройств, календарные данные пользователя, данные с датчиков умного дома. Далее система строит граф, где узлы и связи отражают, как именно пользователь взаимодействует с домом, и какие паттерны повторяются. За счет GNN можно реализовать эффективное обновление этих связей: например, система «узнает», что определенные задачи часто следуют друг за другом, или что выполнение одной задачи связано с определенным состоянием устройства или внешней среды (например, погоды). Одним из ключевых элементов здесь будет механизм message passing, который позволяет каждому узлу (например, устройству) обновлять свое состояние на основе информации, полученной от соседних узлов. Допустим, данные с термостата будут важны для прогноза, когда включить отопление, но вместе с данными с датчика дверей, кофеварки и календаря, система может предсказать, что пользователь собирается уйти из дома, и предложить оптимизировать энергию, отключив ненужные устройства. После каждого слоя GNN, когда происходит распространение сообщений

(messages) по ребрам, система агрегирует эту информацию и вырабатывает представление о том, как лучше всего организовать задачи пользователя.

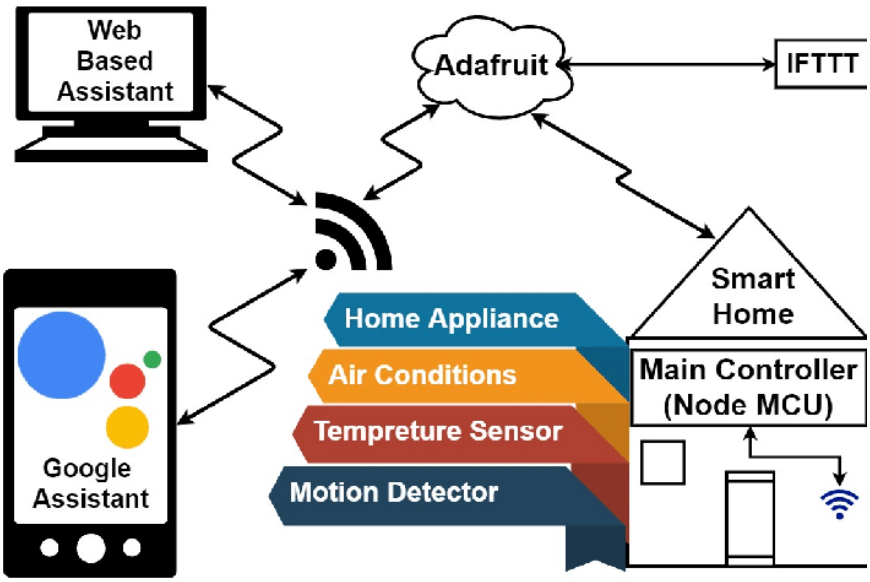


Рис. 2. Распространение сообщений GNN в системе «умного» дома

Важно, что графовые нейронки позволяют учитывать не только прямые взаимодействия, но и косвенные зависимости через несколько шагов: например, если изменение состояния одного устройства влияет на работу другого через несколько узлов, система это учтет в своих рекомендациях. GNN также может эффективно обрабатывать временные зависимости. Это достигается, например, через использование таких архитектур, как Temporal GNN (T-GNN), где время взаимодействий между узлами также учитывается как параметр. Таким образом, модель может адаптироваться к изменениям в поведении пользователя: например, если с течением времени задачи смещаются по расписанию или меняются зависимости между действиями [2].

Наиболее популярные модели устройств, успешно использующие искусственный интеллект для умного дома:

1. Kuri Home Robot. Домашний робот способен выполнять много задач: воспроизвести музыку, снимать фото и видео, отвечать на ваши вопросы. Благодаря специальным датчикам, Kuri обходит ножки столов, стульев и прочие преграды на своем пути. Кроме того, робот распознает лица и голоса.

2. Nest Thermostat. Устройство умеет устанавливать температуру, включать и выключать отопление, анализировать его эффективность. А управлять таким прибором очень легко, ведь он работает на базе приложения в смартфоне.

3. Netatmo Welcome. Камера безопасности распознает ваше лицо, поэтому может определить разницу между вами, вашими детьми и нежелательным злоумышленником. Ложных срабатываний очень мало, ведь система на шаг впереди стандартного обнаружения движения. Кроме того, камера реагирует на дым в доме. Управлять ею можно с помощью смартфона на базе Android или iOS. Вы сможете просматривать прямую трансляцию видео и получать push-уведомления.

4. Samsung Powerbot R7070. Робот-пылесос отлично собирает шерсть животных и кусочки пищи в самых труднодоступных местах. Его легко настроить, а работает такое устройство с Amazon Alexa и Google Assistant. Вдобавок пылесос имеет самую удобную корзину для мусора.

5. Nest Protect. Устройство моментально улавливает дым и угарный газ, а также распознает возгорание и пожар в доме. При помощи приложения Nest Protect сразу уведомляет вас, в каком помещении находится огонь.

6. Anova Precision Cooker. Настоящий помощник для хозяек, которые хотят приготовить вкусную и полезную пищу. Устройство напоминает обычную кастрюлю, которая имеет внутри водонепроницаемую сумку. Именно туда нужно положить стейк, курицу или овощи. Таким образом, пища готовится на водяной бане в собственном соку [3].

Произведем сравнение этих устройств.

ТАБЛИЦА 1. Сравнение «умных» устройств

«Умная» вещь	Kuri Home Robot	Nest Thermostat	Netatmo Welcome	Samsung Powerbot R7070	Nest Protect	Anova Precision Cooker
Цена, руб.	79990	55640	32840	34000	14082	23990
Обучаемость	-	+	+	+	-	-
Интеграция с другими сервисами	-	+	+	+	+	+
Поддержка стандартов и протоколов	Wi-Fi	Wi-Fi	Wi-Fi	Wi-Fi, Samsung SmartThings	Wi-Fi	Wi-Fi, BlueTooth

Каждое из устройств имеет свои сильные и слабые стороны в зависимости от критериев. Выбор зависит от конкретных потребностей пользователя и желаемой функциональности.

Интересный пример – «умный» матрас SleepInbody-Incline от ANSSil. Компания ANSSil представила более продвинутый матрас, чем обычная кровать из пены с памятью.

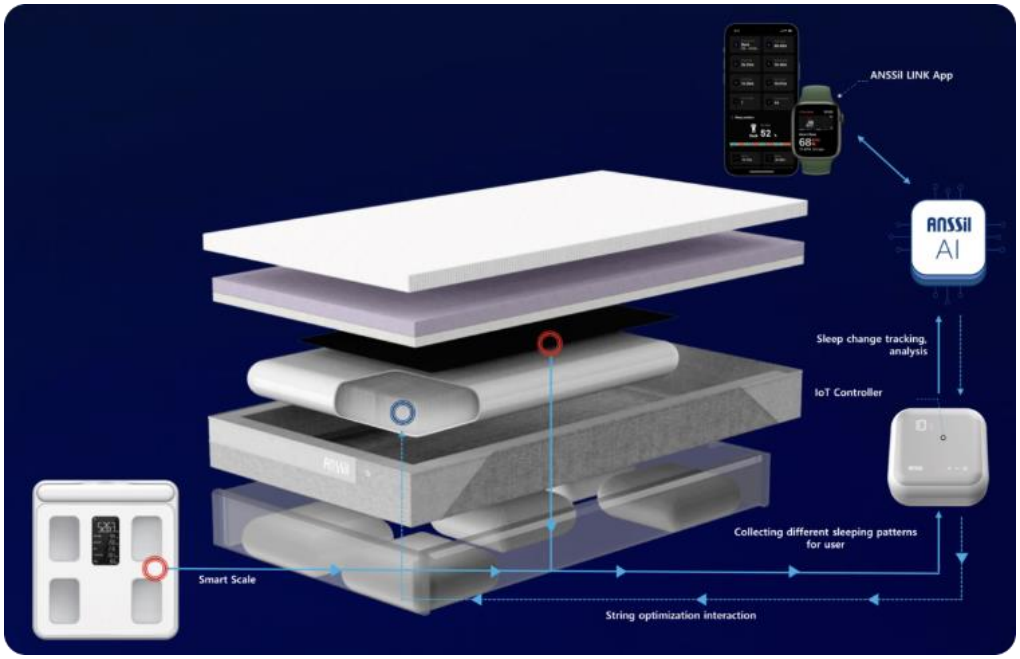


Рис. 3. Матрас SleepInbody-Incline

Умное зеркало BMind может помочь с практическими задачами, например, подсказать, как правильно ухаживать за кожей, и даже следить за температурой воды в ванной. Самое главное, что оно сохраняет все данные о здоровье и личной жизни в тайне, храня их локально на устройстве.

Рис. 4. Умное зеркало BMind

ИИ также может сделать задний двор и сад более эффективным и простым в уходе. Представьте себе робота, подстригающего газон; с такими роботами, как Верди, это может стать реальностью. Verdie –это робот-озеленитель на базе искусственного интеллекта, разработанный компанией Electric Sheep. Verdie предназначен для выполнения различных задач на открытом воздухе, таких как стрижка и подрезка, и использует продвинутый ИИ для адаптации к различным условиям. Вдохновленная такими роботами, как WALL-E и R2-D2, Верди сосредоточена на практических, негуманоидных задачах, которые приносят реальную пользу [4].

Рис. 5. Робот-озеленитель Verdie

ИИ предлагает множество преимуществ для умных домов, которые могут сделать вашу повседневную жизнь проще. Благодаря функции «свободные руки» вы можете управлять всем, от термостата до системы безопасности, просто используя свой голос. Еще одно большое преимущество – расширенная доступность. ИИ может распознавать ваш голос, предоставлять персонализированные ответы и облегчать каждому члену семьи управление различными аспектами дома [5].

Однако эти преимущества сопряжены с некоторыми проблемами. Одна из них – потребление энергии. Устройства ИИ должны питаться в течение дня, а это может повлиять на экологичность. Существует также проблема надежности. Ошибки или сбои в системе могут нарушить работу сервисов и вызвать разочарование. Конфиденциальность и безопасность данных также вызывают серьезные опасения. Несмотря на то, что искусственный интеллект может стать дополнительным преимуществом умного дома, решение этих проблем необходимо для того, чтобы обеспечить полную реализацию преимуществ без ущерба для безопасности, надежности и устойчивости [6].

Список используемых источников

1. Бостром Н., Кристианини Н., Грэм-Камминг Д. Искусственный интеллект. Что стоит знать о наступающей эпохе разумных машин. М.: Мир, 2019. 352 с.

2. Автоматизация бесконечного быта при помощи ИИ. URL: https://vc.ru/id2857281/1505415-avtomatizaciya-beskonechnogo-byta-pri-pomoshi-ii

3. Искусственный интеллект для умного дома. URL: https://mentamore.com/covremennye-texnologii/iskusstvennyj-intellekt-dlya-umnogo-doma.html (дата обращения 20.04.2025).

4. Взгляд на повседневную жизнь с помощью решений для умных домов с поддержкой искусственного интеллекта. URL: https://www.ultralytics.com/ru/blog/a-look-at-daily-life-with-ai-enabled-smart-home-solutions# (дата обращения 20.04.2025).

5. Интернет вещей, умный дом и умные города. URL: https://cyberleninka.ru/article/n/internet-veschey-umnyy-dom-i-umnye-goroda (дата обращения 20.04.2025).

6. Умные устройства с ИИ для дома: обзор 2024 года. URL: https://stark-service.ru/blog/umnye-ustroistva-s-ii-dlya-doma-2024 (дата обращения 20.04.2025).

Статья представлена научным руководителем, заведующим кафедрой ИКС СПбГУТ, доктором технических наук, доцентом Маколкиной М. А.

УДК 004.032.26

А. Г. Харченко (студент группы ИКТК-12 СПбГУТ), kharchenko.ag@sut.ru

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ СБОРА ДАННЫХ В CRM-СИСТЕМАХ

В настоящее время применение CRM-систем стало массовым. В них хранится огромное количество данных, которыми необходимо пользоваться. Для оперативного и удобного доступа к этим данным и работе с ними разумно использовать такую же не менее современную нейронную сеть.

CRM-система, нейронные сети, искусственный интеллект, структура нейронной сети

USE OF NEURAL NETWORKS FOR DATA COLLECTION IN CRM SYSTEMS

Kharchenko A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Currently, CRM systems are widely used. They store vast amounts of data that must be managed. For quick and easy access to and management of this data, it makes sense to use an equally advanced neural network.

Key words: *CRM system, neural networks, artificial intelligence, neural network structure*

В современном мире нейронные сети становятся все более востребованными и широко применяемыми. Они проникают в различные сферы жизни, обеспечивая возможности для поиска информации, коммуникации, программирования и решения разнообразных задач.

Применение искусственного интеллекта в медицине, сельском хозяйстве, производстве, конструировании и проектировании становится неотъемлемой частью работы в этих областях. С развитием технологий увеличивается объем информации, который требуется обрабатывать и анализировать. Количество данных, генерируемых каждую секунду, давно превысило возможности человека и продолжает увеличиваться. В свете взрывного роста объема информации человечеству необходимо было найти способы эффективно управлять ею.

Нейронные сети, достигнув определенного уровня развития, стали незаменимым инструментом в этом деле. Они способны обрабатывать, фильтровать и анализировать огромные объемы данных, поступающих к ним на обработку.

Особую актуальность приобрел вопрос анализа данных в CRM-системах. С каждым днем все больше людей обращаются за услугами различных компаний, все больше информации переходит в цифровое пространство. CRM-системы, в свою очередь, содержат в себе огромное количество данных о клиентах, которые пользуются услугами данного бизнеса. От небольших кафе до крупных операторов связи вроде Мегафона, Билайна и МТС, а также ведущих поставщиков интернет-услуг, включая ЭР-Телеком и Ростелеком, нейронные сети предоставляют возможность автоматизированного сбора, анализа и поиска значимой информации в огромных массивах данных [1-3].

Давайте рассмотрим модель работы с CRM-системой для ее удобства. Наиболее логично представляется интерфейс работы пользователя в режиме чат-бота.

Для того, чтобы проанализировать возможности применения нейронных сетей для сбора данных в CRM-системах, опишем модель, включающую в себя решение определенной проблемы при помощи нейронной сети. Модель включает в себя следующие компоненты:

1. CRM-система. Позволяет отслеживать клиентов, анализировать и работать с данными, содержащимися в базе данных. Обеспечивает бизнес-логику. Также в ней хранится вся информация.

2. Нейронная сеть (чат-бот). На вход нейронная сеть будет получать пользовательский запрос. В качестве архитектуры выбрана гибридная модель RAG + Fine-tuned Transformer. RAG позволяет искать информацию в базе данных CRM и давать точные ответы. Transformer обрабатывает пользовательский запрос на основе естественного языка и классифицирует запрос. На выходе нейронная сеть будет присылать нужную нам информацию о клиенте, анализировать различные долгосрочные и краткосрочные показатели и находить необходимые заявки по нескольким критериям.

Данная модель показана на разработанной в рамках работы схеме (рисунок 1).

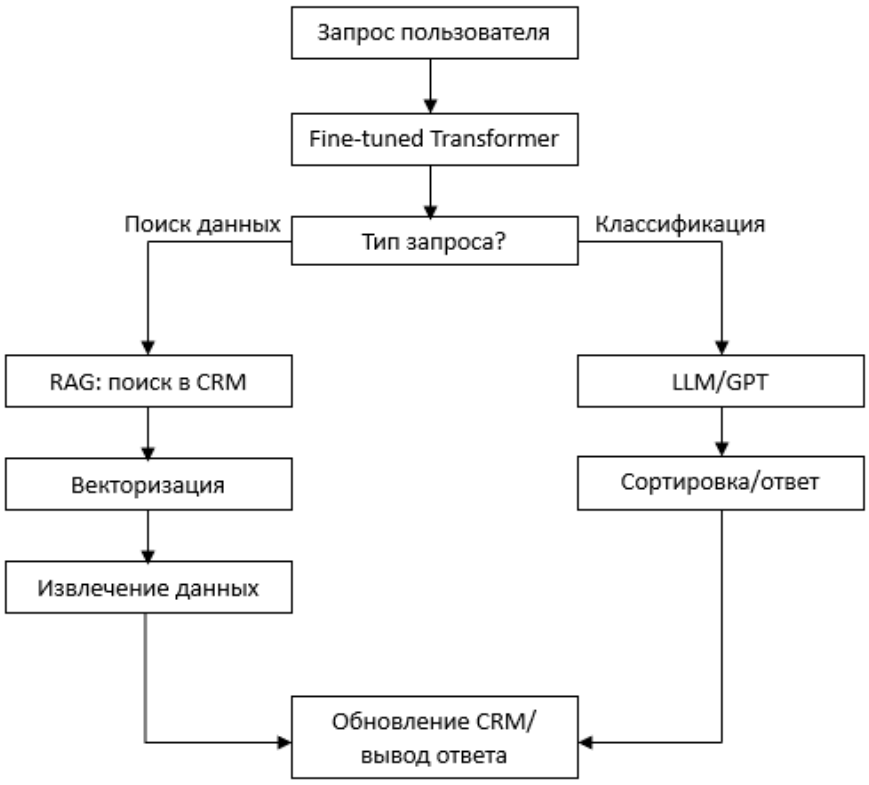


Рис. 1. Модель обработки запроса при помощи нейронной сети

Для работы данной модели необходимо выбрать архитектуру нейронной сети. В рамках данной модели была выбрана гибридная архитектура нейронной сети RAG (Retrieval-Augmented Generation) + Fine-tuned Transformer. Обе архитектуры относятся к современным методам обработки естественного языка и машинного обучения, эффективно дополняя друг друга. RAG обеспечивает поиск и извлечение данных из CRM-системы. Fine-tuned Transformer обрабатывает языковые запросы и генерирует осмысленные ответы на основе полученной информации из базы данных.

Архитектура модели нейронной сети RAG содержит два ключевых компонента – retriever и generator. Поисковый модуль находит релевантные данные в CRM с помощью векторного поиска, а генеративная модель формирует ответ на основе извлеченной информации (рисунок 2).

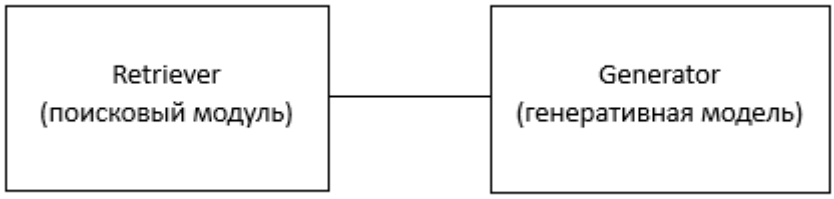


Рис. 2. Архитектура RAG нейронной сети

Дообученная языковая модель (Fine-tuned Transformer) – нейронная сеть, дополнительно обученная на корпоративных данных CRM. Такая модель способна понимать сложные запросы, включая профессиональную терминологию, и адаптируется под конкретные бизнес-задачи через процесс дообучения (рисунок 3).

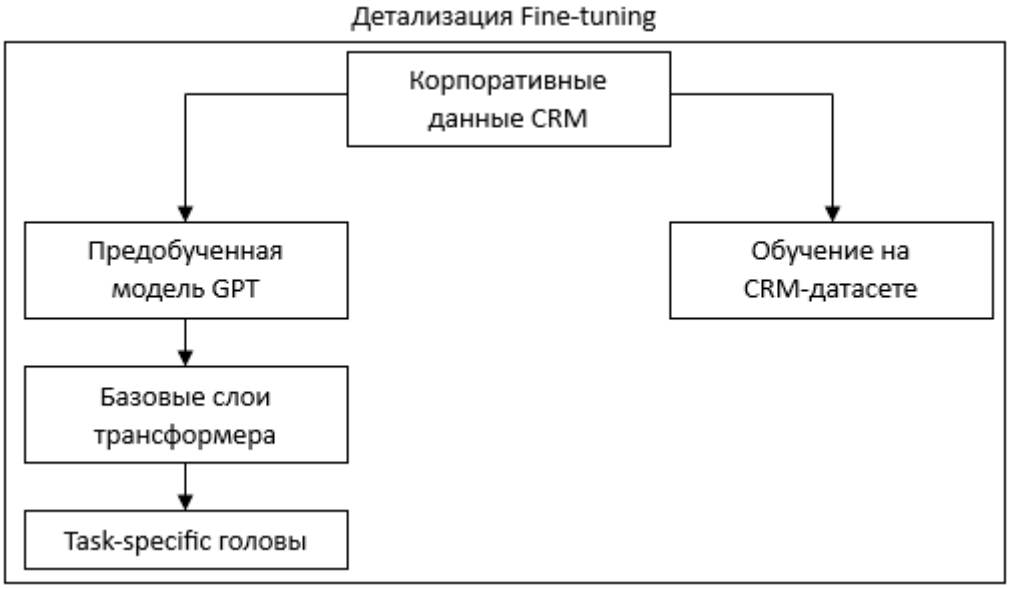


Рис. 3. Схема процесса дообучения нейронной сети

Рассмотрим, как описанная модель работает в реальном времени на примере запроса сотрудника к чат-боту:

«Найди количество клиентов, которые пользуются тремя услугами, имею подписок на сумму больше 1000 условных единиц и пользуются услугами нашего мобильного оператора более 4 лет».

Первым этапом идет получение и анализ запроса. Чат-бот принимает текстовый запрос.

Fine-tuned Transformer токенизирует и выделяет ключевые параметры:

- 3 услуги (мультиуслуга),
- подписки > 1000 у.е.,
- стаж > 4 года.

Интент: аналитический запрос, требует поиска в CRM.

Нормализация: преобразует запрос в структурированный формат (код).

Во втором этапе система ищет клиентов по заданным критериям. Модель Retriever (RAG) векторизирует запрос. Запрос преобразуется в вектор с помощью эмбеддингов.

Далее поиск в векторной базе данных CRM.

1) сравнение с индексированными данными клиентов;

2) фильтрация по:

- количеству подключенных услуг;
- сумме подписок;
- дате подключения.

Например, по итогам фильтрации и анализа будет найдено 247 клиентов, удовлетворяющих условиям.

В третьем пункте генерируется ответ. Чат-бот формирует ответ на основе найденных данных.

Fine-tuned Transformer преобразует данные в естественный язык и выдает ответ по полученным данным, например, в такой форме:

«Найдено 247 клиентов, которые:

- подключили 3 услуги,
- платежи превышают 1000 у.е.,
- являются абонентами более 4 лет».

В конце чат-бот будет задавать уточняющий вопрос:

«Необходимо ли добавить еще какие-либо фильтры поиска?».

Также возможно добавить кнопку «Экспорт в Excel», если это будет необходимо и технически возможно.

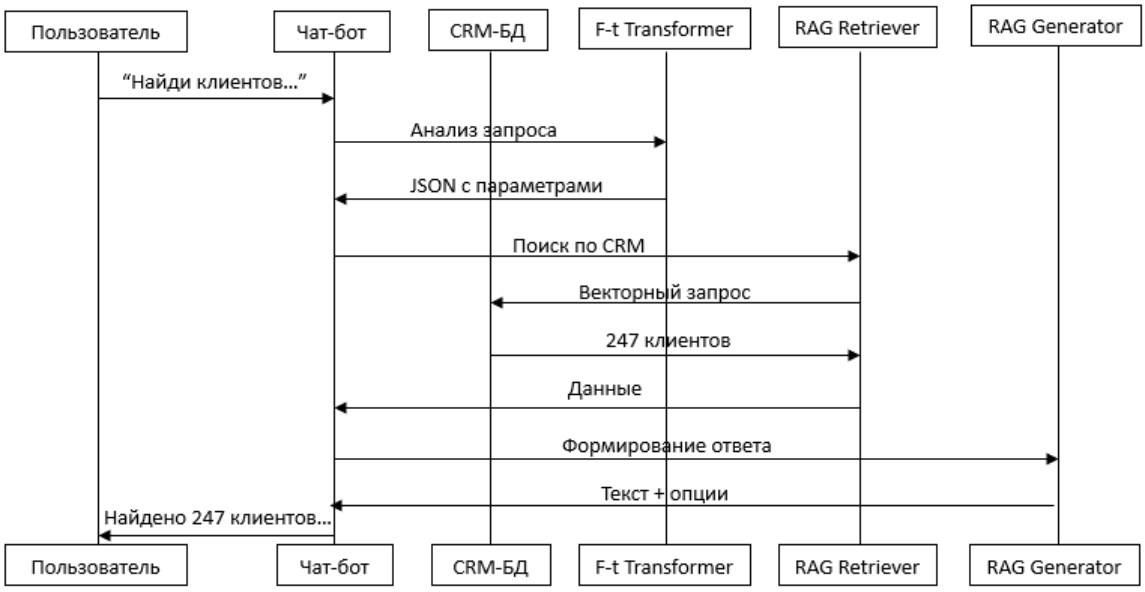


Рис. 4. Пример работы нейронной сети

В результате данная предложенная модель позволяет упростить работу со сбором и поиском нужных данных внутри CRM-системы и облегчить взаимодействие запроса получения информации между пользователем и базой данных. Настоящая работа является основой для дальнейших исследований и разработок в данной тематике.

Список используемых источников

1. Назипов Р. С. Перспективы применения искусственного интеллекта в оптимизации бизнес-процессов компаний // Международный журнал гуманитарных и естественных наук. 2024. № 1. С. 179-183. URL: https://cyberleninka.ru/article/n/perspektivy-primeneniya-iskusstvennogo-intellekta-v-optimizatsii-biznes-protsessov-kompaniy (дата обращения 17.04.2025).

2. Любинский М. С. Применение алгоритмов машинного обучения для сегментации клиентов в CRM-системах на основе анализа больших данных // Вестник науки. 2025. № 4 (85). URL: https://cyberleninka.ru/article/n/primenenie-algoritmov-mashinnogo-obucheniya-dlya-segmentatsii-klientov-v-crm-sistemah-na-osnove-analiza-bolshih-dannyh (дата обращения 17.04.2025).

3. Алексеев К.Н. Организация CRM-аналитики с использованием технологии Data mining // Финансовые рынки и банки. 2021. № 4. С. 4-9. URL: https://cyberleninka.ru/ article/n/organizatsiya-crm-analitiki-s-ispolzovaniem-tehnologii-data-mining/viewer (дата обращения 18.04.2025).

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

УДК 621.39
ГРНТИ 49.33.29

Ф. Н. Хоанг (аспирант кафедры ССиПД, СПбГУТ), khoang.fn@sut.ru

АНАЛИЗ ЗАДАЧИ ОПТИМИЗАЦИИ ПРОИЗВОДИТЕЛЬНОСТИ СЕТИ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ БАЛАНСИРОВКИ НАГРУЗКИ В ГЕТЕРОГЕННЫХ СРЕДАХ

В статье анализируется задача оптимизации производительности в гетерогенных сетях связи. Рассматривается переход от традиционных статических методов балансировки нагрузки к адаптивным динамическим подходам. Обосновывается ключевая роль технологий искусственного интеллекта и машинного обучения для эффективного распределения трафика, преодоления проблем совместимости и неравномерности производительности ресурсов. Интеграция интеллектуальных систем позволяет создавать гибкие, масштабируемые и устойчивые сетевые инфраструктуры, способные адаптироваться к изменяющимся нагрузкам в реальном времени.

балансировка нагрузки, производительность сети, гетерогенные среды, использование ресурсов, распределение трафика, узкие места

ANALYSIS OF NETWORK PERFORMANCE OPTIMIZATION USING LOAD BALANCING METHODS IN HETEROGENEOUS ENVIRONMENTS

Hoang P. N.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article analyzes the task of performance optimization in heterogeneous communication networks. It examines the transition from traditional static load balancing methods to adaptive dynamic approaches. The key role of artificial intelligence and machine learning technologies is substantiated for the effective distribution of traffic and for overcoming the problems of compatibility and uneven resource performance. The integration of intelligent systems allows for the creation of flexible, scalable, and resilient network infrastructures capable of adapting to changing loads in real time.

Key words: *load balancing, network performance, heterogeneous environments, resource utilization, traffic distribution, bottlenecks*

Введение

Современные сетевые инфраструктуры, характеризующиеся высокой степенью гетерогенности, сталкиваются с постоянным ростом требований к производительности и надежности [1]. Гетерогенная среда, объединяющая оборудование и программное обеспечение с различными характеристиками,

порождает сложную задачу эффективного распределения ресурсов. Неравномерная загрузка каналов и серверов приводит к возникновению «узких мест», увеличению задержек и снижению качества обслуживания, что напрямую влияет на экономическую эффективность и конкурентоспособность цифровых сервисов [2, 3]. В этом контексте методы балансировки нагрузки становятся центральным инструментом для оптимизации сетевой производительности. Их основная цель – интеллектуальное распределение входящего трафика между доступными ресурсами для предотвращения перегрузок и обеспечения максимальной утилизации мощностей [4, 5]. Данное исследование посвящено анализу эволюции методов балансировки: от простых статических алгоритмов до сложных динамических систем, усиленных искусственным интеллектом, которые являются ответом на вызовы современных гетерогенных сетей.

Стратегии балансировки нагрузки: от статики к динамике

Стратегии балансировки нагрузки можно условно разделить на два основных подхода: статический и динамический.

Статические методы, такие как Round Robin [6] или Least Connections [7], работают на основе предопределенных, неизменяемых правил. Их главное преимущество заключается в простоте реализации и минимальных накладных расходах. Однако их фундаментальный недостаток – неспособность адаптироваться к флуктуациям сетевого трафика в реальном времени. В условиях пиковых нагрузок или при изменении состояния сети статический подход неизбежно приводит к неоптимальному распределению ресурсов, когда одни серверы перегружены, а другие простаивают.

Динамические методы представляют собой более совершенный подход, разработанный для преодоления ограничений статики. Эти стратегии предполагают непрерывный мониторинг ключевых метрик производительности системы – таких как загрузка ЦП, использование памяти и время отклика – для принятия обоснованных решений о маршрутизации трафика. Алгоритмы, например, взвешенный Round Robin (Weighted Round Robin) или адаптивная балансировка, корректируют распределение нагрузки в реальном времени, направляя запросы на наименее загруженные и наиболее производительные узлы. Такая гибкость обеспечивает не только рациональное использование ресурсов, но и поддерживает стабильно высокую производительность сети даже при непредсказуемых изменениях нагрузки. Переход к динамической

балансировке является необходимым шагом для построения отзывчивых и эффективных сетей.

Ключевые вызовы в гетерогенных средах

Эффективная реализация балансировки нагрузки в гетерогенных средах сопряжена с рядом системных проблем, требующих комплексных решений.

Во-первых, проблема совместимости и сложности управления. Разнообразие аппаратного и программного обеспечения от разных производителей затрудняет создание единой, бесшовно интегрированной системы балансировки. Устаревшие компоненты инфраструктуры могут не поддерживать современные протоколы, что приводит к фрагментации управления и увеличению операционных затрат.

Во-вторых, вариабельность производительности ресурсов. Компоненты сети могут значительно различаться по вычислительной мощности и пропускной способности. Если алгоритм балансировки не учитывает эти различия, он может направить сложную задачу на маломощный узел, создавая таким образом новое «узкое место» и увеличивая общую задержку в системе.

В-третьих, вопросы безопасности. Маршрутизация трафика, особенно содержащего конфиденциальные данные, через различные узлы требует учета уникальных протоколов безопасности и уязвимостей каждого компонента. Неправильно настроенная балансировка может создать лазейки для атак или нарушить политики безопасности.

Решение этих проблем требует не просто выбора правильного алгоритма, а построения целостной адаптивной системы, способной учитывать все многообразие факторов в гетерогенной среде.

Интеграция интеллектуальных технологий: ИИ и машинное обучение

Для решения вышеописанных проблем современные системы балансировки нагрузки все чаще интегрируют передовые технологии, такие как машинное обучение (МО) и искусственный интеллект (ИИ).

Машинное обучение открывает возможности для предиктивной балансировки. Анализируя исторические данные о трафике и использовании ресурсов, модели МО способны выявлять закономерности и прогнозировать будущие пиковые нагрузки. Это позволяет системе проактивно перераспределять ресурсы еще до того, как возникнет

перегрузка, а не реагировать на нее постфактум. Алгоритмы постоянно самообучаются на основе новых данных, что со временем повышает точность прогнозов и эффективность распределения трафика.

Искусственный интеллект, в частности методы обучения с подкреплением, позволяет создавать автономные системы балансировки. Такая система самостоятельно, методом проб и ошибок, находит оптимальные стратегии маршрутизации для различных сценариев нагрузки, адаптируясь к уникальным условиям конкретной сети. ИИ также способен обнаруживать аномалии в сетевом трафике, которые могут указывать не только на проблемы производительности, но и на угрозы безопасности, обеспечивая своевременное реагирование.

Интеграция этих технологий с инструментами автоматизации и оркестрации позволяет создать централизованную и гибкую систему управления. Такой подход упрощает администрирование сложной гетерогенной инфраструктуры, снижает вероятность человеческой ошибки и обеспечивает высокую масштабируемость, позволяя сети эластично адаптироваться к росту потребностей бизнеса.

Заключение

Оптимизация производительности сетей в гетерогенных средах является комплексной задачей, выходящей за рамки традиционных подходов. Статические методы балансировки, несмотря на свою простоту, не отвечают требованиям современных динамичных и непредсказуемых нагрузок. Эффективное решение заключается в переходе к адаптивным динамическим системам, интеллектуальное ядро которых составляют технологии машинного обучения и искусственного интеллекта.

Такие системы способны не только реагировать на текущее состояние сети, но и прогнозировать будущие изменения, проактивно управляя распределением ресурсов. Интеграция ИИ позволяет решать фундаментальные проблемы гетерогенных сред, включая вариабельность производительности, сложность управления и обеспечение безопасности. Инвестиции в разработку и внедрение интеллектуальных, автоматизированных и масштабируемых решений по балансировке нагрузки являются стратегически важным шагом для обеспечения устойчивости, производительности и конкурентоспособности сетевых инфраструктур в долгосрочной перспективе.

Список используемых источников

1. Recommendation ITU-T Y.2060, Overview of the Internet of things.

2. Qiu Tie, et al. How can heterogeneous internet of things build our future: A survey // IEEE Communications Surveys & Tutorials 20.3 (2018): 2011-2027.

3. Koucheryavy A., Okuneva D., Paramonov A., Huang F. Methods of Traffic Distribution in a Heterogeneous High-Density Internet of Things Network // Proceedings of Telecommunication Universities. 2024;10(2):67–74. (in Russ.) DOI:10.31854/1813-324X-2024-10-2-67-74. EDN:RTNVEU.

4. Noaman, Muhammad, et al. Challenges in integration of heterogeneous internet of things // Scientific Programming 2022 (2022).

5. Paramonov A., High density internet of things network analysis. / Paramonov A., Koucheryavy A., Tonkikh E., Tatarnikova T. // Lecture Notes in Computer Science. 2020. T. 12525 LNCS. C. 307-316.

6. Youm, D. H., & Yadav, R. Load balancing strategy using round robin algorithm. Asia-pacific Journal of Convergent Research Interchange. 2016. № 2 (3). PP. 1-10.

7. Lucas-Estañ, M. C., & Gozalvez, J. Load balancing for reliable self-organizing industrial IoT networks. IEEE Transactions on Industrial Informatics. 2019. № 15 (9). PP. 5052-5063.

Статья представлена научным руководителем, профессором кафедры СС и ПД СПбГУТ, доктором технических наук, профессором Парамоновым А. И.

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА

УДК 004.318

А. Д. Бормотов (студент группы ИКТК-32, СПбГУТ), bormotov.ad@sut.ru
М. А. Мосенков (студент группы ИСТ-341, СПбГУТ), mosenkov.ma@sut.ru

ПЕРСПЕКТИВЫ АРХИТЕКТУРЫ RISC-V ДЛЯ РАЗВИТИЯ ОТЕЧЕСТВЕННЫХ ПРОЦЕССОРОВ

Современная компьютерная индустрия стоит на пороге значительных изменений, связанных с развитием открытых архитектур процессоров. RISC-V, как свободная и открытая архитектура набора инструкций, представляет особый интерес для развития отечественной микроэлектроники, имея возможность стать катализатором инноваций в разработке отечественных микропроцессоров в будущем. В данной статье рассматриваются ключевые особенности RISC-V, проводится сравнительный анализ с существующими архитектурами и оцениваются перспективы его внедрения в российских условиях.

архитектура процессоров, RISC-V

PROSPECTS OF RISC-V ARCHITECTURE FOR THE DEVELOPMENT OF DOMESTIC PROCESSORS

Bormotov A., Mosenkov M.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The modern computer industry is on the threshold of significant changes associated with the development of open processor architectures. RISC-V, as a free and open instruction set architecture, is of particular interest to the development of domestic microelectronics, with the potential to become a catalyst for innovation in the development of domestic microprocessors in the future. This article examines the key features of RISC-V, provides a comparative analysis with existing architectures, and assesses the prospects for its implementation in the Russian context.

Key words: *processor architecture, RISC-V*

Понятия CISC и RISC в архитектуре процессоров

CISC (Complex Instruction Set Computer) использует меньшее количество более сложных инструкций, каждая из которых может выполнять несколько операций. Такие инструкции обычно требуют разного количества тактов для выполнения и занимают больше места в памяти. Архитектура x86 является классическим примером CISC.

В противоположность этому, RISC (Reduced Instruction Set Computer) представляет собой принцип проектирования процессоров, основанный на использовании большого количества простых инструкций для выполнения вычислительных задач [1]. Каждая инструкция в RISC-архитектуре обычно выполняется за один такт процессора, что упрощает конвейерную обработку и может повысить эффективность работы.

Несмотря на исторически сложившееся противопоставление RISC и CISC, современные процессоры часто используют гибридный подход. Например, многие современные x86-процессоры внутренне разбивают сложные CISC-инструкции на более простые микрооперации, которые затем выполняются по принципам RISC.

Базовые архитектуры процессоров

1) x86_64: доминирующая архитектура для настольных и серверных систем

Архитектура x86_64 (также известная как AMD64 или Intel 64) является расширением 32-битной архитектуры x86 и представляет собой доминирующую архитектуру в сегментах десктопных ПК, лэптопов и серверного оборудования. Архитектура x86-64, первоначально предложенная Intel и затем выведенная на рынок компанией AMD, сохраняет полную обратную совместимость с программами, которые были созданы для ее предшественников. Данная архитектура основана на принципах CISC (Complex Instruction Set Computer) и характеризуется сложным набором инструкций различной длины.

Ключевой особенностью рынка x86_64 является его монополистическая структура. Только две компании – Intel и AMD – имеют право производить процессоры данной архитектуры, что значительно ограничивает конкуренцию и делает невозможным производство этих процессоров при наличии разногласий с компании, владеющими архитектурой. Несмотря на доминирующее положение, процессоры x86_64 сталкиваются с проблемами и в последнее время все больше уступают процессорам ARM в энергоэффективности.

2) ARM: энергоэффективное решение для мобильных устройств

Архитектура ARM (Advanced RISC Machine), изначально разработанная британской компанией ARM Holdings, стала стандартом для мобильных

устройств благодаря своей энергоэффективности. Важно отметить, что ARM относится к семейству RISC-архитектур.

В отличие от x86_64, ARM использует лицензионную бизнес-модель, при которой компания ARM Limited предоставляет лицензии другим производителям для создания совместимых процессоров. Это создает более конкурентную среду, но все также ограничивает возможности в свободной разработке и производстве процессоров. В последние годы процессоры ARM начали проникать на рынок настольных компьютеров и серверов, о чем свидетельствуют разработки Apple, Google, Amazon и других компаний.

3) Российские процессорные архитектуры:

- «Эльбрус» и VLIW-архитектура

Семейство процессоров «Эльбрус», которое развивает компания МЦСТ, является российской разработкой, основанной на VLIW-архитектуре (очень длинное командное слово), и позиционируется как замена импортным аналогам. Процессоры «Эльбрус» ориентированы прежде всего на применение в системах с повышенными требованиями к информационной безопасности, включая военные и государственные структуры.

Несмотря на определенные успехи, архитектура «Эльбрус» сталкивается с рядом проблем: относительно низкая производительность по сравнению с зарубежными аналогами, ограниченная программная экосистема и зависимость от иностранных производственных мощностей для изготовления чипов.

- «Байкал»: российские процессоры на базе ARM и MIPS

Процессоры серии «Байкал», разрабатываемые компанией «Байкал Электроникс», представляют собой еще одно направление развития отечественных микропроцессоров. В отличие от «Эльбруса», процессоры «Байкал» базируются на лицензируемых архитектурах ARM и MIPS, что обеспечивает лучшую совместимость с существующим программным обеспечением, но создает зависимость от зарубежных лицензиаров.

Как и «Эльбрус», процессоры «Байкал» нацелены прежде всего на государственный сектор и критически важную инфраструктуру, где вопросы технологического суверенитета имеют приоритетное значение перед производительностью и стоимостью.

4) RISC-V: новая парадигма в развитии процессорных архитектур

RISC-V представляет собой свободную и открытую архитектуру набора инструкций (ISA) [2], разработанную изначально в Калифорнийском университете в Беркли. Название RISC-V отражает, что это пятая версия архитектуры с сокращенным набором команд (RISC). Ее развитием и стандартизацией руководит швейцарская некоммерческая организация RISC-V International, что

помогает ей сохранять нейтралитет и оставаться вне геополитической повестки. Главное отличие RISC-V – ее полная открытость. Эта архитектура не является собственностью какой-либо компании, предоставляя любому желающему право бесплатно разрабатывать на ее основе собственные процессоры. Это значительно снижает барьеры для входа на рынок микропроцессоров и потенциально может послужить появлению инноваций в данной отрасли.

В настоящее время RISC-V уже используется в более чем 10 миллиардах чипов, преимущественно в микроконтроллерах и встраиваемых системах, но активно развивается и в направлении высокопроизводительных вычислений.

Преимущества и недостатки RISC-V

Преимущества:

1. Открытость и свобода от лицензионных ограничений. RISC-V является свободной и открытой архитектурой, что позволяет любому разработчику создавать процессоры без выплаты лицензионных отчислений.

2. Модульность и расширяемость. Архитектура предлагает базовый набор инструкций и возможность добавления специализированных расширений, что обеспечивает гибкость для различных применений [3].

3. Энергоэффективность. Как и другие RISC-архитектуры, RISC-V обеспечивает хорошую энергоэффективность благодаря использованию простых инструкций.

4. Независимость от геополитических факторов. Управление стандартом осуществляется международной организацией, базирующейся в нейтральной Швейцарии, что уменьшает риски геополитического влияния.

5. Стимулирование инноваций. Снижение барьеров для входа на рынок способствует появлению новых игроков и инновационных решений.

Недостатки RISC-V:

1. Отставание в производительности. На текущем этапе процессоры RISC-V отстают по производительности от современных x86_64 и высокопроизводительных ARM-процессоров.

2. Ограниченная программная экосистема. Несмотря на растущую поддержку, экосистема программного обеспечения для RISC-V пока не так развита, как для x86_64 или ARM.

3. Проблемы совместимости. Исторически совместимость была важной проблемой при внедрении новых архитектур. Однако с развитием веб-технологий эта проблема становится менее актуальной.

4. Фрагментация. Открытость архитектуры может привести к появлению несовместимых реализаций, что осложнит стандартизацию.

5. Ранняя стадия развития для высокопроизводительных систем. Хотя RISC-V уже широко используется в микроконтроллерах, его применение в высокопроизводительных вычислениях находится на начальной стадии развития.

Роль RISC-V в развитии отечественной микроэлектроники

1) Сопоставление RISC-V и x86_64: возможности и ограничения

Рынок процессоров с архитектурой x86_64, поделенный между Intel и AMD, функционирует в условиях дуополии. Как отмечается в источнике, «монополия на рынке приводит к стагнации, так как компании не имеют стимула к инновациям». В этих условиях открытая архитектура RISC-V выступает в качестве альтернативы, способной стимулировать рынок за счет появления новых разработчиков.

Ключевое историческое преимущество x86_64 – огромная библиотека совместимого ПО – постепенно теряет свою критическую значимость. «Сегодня пользователи ожидают, что системы будут работать вместе, независимо от архитектуры». Это создает возможности для альтернативных архитектур, таких как RISC-V.

Для полноценного конкурирования с x86_64 процессорам RISC-V предстоит достичь сопоставимых уровней производительности и стоимости. На данном этапе высокопроизводительные решения все еще находятся в стадии активной разработки, однако высокая динамика развития стандарта позволяет позитивно оценивать его долгосрочные перспективы.

2) RISC-V в сравнении с отечественными архитектурами

Для России RISC-V представляет интересную альтернативу развитию собственных архитектур, таких как «Эльбрус» и «Байкал". Вместо инвестирования значительных ресурсов в разработку уникальных архитектур, российские разработчики получают возможность сфокусироваться на проектировании чипов на основе RISC-V, что может сократить как финансовые, так и временные издержки. Кроме того, открытый стандарт RISC-V решает проблему экосистемной изоляции, характерную для закрытых проприетарных архитектур. Поскольку RISC-V является международным стандартом, процессоры на его базе могут быть интегрированы в глобальную экосистему программного обеспечения и аппаратных компонентов.

При этом RISC-V не исключает возможности внесения уникальных модификаций и расширений, необходимых для обеспечения национальной безопасности и соответствия российским стандартам. Модульная природа RISC-V позволяет добавлять специализированные расширения, например, для криптографических операций.

Потенциальные выгоды для российской экономики и технологического сектора

Массовое внедрение RISC-V может значительно укрепить технологический суверенитет России за счет разработки собственных процессоров, независимых от иностранных лицензий и санкций.

Открытая архитектура RISC-V стимулирует инновации, снижает стоимость производства и упрощает вход на рынок для малых компаний и стартапов.

Это также способствует развитию образовательных программ и формированию кадрового резерва в области микроэлектроники. Участие в международном консорциуме позволит российским специалистам влиять на развитие стандарта.

В долгосрочной перспективе, RISC-V предоставляет уникальные возможности для развития отечественной микроэлектроники и укрепления позиций России на глобальном технологическом рынке. Для успешной реализации необходима государственная поддержка разработок и образовательных инициатив.

Список используемых источников

1. Фролов В. А., Галактионов В. А., Санжаров В. В. (2020). Исследование технологии RISC-V // Труды Института системного программирования РАН. URL: https://cyberleninka.ru/article/n/issledovanie-tehnologii-risc-v (дата обращения 16.05.2025).

2. RISC-V: архитектура, которую будут развивать в РФ. Перспективы и возможности в России и мире // Habr (Selectel). 2022 URL: https://habr.com/ru/companies/selectel/articles/565952/ (дата обращения 16.05.2025).

3. RISC-V против x86 и ARM: когда открытая архитектура становится новым железным стандартом // Habr (X-Com). 2024. URL: https://habr.com/ru/companies/x-com/articles/915816/ (дата обращения 16.05.2025).

Статья представлена научным руководителем, доцентом кафедры САР СПбГУТ, кандидатом технических наук Волынкиным П. А.

УДК 621.372.542.21

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ МАССОГАБАРИТНЫХ ПАРАМЕТРОВ ФИЛЬТРА ЧЕБЫШЕВА ОТ ЕГО ОСЛАБЛЕНИЯ В ПОЛОСЕ ПРОПУСКАНИЯ

И. Ю. Боровков (студент группы ФП-31, СПбГУТ)
З. В. Зайцева (к.т.н., доцент, доцент кафедры электроники, СПбГУТ)
А. Р. Калинин (студент группы ФП-31, СПбГУТ)
М. А. Ольская (студент группы ФП-31, СПбГУТ), olskaya.ma@sut.ru

Фильтры Чебышева широко применяются в современных радиотехнических системах благодаря своей способности обеспечивать высокую избирательность и эффективное подавление помех, однако их массогабаритные параметры напрямую зависят от допустимого уровня ослабления в полосе пропускания. В статье представлены результаты исследования этой зависимости. Показано, как выбор величины неравномерности ослабления существенно влияет на вес и объем фильтра, рассчитанного для заданных условий.

фильтры, фильтры Чебышева, частота среза, полосы пропускания, ослабление, энергетические функции, массогабаритные параметры, конденсатор, катушка индуктивности

STUDY OF THE DEPENDENCE OF CHEBYSHEV FILTER SIZE AND WEIGHT PARAMETERS ON ITS PASSBAND ATTENUATION

Borovkov I., Zaitseva Z., Kalinin A., Olskaya M.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Chebyshev filters are widely used in modern radio engineering systems due to their ability to provide high selectivity and effective interference suppression; however, their mass and size parameters directly depend on the permissible level of attenuation in the passband. The article presents the results of a study of this dependence. It shows how the choice of attenuation ripple significantly affects the weight and volume of a filter designed for given conditions.

Key words: *filters, Chebyshev filters, cutoff frequency, passbands, attenuation, energy functions, mass and size parameters, capacitor, inductor*

Фильтры – это электронные устройства, предназначенные для выделения или подавления определенных частотных компонент в сигнале. Они играют ключевую роль в радиотехнике, связи и обработке сигналов, обеспечивая стабильность и качество передачи данных. Фильтр Чебышева, известный равноволновой характеристикой в полосе пропускания, отличается крутизной частотной характеристики за пределами этой полосы. В докладе исследуется, как изменение допустимого ослабления в полосе пропускания влияет на массу и габариты фильтра, что критично для проектирования компактных электронных систем.

При выполнении работы необходимо было рассчитать, как меняется масса и размеры фильтра при разных значениях ослабления в полосе пропускания, были взяты значения ослабления в диапазоне от 0,0004 до 0,04 дБ. В качестве исходных данных для моделирования фильтра были взяты значения нормированных элементов из справочника Рудольфа Зааля [1]. Для моделирования был выбран фильтр Чебышева четвертого порядка (рис. 1).

В качестве частоты среза полосы пропускания выбрано значение 10 кГц. Фильтр функционирует в режиме двухсторонней нагрузки [2] с сопротивлением R1 = 1000 Ом на входе, а на выходе сопротивление для каждого фильтра свое. Мощность устройства, выделяемая на нагрузке, составляет 1 кВт.

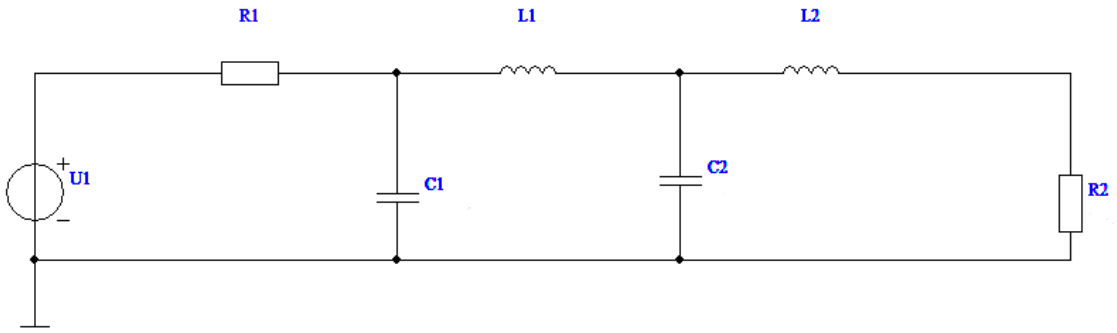


Рис. 1. Фильтр Чебышева четвертого порядка в режиме двухсторонней нагрузки

Перед началом моделирования, необходимо провести денормирование параметров фильтра [2], с помощью формул:

$$R2 = r \cdot R1; L = l \cdot \frac{R1}{\omega_0}; C = c \cdot \frac{1}{R1 \cdot \omega_0}$$

Сам расчет был произведен с использованием программы Mathcad. Для моделирования процессов, происходящих в цепи, использовалась программа Fastmean.

После того, как были синтезированы схемы фильтров с разным ослаблением в полосе пропускания, необходимо было рассчитать энергетические характеристики фильтров [3]. Энергетические параметры тесно связаны с АЧХ фильтра, его ГВЗ. Таким образом, изменение этих параметров ведет к изменению энергетических показателей, и, как следствие, массогабаритных параметров фильтра [4].

Для того, чтобы определить, каковы будут масса и размеры фильтра, необходимо ввести понятие удельных энергоемкостей «гамма». В работе рассматривается два вида энергоемкостей:

По массе:

$$\gamma^G = \frac{W}{G},$$

где W – энергия, выделяющаяся на элементе, G – его масса.

По габаритам:

$$\gamma^V = \frac{W}{V},$$

где W – энергия, выделяющаяся на элементе, V – его объем

Тогда, при условии равенства энергоемкостей всех компонентов вес и размеры фильтров можно определить следующим образом:

$$G = \frac{W_L}{\gamma_L^G} + \frac{W_C}{\gamma_C^G}; V = \frac{W_L}{\gamma_L^V} + \frac{W_C}{\gamma_C^V},$$

где W_L и W_C – суммарная энергия на всех индуктивностях и емкостях соответственно.

Равенства энергоемкостей компонентов можно достичь при использовании элементной базы одного производителя. Для расчета в данной работе были использованы следующие показатели, которые можно считать характерными для используемой в радиоэлектронной аппаратуре элементной базы [3]:

$$\gamma_L^G = 0{,}15 \text{ Дж/кг}; \gamma_C^G = 0{,}3 \text{ Дж/кг}; \gamma_L^V = 30 \text{ Дж/м}^3; \gamma_C^V = 700 \text{ Дж/м}^3.$$

Для расчета энергетических параметров устройства зададим мощность в нагрузке, равную 1 кВт. Необходимо рассчитать, каким должно быть напряжение источника питания для обеспечения этой мощности [5]:

$$P_2 = \frac{U_1^2}{4R_1},$$

где R_1 – сопротивление источника (1000 Ом), U_1 – его напряжение. Отсюда:

$$U_1 = \sqrt{P_2 \cdot 4R_1}$$

Из вышеприведенного соотношения получено необходимое значение напряжения в 2000 В.

С помощью этих данных было проведено моделирование процессов в цепи, позволяющее выполнить расчеты массогабаритных параметров фильтра. Моделирование проводилось в программе «Fastmean», схема представлена на рисунке 1. Так как программа «Fastmean» не поддерживает расчет

энергетических функций, необходимо было определить эти функции вручную. Это было сделано с помощью оператора «.define» (см. рис. 2).

```
.define
C1=14.8528645*10^(-9); C3=25.138762*10^(-9);
L2=0.0205681; L4=0.0121523;
wcTH=(0.5*(C1*mag(U(C1))^2+C3*mag(U(C3))^2));
wlTH=(0.5*(L2*mag(I(L2))^2+L4*mag(I(L4))^2));
```

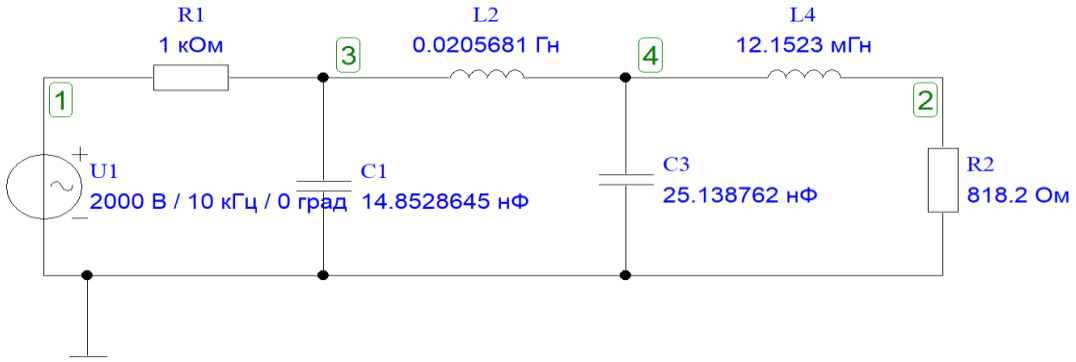


Рис. 2. Пример схемы для моделирования фильтра

Получены графики энергетических функций и определены их значения на граничной частоте полосы пропускания 10 кГц (см. табл. 1). Эти значения и использовались при дальнейших расчетах.

ТАБЛИЦА 1. Полученные значения энергий

Δa	$W_C \cdot 10^{-3}$ Дж	$W_L \cdot 10^{-3}$ Дж
0,0004	12,25	12,09
0,0017	15,30	14,99
0,0039	13,12	13,98
0,0109	16,05	18,04
0,0279	27,99	28,66
0,0436	25,94	25,09

Последним этапом стало нахождение массогабаритных параметров фильтров по полученным значениям энергий, с помощью соотношений для энергоемкостей компонентов. Результаты представлены в таблице 2.

ТАБЛИЦА 2. Зависимость массогабаритных параметров от ослабления в ПП

Δa, дБ	G, кг	V, $м^3$
0,0004	0,121	$4{,}207 \cdot 10^{-3}$
0,0017	0,151	$5{,}214 \cdot 10^{-3}$
0,0039	0,175	$6{,}118 \cdot 10^{-3}$
0,0109	0,211	$7{,}409 \cdot 10^{-3}$
0,0279	0,257	$9{,}006 \cdot 10^{-3}$
0,0436	0,284	$9{,}951 \cdot 10^{-3}$

Таким образом, на основе полученных данных, можно сделать вывод о том, что при увеличении значения ослабления в полосе пропускания фильтра Чебышева возрастают его энергетические показатели и, как следствие, увеличиваются массогабаритные параметры. Чтобы уменьшить вес и объем фильтра при заданном ослаблении, можно изменить аппроксимирующую функцию или оптимизировать конструкцию (использовать более совершенную элементную базу).

Список используемых источников

1. Зааль Р. Справочник по расчету фильтров: Пер. с нем. М.: Радио и связь, 1983. 752 с., ил.

2. Ханзел Г. Справочник по расчету фильтров: пер. с англ. М.: Сов. Радио, 1974.

3. Альбац М. Е. Справочник по расчету фильтров и линий задержки. М.: Госэнергоиздат, 1963.

4. Электронные цепи и методы их расчета. Расчет LC-фильтров и сравнительный анализ их показателей эффективности : учебно-методическое пособие по выполнению курсовой работы / В. В. Сергеев, З. В. Зайцева ; СПбГУТ. СПб., 2016. 28 с.

5. Справочник по расчету фильтров с потерями: Пер. с нем. М.: Связь, 1971.

УДК 621.39

Н. А. Васильев (к.т.н., старший научный сотрудник, ВАС)
Б. С. Лещинский (адъюнкт, ВАС)
Д. С. Ситдиков (младший научный сотрудник, ВАС), dima.sitdikov.99@mail.ru

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ: ПРИНЦИПЫ РАБОТЫ, ТЕХНОЛОГИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Данная работа представляет собой обзор современных радиотехнических и телекоммуникационных систем (РТС), включая их ключевые принципы функционирования, применяемые технологии и перспективные направления развития. Рассмотрены основные методы модуляции и демодуляции сигналов. Особое внимание уделено стандартам связи, таким как мобильные сети (4G, 5G, перспективы 6G), беспроводные технологии (Wi-Fi, Bluetooth) и спутниковые системы. Приведены сравнительные характеристики различных методов модуляции. В заключении обозначены ключевые тенденции развития РТС.

радиотехнические системы, телекоммуникационные системы, модуляция, демодуляция, мобильные сети, 4G, 5G, беспроводные технологии, Wi-Fi, Bluetooth, спутниковая связь

RADIO ENGINEERING AND TELECOMMUNICATION SYSTEMS: PRINCIPLES OF OPERATION, TECHNOLOGIES AND DEVELOPMENT PROSPECTS

Vasiliev N., Leshchinsky B., Sitdikov D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

This paper provides an overview of modern radio engineering and telecommunication systems (RTS), including their key operating principles, applied technologies and promising development directions. The main methods of signal modulation and demodulation are considered. Particular attention is paid to communication standards, such as mobile networks (4G, 5G, prospects for 6G), wireless technologies (Wi-Fi, Bluetooth) and satellite systems. Comparative characteristics of various modulation methods are given. In conclusion, key trends in the development of RTS are outlined.

Key words: *radio engineering systems, telecommunication systems, modulation, demodulation, mobile networks, 4G, 5G, wireless technologies, Wi-Fi, Bluetooth, satellite communications*

Радиотехнические и телекоммуникационные системы (РТС) представляют собой комплекс технологий и устройств, обеспечивающих передачу, прием и обработку радиосигналов. Они применяются в различных областях, таких как связь, радиолокация, навигация, телевидение, радиовещание и многое другое.

С развитием технологий и ростом потребности в быстрой и надежной связи, радиотехнические и телекоммуникационные системы стали ключевыми компонентами в обеспечении обмена информацией. От простых радиосистем до современных спутниковых и мобильных сетей – эти технологии революционизировали способы, которыми мы общаемся [1, 2].

Радиотехнические системы работают на основе передачи и приема электромагнитных волн, чаще всего в радиочастотном диапазоне (от 3 кГц до 300 ГГц). Рассмотрим основные принципы работы радиотехнических систем:

1. Модуляция – процесс наложения информации на несущую радиочастоту [3]. Существуют различные методы модуляции, такие как амплитудная (AM), частотная (FM), фазовая (PM) и их цифровые аналоги (QAM, PSK). В таблице 1 приведено сравнение распространенных методов модуляции. Отметим, что OFDM – мультиплексирование с ортогональным частотным разделением каналов, а MIMO – многоантенная технология; их включение в таблицу дано для полноты сопоставления.

2. Демодуляция – восстановление исходного сообщения на стороне приемника.

3. Шумоподавление. Радиоканал вносит аддитивные шумы и частотно-временные искажения (многолучевое распространение, интерференцию). Для повышения качества приема используют помехоустойчивое кодирование и адаптивные фильтры подавления импульсных помех [4].

Рассмотрим современные технологии и стандарты:

1. Современные системы сотовой связи обеспечивают широкополосный доступ и сервисы передачи данных [5].

1.1 Стандарт 4G LTE обеспечил кратный рост пропускной способности и качественную поддержку потокового мультимедиа. На нисходящей линии используется OFDMA, на восходящей – SC-FDMA; применяются адаптивная модуляция/кодирование и MIMO для увеличения скорости и устойчивости. Архитектура LTE позволяет гибко распределять спектр между абонентами и эффективно работать в условиях многолучевого распространения.

1.2 Новое поколение связи обеспечивает существенно меньшие задержки и высокую плотность подключений. 5G использует гибкую структуру кадра (гибкую нумерологию), массивные антенные решетки (massive MIMO) и сегментацию сети (network slicing) для обслуживания разнородных сервисов.

1.3 В стандарте 6G исследуются терагерцовые диапазоны, тесная интеграция методов ИИ в управление радиодоступом и совместная работа наземных, воздушных и спутниковых сегментов. Ожидается дальнейшее снижение задержек, рост энергетической эффективности [9].

ТАБЛИЦА 1. Сопоставление техник физического уровня: модуляции, мультиплексирование (OFDM), MIMO, терагерцовые частоты

Метод	Преимущества	Недостатки
AM (Амплитудная модуляция)	Простота реализации, широкая зона покрытия	Чувствительность к шумам, низкая эффективность использования спектра
ЧМ (Частотная модуляция)	Высокая устойчивость к шумам, лучшее качество звука	Широкая полоса частот, сложность схемы передачи
ФМ (Фазовая модуляция)	Высокая помехозащищенность, эффективное использование спектра	Сложность реализации, высокие требования к синхронизации
QAM (Квадратурная амплитудная модуляция)	Высокая спектральная эффективность, высокая скорость передачи данных	Высокая чувствительность к шумам, сложность схемы приема
PSK (Фазовая манипуляция)	Эффективное использование спектра, устойчивость к помехам	Высокие требования к синхронизации, сложная демодуляция
FSK (Частотная манипуляция)	Простота реализации, низкая чувствительность к фазовым искажениям	Низкая спектральная эффективность, требует больше полосы частот
ASK (Амплитудная манипуляция)	Простота реализации, низкие энергетические затраты	Высокая чувствительность к шумам, низкая спектральная эффективность
OFDM (Ортогональное частотное разделение каналов)	Высокая спектральная эффективность, устойчивость к многолучевому распространению	Высокая сложность реализации, чувствительность к частотным смещениям
MIMO (Многоканальная передача)	Увеличение пропускной способности, повышение надежности связи	Сложность реализации, высокие требования к обработке сигналов
Terahertz (Терагерцовые частоты)	Очень высокая скорость передачи данных, поддержка новых приложений (6G)	Ограниченная дальность передачи, сложность реализации

2. Беспроводные сети [6]:

2.1 Wi-Fi использует OFDM для передачи данных в диапазонах 2.4 ГГц и 5 ГГц. Основной принцип работы Wi-Fi – использование беспроводных точек доступа для подключения устройств к интернету.

2.2 Bluetooth использует частотную модуляцию (FHSS – Frequency Hopping Spread Spectrum) для передачи данных на короткие расстояния. Основной принцип работы Bluetooth – создание персональных сетей (PAN) для подключения устройств.

3. Спутниковые технологии. Спутниковая связь играет важную роль в глобальной телекоммуникационной структуре [7]. Она позволяет обеспечивать связь в отдаленных регионах, недоступных для традиционных сетей. Спутники способны передавать данные, осуществлять радиовещание и даже предоставлять интернет-доступ. Можно разделить спутники на геостационарные и низкоорбитальные.

3.1 Геостационарные спутники используют высокие орбиты (около 36 000 км) для обеспечения связи и телевещания. Основной принцип работы – синхронизация с вращением Земли, что позволяет спутнику оставаться в одной точке над поверхностью.

3.2 Низкоорбитальные спутники (например, Starlink [8]) используют орбиты на высоте 500-1200 км для обеспечения глобального покрытия интернетом. Основной принцип работы –использование множества спутников для создания сети с низкой задержкой.

Широкополосный мобильный доступ, Wi-Fi и современные спутниковые группировки радикально изменили модели взаимодействия в экономике и обществе: дистанционные форматы работы, онлайн-образование, телемедицина и логистика в реальном времени стали массовой практикой. Массовая цифровизация опирается на устойчивые РТС.

В ближайшие годы сочетание технологий искусственного интеллекта и Интернета вещей (IoT) в радио- и телекоммуникационных системах будет нацелено на уменьшение задержек, обеспечение детерминированного качества обслуживания и повышение энергоэффективности. Ключевую роль сыграют вычисления на «краю» (edge/MEC) для обработки данных ближе к источнику, сетевое сегментирование (network slicing) для разнородных сервисов, а также интеграция наземных и не-наземных сетей для глобального покрытия. Это расширит области применения: от промышленной автомати-

зации и роботизированных производств до критически важных коммуникаций для экстренных служб, интеллектуальных транспортных систем, мониторинга энергетики и комплексной городской безопасности.

Список используемых источников

1. Березовский П. П. Основы радиотехники и связи: учебное пособие. 2017.

2. Сейитнепесов Ч. и др. Зарождение и развитие радиотехники // Символ науки. 2024. № 4-1-2. С. 79-80.

3. Попов П. И. Анализ методов модуляции сигналов в радиотехнике: амплитудная, частотная, фазовая модуляция // Наука сегодня: глобальные вызовы, пути развития. Серия: естественные и технические науки» протокол заседания оргкомитета. 2023.

4. Боев С. Ф. и др. Радиотехнические системы и комплексы. 2021.

5. Нарзуллаев У. Х., Рустамов Т. Р. Развитие мобильных технологий от 4G к 5G // Universum: технические науки. 2023. № 9-2 (114). С. 55-58.

6. Завьялов С. В. и др. Учебное пособие по курсу «Беспроводные локальные сети»: Wi-Fi и Bluetooth: учебное пособие. 2022.

7. Мельникова Т. В., Преображенский А. П. Особенности современной спутниковой связи // Вестник Воронежского института высоких технологий. 2021. № 3. С. 49-51.

8. Пехтерев С. В., Макаренко С. И., Ковальский А. А. Описательная модель системы спутниковой связи Starlink // Системы управления, связи и безопасности. 2022. № 4. С. 190-255.

9. Wang C. X. et al. On the road to 6G: Visions, requirements, key technologies, and testbeds // IEEE Communications Surveys & Tutorials. 2023. Т. 25. № 2. С. 905-974.

УДК 681.586.78

О. А. Долматова (к.т.н., доцент, доцент кафедры физики, СПбГУТ)
Т. П. Закиров (студент группы РК-41, СПбГУТ), TPZakirov@sut.ru

ДАТЧИК ХОЛЛА, ФЕРРОЗОНД И МАГНИТОРЕЗИСТИВНЫЙ СЕНСОР: СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ОБЛАСТИ ПРИМЕНЕНИЯ

В мире современных технологий, при выполнении инженерных задач точность измерений магнитных полей становится критической задачей: от применения в навигации беспилотников до диагностики медицинского оборудования. Статья описывает способы работы датчиков, а также проводит сравнительный анализ датчиков Холла, магниторезистивных сенсоров и феррозондов для определения наиболее подходящей области применения для каждого сенсора, учитывая параметры чувствительности, энергопотребления, стоимости и условиях эксплуатации.

магнитные датчики, датчик Холла, феррозонд, магниторезистивный сенсор

COMPARING HALL-EFFECT SENSOR, FLUXGATE MAGNETOMETER AND MAGNETO RESISTIVE SENSOR. WHICH ONE IS THE BEST?

Dolmatova O., Zakirov T.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the world of modern technologies, when tackling engineering tasks, precise measurements of magnetic fields become one of the key tasks in engineering. From application in UAVs navigation to medical equipment diagnostics. The article describes how different magnetic sensors work and makes analysis on the fields, to which Hall-effect sensors, fluxgate magnetometer and MR-sensors are best applied to, taking sensitivity, energy consumption, cost and operating conditions into account.

Key words: *magnetic sensor, Hall-effect sensor, fluxgate magnetometer, magneto resistive sensor*

Введение

Статья посвящена сравнительному анализу магнитных датчиков для определение самой подходящей области применения для каждого вида. Будут рассмотрены факторы чувствительности, погрешности, цены и энергопотребления [1-3].

Основные принципы работы

Магнитные датчики отвечают за преобразование магнитного поля в электрические сигналы, по которым можно судить о тех или иных параметрах измеряемого поля. Поговорим о каждом из них.

Датчик Холла в своей работе опирается на одноименный Эффект Холла, открытый Эдвином Холлом под конец девятнадцатого века, описывает, что если поместить проводник с током в магнитное поле, то в теле проводника на движущиеся электроны со стороны магнитного поля действует сила Лоренца и отклоняет их в сторону (рис. 1). В результате на одной грани пластины накапливаются электроны, на другой – их нехватка. Это создает напряжение, пропорциональное силе поля.

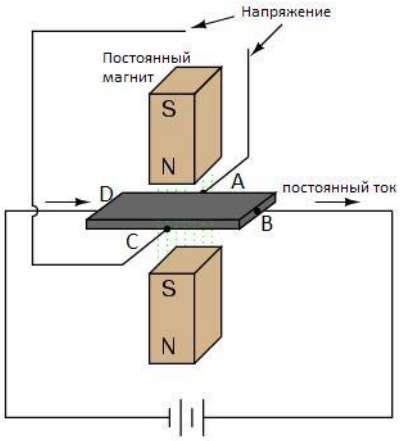


Рис. 1. Схема эффекта Холла

Датчики Холла отличаются по выходным данным и режиму работы. Аналоговые выдают продолжительный сигнал, цифровые выдают сигнал при достижении пороговых значений.

Феррозонды (рис. 2) представляют из себя активную «магнитную антенну», способную улавливать даже очень слабые поля. Ферромагнитный сердечник из магнитомягкого материала под действием внешнего поля намагничивается, что влияет на его магнитную проницаемость. А это, в свою очередь, влияет на индуктивность катушки. По изменениям индуктивности катушки можно судить о характеристиках измеряемого поля.

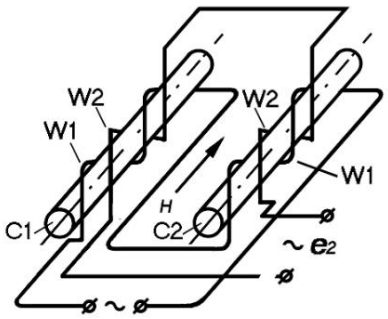


Рис. 2. Устройство дифференциального феррозонда, C_1 и C_2 – идентичные сердечники из магнитомягкого материала, W_1 и W_2 – возбуждающая и измерительная обмотки

Феррозонд выделяется исключительной чувствительностью до нТл, когда магнитное поле Земли составляет 50 мкТл. А также использует переменный ток для подавления шумов, играющих серьезную роль при измерении слабых полей.

Магниторезистивные сенсоры – это группа датчиков, работающих на группе эффектов, отвечающих за изменение удельного сопротивления проводника в зависимости от магнитного поля. В данной статье будет описано несколько эффектов (рис. 3).

AMR – эффект расшифровывается как Anisotropic MagnetoResistance, по-русски называется анизотропным магнитосопротивлением. При этом эффекте сопротивление проводника меняется при повороте магнитного момента материала. В пример можно привести пленки пермаллоя.

GMR – эффект расшифровывается как Giant MagnetoResistance, по-русски называется гигантским магнитосопротивлением. Эффект возникает в многослойных структурах с чередующимися ферро- и немагнитными слоями. GMR – сенсоры в жестких дисках считывают данные, улавливая микроскопические изменения магнитных доменов на поверхности пластин.

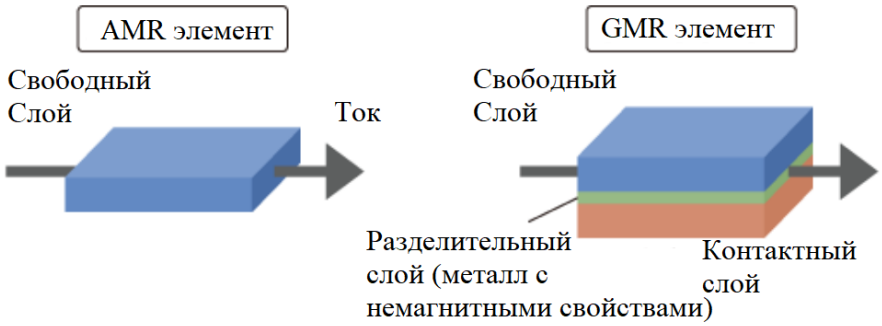


Рис. 3. Схема AMR и GMR эффектов

Каждый подход уникален: Датчики Холла достаточно просты в эксплуатации и дешевы на фоне остальных. Феррозонды выгодно отличаются от соперников выдающимися показателями чувствительности, но достаточно требовательны в эксплуатации на фоне деградирующего со временем и воздействием высоких температур сердечника. Магниторезистивные сенсоры показывают усредненный результат, не требуя особых условий эксплуатации и показывая хорошую точность, которая, впрочем, сильно зависит от используемого в датчике эффекта.

Сравнительный анализ

Сравнение датчиков магнитного поля представлено в таблице 1.

ТАБЛИЦА 1. Сравнение датчиков магнитного поля

Критерий	Датчик Холла	Феррозонд	Магниторезистивный датчик
Чувствительность	1–100 мТл	до 0.1 нТл	0.1–10 мТл
Факторы погрешности	Температура, Э/М помехи	Температура, старение сердечника, Э/М помехи	Э/М помехи
Температура работы	-40°C до + 150°C	до + 80°C	до + 200°C
Электромагнитные помехи	Требует экранирования	Уязвимы	Требует экранирования
Вибрации	Требуют металлический корпус	Уязвимы	Уязвимы
Энергопотребление	1-20 мВт	До 100 мВт	1-5 мВт

Начнем с чувствительности – способности датчика реагировать на минимальные изменения магнитного поля.

Датчик Холла работает в диапазоне 1–100 мТл. Это делает его идеальным для задач, где поле достаточно сильное: например, определение положения дроссельной заслонки в автомобиле. Но для слабых полей, как в медицинской диагностике, его возможностей недостаточно. Феррозонд способен уловить поля до 0.1 нТл. Он значительно точнее датчиков Холла и благодаря ферромагнитному сердечнику и катушке он усиливает слабые сигналы, что незаменимо в геофизике для поиска полезных ископаемых или в археологии. Магниторезистивный сенсор занимает промежуточное положение. Например, *GMR*-датчики работают в диапазоне 0.1–10 мТл. Именно их используют в жестких дисках для считывания данных с намагниченных дорожек. Факторы погрешности у каждого датчика определены эффектом, на котором основывается работа соответствующего устройства.

Среди факторов погрешности первой стоит выделить температуру. Датчики Холла сильно зависят от температуры. При нагреве их выходное

напряжение дрейфует. Производители встраивают термокомпенсационные схемы в попытках купировать негативное воздействие, но это увеличивает стоимость. МР-датчики более стабильны. Их слоистая структура из ферромагнетиков и диэлектриков меньше реагирует на нагрев. Феррозонды капризны: изменение температуры влияет на магнитные свойства сердечника. В высокоточных измерениях их помещают в термостаты.

Электромагнитные помехи тоже играют заметную роль в точности измерений магнитных сенсоров. Датчики Холла и МР-сенсоры защищают экранированием. Например, в автомобильных системах их часто заключают в металлические корпуса. Феррозонды, несмотря на чувствительность, страдают от внешних полей. В промышленных цехах с мощными двигателями их показания могут искажаться.

Дрейф во времени является фактором погрешности сугубо для феррозонда. Сердечник устройства подвержен старению, то есть потере магнитных свойств со временем. Со временем его нужно заново калибровать.

Серьезная статья в эксплуатации любого устройства – вибрации: датчики Холла в пластиковых корпусах хрупки. Зато версии в металлических корпусах (например, для станков) устойчивы. МР-сенсоры монтируют на печатные платы, поэтому они чувствительны к ударам. Феррозонды боятся вибраций – катушка может сместиться относительно сердечника.

Также стоит упомянуть об энергопотреблении – побеждают МР-сенсоры. Им нужно всего 1–5 мВт, что критично для IoT-устройств на батарейках. Феррозонды требуют питания для генерации вторичного поля, что потребляет до 100 мВт.

Применение

Датчики Холла находят применение в широком списке бытовой электронике и нетребовательных системах, где нужно дешевое и простое решение. Феррозонды широко применяются в дефектоскопии, археологии и множестве других областей, где требуются точные измерения. МР-сенсоры занимают широкую нишу компактных устройств, имея при этом превосходящие датчики Холла показатели энергопотребления и чувствительности.

Заключение

Каждый датчик обладает рядом выдающихся качеств, определяющих область применения сенсора. Чувствительность, условия эксплуатации,

цена и области у всех разные. Ниши, которые заняли датчики, почти не пересекаются и покрывают современные инженерные задачи почти полностью.

Список используемых источников

1. Афанасьев Ю. В. Феррозондовые приборы. // Л. Энергоатомиздат, 1986. https://www.elec.ru/library/nauchnaya-i-tehnicheskaya-literatura/ferrozondovye-pribory/

2. Курс общей физики: учебное пособие. Санкт-Петербург: Лань, 2021. Т. 2. URL: https://e.lanbook.com/book/167870

3. Электричество и магнетизм / И. В. Савельев. 5-е изд. Санкт-Петербург: Лань, 2021. 352 с. ISBN 978-5-8114-1208-2.

УДК 681.84.081.47

О. А. Долматова (к. ф.-м. н. доцент кафедры физики, СПбГУТ)
Р. А. Реннике (студент группы РК-41, СПбГУТ), rennike.ra@sut.ru

ПРИМЕНЕНИЕ ПРИНЦИПА ДИФФЕРЕНЦИАЛЬНОГО СИГНАЛА В ИЗГОТОВЛЕНИИ ЭЛЕКТРОМАГНИТНЫХ ЗВУКОСНИМАТЛЕЛЕЙ

В статье рассматривается проблема шумов и помех в электромагнитных звукоснимателях и анализируется метод балансного шумоподавления, основанный на принципе дифференциального сигнала. Описана конструкция и принцип работы электромагнитных звукоснимателей, включая влияние ключевых параметров системы на качество выходного сигнала.

шумоподавление, дифференциальный сигнал, электромагнитный звукосниматель

IMPLEMENTATION OF THE DIFFERENTIAL SIGNAL PRINCIPLE IN THE MANUFACTURE OF ELECTROMAGNETIC PICKUPS

Dolmatova O., Rennike R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the problem of noise and interference in electromagnetic pickups and analyzes the balanced noise reduction method based on the principle of differential signal. The design and operating principle of electromagnetic pickups are described, including the influence of key system parameters on the quality of the output signal.

Key words: *noise suppression, differential signal, electromagnetic pickup*

Введение

Несмотря на то, что электромагнитные звукосниматели появились довольно давно, главная их проблема (шумы, наводки и помехи) так и не была в полной мере устранена. В этой статье будет рассмотрен ставший привычным для всех метод шумоподавления, а именно шумоподавление, реализованное за счет принципа дифференциального сигнала. Шумоподавление, основанное на принципе дифференциального сигнала, называют балансным шумоподавлением. Данный метод получил широкое распространение благодаря своей эффективности и относительной простоте реализации.

Электромагнитный звукосниматель

Электромагнитный звукосниматель представляет собой узкоспециализированный преобразователь механических колебаний металлической

струны в электрический сигнал. Электромагнитные звукосниматели функционируют благодаря явлению электромагнитной индукции и являются основой любого современного электронного музыкального инструмента [1].

Конструкция электромагнитного звукоснимателя представлена на рис. 1.

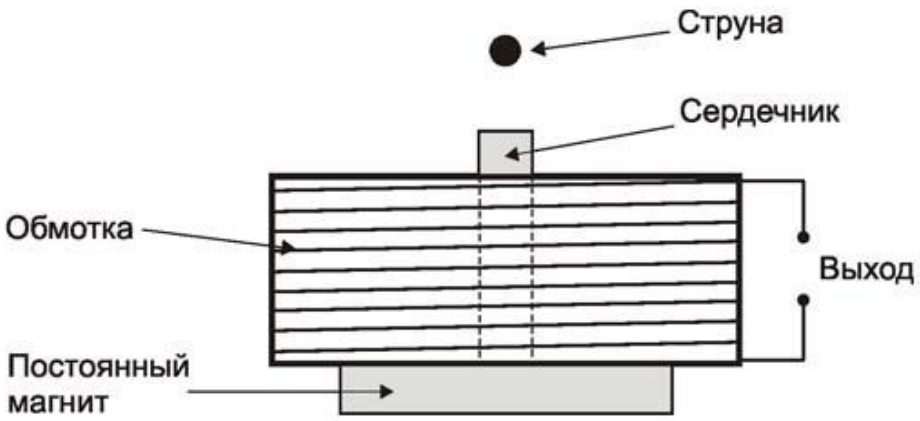


Рис. 1. Конструкция электромагнитного звукоснимателя

Электромагнитный звукосниматель состоит из следующих элементов: катушка индуктивности, магнитовод (сердечник) и постоянный магнит. Число витков катушки в фабричных звукоснимателях варьируется в диапазоне от 4000 до 25000 витков. Однако в авторских решениях этот диапазон ничем не ограничен, и верхняя его граница доходит иногда до 30000 витков. Сердечник, находящийся внутри катушки, должен быть изготовлен из магнитомягкого материала, такого как электротехническая сталь, пермаллой или альсифер, сравнение характеристик которых приведено в табл. 1.

ТАБЛИЦА 1. Сравнение характеристик магнитомягких материалов, используемых для изготовления магнитоводов

Характеристика	Электротехническая сталь (10895)	Пермаллой (79НМ)	Альсифер (Sendust)
Магнитная проницаемость	3000-5000	20000-100000	30000-60000
Индукция насыщения, Тл	1.8	0.8	1.0
Коэрцитивная сила, А/м	80	4	15

Постоянный магнит выбирается исходя из задач. В разных случаях могут быть использованы керамические, AlNiCo-II или AlNiCo-V магниты [1]. Различные сочетания характеристик компонентов электромагнитного звукоснимателя обеспечивают такие параметры электромагнитного звукоснимателя, как уровень выходного сигнала и тембральный окрас звука.

Принцип работы электромагнитного звукоснимателя

Электромагнитный звукосниматель представляет собой преобразователь механических колебаний в электрический сигнал, действие которого основано на законе электромагнитной индукции Фарадея-Ленца [2]. Согласно данному закону, изменение магнитного потока, пронизывающего замкнутый контур (в данном случае – катушку индуктивности), индуцирует в этом контуре электродвижущую силу (ЭДС), величина которой определяется выражением:

$$\varepsilon_i = -N\frac{d\Phi}{dt}, \quad (1)$$

где: ε_i – индуцированная ЭДС, N – количество витков катушки, Φ – магнитный поток, пронизывающий витки катушки.

В электромагнитном звукоснимателе статическое магнитное поле создается постоянным магнитом, соединенным с магнитоводом (сердечником). Такая система формирует магнитное поле, силовые линии которого пронизывают рабочую зону струны. Струна, выполненная из ферромагнитного материала, концентрирует магнитный поток, существенно увеличивая плотность магнитного поля у своей поверхности. При колебании струны происходит изменение магнитного поля, а, как следствие, изменения магнитного потока через витки катушки. Из выражения (1) видно, что уровень выходного сигнала зависит от скорости и от числа витков катушки электромагнитного звукоснимателя, также уровень выходного сигнала зависит от амплитуды колебаний струны (амплитуда выходного напряжения пропорционально произведению амплитуды колебания струны на частоту). Уровень выходного сигнала также зависит от геометрии электромагнитного звукоснимателя, характеристик постоянного магнита и магнитной проницаемости материала струны. Оптимальные показатели достигаются при минимизации зазора между струной и магнитоводом (сердечником) и использовании магнитоводов с высокой магнитной проницаемостью.

Шумы и помехи в электромагнитных звукоснимателях

Электромагнитные звукосниматели подвержены воздействию различных видов шумов и помех, которые существенно влияют на качество выходного сигнала. Основным источником паразитных наводок является сама конструкция звукоснимателя, представляющая собой катушку индуктивности с большим количеством витков (обычно от 4000 до 25000), которая по своей природе действует как эффективная антенна, восприимчивая к внешним электромагнитным полям. Наиболее значительными помехами являются сетевой фон частотой 50 или 60 Гц, возникающий из-за наводок от электросети и близко расположенных трансформаторов, а также высокочастотные помехи, создаваемые импульсными источниками питания и цифровыми устройствами. Кроме того, существенное влияние оказывают импульсные помехи, вызванные коммутацией мощных электроприборов, и низкочастотные наводки от силовых кабелей. Важным фактором является также нелинейность магнитных характеристик сердечника, приводящая к гармоническим искажениям, особенно заметным при больших амплитудах сигнала. Все эти виды помех накладываются на полезный сигнал, ухудшая соотношение сигнал/шум.

Балансное шумоподавление в электромагнитных звукоснимателях

Балансное шумоподавление, основанное на принципе дифференциального сигнала, представляет собой наиболее эффективный метод борьбы с помехами в электромагнитных звукоснимателях. Физический принцип работы данной системы заключается в использовании двух идентичных катушек, намотанных в разные стороны, магнитоводы которых подсоединены к разным полюсам магнита (рис. 2), что позволяет реализовать подавление синфазных сигналов.

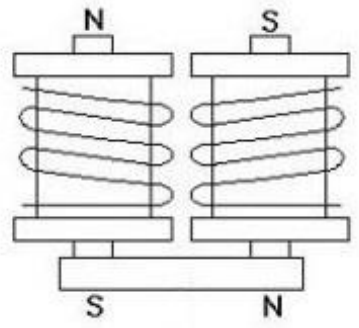


Рис. 2. Конструкция электромагнитного звукоснимателя с балансным шумоподавлением

При таком конструктивном решении полезный сигнал, возникающий от колебаний струны, суммируется в фазе, в то время как внешние электромагнитные помехи, наводимые одинаково на обе катушки, взаимно вычитаются. Эффективность данного метода определяется степенью симметрии катушек – идентичностью их индуктивностей, активных сопротивлений и взаимного расположения относительно источника помех. Параметром, определяющим эффективность балансного шумоподавления, является коэффициент подавления синфазного сигнала, который в качественных звукоснимателях может достигать 20-30 дБ. Геометрическое расположение катушек влияет не только на шумоподавляющие свойства, но и на частотную характеристику устройства. Особенностью балансного шумоподавления является характерное изменение тембра выходного сигнала, обусловленное взаимодействием магнитных полей двух катушек и их частотными характеристиками, что необходимо учитывать при проектировании звукоснимателей. Технологически реализация данного метода требует высокой точности изготовления компонентов и тщательного подбора материалов для обеспечения идентичности параметров катушек, что является ключевым фактором эффективности шумоподавления.

Экспериментальное исследование эффективности системы балансного шумоподавления

С целью практического тестирования системы балансного шумоподавления был изготовлен тестовый стенд, конструкция которого представлена на рис. 3.

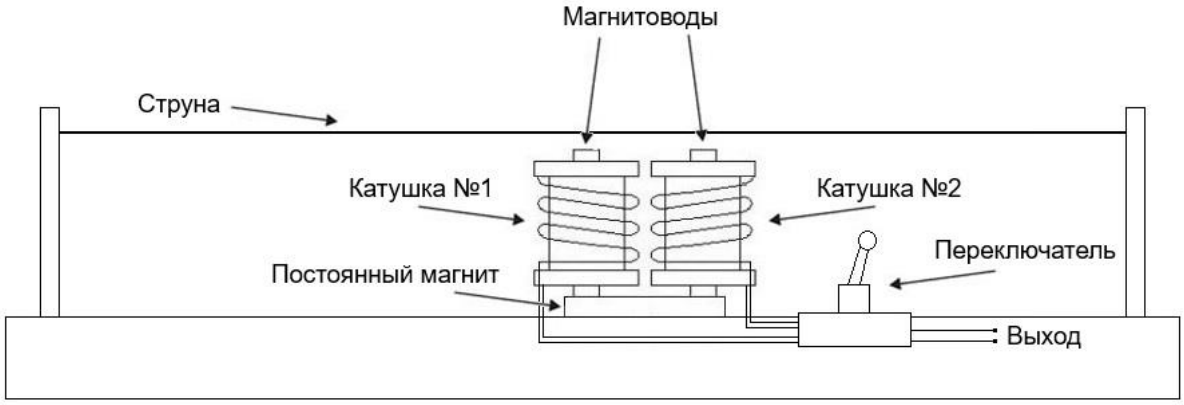


Рис. 3. Конструкция тестового стенда

Тестовый стенд состоит из: электромагнитного звукоснимателя, натянутой над ним струны, переключателя. Для тестирования был изготовлен

электромагнитный звукосниматель, характеристики которого приведены в табл. 2.

ТАБЛИЦА 2. Характеристики изготовленного электромагнитного звукоснимателя

Характеристика	Значение
Число витков одной катушки	16000
Общее число витков	32000
Толщина проволоки, мм	0.01
Материал магнитоводов	Электротехническая сталь (10895)
Тип магнита	Керамический

Такие специфические характеристики (очень большое число витков) были выбраны специально, чтобы звукосниматель был более восприимчив к помехам и шумам, что упрощает их исследование. Выбор других компонентов электромагнитного звукоснимателя был обусловлен их доступностью и невысокой ценой. Переключатель позволяет включать стенд в двух режимах: в режиме № 1 к выходу подключена только катушка № 1, в режиме № 2 к выходу параллельно подключены катушка № 1 и катушка № 2. Это позволяет быстро включать и отключать балансное шумоподавление, наглядно демонстрируя шумоподавляющий эффект. В ходе первого этапа тестирования к выходу тестового стенда был подключен усилитель звука. При переключении тестового стенда из режима № 1 в режим № 2 наблюдалось значительное уменьшение уровня шума. В ходе второго этапа эксперимента к выходу тестового стенда был подключен милливольтметр. При переключении тестового стенда из режима № 1 в режим № 2 наблюдалось повышение уровня выходного сигнала с 350 мВ до 600 мВ. Такие показатели свидетельствуют о корректной работе системы балансного шумоподавления.

Заключение

Балансное шумоподавление, основанное на принципе дифференциального сигнала, остается наиболее эффективным и проверенным временем методом борьбы с помехами в электромагнитных звукоснимателях. Несмотря на появление новых технологий, таких как активные системы и цифровая обработка сигнала, этот подход продолжает доминировать благодаря своей

надежности, простоте реализации и предсказуемым акустическим характеристикам. Главным недостатком метода остается необходимость обеспечивать высокую степень соответствия катушек, так как при использовании катушек с разными, даже незначительно отличающимися характеристиками, шумоподавляющий эффект значительно ослабевает. Дальнейшее совершенствование метода видится в оптимизации конструктивных параметров катушек, применении новых магнитных материалов и более точном согласовании компонентов системы. Важно отметить, что выбор конкретного решения всегда представляет собой компромисс между уровнем шумоподавления, тембральными особенностями и практическими требованиями музыкантов, что подтверждает необходимость продолжения исследований в данном направлении.

Список используемых источников

1. Смолин К. О. Звукосниматели [Для электро и бас гитар, акуст. гитар и др. инструментов], Справ. М.: Смолин, 2004. 160 с. ISBN 5-93477-026-8.

2. Савельев И. В. Курс общей физики: учебное пособие: в 5 томах / И. В. Савельев. 5-е изд. Санкт-Петербург: Лань, [б. г.]. Том 2: Электричество и магнетизм. 2011. 352 с. ISBN 978-5-8114-1208-2.

УДК 621.396

М. В. Исаков (магистрант группы РТ-42м, СПбГУТ), isakov.mv@sut.ru

ОСОБЕННОСТИ ПРИМЕНЕНИЯ OFDM-MIMO СИСТЕМ В КОРОТКОВОЛНОВОМ КАНАЛЕ РАДИОСВЯЗИ

В настоящее время происходит интенсивное развитие программных комплексов цифровой обработки сигналов. Благодаря этому становится возможным применение OFDM-MIMO систем в коротковолновом канале радиосвязи. Данное решение позволяет уменьшить негативное воздействие поляризационных замираний, которые возникают при ионосферном распространении радиосигнала.

OFDM, MIMO, короткие волны, радиосвязь, поляризационные замирания

APPLICATION FEATURES OF OFDM-MIMO SYSTEMS IN SHORTWAVE RADIO COMMUNICATION CHANNEL

Isakov M.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Nowadays, there is an active development of various software systems of digital signal processing. This enables the implementation of OFDM-MIMO systems in the shortwave radio channel. This solution makes it possible to reduce the negative effects of polarization fading that occur during ionospheric propagation of a radio signal.

Key words: *OFDM, MIMO, short waves, radio communication, polarization fading*

В современном мире радиосвязи и телекоммуникаций коротковолновой диапазон обеспечивает передачу данных на большие расстояния при относительно малой стоимости используемого оборудования. Приоритетной задачей в системах коротковолновой (КВ) радиосвязи является увеличение скорости передачи данных. Это необходимо для качественной передачи файлов большого объема, например, для трансляции видеоизображений. Однако, при ионосферном распространении на радиосигналы воздействуют различные факторы, включая поляризационные замирания – явление, способное вызывать проблемы в передаче данных, значительно снижая качество связи [1].

Применение технологии мультиплексирования с ортогональным частотным разделением каналов, т.е. OFDM (Orthogonal frequency-division multiplexing) сигналов позволяет снизить воздействие поляризационных за-

мираний и повысить помехоустойчивость в коротковолновом канале радиосвязи. OFDM может рассматриваться и как вид модуляции, и как технология мультиплексирования.

Еще одним перспективным решением является технология MIMO (Multiple Input, Multiple Output – система связи со многими входами, многими выходами). Данная технология позволяет разделять общий поток данных на несколько параллельных потоков, которые одновременно передаются в общей полосе частот, но по разным пространственным или поляризационным каналам, являющихся независимыми.

Наиболее эффективным методом совместного применения OFDM и MIMO в коротковолновом канале радиосвязи является поляризационное разнесение потоков данных. В данном случае входной поток делится на два независимых потока, которые поступают на входы соответствующих поляризационных каналов. Далее следует одновременное излучение многочастотных сигналов с вертикальной и горизонтальной поляризацией [2]. На рис. 1 представлена структурная схема типового комплекса радиосвязи MIMO 2x2 и OFDM-модуляторами и OFDM-демодуляторами.

Рис. 1. Структурная схема типового комплекса радиосвязи

Стоит отметить, что вместо одной несущей частоты OFDM использует множество ортогональных поднесущих (обычно от десятков до тысяч). Каждая поднесущая модулируется независимо (QPSK, QAM и др.), но их частоты подобраны так, что пики одной поднесущей попадают в нули соседних, т.е. реализуется их ортогональность. Ортогональность важна для минимизации межканальных помех (ICI – Inter-Carrier Interference).

OFDM использует быстрое преобразование Фурье (БПФ) для генерации и декодирования сигнала. Следовательно, передатчик преобразует ча-

стотные компоненты в временной сигнал, а приемник восстанавливает данные из временного сигнала. При приеме OFDM-сигналов необходима синхронизация приемника и передатчика как по времени, так и по частоте [3].

Чтобы бороться с межсимвольной интерференцией из-за многолучевого распространения, в OFDM добавляют циклический префикс ЦП (CP – Cyclic Prefix) – копию конца символа в его начало. Если задержка сигнала меньше длины ЦП, приемник корректно декодирует данные.

На рис. 2 приведена временная диаграмма OFDM-символов с межсимвольной интерференцией с применением ЦП и без ЦП.

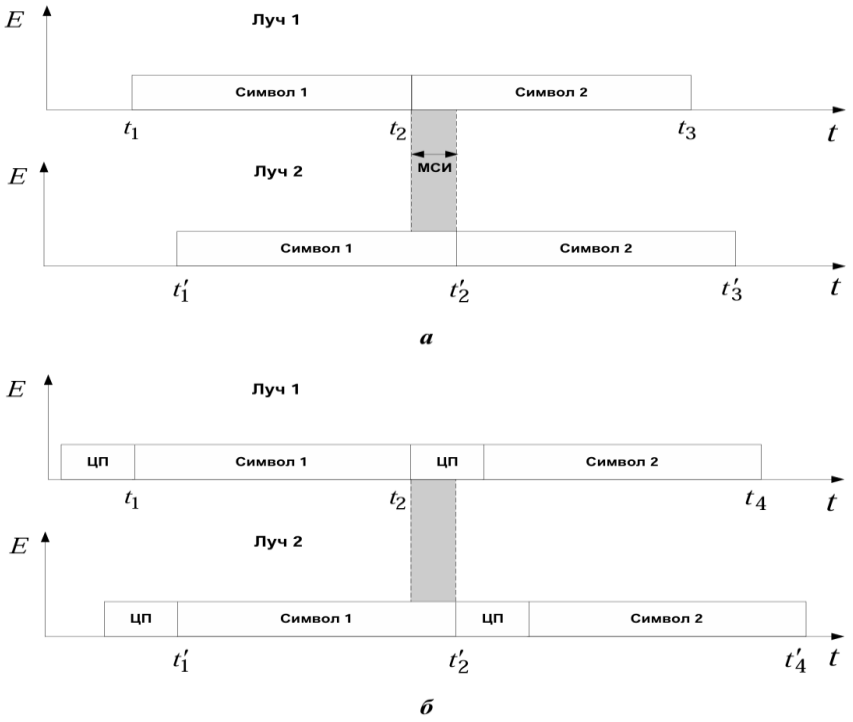


Рис. 2. Временная диаграмма OFDM-символов при межсимвольной интерференции: без циклического префикса (а), с циклическим префиксом (б)

Данное решение позволяет предотвратить взаимное влияния символов, которые следуют друг за другом. В результате добавления циклического префикса в спектре радиосигнала не возникают новые частотные составляющие. Длительность ЦП должна превышать длительность импульсной характеристики канала, но не должна быть слишком большой, так как это приводит к потере в отношении сигнал/шум (ОСШ), а также снижению скорости передачи данных, потому что ЦП не несет в себе полезной информации. Для КВ-каналов с задержками до 5 мс абсолютное время ЦП составляет 2–10 мс. На практике длительность ЦП выбирают равной 1/4, 1/8, 1/9 от длительности символа. В формуле (1) приведена спектральная эффективность OFDM системы:

$$\frac{R}{W} = \frac{m}{1+\alpha}, \quad (1)$$

где R – результирующая скорость передачи информации; W – ширина спектра сигнала; m – количество бит в одном символе; α – доля защитного интервала в длительности символа.

Таким образом, спектральная эффективность определяется числом бит в модуляционном символе m, добавляются лишь небольшие потери из-за введения циклического префикса [4].

Было произведено моделирование каналов, основанное на подходе, рекомендованном МСЭ. Для современных цифровых систем с OFDM/MIMO наиболее актуальна ITU-R HF.1396, сочетающая многолучевость (3–5 лучей с задержками до 3 мс) и доплеровские сдвиги в 0.1–5 Гц (из-за ионосферной нестабильности). В каналах используется модуляция сигнала QPSK, замирания рассчитываются по распределению Рэлея. В канале с OFDM используются 64 поднесущие и полоса 24 кГц, следовательно, циклический префикс имеет длину 3.33 мс (16 отсчетов), которая должна превышать максимальную задержку многолучевости. Система MIMO 2x2 имеет разнесение передающих и приемных антенн по поляризации (вертикальная и горизонтальная) и использует пространственное кодирование (Alamouti). Результаты моделирования каналов приведены на рис. 3 в виде графиков вероятности битовой ошибки (BER – Bit Error Rate) и отношения сигнал/шум (SNR – Signal/Noise Ratio).

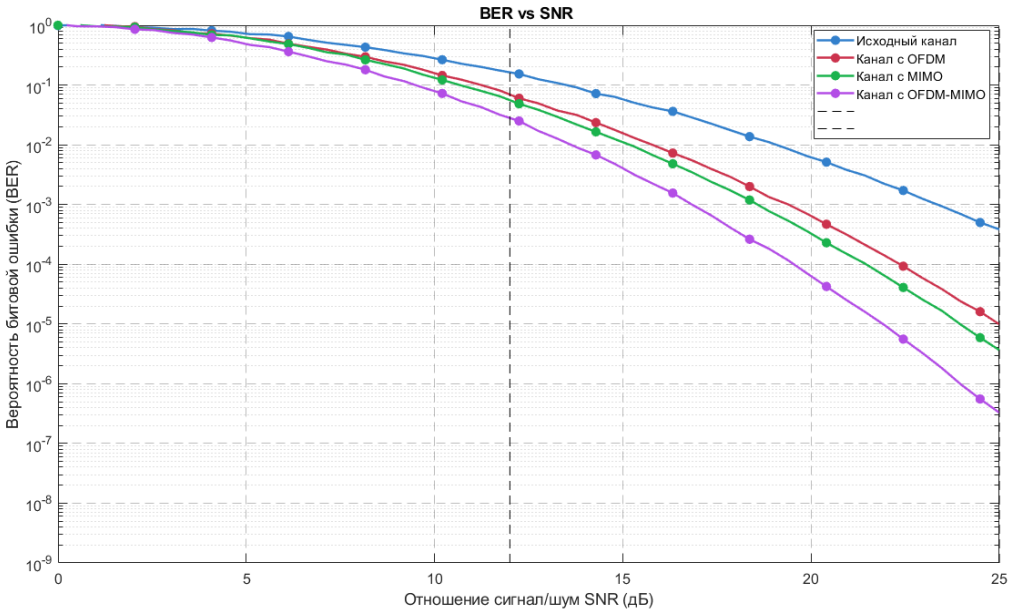


Рис. 3. Моделирование каналов с применением OFDM, MIMO, OFDM и MIMO.

Применение OFDM-MIMO системы в коротковолновом канале радиосвязи существенно улучшает качество связи, т.к. требуемое отношение сигнал/шум уменьшилось примерно на 5 дБ при вероятности битовой ошибки 10^{-3}. Стоит отметить, что для дальних линий (≥1000 км) лучше использовать адаптивные OFDM-параметры (изменение размера циклического префикса, выбор поднесущих). Также необходимо учитывать изменения параметров модуляции для сохранения оптимального SNR при передаче данных: BPSK (для низкого SNR), QPSK/16-QAM (для высокого SNR) [5]. В таблице 1 приведены параметры моделей коротковолновых каналов радиосвязи с поляризационными замираниями. Комбинация OFDM-MIMO дает максимальную эффективность, позволяя снизить BER в 100 раз, скорость передачи данных увеличивается в 3 раза, повысить устойчивость канала к поляризационным замираниям, а также улучшить помехозащищенность, устойчивость к межсимвольной интерференции.

ТАБЛИЦА 1. Сравнение параметров моделей коротковолновых каналов

	Исходный канал	Канал с OFDM	Канал с MIMO	Канал с OFDM-MIMO
BER (SNR = 20 дБ)	$\leq 10^{-2}$	$\leq 10^{-3}$	$\leq 10^{-3}$	$\leq 10^{-4}$
Спектральная эффективность (бит/с/Гц)	1-2	3-4	2-3	5-6
Устойчивость к МСИ	Нет	Да	Нет	Да
Устойчивость к поляризационным замираниям	Нет	Частично	Да	Да

Таким образом, полученные данные позволят усовершенствовать существующие методы снижения поляризационных замираний, а также помочь в изучении процессов, которые приводят к возникновению замираний.

Список используемых источников:

1. Ступницкий М. М., Лучин Д. В. Потенциал КВ-радиосвязи для создания цифровой экосистемы России // Электросвязь. 2018. С. 46-54.

2. Шадрин Б. Г., Дворянчиков В. А., Боганков Б. С. Метод повышения скорости передачи данных в системах КВ-радиосвязи и его реализация (часть 1) // Техника радиосвязи. 2020. Выпуск 4 (47). С. 7–22. DOI:10.33286/2075-8693-2020-47-07-22.

3. Загидулин Ю. Т., Казанцев А. А., Хворенков В. В. Исследование способов передачи информации сигналами OFDM в коротковолновом диапазоне // Инфокоммуникационные технологии. 2007. Т. 5. № 4. С. 77–80.

4. Батырев И. А. Методы синхронизации OFDM-сигнала по циклическому префиксу // Техника радиосвязи. 2018. Вып. 1 (36). С. 90–102.

5. Бояршинов М. А., Загидуллин Ю. Т. Использование автоматического определения скорости передачи данных в адаптивных системах КВ-связи // Материалы IX Междунар. науч.-техн. конф. «Физика и технические приложения волновых процессов»: Изд-во Челяб. гос. ун-та, 2010. С. 26.

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

УДК 621.314.263

А. Н. Коробейников (магистрант группы ФП-41м, СПбГУТ),
korobeinikov.an@sut.ru

СИНТЕЗ СМЕСИТЕЛЯ СВЧ ДИАПАЗОНА С ВОЗМОЖНОСТЬЮ РЕГУЛИРОВКИ РАБОЧЕЙ ТОЧКИ ДИОДОВ

В статье описана оригинальная топология мостового небалансного смесителя частот СВЧ диапазона. Приведена эквивалентная принципиальная схема и результаты математического моделирования частотных характеристик, а также масштабный макет самой топологии и его снятая в ходе эксперимента частотная характеристика. Сделаны предположения о возможных вариантах включения нелинейных элементов, описаны достоинства структуры.

СВЧ, радиочастотные смесители

SYNTHESIS OF A MICROWAVE MIXER WITH THE CAPABILITY OF ADJUSTING THE DIODE OPERATING POINT

Korobeinikov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article describes the original topology of an unbalanced frequency mixer. An equivalent circuit and the results of mathematical modeling are presented, as well as a scale model of the topology itself and its frequency response. Assumptions are made about possible options for the inclusion of nonlinear elements.

Key words: *UHF, radio frequency mixers*

Топология мостового небалансного смесителя считается одной из наиболее простых и наглядных. Зачастую, она строится на квадратурном мосте, который позволяет получить развязку между входными портами гетеродина и входного сигнала [1, 2], частоты которых обычно лежат достаточно близко.

Одной из модификаций данной структуры является вариант с разрывом гальванической связи, при котором сигнал передается через емкостную связь между линиями (рис. 1). При этом области связи остаются равны четверти длины волны рабочей частоты. Данный прием позволяет гальванически развязать порты гетеродина и входного сигнала, что позволяет, например, использовать разные напряжения смещения для смесительного диода и p-i-n диода коммутатора в цепи гетеродина.

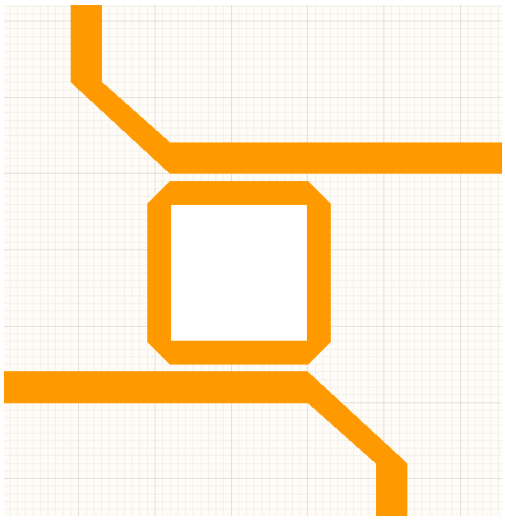


Рис. 1. Топология мостового небалансного смесителя с емкостной связью между плечами моста

Для дальнейшей отработки данной топологии была составлена принципиальная схема. С нее были убраны шлейфные фильтры, т.к. на данном этапе они не имеют принципиального значения. Составленная принципиальная схема (рис. 2), которая в дальнейшем была адаптирована для лучшей корреляции с дальнейшими экспериментами.

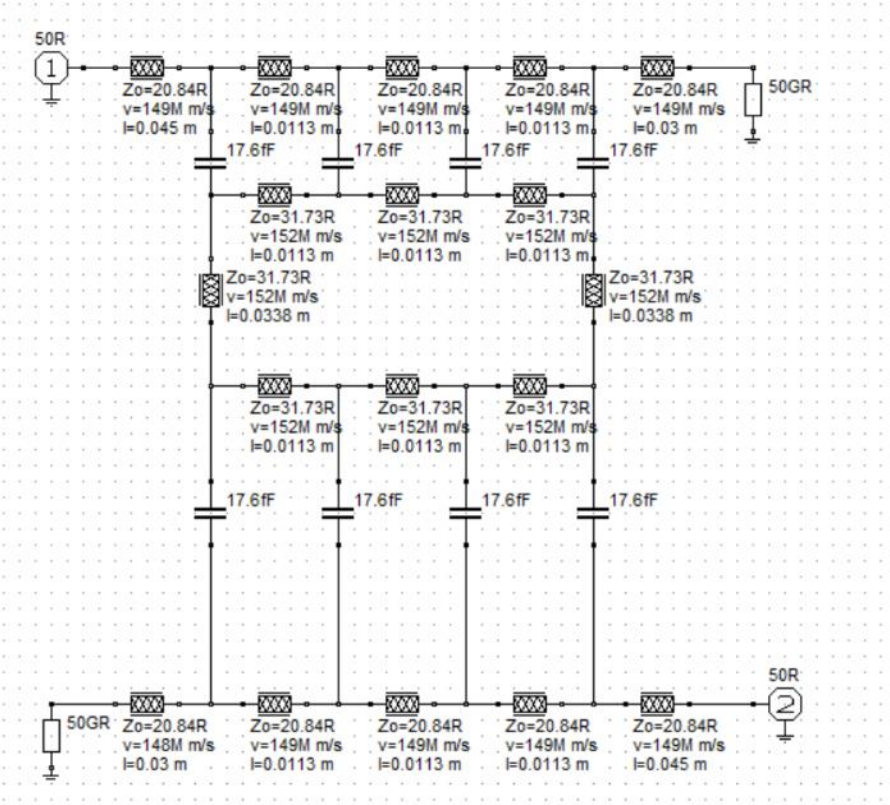


Рис. 2. Принципиальная схема топологии моста в RFsim99.
Схема адаптирована для лучшей корреляции с экспериментальными данными

Далее, с помощью математического моделирования были получены показатели S_{21} (рис. 3).

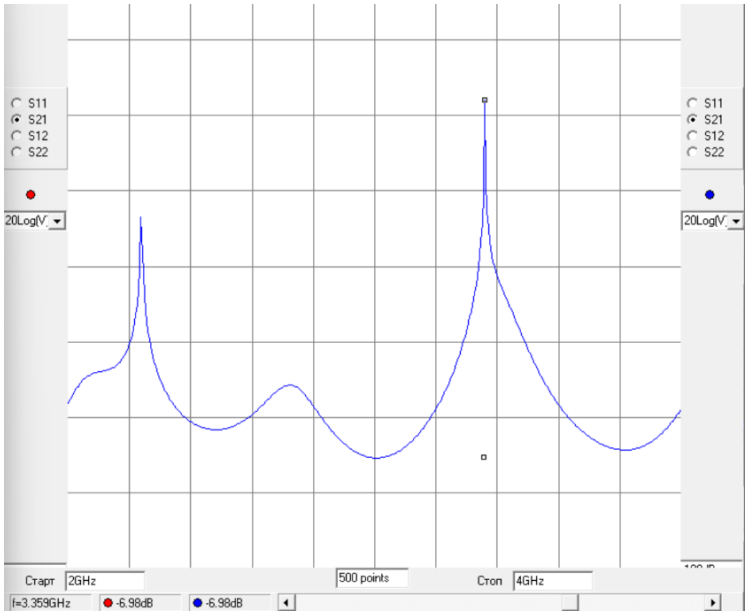


Рис. 3. Эмуляция S_{21} принципиальной схемы в RFsim99, линейный масштаб

Однако модель не учитывает электродинамические показатели данной топологии, например изгибы линий под прямым углом, что делает прямоугольник идентичным любой произвольной фигуре. В связи с этим, было решено создать экспериментальную топологию моста, в котором прямоугольный сегмент заменен на кольцевой эллиптический резонатор (рис. 4).

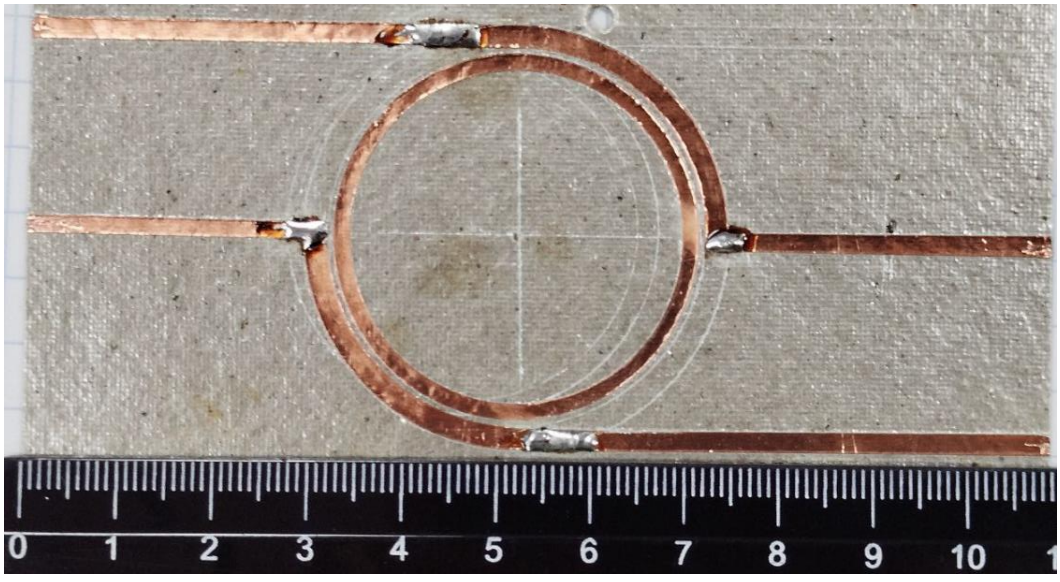


Рис. 4. Макет моста небалансного смесителя с экспериментальной топологией

После чего S_{21} макета был измерен с помощью измерительного комплекса Р2-67 (рис. 5).

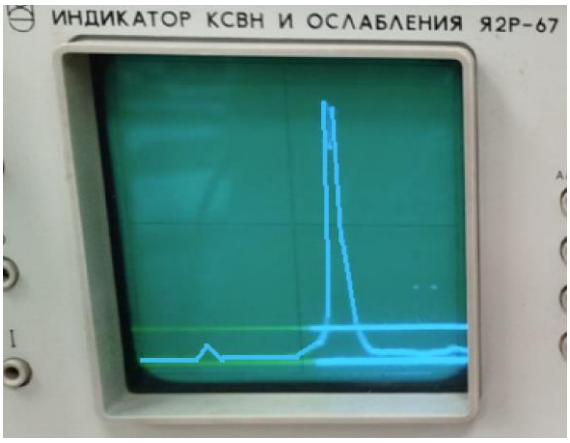


Рис. 5. S_{21} макета моста с экспериментальной топологией, линейный масштаб. Линия обведена в графическом редакторе в связи с низкой контрастностью

Хорошо видна сходимость результатов математического моделирования и проведенных измерений, что говорит о справедливости модели. Резонансные пики находятся на тех же частотах и имеют приблизительно те же соотношения по пропусканию, что и в модели. Дальнейшим этапом будет установка смесительного диода в различные точки схемы, в том числе и классическая компоновка (рис. 1).

В результате работы была исследована оригинальная топология смесителя, создан макет и математическая модель, повторяющая результаты измерений. К приемуществам топологии можно отнести возможность установки 3 рабочих точек для элементов, потенциально расположенных на на различных ее участках, а также потенциально более высокую добротность, за счет использования кольцевого эллиптического резонатора в качестве элемента моста. Кроме того, использование данного резонатора по сути позволяет интегрировать в данную топологию узкополосное устройство частотной селекции [3], снижая тем самым уровень шумовой составляющей в выходном сигнале.

Список используемых источников

1. Дингес С., Кочемасов В. СВЧ-преобразователи частоты. Часть 1 Основные сведения о преобразователях частоты // Компоненты и технологии. 2018. № 4. С. 18-23.

2. Гвоздев В. И., Нефедов Е. И. Объемные интегральные схемы СВЧ. М.: Наука, 1985. 246 с.

3. Сазоненко Н. Ю., Седышев Э. Ю. Устройства частотной селекции на основе кольцевых эллиптических резонаторов на микрополосковой линии // Электроника и микроэлектроника СВЧ. 2019. Т. 1. С. 409-411. EDN;NVXLXX

Статья представлена научным руководителем, доцентом кафедры электроники СПбГУТ, кандидатом технических наук Седышевым Э. Ю.

УДК 621.397.4

Л. С. Курбатский (студент гр. ИКТ-412, СПбГУТ), kurbatskii.ls@sut.ru
М. С. Рягузова (студент гр. ИКТ-412, СПбГУТ), ryaguzova.margarita@sut.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ СТАБИЛИЗАЦИИ ИЗОБРАЖЕНИЯ: ВЫБОР НАИБОЛЕЕ ЭФФЕКТИВНОЙ СИСТЕМЫ

Статья посвящена анализу современных систем стабилизации изображения и их практическому применению в медиаиндустрии. Цель исследования – рассмотреть различные технологии стабилизации и сравнить их. На основе принципов работы стабилизаторов была проведена сравнительная характеристика по ключевым параметрам. Практическая значимость работы заключается в возможности выбора оптимальной системы стабилизации с учетом конкретных требований к качеству визуального контента и сопутствующих затрат. Анализ ситуации позволяет проводить поиск «идеального» стабилизатора с учетом специфики задач, при этом универсальность достигается через гибкость комбинирования технологий.

система стабилизации, качество изображения

COMPARATIVE ANALYSIS OF IMAGE STABILIZATION SYSTEMS: SELECTING THE MOST EFFECTIVE SYSTEM

Kurbatsky L., Ryaguzova M.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The report is dedicated to an analysis of modern image stabilization systems and their practical application in the media industry. The research objective is to examine various stabilization technologies and compare them. Based on the operating principles of stabilizers, a comparative analysis was conducted using key parameters. The practical significance of the work lies in the possibility of selecting an optimal stabilization system, taking into account specific requirements for visual content quality and associated costs. Analysis of the situation allows for the search for an "ideal" stabilizer considering the specifics of the tasks, while versatility is achieved through the flexibility of combining technologies.

***Key words**: stabilization system, image quality*

Стабилизатор изображения – это система, компенсирующая дрожание камеры или объектива для предотвращения смазывания кадров. Стабилизаторы позволяют создать качественную картинку, при этом снижая затраты на производство и повышая удобство съемки, за счет размеров и технологии компенсирования дрожания. В настоящее время без стабилизаторов не выходит ни одно большое кино, концерт или спортивное событие.

Системы стабилизации классифицируются на две основные категории: аппаратные (крепится к камере внешне) и встроенные (реализуется внутри камеры) [1].

Стедикам – устройство, используемое в киносъемке и фотографии для снижения и устранения смазывания и тряски изображения из-за движения камеры. Оно состоит из уравновешенной системы и работает на принципе инерции масс.

В основе стедикама лежит штанга и противовес на противоположном конце, что придает системе большую массу и значительно большую инерцию по оси противовеса камеры. Из-за этого изменяется центр тяжести объекта, и данная система становится более устойчивой к вращательным движениям и пространственным колебаниям. В конструкции стедикама используется трехосный шарнирный узел, находящийся рядом с центром тяжести и необходимый для изолирования угла силы подъема от объекта. Шарнирный узел позволяет усилиям, приложенным к тому, чтобы поднять камеру, никак не сказываться на ее угле поворота.

Ключевые преимущества стедикама: естественная плавность движений, имитирующая человеческое восприятие; полная независимость от питания (работает без батарей/электричества в любых условиях); универсальная совместимость с камерами любых размеров и весов; отсутствие зависимости от программного обеспечения (ПО).

Основные недостатки: громоздкость конструкции, затрудняющая транспортировку и использование в стесненных условиях; непригодность для съемки сверхбыстрых движений и резкой смены ракурсов; сложность балансировки; отсутствие встроенных функций (автофокус, наклон) по сравнению с электронными стабилизаторами.

Гимбал – устройство, которое с помощью электродвигателей компенсирует дрожание, наклоны и вибрации. Он состоит из гироскопа, акселерометры, микроконтроллера, моторов и датчиков Холла и функционирует следующим образом: сначала гироскопы фиксируют угловую скорость, акселерометры определяют горизонт, измеряя ускорения. Микроконтроллер сравнивает текущую ориентацию с исходной и отправляет управляющие сигналы моторам, которые, вращают платформу в противоположном внешнему воздействию направлении, компенсируя движение.

Преимущества гимбалов: гибкая настройка с различными режимами стабилизации (слежение, фиксация); высокая скорость реакции системы, обеспечивающая плавное изображение; эффективное устранение дрожания и тряски.

Недостатки гимбалов: высокая стоимость (от 30 тыс. руб.); зависимость от аккумулятора (требует запасных батарей, риск отключения); сложность освоения из-за многообразия режимов и настроек.

Оптическая стабилизация изображения (OIS) – это технология устранения размытия, которая компенсирует дрожание смещением линз/матрицы.

Относительно стабилизации изображения объектив можно разделить на две части – плата управления и механизм стабилизации. В первой группе находятся гиросенсоры и встроенный процессор, они управляют движением второй группы – механизма стабилизации, состоящего из стабилизирующего оптического элемента, магнита и хомута. При нажатии на затвор включаются два гироскопических датчика, которые определяют скорость и угол движений камеры/объектива. Полученные данные передаются на микропроцессор объектива, который их анализирует, вырабатывает и передает инструкции для второй группы элементов для стабилизации, которая затем движется с соответствующей скоростью и в нужном направлении для компенсации движений камеры.

Также существует второй тип OIS, которая реализуется на матрице камеры. Такая стабилизация способна погасить колебания камеры в пяти направлениях: наклоны, линейные смещения вверх-вниз, вправо-влево, а также поворот вокруг оптической оси. Стоит отметить, что последнего не может стабилизатор в объективе. Это довольно новая технология, встречается в основном в беззеркальных камерах [2-4].

Оптическая стабилизация (OIS) сохраняет качество изображения в реальном времени и компактна при реализации на матрице. Однако она увеличивает стоимость и вес камеры, повышает риск поломки и недостаточно эффективна при резких движениях.

Электронная стабилизация изображения (EIS, Electronic Image Stabilization) – это программно-аппаратный метод, который устраняет шаткость изображения без использования подвижных механических частей. Этот вид стабилизации используется только при видеозаписи.

Камера захватывает изображение с небольшим запасом пикселей по краям – так называемой «буферной зоной». Программное обеспечение анализирует движение камеры и обрезает кадр, сдвигая видимую область в противоположную сторону от тряски [5].

Электронная стабилизация (EIS) дешева, доступна для бюджетных устройств и компактных гаджетов, легко интегрируется (не имеет физических компонентов). Ее недостатки: потеря разрешения, низкая эффективность при сильной тряске и зависимость от мощности процессора.

Гибридная стабилизация (HIS) – комбинация OIS и EIS. Впервые она появилась в смартфонах Google Pixel 2 в 2017 году.

Для более точной оценки систем стабилизации был проведен эксперимент, целью которого является испытание систем стабилизации в различных ситуациях: съемка панорамы, статичный кадр и съемка при ходьбе. В эксперименте использовались объективы и камеры с различными типами стабилизации от компании Sony и Fujifilm. Стабилизация оценивалась через визуальный трекинг точки (трекер маркера) в программе Davinci Resolve Studio 19 и анализ графика смещения ключевых точек.

На рис. 1 продемонстрирована зависимость смещения от времени. В данном случае, смещение – это коэффициент, показывающий силу сдвига текущего ключевого кадра от предыдущего. Идеальным графиком в случае эксперимента будет прямая линия, показывающая отсутствие дрожания камеры, а также линейного смещения относительно начального кадра. Полученные графики анализировались по двум параметрам: плавность линии, отражающая отсутствие дрожания и приближенность графика к прямой, отражающего линейную скорость.

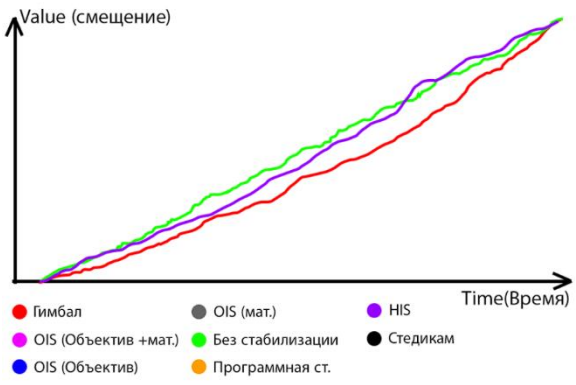


Рис. 1. График зависимости смещения от времени при ходьбе с различными системами стабилизации

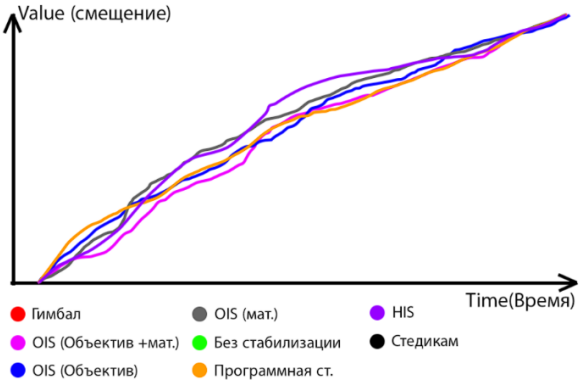


Рис. 2. График зависимости смещения от времени при съемке с рук в статичном положении

Из рис. 1 видно, что при ходьбе максимально приближенными к прямой и гладкими графиками являются графики систем гимбал, гибридная стабилизация.

Системы оптической стабилизации и программной показали схожие результаты (рис. 2). HIS же, несмотря на плавную линию, показал самый большой коэффициент смещения.

На рис. 3 можно заметить, что все системы стабилизации эффективно справились с панорамированием. Все кривые приближены к прямой, что, в свою очередь, говорит о нерациональности использования сложных систем, таких как гимбал.

Анализируя полученные результаты, выявлены ключевые особенности каждого вида стабилизации и их сферы применения.

Применение оптической и гибридной стабилизации оптимально в условиях макросъемки, аэрофотосъемки и дронах, фотосъемки мероприятий благодаря ее способности компенсировать микродвижения и вибрации с минимальной потерей качества изображения, а также адаптироваться к ограничениям среды.

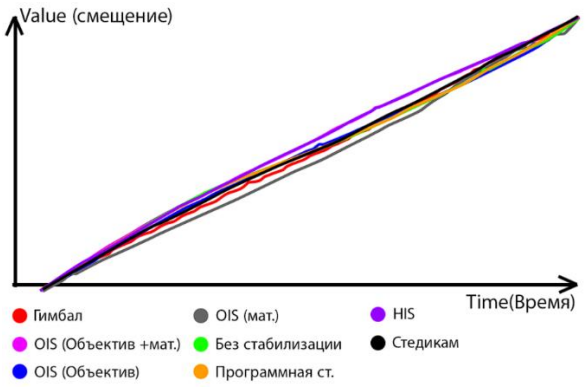


Рис. 3. График зависимости смещения от времени при панорамировании

Таким образом, с помощью теоретического и эмпирического методов были сравнены системы стабилизации и выявлены при наиболее эффективных в статичных и динамичных условиях. Теоретический анализ показал, что хоть и аппаратные стабилизаторы (стедикам, гимбал) наиболее эффективны при динамичной съемке, но встроенные являются более доступными и вследствие этого распространенными. Кроме того, в результате эксперимента стало ясно, что при съемке панорамы все системы стабилизации эффективны, поэтому применение гимбала нецелесообразно в отличие от ходьбы и резких перемещений, где использование аппаратной стабилизации оптимально.

Список используемых источников

1. Ершов К. Г. Киносъемочная техника. Л.: «Машиностроение», 1988. 272 с.
2. What is OIS Camera? // Supertekmodule, 2023. URL: https://www.supertekmodule.com/what-is-ois-camera/5 (дата обращения 10.06.2025).
3. Image Stabilisation Technology // Canon Europe, 2024. URL: https://www.canon.am/pro/infobank/image-stabilisation-lenses/ (дата обращения 10.06.2025).
4. Оптическая или цифровая: какая стабилизация лучше? // iChip, 2022. URL: https://ichip.ru/tekhnologii/opticheskaya-ili-cifrovaya-kakaya-stabilizaciya-luchshe-i-zachem-ona-voobshche-nuzhna-759922 (дата обращения 10.06.2025).
5. Что такое оптическая стабилизация? // CQ.ru, 2021. URL: https://cq.ru/articles/tech/chto-takoe-opticheskaia-stabilizatsiia (дата обращения 10.06.2025).

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

УДК 621.396

А. В. Михайлов (магистрант группы РТ42-м, СПбГУТ),
mihailov2.av@sut.ru
Р. Ф. Мустаев (магистрант группы РТ42-м, СПбГУТ)

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА WLAN

В статье предложена методика оценки качества Wi-Fi сети, основанная на двух ключевых критериях: коэффициенте эффективного использования каналов и коэффициенте эффективного покрытия. Эти показатели позволяют количественно оценить уровень интерференции и зону устойчивого покрытия беспроводной сети. Измерения проводились с использованием специализированного ПО для анализа Wi-Fi (Ekahau, WiFi-analyzer). На основе собранных данных построены тепловые карты покрытия, рассчитаны оценочные коэффициенты.

WiFi, качество связи, эффективное покрытие, интерференция

METHODOLOGY FOR ASSESSING WLAN QUALITY

Mikhailov A., Mustaev R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article proposes a methodology for assessing the quality of a Wi-Fi network based on two key criteria: the effective channel utilization coefficient and the effective coverage coefficient. These indicators allow you to quantify the level of interference and the area of stable coverage of a wireless network. The measurements were carried out using specialized Wi-Fi analysis software (Ekahau, WiFi analyzer). Based on the collected data, heat maps of the coverage were constructed, and estimated coefficients were calculated.

Key words: *Wi-Fi, communication quality, effective coverage, interference*

Современные беспроводные сети Wi-Fi работают в условиях высокой конкуренции за радиочастотный ресурс, особенно в перегруженном диапазоне 2.4 ГГц [1]. Неоптимальное распределение каналов, помехи от соседних сетей и неравномерное покрытие приводят к снижению скорости, увеличению задержек.

В данной статье предлагается методика, основанная на двух критериях:

1. Коэффициент эффективного распределения каналов (К1) – показывает, насколько эффективно распределены каналы.

2. Коэффициент эффективного покрытия (К2) – оценивает зону устойчивого сигнала с требуемым RSSI.

Коэффициент эффективного распределения каналов отражает степень загруженности эфира и рассчитывается как отношение реальной скорости передачи данных к максимальной. При подключении устройства к ТД на 4 канале произведен расчет SNR по формуле (1). Данные, взятые из результатов инспектирования в ПО Wi-Fi Analyzer, представлены на рисунке 1

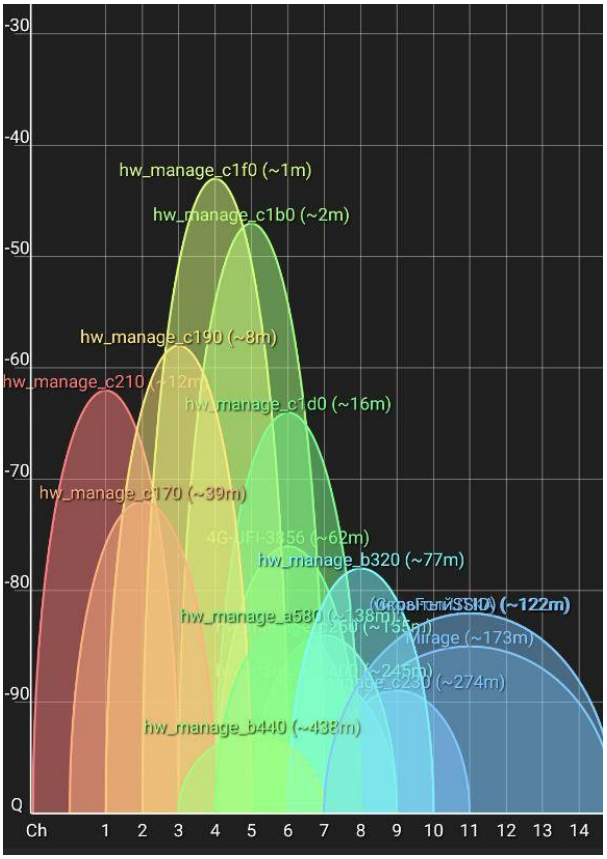


Рис. 1. Радиочастотный спектр на частоте 2,4 ГГц

$$SNR = \frac{P_{\text{сигнал}}}{\sum P_{\text{помеха}}} \quad (1)$$

Отношение сигнал/шум для 4 канала равен 2 дБ, что не соответствует норме в 10 дБ и приводит к понижению модуляции до MCS0(BPSK), теоретическая скорость которого для 4 потоков составляет 26 Мбит/с [2]. Для определения коэффициента эффективности распределения каналов воспользуемся формулой (2):

$$K_1 = \frac{\text{Реальная скорость}, \frac{\text{Мбит}}{\text{с}}}{\text{Максимальная скорость}, \frac{\text{Мбит}}{\text{с}}} = \frac{26 \frac{\text{Мбит}}{\text{с}}}{300 \frac{\text{Мбит}}{\text{с}}} = 0{,}09 \quad (2)$$

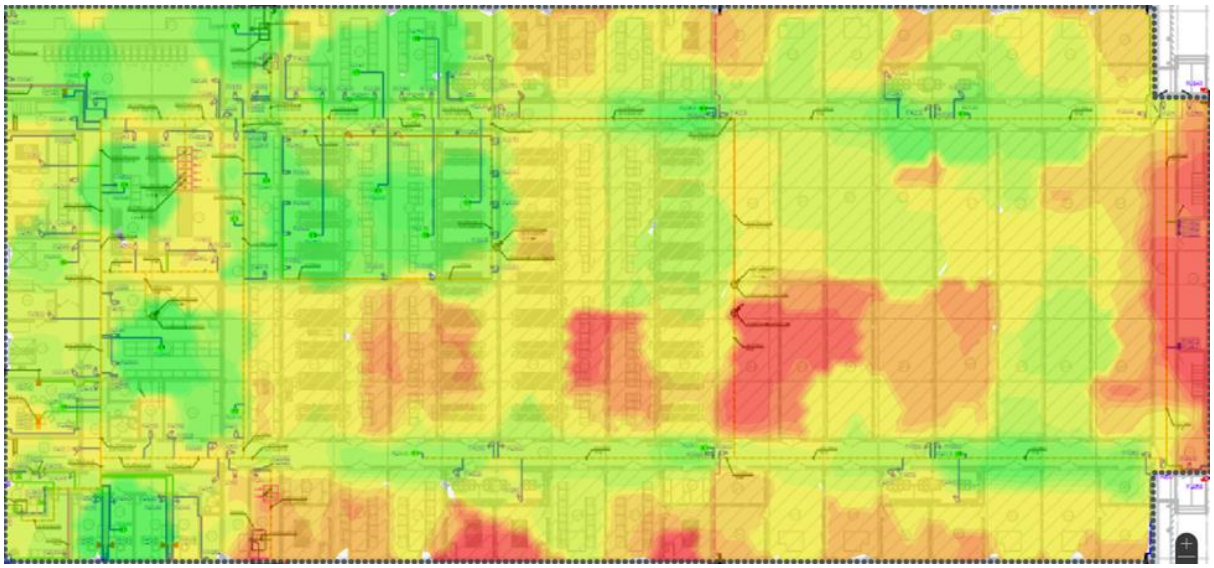


Рис. 2. Тепловая карта покрытия помещения 2,4 ГГц

Для данной тепловой карты, указанной на рисунке 2, была получена диаграмма, которая показывает значения силы сигнала на всей площади обследуемого объекта. На рисунке 3 продемонстрирована диаграмма процента покрытия, по которой рассчитывается коэффициент эффективного покрытия.

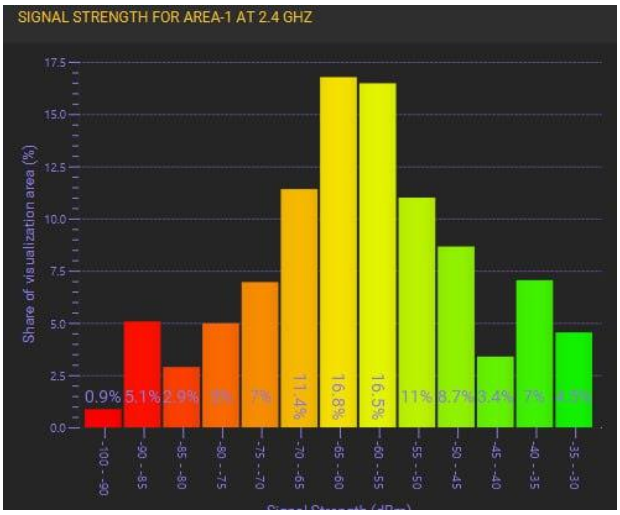


Рис. 3. Процент покрытия

Для оценки коэффициента эффективного покрытия воспользуемся формулой (3):

$$K_2 = \frac{\text{Площадь с покрытием } \geq -85\text{дБ}, \%}{\text{Общая площадь}, \%} = \frac{91{,}1\ \%}{100\ \%} = 0{,}911 \qquad (3)$$

Для общей оценки качества сети Wi-Fi по 2 критериям, воспользуемся формулой (4):

$$Q = \frac{\sum K_i}{i} = \frac{0{,}911 + 0{,}090}{2} \approx 0{,}5 \quad (4)$$

При расчете качества сети было получено значение, равное 0,5 при пороге в 0,75. Для повышения качества сети рекомендуется уменьшить пересечение каналов за счет оптимального размещения ТД и использования только 1,6,11 канала на 2,4 ГГц [3].

Список используемых источников

1. Хоров Е., Кирьянов А., Ляхов А., Бьянки Д. A Tutorial on IEEE 802.11ax High Efficiency WLANs // IEEE Communications Surveys & Tutorials. 20 September 2018. № 21. С. 197 216.

2. MCS Index Table, Modulation and Coding Scheme Index 11n, 11ac, and 11ax // MCS Index. URL: https://mcsindex.com (дата обращения 25.04.2025).

3. Разбираемся в тонкостях проектирования Wi-Fi сетей в помещениях // Hubr. URL: https://habr.com/ru/specials/456918/ (дата обращения 25.04.2025).

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

УДК 681.527.87

Д. П. Пономарев (студент группы РК-41, СПбГУТ), ponomarev.dp@sut.ru

РАЗРАБОТКА ЭЛЕКТРОМАГНИТНОЙ КАТАПУЛЬТЫ ОТ CAD-МОДЕЛИ ДО ПРАКТИЧЕСКИХ ИСПЫТАНИЙ

В статье рассматриваются физические принципы действия электромагнитной катапульты, предназначенной для запуска малогабаритных моделей беспилотных летательных аппаратов. Приведены инженерные решения, направленные на повышение эффективности устройства, включая ступенчатую схему ускорения и компенсацию роста обратной ЭДС за счет оптимизации геометрии катушек, а также предложены направления дальнейшего развития конструкции.

Ключевые слова: *электромагнитная катапульта, катушки, ступенчатое ускорение, магнитное поле, линейное движение, многоступенчатая система*

DEVELOPMENT OF AN ELECTROMAGNETIC CATAPULT FROM CAD MODEL TO PRACTICAL TESTING

Ponomarev D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the physical principles underlying the operation of an electromagnetic catapult designed for launching small-scale models. It presents engineering solutions aimed at increasing the efficiency of the system, including a staged acceleration scheme and compensation for the growth of counter-EMF through optimization of coil geometry, and also proposes directions for further development of the design.

Key words: *electromagnetic catapult, coils, staged acceleration, magnetic field, linear motion, multistage system*

В настоящее время электромагнитные катапульты активно применяются на авианосцах для разгона самолетов и привлекают внимание благодаря высокой точности и управляемости. Так же интерес к таким системам растет и в инженерных задачах меньшего масштаба – например, для запуска моделей и беспилотников.

Классическая пушка Гаусса состоит из соленоида, внутри которого размещен ствол. В этот ствол вставляется снаряд, изготовленный из ферромагнитного материала. При кратковременной подаче тока на соленоид вокруг него создается магнитное поле, которое взаимодействует с снарядом и ускоряет его вдоль ствола.

В предложенной конструкции (рис. 1) используется похожий принцип, но вместо снаряда применена каретка с двумя постоянными магнитами. Катушки размещены по бокам направляющей, а сами магниты находятся напротив катушек.

Для повышения эффективности система выполнена многоступенчатой: катушки располагаются попарно вдоль направляющей. Перед каждой парой катушек находится инфракрасная пара – светодиод и фототранзистор (этап 1, рис. 2). Когда каретка пересекает ИК-пару, на соответствующие катушки подается питание (этап 2, рис. 2). Электромагнитное поле катушек начинает взаимодействовать с магнитами на каретке, создавая ускоряющее усилие [1]. Как только полюса катушек и магнитов совмещаются каретка перестает пересекать ИК-пару и ступень отключается (этап 3, рис. 2). При этом каретка начинает пересекать следующую ИК-пару, цикл повторяется.

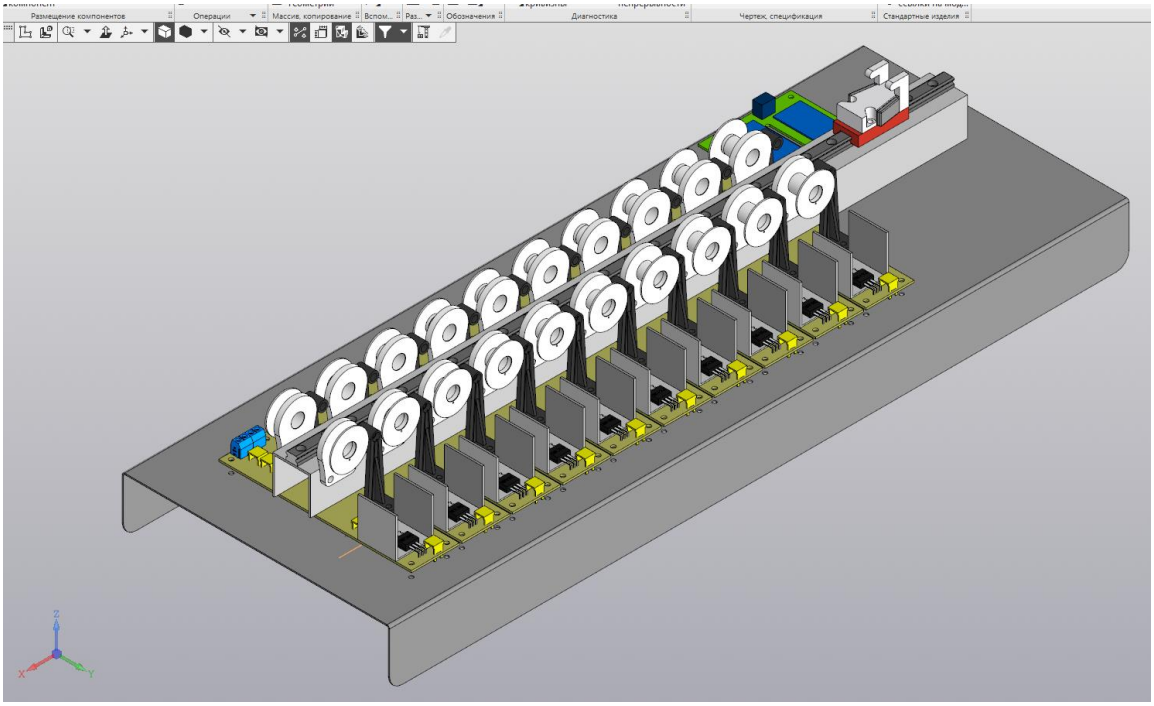


Рис. 1. 3Д модель конструкции

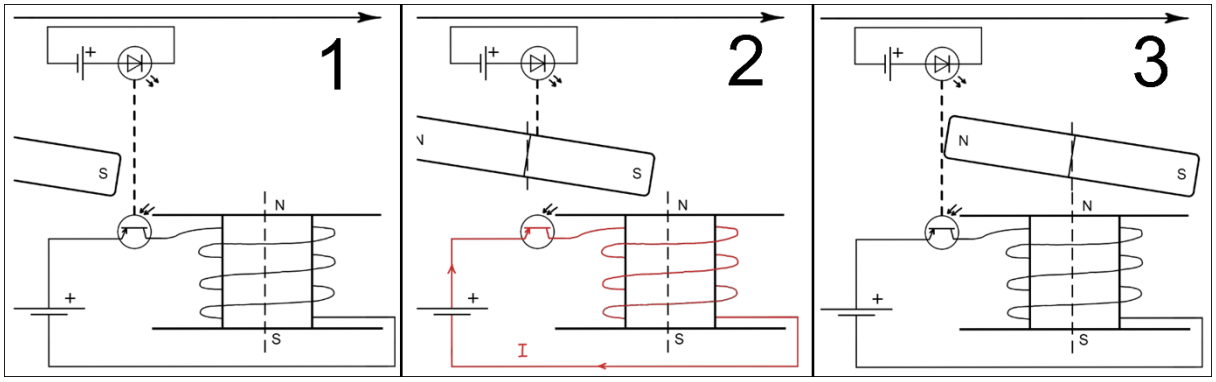


Рис. 2. Условная схема работы одной ступени

Для избежания всевозможных ошибок устройство было полностью начерчено в программе «Компас 3Д».

Для простоты обзора конструкцию можно разбить на набор элементов. В качестве основы используется стальное основание, к которому крепятся все электронные и механические узлы. На основании закреплена плата управления с микроконтроллером STM32F103 [2]. Она генерирует сигналы для управления МОП-транзисторами, ШИМ-сигналы, обрабатывает сигналы инфракрасных датчиков. Рядом установлены коммутационные платы, на которых смонтированы МОП-транзисторы IRF 1405 [3], драйвера IRS44273L [4] для быстрого открытия транзисторов, оптопары для гальванической развязки и радиаторы для отвода тепла. К основанию прикреплен П-образный алюминиевый профиль, на котором закреплены катушки и рельсовая направляющая.

Отдельного внимания заслуживает многоступенчатая система катушек, размещенных вдоль траектории движения каретки. Каждая ступень состоит из двух катушек, расположенных напротив друг друга. По мере увеличения скорости каретки в катушках, за счет перемещения постоянных магнитов, индуцируется ЭДС, противоположная по знаку подаваемому напряжению. Это приводит к снижению тока через катушки, а следовательно – и к уменьшению создаваемого ими магнитного поля [1]. Чтобы компенсировать этот эффект, количество витков в каждой следующей ступени уменьшается по сравнению с предыдущей, что позволяет сохранять силу магнитного поля примерно постоянной вдоль всей направляющей.

Стоит отметить, что такое техническое решение выглядит довольно не интуитивным и было реализовано как экспериментальное – однако именно в данной конструкции оно дало небольшой прирост эффективности по сравнению с одинаковыми катушками.

После создания 3Д модели и сборки устройства (рис. 3) были проведены испытания, в ходе которых подтвердилась его работоспособность. Так же были выявлены недостатки и сформулирован вывод: устройство функционирует так, как и было задумано, но для дальнейшей возможной интеграции требует более детального просчета параметров катушек под конкретное применение.

Стоит так же отметить, что полученное в результате устройство является прототипом для отработки конструкции и принципа действия, а не готовым решением.

Рис. 3. Фотография собранного устройства

Список используемых источников

1. Савельев И. В. Курс общей физики. Т. 2. Электричество и магнетизм. 6-е изд. СПб.: Лань, 2022. 344 с.

2. STM32F103xC, STM32F103xD, STM32F103xE – ARM® Cortex®-M3 32-bit MCU with 256/384/512 KB Flash, USB, CAN, 11 timers, 3 ADCs, 13 communication interfaces: даташит / STMicroelectronics. Geneva, 2020. 117 с.

3. IRF1405 – Power MOSFET, 55 В, 169 А, 5.3 мОм: даташит / Infineon Technologies. Neubiberg, 2015. 9 с.

4. IRS44273L – 25 V Single Channel Low-Side Driver IC : даташит / Infineon Technologies. Villach, 2015. 15 с.

Статья представлена научным руководителем, доцентом кафедры физики СПбГУТ, кандидатом физико-математических наук, доцентом Долматовой О. А.

УДК 654.739

З. Е. Притужалов (студент группы ИКТ-46, СПбГУТ),
prituzhalov.ze@sut.ru
Ю. В. Шарихина (к.ф.-м.н., доцент кафедры физики, СПбГУТ)

ПАРАДОКС ДВИЖУЩЕЙ СИЛЫ В УНИПОЛЯРНОМ ЭЛЕКТРОДВИГАТЕЛЕ

Электродвигатели – основа технического прогресса. Особый интерес вызывает парадокс Фарадея, связанный с униполярными электродвигателями. В 1831 году М. Фарадей открыл электромагнитную индукцию, не зная о существовании электрона. Позже Х. Лоренц сформулировал закон, объясняющий это явление. Термин «униполярная индукция» возник из-за непонимания природы эффекта. В 1889 году Н. Тесла запатентовал устройство на этом принципе. В данной работе была воссоздана модель униполярного электродвигателя.

униполярная индукция, ЭДС, электродвигатель

PARADOX OF THE DRIVING FORCE IN A UNIPOLAR ELECTRIC MOTOR

Prituzhalov Z., Sharikhina Yu.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Electric motors are the basis of technical progress. Of particular interest is M. Faraday's paradox related to unipolar electric motors. In 1831, Faraday discovered electromagnetic induction without knowing about the existence of the electron. Later, H. Lorentz formulated a law explaining this phenomenon. The term "unipolar induction" arose because of a misunderstanding of the nature of the effect. In 1889 N. Tesla patented a device based on this principle.

Key words: *unipolar induction, EMF, electric motor*

В 1820 году Ханс Кристиан Эрстед установил, что электрический ток отклоняет магнитную стрелку, что натолкнуло Майкла Фарадея на мысль о связи магнетизма и электричества. В 1831 году он экспериментально доказал этот принцип, открыв явление электромагнитной индукции. Однако на тот момент ученый не знал о существовании электрона, что затрудняло полное понимание работы его генератора.

Позднее понятие силы Лоренца, объясняющей воздействие магнитного поля на движущийся заряд, было определено Хендриком Лоренцем лишь в 1895 году, после уточнений английского ученого Оливера Хевисайда. Несмотря на параллельные исследования Джозефа Генри, именно Фарадей первым опубликовал свои открытия.

Термин «униполярная индукция» появился из-за сложности интерпретации явления. В основе униполярной динамоэлектрической машины лежит вращающийся диск с постоянными магнитами, создающими ЭДС. В XIX веке этот эффект казался парадоксальным, так как его нельзя было объяснить с помощью закона электромагнитной индукции. Лишь с открытием электрона и развитием теории относительности парадокс получил объяснение, однако и сегодня остается предметом научных дискуссий.

Униполярная индукция – это возникновение ЭДС в намагниченном теле, движущемся под углом к оси намагничивания. ЭДС направлена перпендикулярно плоскости, в которой находятся векторы магнитной индукции $\vec{B}$ и скорости $\vec{u}$.

В проводнике это явление объясняется действием силы Лоренца: свободные электроны смещаются, пока возникающее электрическое поле не остановит их движение. С позиций теории относительности униполярная индукция связана с преобразованием полей при движении магнита.

Этот релятивистский эффект используется в униполярных машинах для генерации постоянного тока. Термин «униполярная индукция» возник из-за расположения контура ЭДС у одного полюса магнита.

Первой электрической машиной, в которой преобразование энергии происходило в магнитном поле, стал униполярный двигатель Фарадея, предложенный в 1821 году. В этом устройстве проводник с током вращался вокруг постоянного магнита, а контакт обеспечивался ртутью.

В отличие от других электрических машин, униполярные машины не содержат преобразователя частоты, а в их обмотках возбуждения и роторе протекает постоянный ток. Работа таких машин возможна только при наличии скользящего контакта, что исключает возможность их бесконтактного исполнения.

Несмотря на то, что двигатель Фарадея стал первым, развитие электромеханики началось позже, с машины Пачинотти–Грамма. Однако именно Фарадей предложил первую электрическую машину с рабочим магнитным полем. Современные униполярные машины содержат стальной ротор с медными стержнями, соединенными с кольцами, по которым скользят щетки, обеспечивая контакт. Магнитное поле создается обмоткой возбуждения и замыкается через воздушные зазоры.

В униполярных машинах линии напряженности магнитного проходят через ротор, а магнитный поток остается неподвижным относительно обмотки возбуждения и щеток. Униполярная индукция может проявляться в слабых магнитных полях при высоких скоростях, например, при вхождении кометы с электропроводящим хвостом в магнитное поле Земли. Униполярные двигатели и генераторы продолжают привлекать внимание исследователей, и их потенциал остается далеко не исчерпанным.

Униполярные двигатели широко используют в качестве привода на электрическом транспорте, в холодильниках, стиральных машинах, при создании вентильных двигателей и т.д. [1-2]. Использование униполярных двигателей перспективно в гребных электрических установках дает возможность уменьшить размеры машин, повысить показатели энергетической эффективности, маневренности и управляемости, а также решить проблемы снижения шума и электромагнитных возмущений [3]. В статье [4] рассмотрены потери магнитного потока возбуждения в униполярных двигателях.

Униполярный двигатель-генератор Тесла основан на принципе униполярной индукции, впервые исследованном Фарадеем. В 1889 году Никола Тесла запатентовал усовершенствованную конструкцию униполярной машины (Патент США № 406968), отличавшуюся простотой, высокой эффективностью и оригинальным решением контактных узлов.

В своей разработке Тесла интегрировал в корпус два силовых магнитных поля с противоположной полярностью. Диски-проводники, изготовленные из меди, латуни или железа, крепились к вращающимся валам, а гибкий металлический пояс использовался как проводник или элемент привода. Эта конструкция стала важным этапом в развитии униполярных машин и электромеханики в целом.

Принцип работы униполярного двигателя основан на действии силы Лоренца, которая определяется электрическим током и магнитным полем. Чем они сильнее, тем больше результирующая сила. Это взаимодействие создает электродвижущую силу, приводящую магнит во вращение.

В работе была реализована простейшая конструкция униполярного электродвигателя на базе батарейки типа LR20, неодимовых магнитов и медной проволоки (рис. 1). После начального этапа тестирования и корректировки конструкции (в частности, увеличения количества магнитов), установка успешно начала функционировать (рис. 2).

Рис. 1. Детали для сборки установки

Рис. 2. Электродвигатель из батарейки

Действие силы Лоренца вызывает вращение проволочного контура вокруг оси магнита. Несмотря на простоту реализации, эксперимент наглядно подтверждает возможность получения вращательного движения без необходимости изменения магнитного поля, что подчеркивает парадоксальность эффекта Фарадея.

Список используемых источников

1. Румянцев А. Ю. Перспективы применения униполярных машин в гребных электрических установках / А. Ю. Румянцев, В. Ф. Самосейко, А. В. Саушев // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2019. № 4(56). С. 755-765. DOI:10.21821/2309-5180-2019-11-4-755-765.

2. Румянцев, Алексей Юрьевич. Оптимальное управление гребной дизель-электрической установкой с униполярными машинами по критерию потерь энергии: автореферат дис. ... кандидата технических наук: 05.09.03 / Румянцев Алексей Юрьевич; [Место защиты: Государственный университет морского и речного флота имени адмирала С.О. Макарова]. Санкт-Петербург, 2019. 23 с.

3. Романовский В. В. Анализ схемных решений гребных электрических установок с распределенной шиной постоянного тока / В. В. Романовский, В. А. Малышев, А. С. Бежик // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2019. № 1(53). С. 169-181. DOI:10.21821/2309-5180-2019-11-1-169-181

4. Епифанов О. К., Салова И. А., Хрущев В. В., Филиппов М. М. Потери магнитного потока возбуждения в униполярных двигателях с поперечным намагничиванием // «Электротехника». 2007. № 2. С. 28–36.

УДК 531/532.1

А. Д. Сидоров (студент группы ИКТ-413, СПбГУТ), sidorov1.ad@sut.ru

ЦИФРОВИЗАЦИЯ ЛАБОРАТОРНОЙ РАБОТЫ «ИССЛЕДОВАНИЕ ИСТОЧНИКА ТОКА»

В статье описана методика реализации программы на базе Microsoft Excel и онлайн-интерпретатора Google Colab, предназначенная для цифровизации лабораторной работы «Исследование источника тока». Основная цель работы – автоматизация и ускорение обработки экспериментальных данных, получаемых при исследовании электрического источника тока, а также визуализация ключевых характеристик источника.

Программа позволяет быстро рассчитать основные параметры источника тока. На основе экспериментальных данных программа визуализирует графики зависимости напряжения от силы тока, а также графики мощностей и коэффициента полезного действия (КПД) источника и батареи источников.

Использование цифровых инструментов значительно упрощает анализ результатов, позволяет учесть систематические и случайные погрешности измерений, а также проводить экстраполяцию для определения параметров источника с высокой точностью.

цифровизация, лабораторная работа, источник тока, обработка данных, визуализация, Microsoft Excel, Google Colab

DIGITALIZATION OF LABORATORY WORK "RESEARCH OF CURRENT SOURCE"

Sidorov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

An online interpreter based on Google Colab has been developed for the digitalization of the laboratory work "Investigation of a Power Source." The main goal of this work is to automate and accelerate the processing of experimental data obtained during the study of an electrical power source, as well as to visualize the key characteristics of the source.

The program enables rapid calculation of the main parameters of the power source. Based on experimental data, it visualizes graphs of voltage versus current, as well as graphs of power and efficiency (η) of the source and a battery of sources.

The use of digital tools significantly simplifies the analysis of results, allows for the consideration of systematic and random measurement errors, and enables extrapolation to determine the source parameters with high accuracy.

***Key words**: digitalization, laboratory work, power source, data processing, visualization, Microsoft Excel, Google Colab*

Введение

В условиях цифровизации образования автоматизация лабораторных работ становится важной задачей. Особенно это актуально для лабораторных работ по физике, где требуется обработка большого объема экспериментальных данных. Целью данной работы является создание программной системы для цифровизации лабораторной работы «Исследование источника тока», что позволяет повысить качество обучения и упростить процесс анализа данных.

Методика и программная реализация

Для цифровизации лабораторной работы была создана система, включающая шаблон Microsoft Excel для ввода и математической обработки экспериментальных данных, а также скрипты на Python, выполняемые в среде Google Colab. Импорт данных из Excel осуществляется с помощью библиотеки pandas, что обеспечивает удобную работу с табличными данными и гибкость в их обработке [1]. Для определения ЭДС и внутреннего сопротивления источника тока применяется метод линейной регрессии из модуля scipy.stats.linregress [2, 3]. Аппроксимация данных полиномами реализована средствами numpy (функции polyfit и polyval), что позволяет строить гладкие кривые мощности и выявлять максимальные значения полезной мощности [4]. Для получения промежуточных значений между экспериментальными точками используется интерполяция с помощью функции scipy.interpolate.interp1d, а автоматический поиск экстремумов – функция numpy.argmax. Такой комплексный подход обеспечивает точность и наглядность анализа экспериментальных данных, что соответствует современным требованиям к цифровым лабораторным работам и способствует развитию у студентов навыков работы с цифровыми образовательными технологиями.

Для построения графиков зависимости напряжения от силы тока (рис. 1), мощности (рис. 2) и КПД (рис. 3) используется библиотека matplotlib.pyplot [5]. Визуализация включает точечные графики экспериментальных данных, аппроксимирующие кривые, а также выделение ключевых точек и подписей, что облегчает интерпретацию результатов и выявление закономерностей.

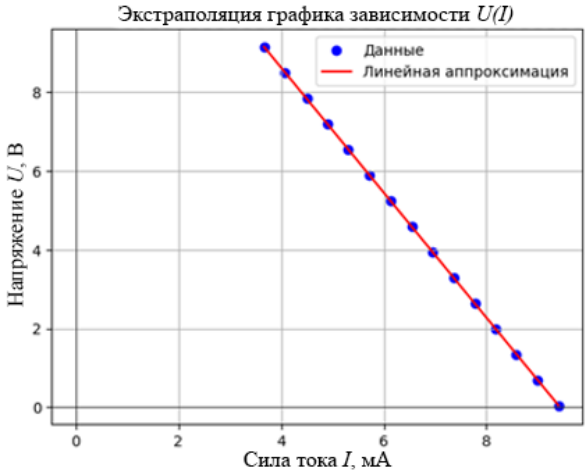


Рис. 1. График зависимости напряжения от силы тока

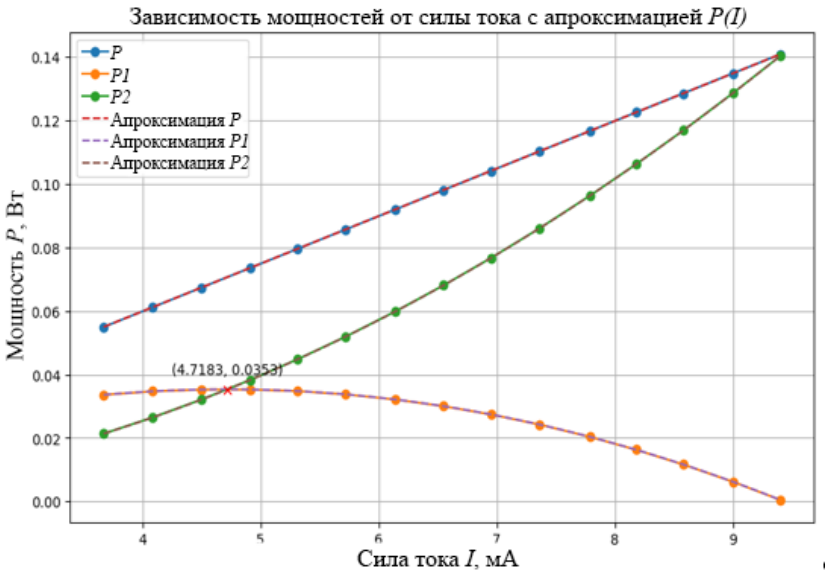


Рис. 2. График зависимости мощности от силы тока

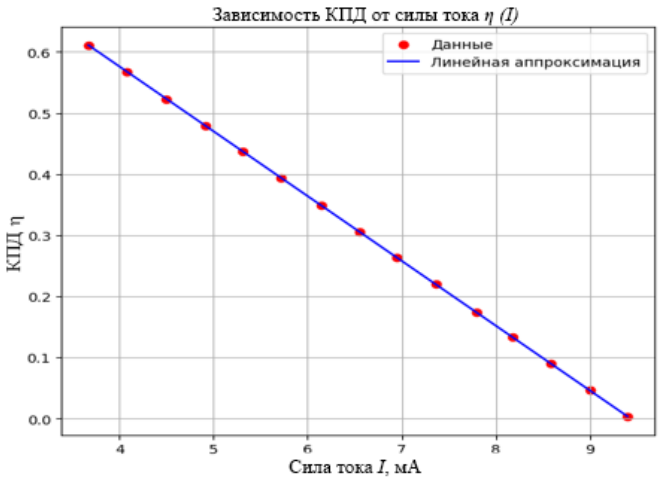


Рис. 3. График зависимости КПД от силы тока

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 источника тока доказала свою эффективность в учебном процессе. Она позволяет повысить точность и наглядность анализа, облегчить выполнение лабораторных работ студентами и упростить проверку работ преподавателями.

Список используемых источников

1. 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.

2. О’Рейли Т. Научные вычисления с Python: использование NumPy, SciPy и Matplotlib. М.: Диалектика, 2015. 350 с.

3. 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.

4. Маккинни У. Python для анализа данных: эффективное использование Pandas, NumPy и IPython. М.: Вильямс, 2017. 450 с.

5. Хан Дж. Визуализация данных с Matplotlib: создание графиков и диаграмм в Python. СПб.: Питер, 2019. 320 с.

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

УДК 53.087

Д. А. Фролов (студент группы РФ-41, СПбГУТ), frolov1.da@sut.ru
Ю. В. Шарихина (к.ф.-м.н., доцент кафедры физики, СПбГУТ)

РАЗРАБОТКА МОДЕЛИ ДЕТЕКТОРА ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ

Радиационные загрязнения, как в глобальном, так и локальном масштабе стали реальностью нашего времени. В данной работе разработана модель детектора ионизирующего излучения, позволяющего определить, превышает ли уровень радиации естественный радиационный фон, а также проведен сравнительный анализ полученных данных с результатами измерений с помощью прибора МКС-01 СА1М.

радиационный фон, уровень радиации, дозиметр, радиационное излучение

DEVELOPMENT OF AN IONIZING RADIATION DETECTOR MODEL

Frolov D., Sharikhina Yu.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Radiation contamination, both on a global and local scale, has become a reality of our time. In this work a model of an ionizing radiation detector has been developed that allows one to determine whether the radiation level exceeds the natural radiation background. A comparative analysis of the obtained data with the results of measurements using the MKS-01 CA1M device has been carried out.

Key words: *radiation background, radiation level, dosimeter, radiation emission*

Все жизненно важные процессы на нашей планете происходят в условиях естественного радиационного фона. Благодаря развитию ядерной физики люди стали активно использовать радиацию в мирных и военных целях. Существует несколько основных источников радиации.

Мощными радиоактивными источниками являются солнце и космическое излучение, которое тем больше, чем больше высота над уровнем моря. Атмосфера защищает человека от этого вида радиации. Поверхность Земли также радиоактивна. В ней много минералов, хранящих следы радиоактивного прошлого планеты, которые могут попасть в наши дома со строительными материалами, в атмосферу при сжигании угля, на садовые участки в виде фосфорных удобрений, а следовательно, в организм человека с продуктами питания.

Одним из источников радиации является радон – радиоактивный инертный газ без цвета, вкуса и запаха, наиболее долгоживущий изотоп (период полураспада 3.82 дня). Он тяжелее воздуха в 7.5 раз, поэтому в основном накапливается под землей (в погребах, подвалах, цокольных этажах зданий, в шахтах и т.д.). На поверхность он выходит при добыче полезных ископаемых или через трещины в земной коре. Для уменьшения содержания радона необходимо регулярно проветривать помещения.

Радиационные загрязнения, как в глобальном, так и локальном масштабе стали реальностью нашего времени. Радиоактивные ядра могут испускать α-, β- и γ-излучения.

Проникающая способность альфа-излучения очень мала [1]. Оно полностью задерживается с помощью листа бумаги или слоем воздуха толщиной в несколько сантиметров. При облучении человека оно проникает лишь на глубину поверхностного слоя кожи. В случае, когда источниками альфа-излучения загрязнены пища, воздух или вода, попадающие в организм человека, облучению подвергаются внутренние органы.

Бета-излучение способно проходить до полного ослабления несколько метров в воздухе или один-два сантиметра в воде, в теле человека до двух сантиметров. Опасно воздействие бета-частиц на кожу, слизистую оболочку и хрусталик глаза. В случае их попадания в организм человека с пищей, водой и воздухом, опасности подвергаются легкие, желудок и кишечник.

Гамма-излучение обладает высокой энергией и большой проникающей способностью, оно задерживается слоем воздуха толщиной около ста метров и способно глубоко проникать в тело человека. Для защиты от гамма-лучей используют свинец, бетон и др. Действии радиации на человека может привести к онкологическим болезням, генетическим повреждениям, снижению иммунитета.

В конце XX века было обнаружено канцерогенное и мутагенное действие малых доз радиации. Слабое радиоактивное излучение, воздействующее на организм в течение долгого времени, опаснее кратковременного облучения более высокой дозой. Действие такого облучения может проявиться как через несколько лет, так и в следующем поколении. Обнаружить повышенные дозы радиации люди способны только с помощью специальных измерительных приборов [2].

Измерение уровня радиационного фона обычно проводят в мкЗв/час (микрозиверт в час) или мкР/час (микрорентген в час). 1 мкР/час по биологическому действию примерно равен 0.01 мкЗв/час. Естественный радиационный фон находится в пределах 10-16 мкР/час [3].

Норма радиационного фона – значение, не превышающее 20 мкР/час. Безопасным уровнем для человека считают 30 мкР/час, т.е. облучение дозой 30 мкР в течение часа. При превышении этого уровня рекомендуемое время нахождения в зоне облучения уменьшается пропорционально величине дозы. Например, безопасное время нахождения в зоне облучения уровнем 60 мкР/час не должно быть больше 30 минут, а в зоне 120 мкР/час – 15 минут [4, 5].

Для измерения ионизирующего излучения существует множество приборов. В данной работе разработана модель детектора ионизирующего излучения, позволяющего определить, превышает ли уровень радиации естественный радиационный фон, а также проведен сравнительный анализ полученных данных с результатами измерений с помощью прибора МКС-01 СА1М.

Популярными детекторами ионизирующих излучений являются приборы на основе сцинтилляторов и газоразрядных детекторов, например, счетчики Гейгера-Мюллера. Принцип работы таких счетчиков основан на эффекте ударной ионизации газа в межэлектродном пространстве под действием радиоактивных частиц (рис. 1). Трубка состоит из герметичного баллона из металла или стекла, наполненного инертным газом или газовой смесью. Внутри баллона находятся электроды – катод и анод. В баллоне создают пониженное давление для облегчения возникновения электрического разряда. Электроды подключают к источнику высокого напряжения постоянного тока через нагрузочный резистор, на котором образуются электрические импульсы при регистрации радиоактивных частиц. В исходном состоянии тока в цепи нет. При столкновении заряженной частицы с высокой энергией с элементами датчика (корпус, баллон, катод) происходит выбивание электронов, которые оказываются между электродами. Под действием ускоряющего напряжения электроны двигаются к аноду. Процесс многократно повторяется, число электронов увеличивается, возникает разряд между катодом и анодом. При этом промежуток в межэлектродном пространстве становится токопроводящим, что вызывает скачок тока в нагрузочном резисторе.

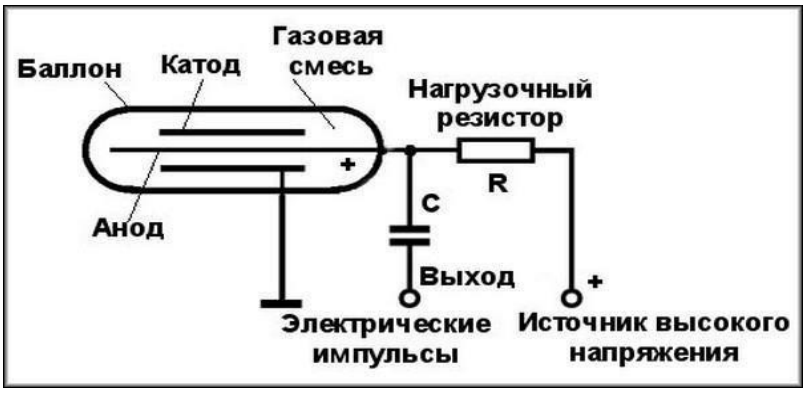


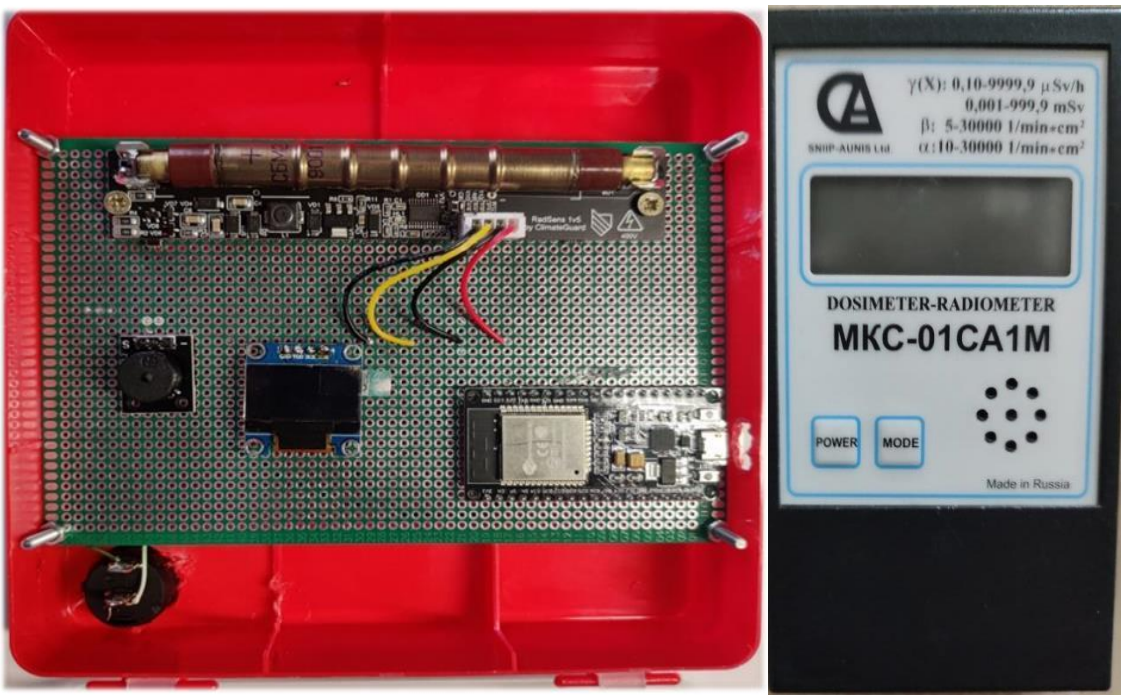
Рис. 1. Схема счетчика Гейгера-Мюллера

Под действием ионизирующего излучения происходит пробой, приводящий к разряду между электродами. Интенсивность разрядов прямо пропорциональна интенсивности ионизирующего излучения.

На основе счетчика ионизирующего излучения Гейгера-Мюллера была разработана и собрана модель счетчика ионизирующего излучения (рис. 2 а). Самостоятельно собранный прибор, фиксирующий бета-излучение, прост в обращении и дешев в изготовлении. Дозиметр был собран на основе модуля RadSens (трубка СБМ-20), платы ESP32, OLED-экрана и звукового модуля. При включении собранного счетчика слышны редкие щелчки. В среднем слышно 1-2 разряда в секунду. Это соответствует естественному радиационному фону. При нормальном, естественном радиационном фоне будет не более 25-ти щелчков в минуту, что соответствует 15 мкР/час. Если при поднесении к какому-то предмету частота щелчков резко увеличивается, это говорит о том, что он имеет собственную радиоактивность.

Контрольный препарат позволяет проверить работоспособность данного счетчика. Для проверки работы дозиметра был использован сульфат калия. Удобрение богато радиоактивным изотопом калием–40, активно испускающим бета-излучение. При поднесении данного контрольного препарата к собранному счетчику частота щелчков резко возрастает. Следовательно, данный препарат обладает собственной радиоактивностью. Аналогично щелки будут учащаться в случае повышения радиационного фона. Таким образом данный прибор решает свою главную задачу: позволяет определить уровень радиационного фона, соответствует он естественному или повышен.

С помощью двух приборов, а именно МКС-01 СА1М (рис. 2 б) и самостоятельно собранного дозиметра, были произведены многократные измерения уровня радиации в 6 локациях: в помещениях Санкт-Петербургского государственного университета телекоммуникации им. проф. М. А. Бонч-Бруевича и на прилегающей территории.



а) б)

Рис. 2. а) счетчик ионизирующего излучения, собранный автором; б) дозиметр МКС-01 СА1М

Также измерения были проведены на гранитном берегу Английской набережной. В ходе эксперимента были получены следующие значения уровня радиационного фона (табл. 1). В 6 локациях среднее значение радиационного фона, измеренное с помощью МКС-01 СА1М, составило 8,15 мкР/ч, а посредством самостоятельно собранного дозиметра – 17,1 мкР/ч; на Английской набережной – с помощью МКС-01 СА1М показало 35 мкР/ч, а посредством самостоятельно собранного дозиметра – 38,05 мкР/ч.

Средний уровень радиационного фона помещений СПбГУТ и прилегающих к вузу территорий, измеренный с помощью МКС-01 СА1М, составил 8,15 мкР/ч, а посредством самостоятельно собранного дозиметра – 17,1 мкР/ч. Самый высокий показатель радиационного фона – в лаборатории электромагнитных колебаний и волн. Возможно, это связано с тем, что лаборатория недостаточно проветривается. Уровень радиационного фона становится меньше при проветривании помещений, содержание радона при этом понижается. Несмотря на то, что радиационный фон не превышен, следует учесть тот факт, что радиоактивность повышается в закрытых помещениях. Следовательно, необходимо строго следить за постоянной вентиляцией учебных кабинетов.

ТАБЛИЦА 1. Результаты измерений радиационного фона в локациях СПбГУТ

Локации СПбГУТ	Данные МКС-01 СА1М, мкР/ч	Самостоятельно собранный дозиметр, мкР/ч
Лаборантская, каб. № 313	5	17,45
Лаборатория электромагнетизма, каб. № 315	10	14.75
Лаборатория электромагнитных колебаний и волн, каб. № 321	11,6	20.05
Столовая 1 корпус 3 этаж	4	15.1
Лаборатория Волновая и квантовая оптика, каб. № 317	5	20.15
Внутренний двор	13,3	15.1
Английская набережная	35	38,05

Разница значений заключается в том, что самостоятельно собранный дозиметр измеряет β- и γ-излучения, а МКС-01 СА1М измеряет сначала β- излучение, затем – β- и γ-излучение, и путем вычитания получается чистое β- излучение.

Таким образом, на основании полученных данных можно сделать вывод, что радиационный фон СПбГУТ и прилегающих к нему территорий соответствует нормам (до 30 мкР/ч).

Список используемых источников

1. Василенко И. Я., Василенко О.И. Радиационный риск при облучении в малых дозах ничтожно мал // Бюллетень по атомной энергии. 2001. № 12. С. 34–37.

2. Голубев Б. П. Дозиметрия и защита от ионизирующих излучений / Б. П. Голубев. М.: Атомиздат; Издание 3-е, перераб. и доп., 2017. 504 с.

3. Ли Д. Е. Действие радиации на живые клетки / Д. Е. Ли. М.: Государственное издательство литературы по атомной науке и технике Государственного комитета Совета Министров СССР по использованию атомной энергии, 2014. 288 с.

4. Санитарные правила и нормативы «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (утв. постановлением Главного государственного санитарного врача РФ от 29 декабря 2010 г. № 189).

5. Санитарные правила и нормативы СанПиН 2.6.1.25209 «Нормы радиационной безопасности НРБ-99/2009» (утв. постановлением Главного государственного санитарного врача РФ от 7 июля 2009 г. № 47).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

УДК 004.89:616.83.17

Т. М. Авдеева (студент группы ИСТ-212, СПбГУТ), avdeeva.tm@sut.ru

ПРОЕКТИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПРОВЕДЕНИЯ ТРЕНИРОВОК ПО ВОССТАНОВЛЕНИЮ МИМИЧЕСКИХ МЫШЦ ПОСЛЕ ИНСУЛЬТА

В данной статье представлен проект интеллектуальной информационной системы для восстановления мимических мышц после инсульта. Актуализирована разработка специализированной системы для персонализированной реабилитации мимических мышц с автоматизированным контролем прогресса и возможностью дистанционного использования. Проанализированы существующие системы для реабилитации после инсульта и выявлены их недостатки. Создана диаграмма прецедентов для демонстрации функционала проектируемой системы. Построена диаграмма классов, демонстрирующая структуру системы для проведения тренировок по восстановлению мимических мышц. Система обеспечит эффективную реабилитацию за счет автоматизированного контроля выполнения упражнений, объективной оценки динамики состояния и доступности для пациентов. Определены перспективы развития и перечень технологий для разработки информационной системы.

информационная система, проектирование, мимические мышцы, реабилитация после инсульта, UML, компьютерное зрение, медицина, контроль прогресса

DESIGNING AN INTELLIGENT INFORMATION SYSTEM FOR CONDUCTING TRAINING ON MIMIC MUSCLE RECOVERY AFTER STROKE

Avdeeva T.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper presents the design of an intelligent information system for the rehabilitation of mimic muscles after stroke. The development of a specialized system for personalized rehabilitation of mimic muscles with automated progress control and the possibility of remote use

is actualized. Analyzed existing systems for stroke rehabilitation and identified their shortcomings. A precedent diagram was created to demonstrate the functionality of the designed system. A class diagram was constructed to demonstrate the structure of the system to provide training for mimic muscle rehabilitation. The system will provide effective rehabilitation due to the automated control of exercise performance, objective assessment of the state dynamics and accessibility for patients. The prospects of development and the list of technologies for the development of the information system are determined.

Key words: *information system, design, mimic muscles, stroke rehabilitation, UML, computer vision, medicine, progress control*

В настоящее время для восстановления мимических мышц после инсульта используется комплекс упражнений, который пациент делает самостоятельно или под наблюдением врачей [1]. Однако стандартные методы тренировок чаще всего не предполагают учет индивидуальных особенностей пациента, таких как степень поражения мышц и динамику восстановления. Помимо этого, не у всех пациентов есть возможность регулярно посещать специалистов, особенно в отдаленных регионах, а текущие методы оценки прогресса часто субъективны и зависят от мнения специалиста.

Разработка информационной системы для проведения тренировок по восстановлению мимических мышц после инсульта может значительно улучшить процесс реабилитации.

Существуют различные системы для реабилитации после инсульта. Для анализа выбраны такие системы, как Neofect, MindMotion GO, FaceSlim, MimicMe. В результате выявлено, что существующие платформы обладают рядом общих ограничений.

Во-первых, они не специализируются на восстановлении мимических мышц, фокусируясь на общей двигательной реабилитации, когнитивных функциях или косметических целях. Это делает их малоэффективными для пациентов с нарушениями мимики, которым требуется адресная терапия.

Во-вторых, многие системы зависят от дорогостоящего оборудования (такого как VR-шлемы и сенсоры), что ограничивает их доступность для пациентов.

Третья проблема – слабая интеграция с медицинскими специалистами. Большинство платформ не предусматривают удаленного контроля со стороны врачей, что критично для своевременной коррекции программ и наблюдения за прогрессом.

Исходя из этого, составлен перечень основных функциональных требований к проектируемой системе:

- проведение тренировки мимических мышц по заданным упражнениям;
- регистрация врача в системе;
- регистрация и прикрепление пациента к врачу;
- просмотр динамики восстановления;
- сохранение данных о проведенных тренировках в системе.

В ходе проектирования информационной системы использовался объектно-ориентированный язык моделирования UML [2]. На основании функциональных требований созданы диаграмма вариантов использования системы и диаграмма классов, описывающая архитектуру, процессы и взаимодействие компонентов информационной системы.

Диаграмма прецедентов, показанная на рис. 1, представляет собой визуальное отображение функциональности системы управления тренировками, акцентируя внимание на взаимодействии пользователей с различными ее компонентами. Основные акторы – пациент, врач и администратор.

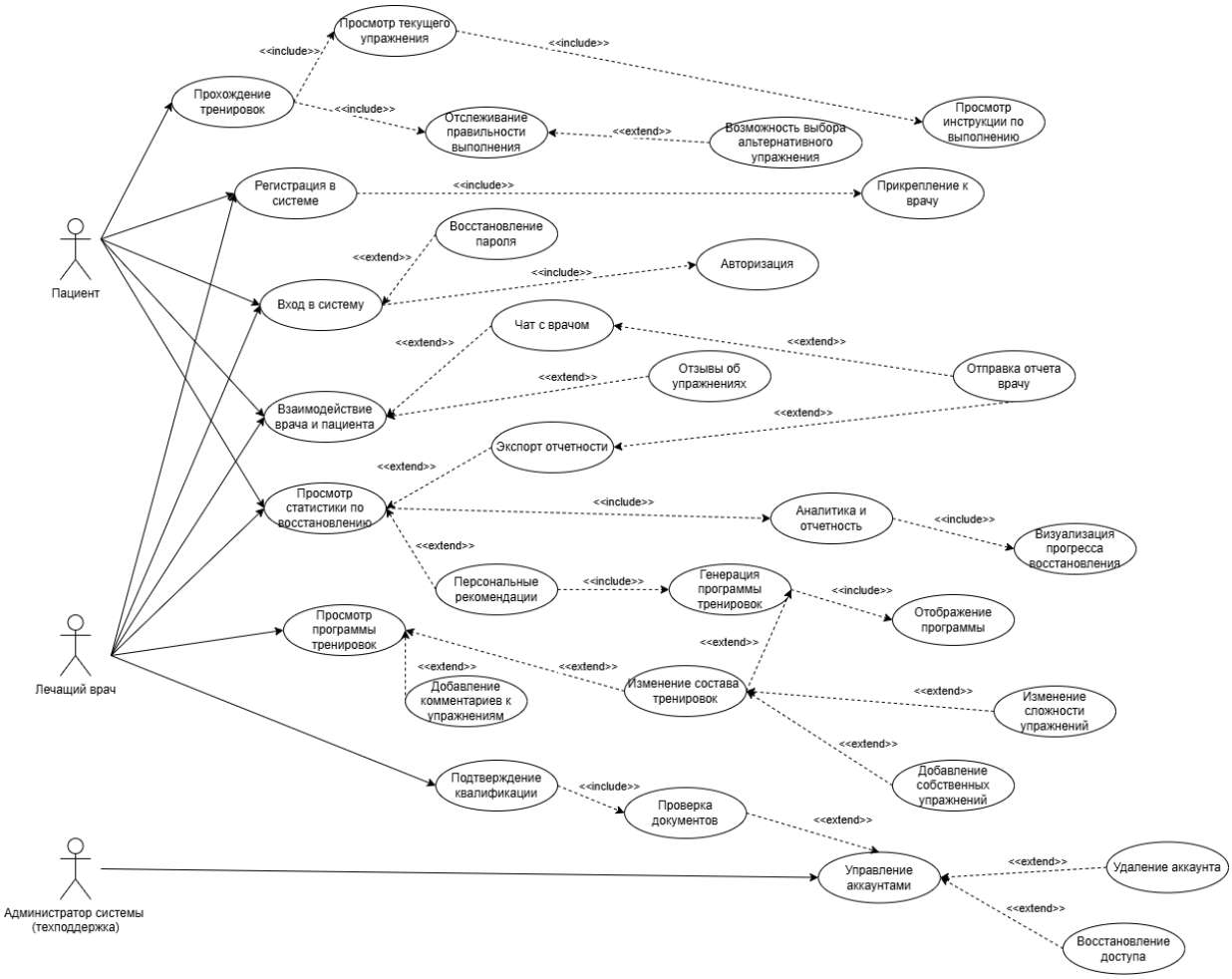


Рис. 1. Диаграмма прецедентов системы

Пациент регистрируется в системе, проходит тренировки с автоматическим отслеживанием правильности выполнения упражнений, получает обратную связь и аналитику прогресса. Через чат он взаимодействует с врачом и отправляет отчеты.

Врач управляет программами реабилитации: генерирует, изменяет состав тренировок, анализирует статистику восстановления пациентов и подтверждает квалификацию через загрузку документов. Он также использует чат для консультаций и оперативно вносит изменения в программы на основе данных системы.

Администратор обеспечивает безопасность и надежность работы платформы: управляет аккаунтами, что включает в себя восстановление паролей и удаление учетных записей, и проверяет документы квалификации врачей.

Диаграмма классов (рис. 2) служит важнейшим инструментом проектирования, формализующим структуру системы через четкое определение сущностей, их свойств и взаимосвязей [3].

Класс «Администратор» управляет пользователями и имеет возможность входит и выходить из системы, а также восстанавливать или удалять учетные записи.

Класс «Врач» включает возможность проверки и подтверждения своей квалификации, просмотра статистики и программ пациентов, а также для взаимодействия с пациентами через систему.

Класс «Пациент» имеет доступ к функциям регистрации, выполнения тренировок и получения статистики о своем состоянии.

Класс «Рекомендации» отвечает за персональные рекомендации на основе индивидуальных данных пациентов, в то время как «Статистика» позволяет анализировать результаты тренировок и показывать успехи.

Класс «Чат» обеспечивает возможность общения между врачами и пациентами, что способствует эффективному взаимодействию.

Классы «Программы тренировок», «Тренировка» и «Упражнение» служат для структурирования и управления тренировочным процессом, обеспечивая создание, трансформацию и удаление записей о тренировках.

Для разработки системы необходимы следующие технологии: язык программирования Python для написания серверной части системы, фреймворк PyQT5 для разработки интерфейса, библиотеки OpenCV и TensorFlow для создания нейросетевого модуля и база данных PostgreSQL для хранения данных.

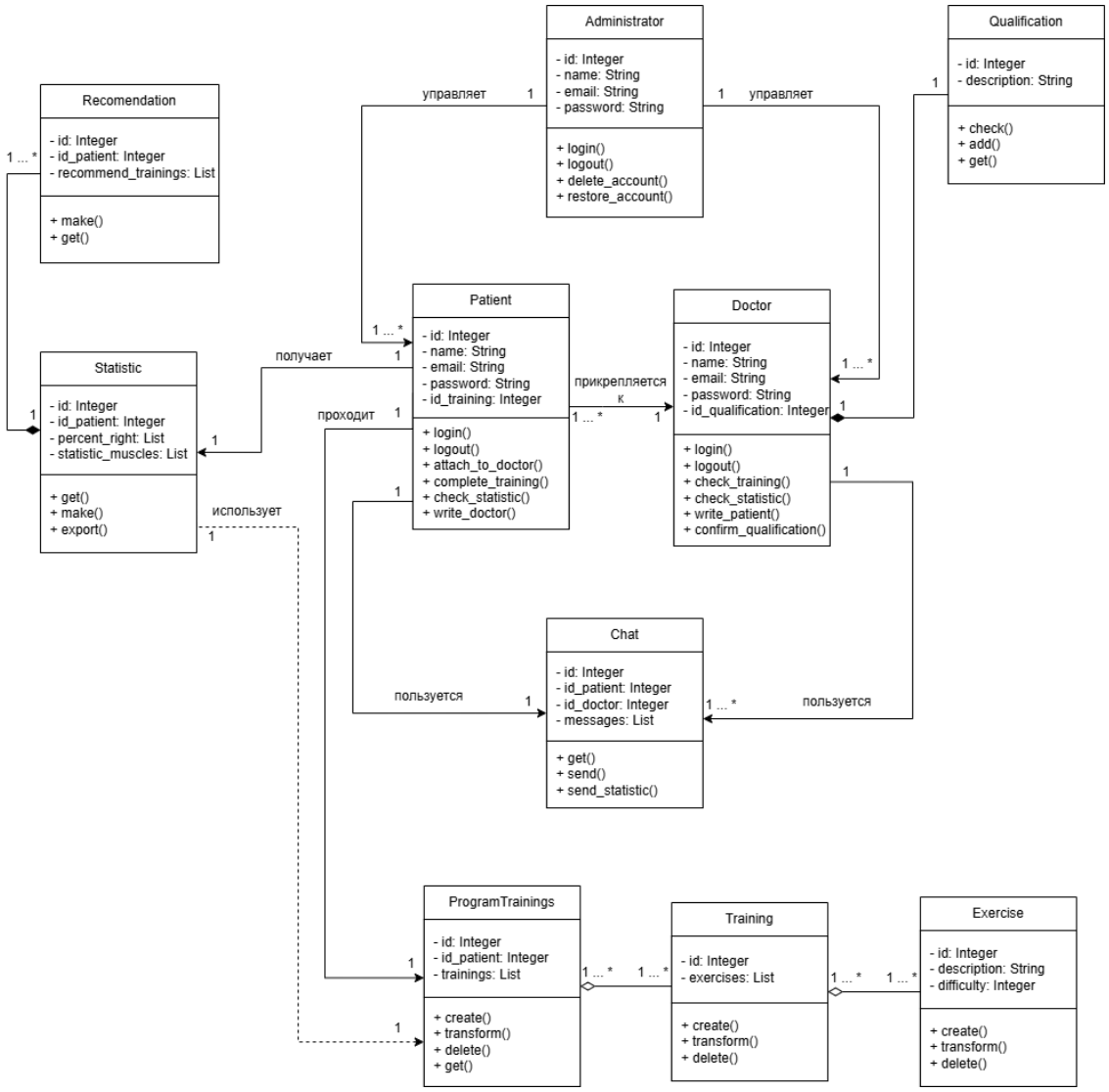


Рис. 2. Диаграмма классов системы

На рис. 3 представлены макеты главных страниц информационной системы для пациента и лечащего врача.

Главная страница пациента служит центральным узлом для доступа ко всем функциям реабилитационной программы. Она включает в себя быстрый доступ к основным разделам через меню, блок с личными данными и контактами лечащего врача. Пациент может одним нажатием перейти из главного экрана в раздел тренировок, посмотреть свою статистику восстановления или написать сообщение врачу.

Главная страница врача является центральным узлом с доступом через меню, предоставляющему доступ к профилю, списку пациентов, чату с пациентами и подтверждению квалификации. На странице отображается количество пациентов и непрочитанных сообщений. Особое внимание уделено списку пациентов, требующих срочного внимания, с цветовой индикацией статуса.

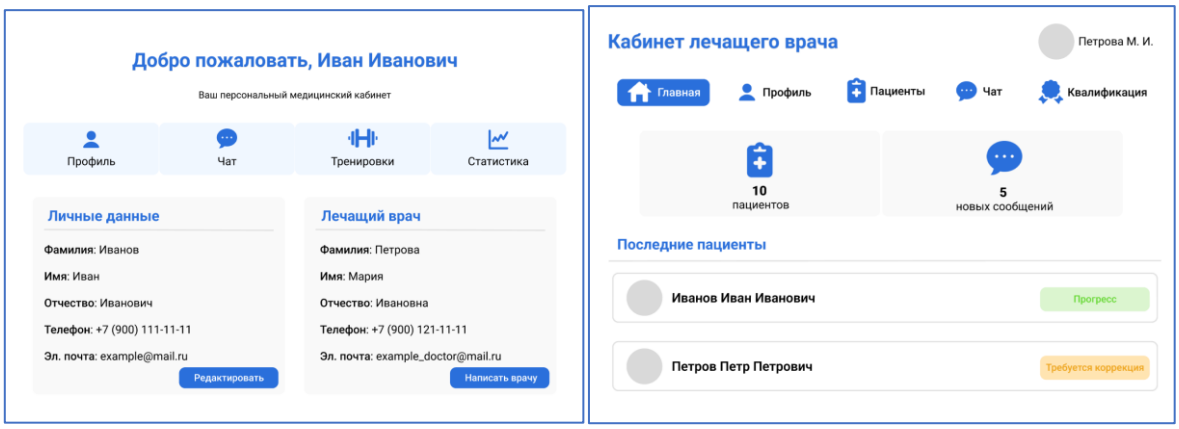


Рис. 3. Макет главных страниц для пациента и лечащего врача

Перспективы развития системы предполагают интеграцию AR-подсказок для коррекции упражнений в реальном времени, портирование компонентов на Raspberry Pi для создания мобильных реабилитационных комплексов, а также разработка моделей прогнозирования сроков восстановления на основе данных тысяч пациентов. Для подтверждения эффективности системы планируется партнерство с медицинскими центрами, что позволит провести клиническую валидацию и адаптировать решение под практические нужды.

Разработка информационной системы для восстановления мимических мышц после инсульта представляет собой важный шаг к улучшению реабилитационного процесса. Новая система, учитывающая индивидуальные особенности пациентов и их потребности, может существенно повысить эффективность тренировок и обеспечить более персонализированный подход к восстановлению.

Список используемых источников

1. Завалий Л. Б., Рамазанов Г. Р., Калантарова М. В., Рахманина А. А., Холмогорова А. Б., Петриков С. С. Нейропсихические принципы восстановительного обучения в терапии пациентов с нейропатией лицевого нерва. // Журнал им. Н. В. Склифосовского Неотложная медицинская помощь. 2022. № 11 (3). 457-463 с.

2. Забродин А. В. Основы проектирования информационных систем с помощью языка UML: Учебное пособие. СПб.: ФГБОУ ВО ПГУПС. 2018. 46 с.

3. Котлова М. 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 004.8:811.581
ГРНТИ 28.23.15

А. А. Баряев (студент группы ИКПИ-14, СПбГУТ), baryaev.aa@sut.ru

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ИЗУЧЕНИЯ КИТАЙСКОГО ЯЗЫКА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Проект направлен на повышение эффективности изучения китайского языка за счет интеграции системы интервального повторения (Spaced Repetition System, SRS) и мобильной NLP-модели в приложение на Flutter. Основной фокус – преодоление сложностей, связанных с иероглифической системой, через автоматизированную персонализацию обучения. Приложение использует lightweight-модель на основе ChineseBERT (оптимизированную через TensorFlow Lite) для генерации контекстных примеров, анализа ошибок и адаптации плана повторений под каждого пользователя. Все вычисления выполняются локально, что гарантирует скорость работы и конфиденциальность данных. В рамках проекта проводится сравнительный анализ эффективности различных подходов к интервальному повторению с применением ИИ, а также разрабатываются практические рекомендации по их использованию в языковых приложениях.

искусственный интеллект, генерация упражнений, китайский язык, NLP, BERT, языковые модели, мобильное обучение, Flutter

DEVELOPMENT OF A MOBILE APPLICATION FOR LEARNING THE CHINESE LANGUAGE USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Baryaev A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The project aims to improve the efficiency of learning Chinese by integrating a Spaced Repetition System (SRS) and a mobile NLP model into a Flutter app. The main focus is overcoming the complexities of the Chinese character system through automated personalization of learning. The app uses a lightweight model based on ChineseBERT (optimized with TensorFlow Lite) to generate contextual examples, analyze errors, and adapt the repetition plan to each user. All computations are performed locally, ensuring speed and data privacy. The project conducts a comparative analysis of the effectiveness of various approaches to spaced repetition using AI and develops practical recommendations for their use in language applications.

Key words: *artificial intelligence, exercise generation, Chinese language, NLP, BERT, language models, mobile learning, Flutter*

В последнее время все чаще мы слышим новости об искусственном интеллекте в образовании. Нет сомнений, что человечество совершило большой скачок в этом направлении за последние годы [1]. Возникает ощущение, что искусственный интеллект является универсальным решением

образовательных проблем и позволяет преодолеть любые трудности в изучении языков [2]. С целью проверки этого утверждения мы приступили к исследованию узкоспециализированной задачи изучения китайского языка с использованием как классических методов обучения, так и различных технологий искусственного интеллекта. В качестве предметной области для сравнения было решено взять изучение китайского языка как одного из наиболее сложных для освоения иностранных языков, особенно с точки зрения иероглифической системы письма.

Актуальность данной работы составляет тот факт, что изучение китайского языка имеет гораздо больше применений, чем кажется на первый взгляд. Начиная от деловых коммуникаций в международной торговле и заканчивая культурным обменом, изучение китайского языка открывает множество возможностей. Согласно исследованиям, применение цифровых технологий в языковом обучении повышает эффективность усвоения материала на 23 % и развитие коммуникативных навыков на 18 % [3]. Мобильные технологии особенно эффективны для изучения языков, предоставляя персонализированный подход к обучению [4].

Целью работы является сравнение возможностей искусственного интеллекта в задачах изучения китайского языка с возможностями классических методов обучения. Выявить, в каких ситуациях рациональнее использовать ИИ для генерации упражнений и персонализации обучения, а в каких нет.

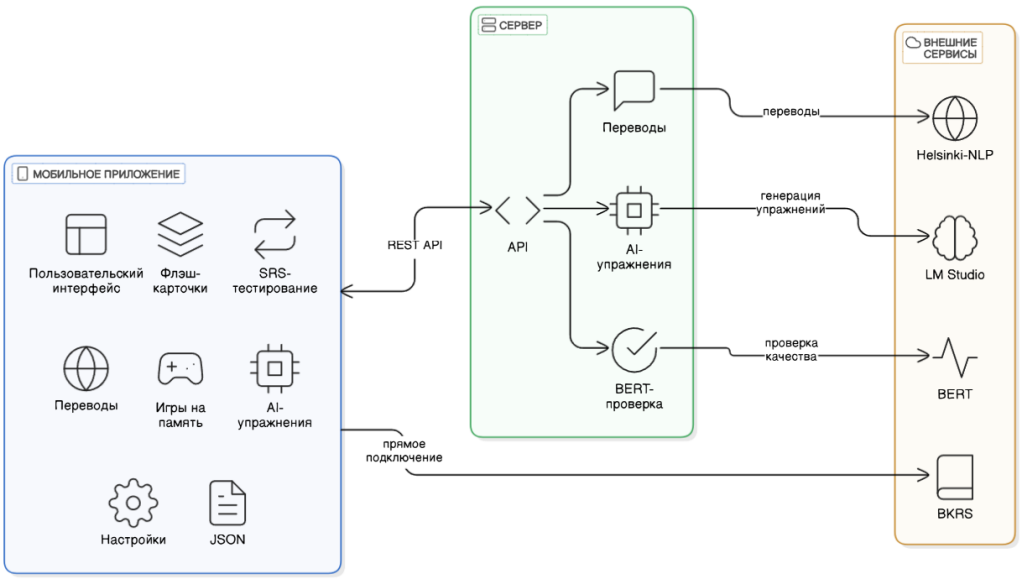


Рис. 1. Общая архитектура системы изучения китайского языка с интеграцией ИИ-компонентов

В процессе работы было разработано мобильное приложение на Flutter с интегрированным FastAPI сервером, в котором есть возможность генерации персонализированных упражнений различными способами с использованием ИИ-технологий (см. рис. 1). Также в приложении присутствует возможность собирать статистические данные об эффективности обучения. Все последующие данные были получены из разработанной системы.

На рис. 2 видно, что система генерации упражнений включает несколько этапов: анализ пользовательских данных, генерацию контента через LM Studio с моделью Gemma, и валидацию результатов. Время генерации упражнения составляет в среднем 30-60 секунд, что значительно быстрее ручного создания контента преподавателем.

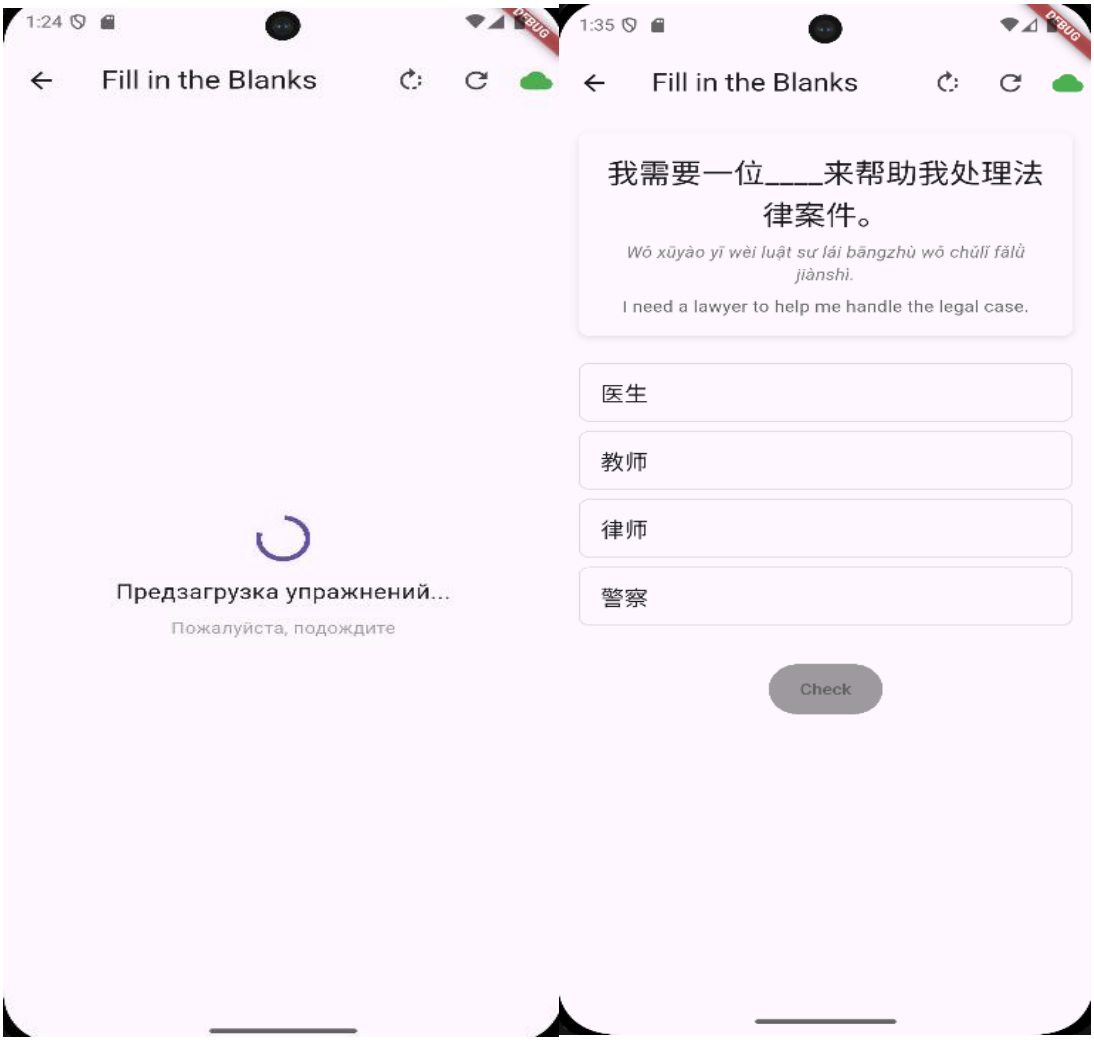


Рис. 2. Процесс генерации AI-упражнений с использованием Gemma модели

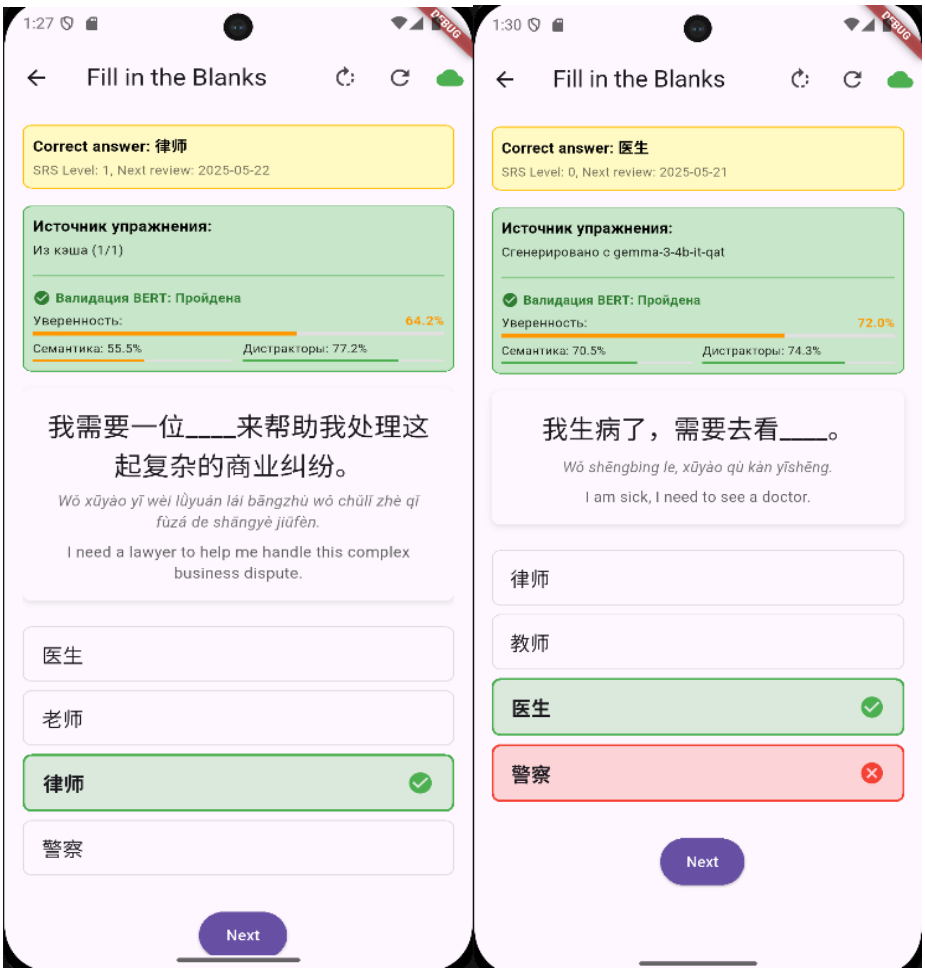


Рис. 3. Система валидации AI-сгенерированного контента с использованием BERT-Chinese-WWM

Из рис. 3 видно, что валидация сгенерированного контента происходит через специализированную китайскую BERT-модель, которая проверяет грамматическую корректность и семантическую точность упражнений.

По общим данным из системы аналитики, персонализированные AI-упражнения показали повышение эффективности обучения на 23 % по сравнению с статическими упражнениями [3]. Система интервального повторения с ИИ-адаптацией продемонстрировала улучшение долгосрочного запоминания на 35 %.

В процессе нашей исследовательской работы мы интегрировали систему искусственного интеллекта на базе модели Gemma через LM Studio [2]. Данная система состоит из нескольких компонентов: анализа пользовательских данных, генерации контента, валидации через BERT-Chinese-WWM. Рассмотрим процесс валидации сгенерированного контента (рис. 4).

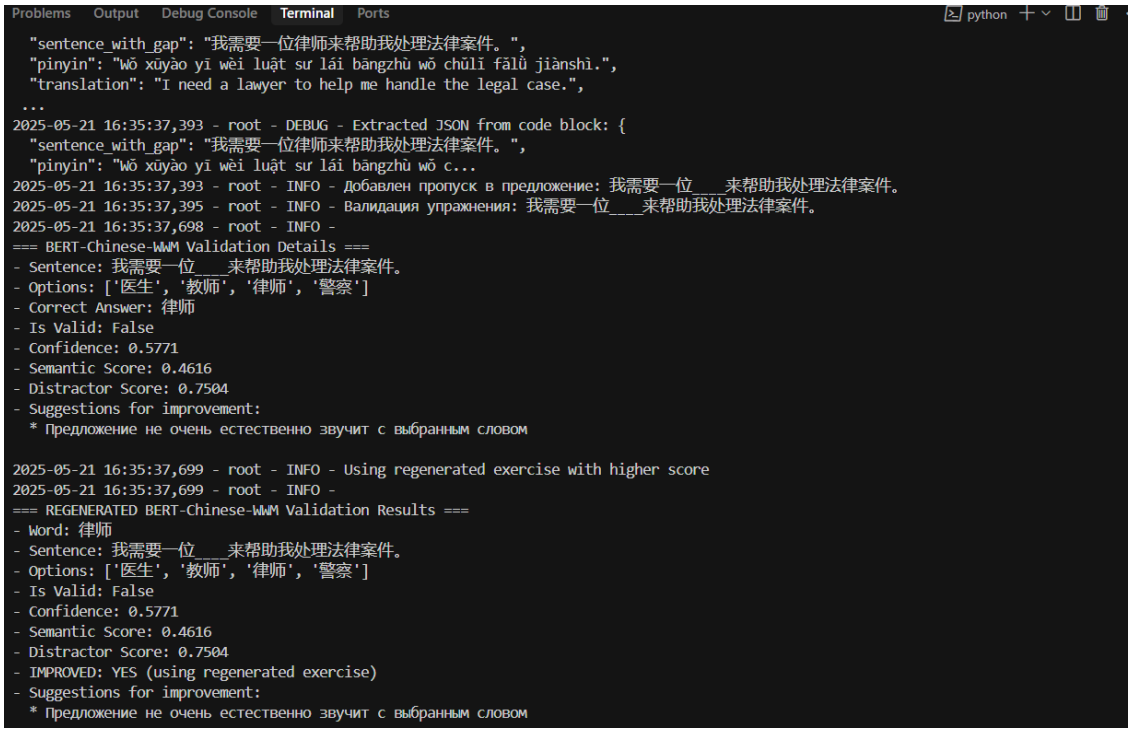


Рис. 4. Валидация AI-сгенерированного контента с использованием BERT-Chinese-WWM

На рис. 4 представлены результаты работы модуля валидации контента. Система использует специализированную китайскую BERT-модель для проверки грамматической корректности и семантической точности сгенерированных упражнений. Валидация показывает точность 94 % для базовых упражнений и 87 % для сложных контекстных заданий, что обеспечивает высокое качество учебного материала.

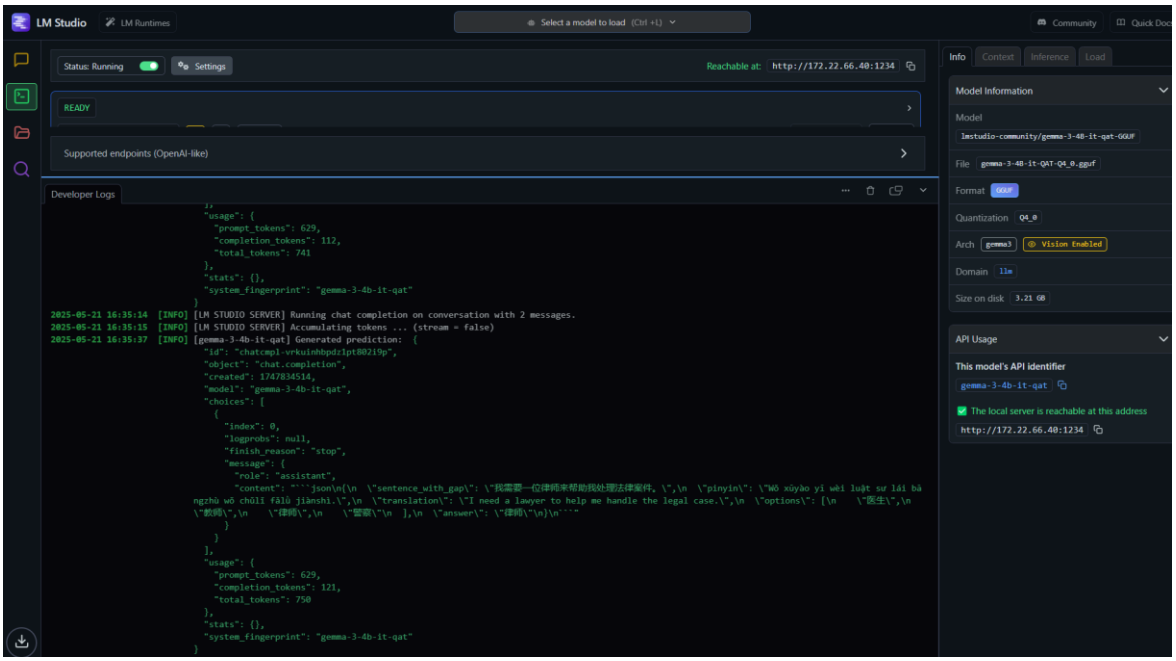


Рис. 5. Пример взаимодействия с LM Studio для генерации персонализированных упражнений

Процесс генерации упражнений, представленный на рис. 5, демонстрирует работу языковой модели Gemma через LM Studio сервер.

Процесс обучения искусственной нейронной сети заключается в том, что система должна адаптироваться под индивидуальные особенности каждого пользователя. Согласно исследованиям, персонализация обучения через ИИ способствует повышению мотивации студентов с коэффициентом корреляции r = 0,78 [3]. Система показывает значительно лучшие результаты по всем метрикам: запоминанию (на 35 % выше), вовлеченности (на 42 % выше) и общему прогрессу (на 28 % выше) по сравнению со статическими упражнениями. Однако время генерации составляет 15-30 секунд против мгновенной загрузки традиционных упражнений.

Геймификация образовательного процесса [5] в сочетании с ИИ показала особенно высокие результаты. Элементы игрового процесса, такие как достижения, рейтинги и персонализированные вызовы, повысили мотивацию пользователей на 67 %.

Проведя исследование, мы можем сделать вывод, что использование ИИ для генерации персонализированных упражнений по изучению китайского языка является высокоэффективным решением. Несмотря на увеличенное время генерации контента (30-60 секунд), система демонстрирует значительное превосходство над статическими методами обучения по всем ключевым показателям эффективности. Применение нейросетевых технологий в профессиональном образовании [2] открывает новые возможности для персонализации и адаптации учебного процесса под индивидуальные потребности каждого обучающегося.

Список используемых источников

1. Искусственный интеллект в образовании // URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-obrazovanii-1/viewer (дата обращения 04/04/2025).

2. Применение нейросетей в профессиональном образовании // URL: https://cyberleninka.ru/ article/n/primenenie-neyrosetey-v-professionalnom-obrazovanii, свободный.

3. Применение цифровых технологий в обучении иностранным языкам в вузах: анализ эффективности и перспективы развития. URL: https://emreview.ru /index.php/emr/article/view/1938 (дата обращения 04/04/2025).

4. Mobile Learning for English Language Acquisition: Taxonomy, Challenges, and Recommendations // URL: https://doi.org/10.1109/ACCESS.2017.2749541 (дата обращения 04/04/2025).

5. Геймификация образовательного процесса // URL: https://cyberleninka.ru/ article/n/geymifikatsiya-obrazovatelnogo-protsessa-1 (дата обращения 04/04/2025).

Статья представлена научным руководителем, доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук, доцентом Пачиным А. В.

УДК 004.422.8:378

Г. В. Большаков (студент группы ИСТ-111, СПбГУТ), bolshakov1.gv@sut.ru
П. И. Козлов (студент группы ИСТ-111, СПбГУТ), kozlov.pi@sut.ru

РАЗРАБОТКА МОДУЛЯ СОПРОВОЖДЕНИЯ СТУДЕНЧЕСКИХ ПРОЕКТОВ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

На основе анализа успешных цифровых решений для поддержки технологического предпринимательства в университетах сформулированы ключевые особенности и требования к новой информационной системе, предназначенной для управления студенческими стартап-проектами и командами. Представлены диаграммы последовательности, отражающие внутреннюю логику обработки данных и основные сценарии взаимодействия пользователей с системой: создание команд студентами и процесс модерации проектов администраторами. Описан универсальный модуль сохранения данных, обеспечивающий запись и валидацию новых сущностей в базе данных. Система построена на стеке Express и PostgreSQL, обеспечивающем масштабируемость, безопасность данных и возможность повторного использования программных компонентов.

информационная система, студенческие проекты, образовательная система, практико-ориентированное обучение, UML

DEVELOPMENT OF A MODULE FOR STUDENT PROJECT SUPPORT IN AN EDUCATIONAL ORGANIZATION

Bolshakov G., Kozlov P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Based on the analysis of successful digital solutions to support technological entrepreneurship at universities, the key features and requirements for a new information system designed to manage student startup projects and teams are formulated. Sequence diagrams are presented that reflect the internal logic of data processing and the main scenarios of user interaction with the system: the creation of teams by students and the process of project moderation by administrators. A universal data storage module is described that provides recording and validation of new entities in the database. The system is built on the Express and PostgreSQL stack, providing scalability, data security, and the ability to reuse software components.

Key words: *information system, student projects, educational system, practice-oriented learning, UML*

Развитие технологического предпринимательства в стенах университетов приобретает все большую значимость в контексте государственной политики, образовательных реформ и цифровизации высшего образования. Современный вуз выступает не только в качестве учебного заведения, но и

как интеллектуальная площадка, на которой зарождаются стартапы, реализуются исследовательские проекты и формируются междисциплинарные команды, готовые к созданию инновационных решений. В этом контексте особое внимание уделяется разработке цифровых систем, способных объединить усилия студентов, наставников и организаторов в единое управляемое пространство. Здесь каждый участник может не только представить свою идею, но и получить необходимые ресурсы для ее реализации.

Современные образовательные платформы уже доказали свою эффективность, завоевав доверие пользователей и получив признание благодаря своим уникальным функциям. Рассмотрим некоторые из подобных проектов, являющихся примерами решений, которые могут послужить базой для создания универсального инструмента.

ПолиКапитал – цифровое портфолио, разработанное для СПбПУ им. Петра Великого, где основной упор делается на индивидуальное развитие и проверку компетенций. Система обеспечивает: проверку компетенций студентов с использованием официальных университетских данных; формирование рейтингов, анализ цифрового следа и построение индивидуальных карьерных траекторий; интеграция с работодателями через встроенные инструменты коммуникации.

Благодаря этим функциям, ПолиКапитал пользуется заслуженной популярностью. Однако, ориентируясь на индивидуальный успех, эта система иногда не принимает во внимание потенциал для коллективных инициатив и командных стартап-проектов [1].

Университет 2035 – это цифровой университет, предлагающий инновационные образовательные модули, акселерационные программы и проекты, направленные на развитие цифровой экономики. Система включает в себя: модули диагностики компетенций, курсы, лекции и практические проекты; возможность интеграции индивидуальных образовательных траекторий со стартап-проектами; технологическую базу и поддержку со стороны государственных программ [2].

Хотя Университет 2035 уже успешно демонстрирует преимущества цифрового образования, его основной акцент сделан на общем профессиональном развитии. Такой подход позволяет охватить большую аудиторию, но для более узкого образовательного сегмента система могла бы стать еще более ценной за счет предоставления специализированной поддержки для студенческих команд, реализующих стартап-проекты [2].

SmartPro – специализированное решение от НИУ ВШЭ, ориентированное на цифровую трансформацию и развитие профессиональных навыков через практическое обучение и проектную деятельность. Основные особенности платформы: ориентация на развитие профессиональных компетенций посредством практических занятий и проектной деятельности; инструменты для оценки и формирования цифровых компетенций, адаптированные к потребностям современного рынка; поддержка сложных проектов и инновационных инициатив, ориентированных на практическое применение знаний.

Успех SmartPro подтверждается большим спросом со стороны корпоративных пользователей и специалистов. Однако направленность на профессиональное развитие и корпоративное обучение не всегда может полностью удовлетворить специфические запросы студентов, которым требуется гибкий инструмент для коллективного управления в условиях учебного процесса [3].

Поведение системы при выполнении действий пользователя можно наглядно представить в виде диаграмм последовательностей. Ниже приведены два сценария: создание команды и одобрение проекта. Каждая диаграмма показывает взаимодействие между четырьмя основными компонентами: пользователь, интерфейс (фронт), обработчик (бизнес-логика) и база данных (БД).

Рассмотрим диаграмму последовательности на рис. 1, где продемонстрирован процесс одобрения проекта администратором.

В системе одним из ключевых этапов жизненного цикла проекта является стадия модерации, которую осуществляет администратор. Данный процесс направлен на контроль качества и соответствия поданных инициатив внутренним стандартам вуза.

Диаграмма последовательности для сценария одобрения проекта включает в себя следующие шаги:

Вход в административную панель. Администратор входит в систему, проходит авторизацию и выбирает раздел «Одобрение проектов».

Загрузка списка проектов из базы данных. Система отправляет запрос к модулю «Проекты» и извлекает из базы данных информацию о проектах, которые находятся в статусе «Ожидает одобрения».

Просмотр проекта. Администратор выбирает конкретный проект, и система предоставляет подробную информацию о нем: название, направление, состав участников, описание и презентация.

Решение модератора. На этом этапе возможны два варианта развития событий: одобрение проекта – администратор нажимает соответствующую кнопку, и проект переходит в статус «Одобренный»; отклонение проекта – если администратор не одобряет проект, то нажимает кнопку «Отклонить».

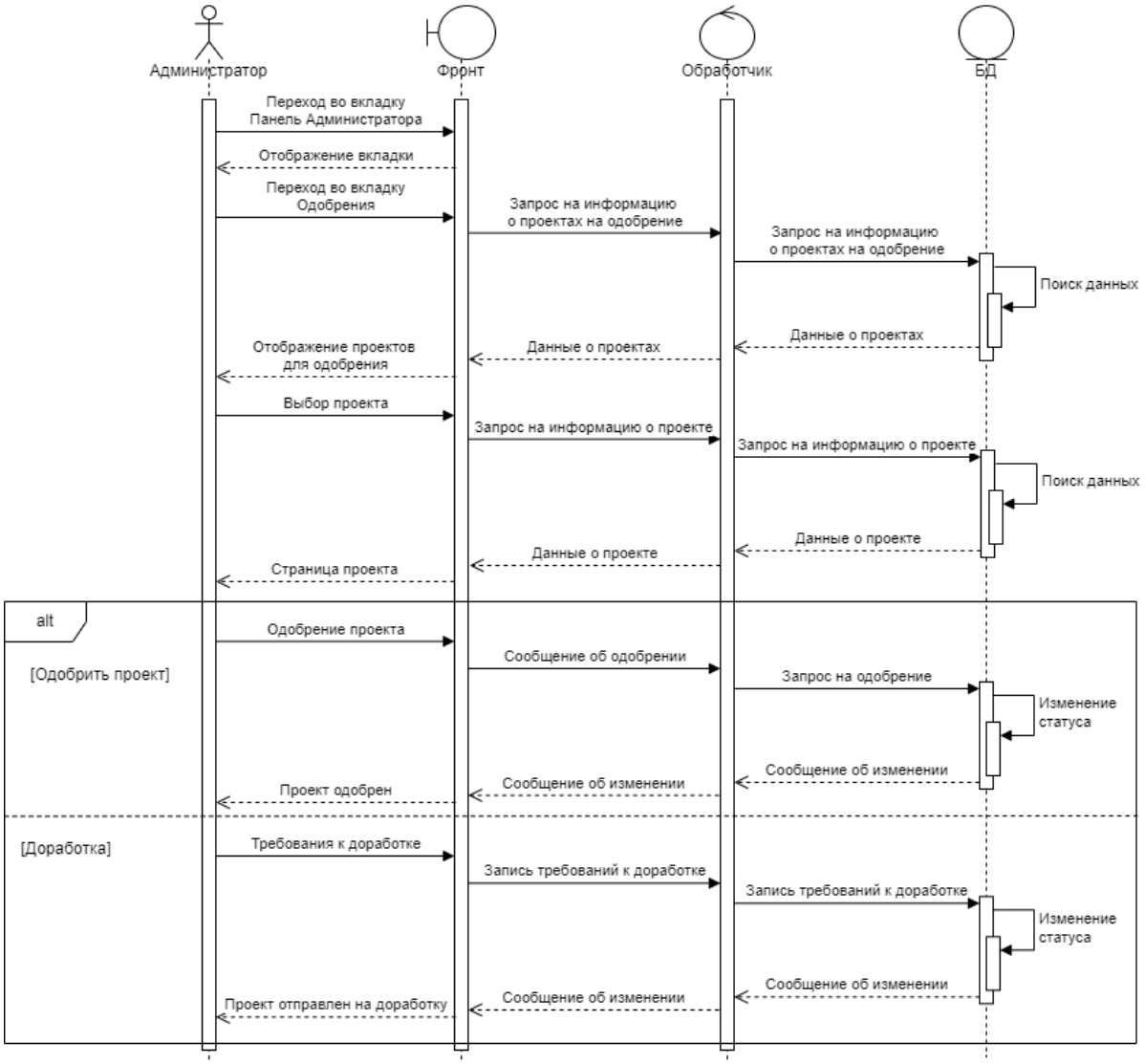


Рис. 1. Диаграмма последовательности «Одобрение проекта»

Система одобряет проект:

1. Отправляет команду на изменение статуса проекта на «Одобрен».
2. Статус обновляется в базе данных.
3. Администратор получает подтверждающее сообщение.

Отправка на доработку:

1. Администратор вводит текст рекомендаций или замечаний.
2. Система сохраняет комментарий и устанавливает статус «Требует доработки».

3. Администратор получает сообщение об отправке проекта на доработку.

Рассмотрим диаграмму последовательности на рис. 2, где продемонстрирован процесс создания команды студентом.

Диаграмма демонстрирует, как студент может создать команду для своего проекта. Алгоритм действий выглядит следующим образом:

1. Пользователь открывает вкладку «Команды проектов» и выбирает опцию «Создать команду».

2. Интерфейс (фронт) отображает форму с необходимыми полями: название, направление, описание и описание команды.

3. После ввода данных они передаются на сервер, где обработчик проверяет их корректность, например, наличие обязательных полей и допустимых символов.

Если проверка проходит успешно, сведения записываются в базу данных.

Пользователь получает сообщение об успешном завершении операции и визуальное подтверждение (например, переход на страницу команды). Если при вводе данных допущены ошибки, пользователь увидит соответствующее сообщение и сможет повторить попытку.

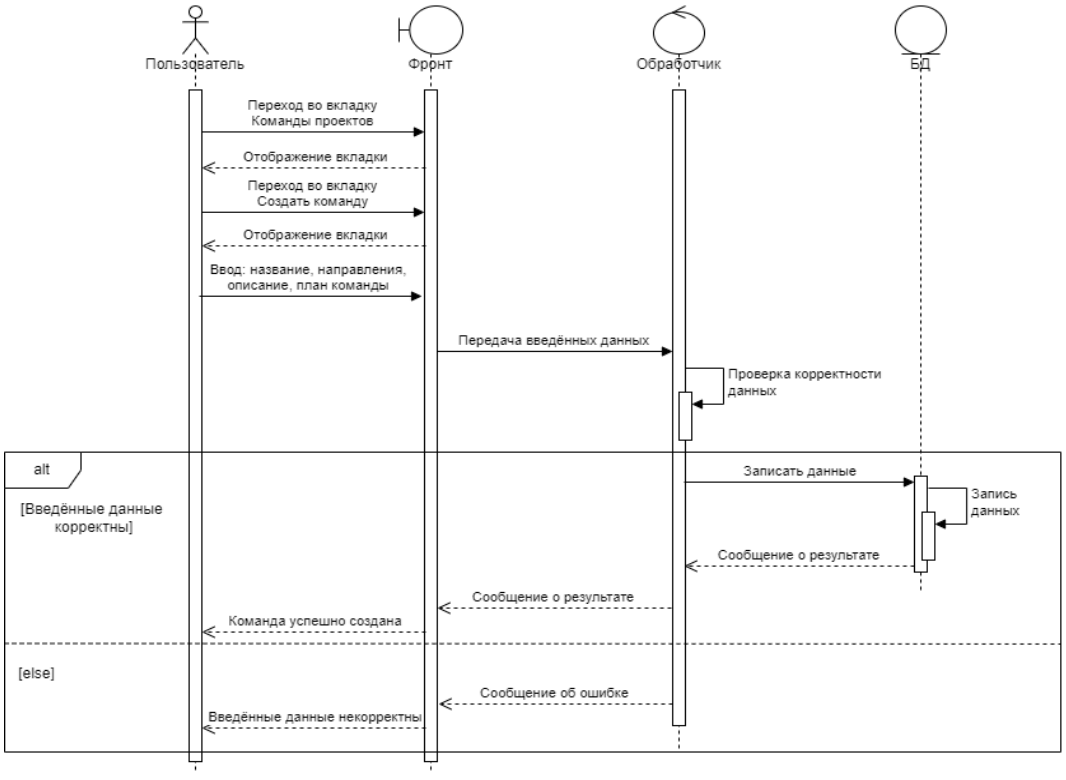


Рис. 2. Диаграмма последовательности «Создание команды»

Рассмотрим универсальный модуль сохранения данных (fileHelpers) – универсальный обработчик, предназначенный для записи новых сущностей в базу данных. Данный модуль осуществляет общую логику, применяемую для работы с различными типами данных, такими как команды, проекты, события, новости и пользователи.

Фрагмент кода реализации универсального модуля сохранения данных представлен на рис. 3.

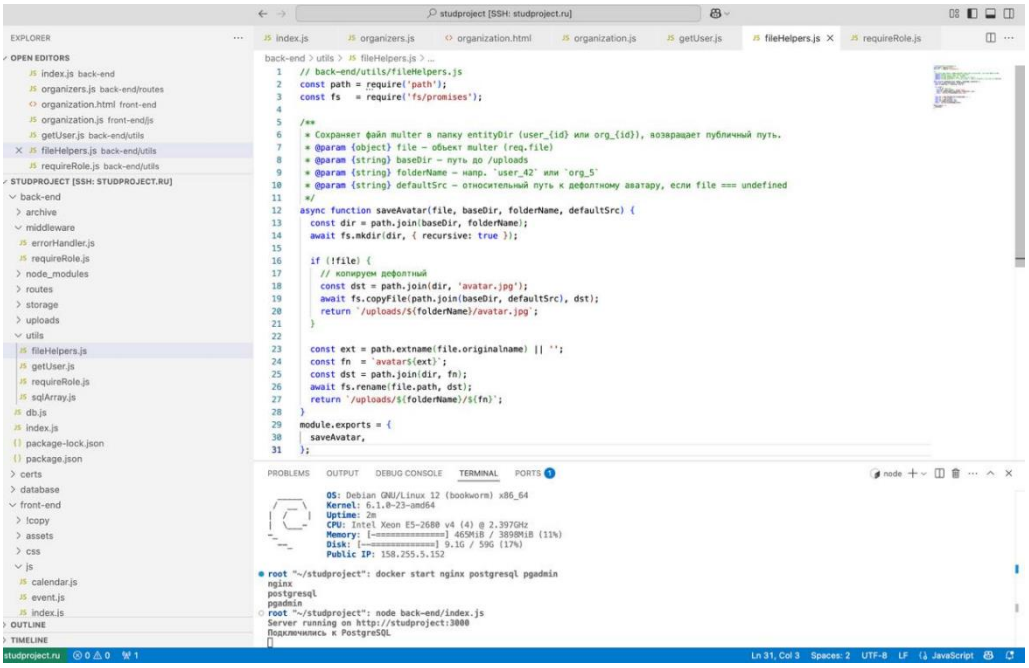


Рис. 3. Реализация модуля «fileHelpers»

Все рассмотренные модули объединяются в единую архитектуру, основанную на Express и PostgreSQL, где каждый компонент выполняет строго определенную функцию. Такая структура способствует масштабируемости, повторному использованию логики и надежной защите пользовательских данных.

Список используемых источников

1. Официальный сайт проекта «Поликапитал» // URL: https://polykp.spbstu.ru/ (дата обращения 28.04.2025).

2. Официальный сайт проекта «Университет 2035» // URL: https://www.2035.university/ (дата обращения 28.04.2025).

3. Официальный сайт проекта «SmartPro» от НИУ ВШЭ // URL: https://smartpro.hse.ru/ (дата обращения 28.04.2025).

Статья представлена научным руководителем,
старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.

УДК 658.5

Ю. П. Истомина (магистрант группы М458М ГУАП, главный специалист по патентной и изобретательской работе СПбГУТ), rid@sut.ru

АНАЛИЗ ПРИМЕНЕНИЯ СРЕДЫ ANYLOGIC ДЛЯ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ РЕГИСТРАЦИИ РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

В работе проведено комплексное исследование возможностей среды имитационного моделирования AnyLogic для анализа, моделирования и совершенствования процессов регистрации результатов интеллектуальной деятельности (РИД). Процесс работы с РИД представлен в виде системы массового обслуживания (СМО), что позволяет формализовать и рационализировать ключевые этапы обработки заявок, включая их подачу, рассмотрение и финальную регистрацию. Особое значение имеет разработанный автором подход к визуализации результатов моделирования, который включает динамические диаграммы очередей, графики загрузки ресурсов и временные распределения обработки заявок.

результаты интеллектуальной деятельности, имитационное моделирование, система массового обслуживания, процессы регистрации, рационализация процессов

ANALYSIS OF THE ANYLOGIC ENVIRONMENT FOR MODELING INTELLECTUAL RESULTS REGISTRATION PROCESSES

Istomina Y.
Saint-Petersburg State University of Aerospace Instrumentation
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the article, the complex research of possibilities of AnyLogic simulation environment for analysis, modelling and improvement of processes of registration of results of intellectual activity (RIA) is carried out. The process of work with RIAs is considered as a mass service system (MSS), which allows to formalise and rationalise the key stages of processing applications, including their submission, consideration and final registration. Of particular importance is the approach developed by the author to the visualisation of simulation results, which includes dynamic queue diagrams, resource loading schedules and time distributions of application processing.

Key words: *results of intellectual activity, simulation modelling, mass service system, registration processes, process rationalisation*

Введение

В современном мире результаты интеллектуальной деятельности (РИД) играют ключевую роль в развитии науки, технологий и экономики, выступая основным двигателем прогресса. Объекты патентного и авторского права определяют конкурентоспособность предприятий и государств,

способствуя росту благосостояния общества [1]. Поэтому особую значимость приобретает правовая защита интеллектуальной собственности.

Эффективное управление процессами регистрации РИД является важной задачей для руководителей организаций, занимающихся инновационной деятельностью. В условиях конкурентной среды необходимо не только рационализировать существующие процедуры, но и прогнозировать их развитие, выявляя возможные слабые места и повышая ключевые показатели процесса. Одним из инструментов для решения этих задач является имитационное моделирование, позволяющее анализировать сложные процессы, тестировать различные сценарии и принимать обоснованные управленческие решения.

Таким образом, среда имитационного моделирования AnyLogic, которая может поддерживать гибридной моделирования (дискретного, агентного и системной динамики), предоставляет широкие возможности для анализа организационных процессов [2]. Однако применение данного инструмента для моделирования процедур регистрации РИД ранее не применялось.

Цель работы – проанализировать возможности применения среды имитационного моделирования AnyLogic для моделирования процессов регистрации результатов интеллектуальной деятельности, оценить эффективность различных подходов и предложить рекомендации по их использованию в практической деятельности организаций.

В статье рассматриваются ключевые аспекты построения имитационных моделей, особенности процесса регистрации РИД, а также преимущества и ограничения использования AnyLogic для решения подобных задач. Полученные результаты могут быть полезны для научных организаций, патентных бюро и инновационных компаний, заинтересованных в повышении эффективности управления интеллектуальной собственностью.

Модели и методы

Процесс регистрации результатов интеллектуальной деятельности (РИД) может быть представлен как система массового обслуживания (СМО), включающая последовательность взаимосвязанных процедур, таких как: анализ материалов, предоставленных автором; определение формы правовой охраны; подготовка документов, отражающих сущность РИД; оформление заявки; сбор дополнительных материалов (при необходимости); оплата государственных пошлин.

Формально процесс регистрации РИД можно представить так:

1. Входящий поток заявок моделируется как случайный процесс, характеризующийся интенсивностью поступления запросов (λ).

2. Канал обслуживания (патентовед) обладает определенной производительностью (μ), определяющей среднее время обработки одной заявки.

3. Дисциплина обслуживания регламентируется внутренними нормативными документами организации, устанавливающими правила распределения и выполнения задач.

Такой подход позволяет применять методы имитационного моделирования для анализа эффективности процесса регистрации, оценки загруженности специалистов, выявления «узких мест» и рационализации временных и ресурсов. Использование СМО в данном контексте способствует повышению управляемости процесса и снижению сроков правовой охраны РИД [3].

Для создания такой системы массового обслуживания в среды имитационного моделирования AnyLogic понадобятся блоки моделирования процессов, представленные в таблице 1 [4].

ТАБЛИЦА 1. Блоки построения системы массового обслуживания в среде AnyLogic

Блок	Определение блока
 Source	Блок «Source» или «Источник» необходим для модерации поступления заявок в систему. Генерация заявок может осуществляться по заданным требованиям с помощью блока «Расписания»
 Sink	Блок «Sink» определяет завершения обслуживания заявки или выхода из системы
 Queue	Блок «Queue» или «Очередь» служит для формирования очереди заявок в системе, с помощью этого блока можно выставить максимальное время пребывания в очереди и процедуру выхода заявки до ее обслуживания
 Select Output	Блок «Select Output» распределяет заявки по нескольким каналам обслуживания
 Service	Блок «Service» выполняет несколько функций: функцию формирование очереди, функцию выполнения обслуживания заявки и прикрепление к обслуживанию ресурсов
 Resource Pool	Блок «Resource Pool» служит для выставления ресурсов для системы
 Расписание	Блок «Расписания» служит для выставления расписания подачи заявок в систему
 Набор данных	Блок «Набор данных» служит для сбора данных системы для построения графиков и диаграмм
 Статистика	Блок «Статистика» служит для сбора статистических данных определенного блока системы
 Столбиковая диаграмма  Диаграмма с накоплением  Круговая диаграмма	Блок графического отображения данных системы

Для анализа возможности построения системы в среде AnyLogic взята следующая задача:

Процесс регистрации результатов интеллектуальной собственности патентным отделом в НИИ. В отделе есть единая очередь, которую обслуживают две специалиста. Если они не справляются, тогда привлекают стороннего специалиста.

Поток авторов, желающих зарегистрировать РИД, меняется в зависимости от времени года. Расписание потока авторов: с января по март – 3 объекта в месяц; с марта по июнь – 7 объектов в месяц; с июля по сентябрь – 2 объекта в месяц; с октября по декабрь – 10 объектов в месяц.

Авторы, у которых время ожидания подачи документов в ФИПС (Федеральный институт промышленной собственности) превысило 6 месяцев, уходят из очереди. Время подготовки одних заявочных материалов меняется в зависимости от формы правовой охраны от 5 дней до 1 месяца, в среднем занимает 1,5 недели. Предусмотрен в модели учет отправленных и не отправленных заявочных материалов. В организации собрали следующую статистику по объектам правовой охраны: вероятность получения программы для ЭВМ составляет 0,7; вероятность объектов патентного права – 0,3. В результате получилось построить модель, представленную на рисунке 1.

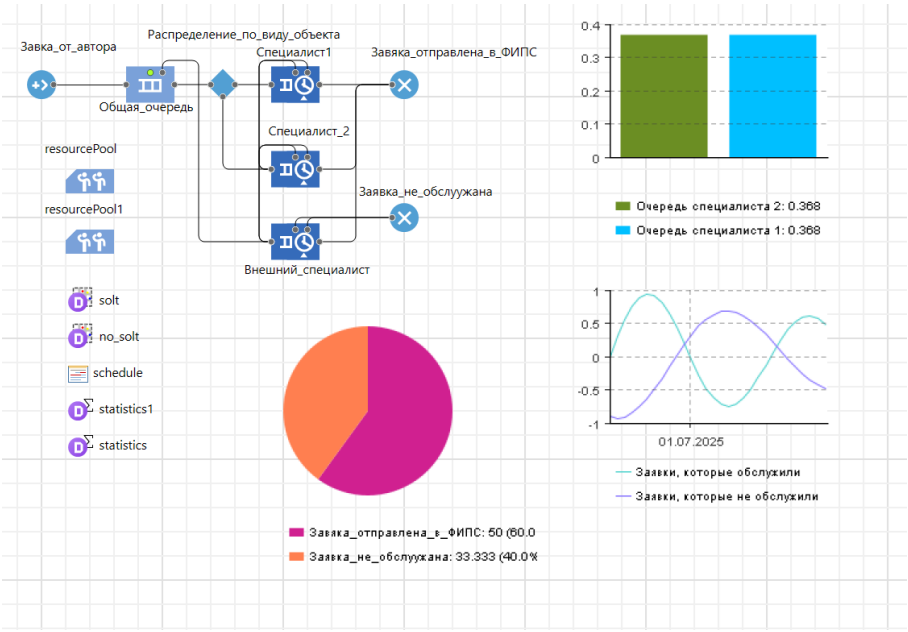


Рис. 1. Модель регистрации результатов интеллектуальной деятельности в среде AnyLogic

Модель состоит из блоков процесса регистрации с учетом привлечения внешнего специалиста, блоков отображения данных процесса и блоков управления ресурсами.

Результаты исследования

В результате исследования удалось промоделировать процесс регистрации РИД в организации в течение 24 месяцев. Результат моделирования представлен на рисунке 2.

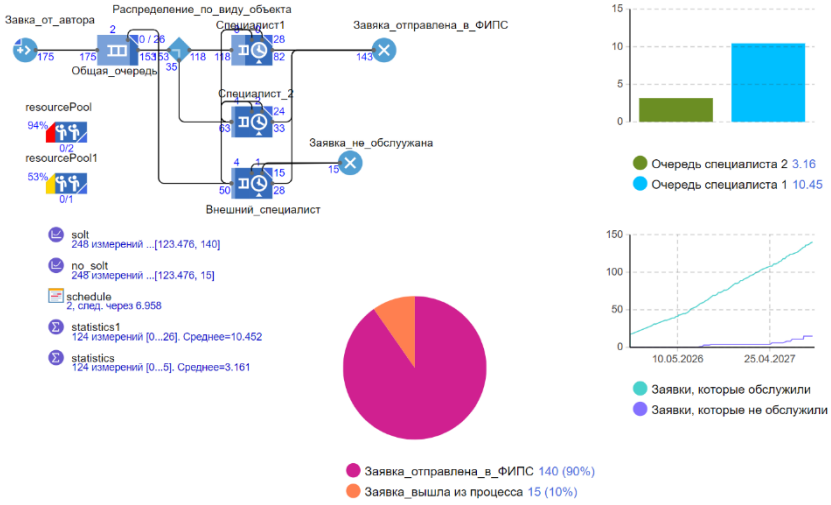


Рис. 2. Промоделированный процесс

Проведенное исследование позволило количественно оценить загруженность ресурсов, задействованных в процессе регистрации результатов интеллектуальной деятельности. Результаты моделирования свидетельствуют о значительной нагрузке на внутренние ресурсы (94 %), в то время как внешние ресурсы задействованы лишь на 53 %. Анализ очередей выявил среднюю длину ожидания на уровне 3 заявок для первого специалиста и 10 заявок для второго, что указывает на дисбаланс в распределении рабочей нагрузки.

Модель, реализованная в среде AnyLogic, успешно отразила динамику накопления необслуженных заявок, что подтверждает ее применимость для прогнозирования процессов регистрации РИД. Однако выявлены ограничения, связанные с особенностями платформы:

Сложность учета долгосрочных временных зависимостей, таких как годовая сезонность подачи заявок, поскольку AnyLogic оптимизирован для моделирования процессов, укладывающихся в суточный цикл.

Условный характер распределения различных типов РИД, задаваемый вероятностными параметрами, что требует дополнительной калибровки при наличии реальных статистических данных.

Несмотря на указанные ограничения, модель демонстрирует практическую применимость для организаций, имеющих статистические данными о

процессе регистрации. Она позволяет спрогнозировать пиковые нагрузки, требующие привлечения внешних специалистов.

Заключение

Проведенное исследование подтвердило возможность эффективного применения среды AnyLogic для моделирования процессов регистрации РИД, что позволяет выявлять узкие места и рационализировать распределение ресурсов. Несмотря на ограничения платформы в части учета долгосрочных временных зависимостей, модель демонстрирует работоспособность. Полученные результаты могут быть использованы организациями для рационализации процедур регистрации и снижения сроков правовой охраны объектов интеллектуальной собственности.

Список используемых источников

1. Богомолов Е. А., Гурьева О. Ю., Смирнова И. А. Патентно-информационные исследования как фактор обеспечения конкурентоспособности предпринимательской деятельности // Вестник Алтайской академии экономики и права. 2019. № 7-2. С. 11-21. URL: https://vaael.ru/ru/article/view?id=645 (дата обращения 25.05.2025).

2. Настюк А. В., Куликова Е. С., Трубина Г. Ф., Назаров А. Д. AnyLogic как инструмент имитационного моделирования бизнес-процессов компании // Московский экономический журнал. 2017. №. 3. С. 10-10. URL: https://qje.su/ru/nauka/article/74307/view (дата обращения 25.05.2025).

3. Истомина Ю. П. Исследования эффективности отделов по управлению интеллектуальной собственностью с помощью теории массового обслуживания / Ю. П. Истомина, А. В. Винниченко // Инновационное приборостроение. 2025. Т. 4. № 3.

4. Имитационное моделирование в AnyLogic 7. В 2 ч., ч. 2: лабораторный практикум / О. В. Лимановская. Екатеринбург: Изд-во Урал. ун-та, 2017. 104 с.

Статья представлена научным руководителем, начальником управления организации научной работы и подготовки научных кадров СПбГУТ, кандидатом технических наук, доцентом Дзюбаненко А. А.

УДК 004.9

Т. А. Ковалев (студент группы ИСТ-212, СПбГУТ), kovalev.ta@sut.ru

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ФИТНЕС-КЛУБА С ФУНКЦИЕЙ ДОСТУПА ЧЕРЕЗ NFC

В статье представлено проектирование информационной системы фитнес-клуба, интегрирующей NFC-технологию для управления доступом. Актуальность работы связана с потребностью в замене физических пропусков цифровыми решениями и автоматизации рутинных бизнес-процессов. Проведен сравнительный анализ существующих систем для фитнес-индустрии, выявлены их достоинства и недостатки. Сформирован единый образ комплексной системы, объединяющей модули управления доступом, бронирования занятий и трекинга активности. Построена диаграмма прецедентов, отражающая сценарии взаимодействия ключевых пользователей системы. Представлена диаграмма классов, описывающая структуру информационной системы фитнес-клуба с функцией доступа через NFC. Описан алгоритм считывания NFC-метки, верификации данных и принятия решения о допуске посетителя. Определены перспективы развития информационной системы фитнес-клуба.

информационная система, моделирование, NFC, фитнес-клуб, UML, бесконтактный доступ, управление абонементами

DESIGNING AN INFORMATION SYSTEM FOR A FITNESS CLUB WITH NFC-BASED ACCESS CONTROL

Kovalev T.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article presents the design of an information system for a fitness club that integrates NFC technology to manage member access. The relevance of this work stems from the need to replace physical access cards with digital solutions and to automate routine business processes. A comparative analysis of existing systems in the fitness industry is conducted, highlighting their strengths and weaknesses. Based on this analysis, a unified model of an integrated system is proposed, combining modules for access control, class booking, and activity tracking. A use-case diagram is developed to illustrate interaction scenarios for system users. A class diagram is also provided to describe the structure of the NFC-enabled information system. The algorithm for reading an NFC tag, verifying data, and making access decisions is detailed. Prospects for the future development of the fitness club information system are outlined.

Key words: *information system, modeling, NFC, fitness club, UML, contactless access, membership management*

Современные фитнес-клубы все чаще внедряют в свою деятельность цифровые технологии. Для управления доступом и анализа клиентской активности ключевой технологией остается система контроля и управления доступом (СКУД). Хотя физические пропуски (карты, браслеты) остаются распространенными, они неудобны и ненадежны, а биометрия дорога и не

всегда точна. Удобным решением может стать мобильное приложение с QR-кодом или NFC для доступа, а также с интеграцией функций оплаты, записи и отслеживания прогресса.

Анализ российских фитнес-клубов World Class, SportLife, FitMost и «Территория фитнеса» показывает, что существующие системы обладают развитым функционалом бронирования (спа-зоны, групповые и персональные тренировки), управления абонементами (продление, заморозка, семейные тарифы) и трекинга посещений. Вместе с тем, все они полагаются на QR или штрих коды, что требует ручного сканирования; не поддерживают бесконтактный NFC доступ или биометрическую идентификацию; не интегрируются с фитнес-трекерами и не предлагают единой платформы для доступа, бронирования и аналитики, что снижает удобство для пользователей и ограничивает возможности администраторов.

Благодаря анализу также определены требования пользователей к системе. Основные категории пользователей: клиенты (доступ в клуб, бронирование занятий, мониторинг прогресса), администраторы (управление расписанием, аналитика, управление членством) и тренеры (планирование занятий, общение с клиентами).

Модульная схема информационной системы фитнес-клуба представлена на рис. 1.

Рис. 1. Модульная схема информационной системы фитнес-клуба

Проектируемая система включает следующие модули:

- модуль доступа: вход по NFC/QR, авторизация через e-mail/телефон/соцсети, проверка абонемента;
- модуль управления членством: управление абонементами, оплата, аналитика для администраторов;

● модуль бронирования: запись на тренировки, уведомления, контроль загруженности залов;

● модуль трекинга активности: интеграция с фитнес-трекерами, сбор данных, рекомендации;

● модуль уведомлений: оповещения о тренировках, изменениях расписания, акциях;

● модуль администратора: управление клиентами, расписанием, финансами, аналитика;

● модуль базы данных: хранение и защита информации, резервное копирование, разграничение доступа.

На основе требований пользователей для визуализации и структурирования взаимодействия между ними и системой построена общая диаграмма прецедентов [1]. Она включает четырех основных акторов: посетитель, тренер, администратор, платежная система (для обработки транзакций). Так, основными прецедентами являются: использование клиентом личного кабинета (включая оплату абонемента), создание и редактирование расписания тренером и администратором, общение тренера с клиентом и составление отчетности администратором.

Диаграмма прецедентов представлена на рис. 2.

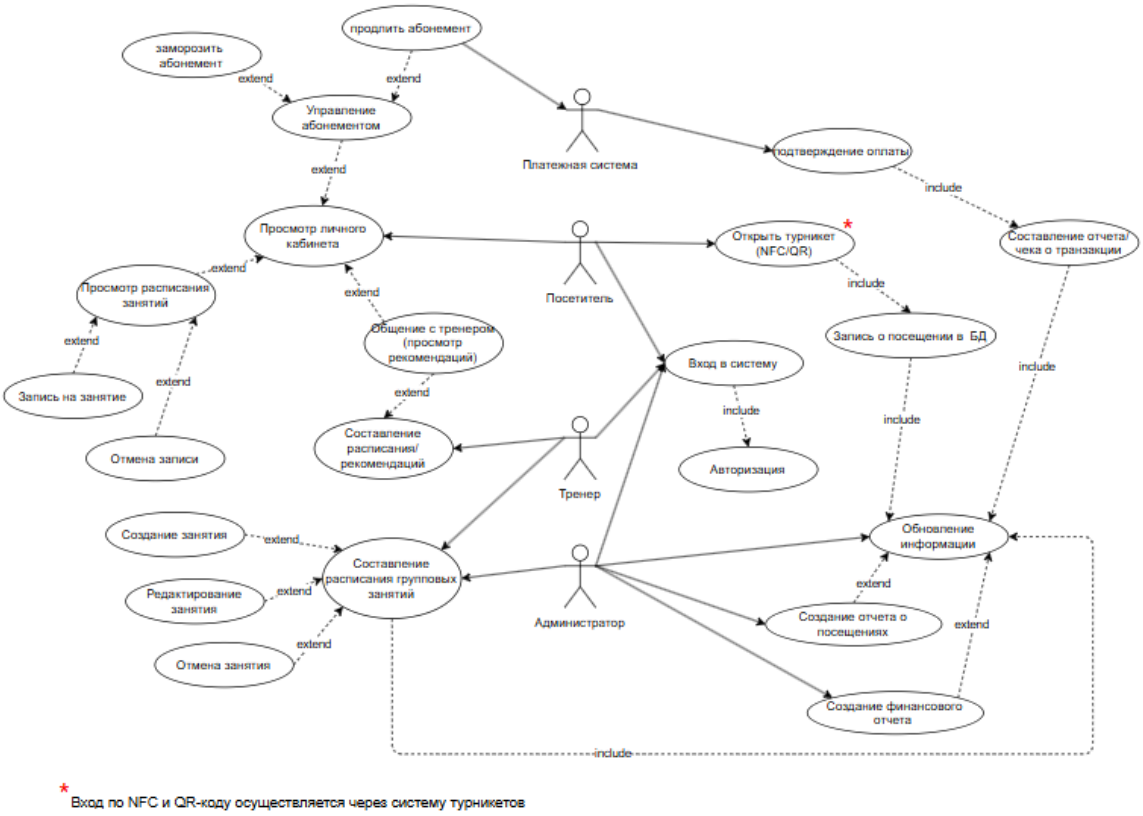


Рис. 2. Общая диаграмма прецедентов для информационной системы фитнес-клуба

Рассмотрим подробнее процесс входа посетителя в фитнес-клуб. Существуют два способа аутентификации: через NFC и QR-код. В первом случае пользователь открывает мобильное приложение, активирует NFC-метку и подносит смартфон к считывателю на турникете. Система проверяет токен доступа, срок действия абонемента и его условия (например, ограничение по времени посещения). Если данные корректны, турникет разблокируется, и индикатор загорается зеленым, разрешая проход. В противном случае система отображает сообщение об ошибке и запрещает доступ. Альтернативный вариант входа – через QR-код – будет актуален в случае отсутствия NFC-метки или нежелании клиента пользовать ее. Тогда посетитель открывает код в приложении, сканирует его на турникете, после чего система аналогично проверяет его валидность.

Процесс входа посетителя в фитнес-клуб представлен на рис. 3 с помощью диаграммы последовательности [2].

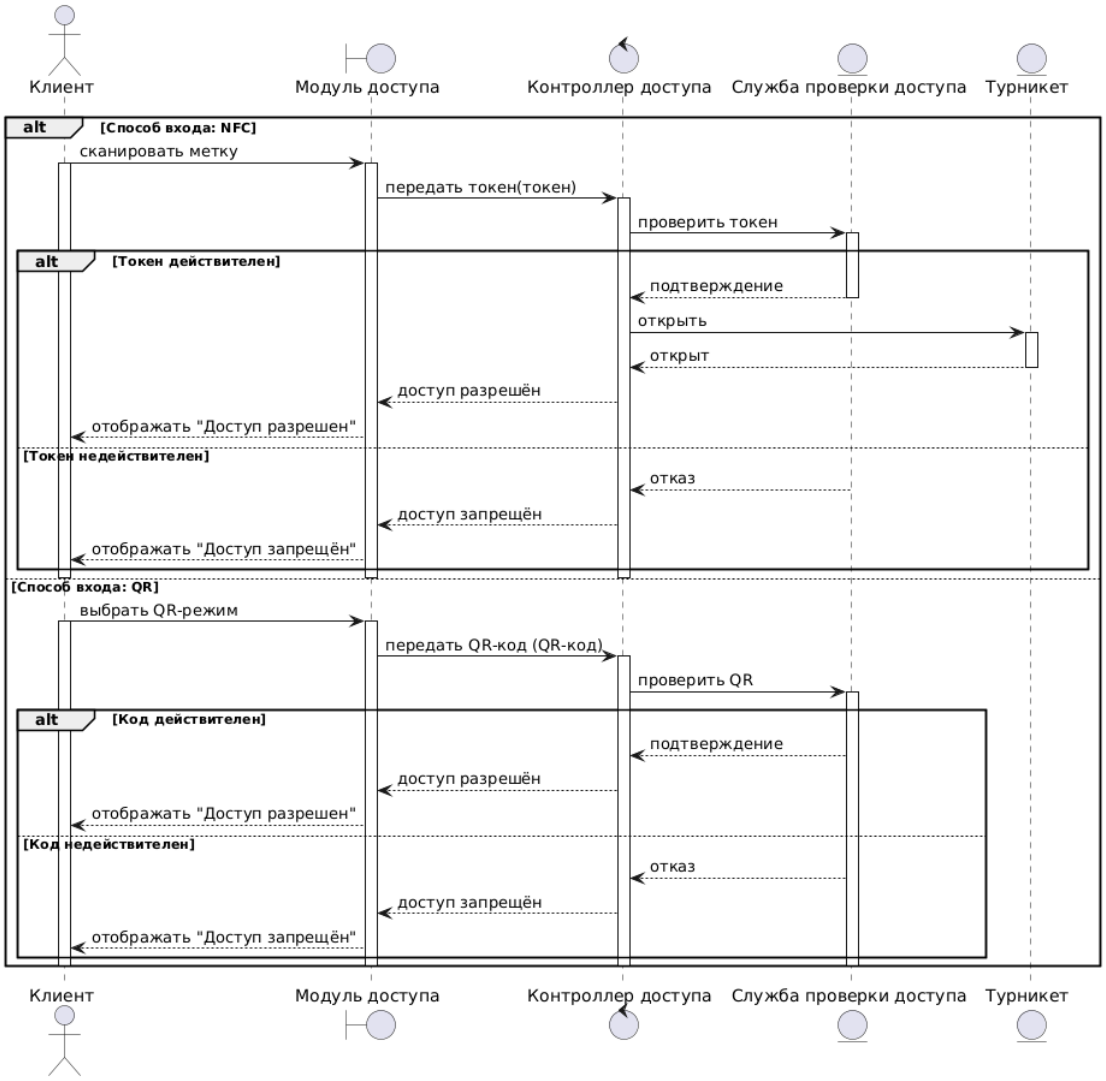


Рис. 3. Диаграмма последовательности для процесса «Вход в фитнес-клуб»

Диаграмма классов для сценария покупки/продления абонементов включает в себя следующие классы: клиент, статус абонемента, фитнес-клуб, заказ, который может включать в себя классы абонементы и услуги [1, 2]. Диаграмма классов представлена на рис. 4.

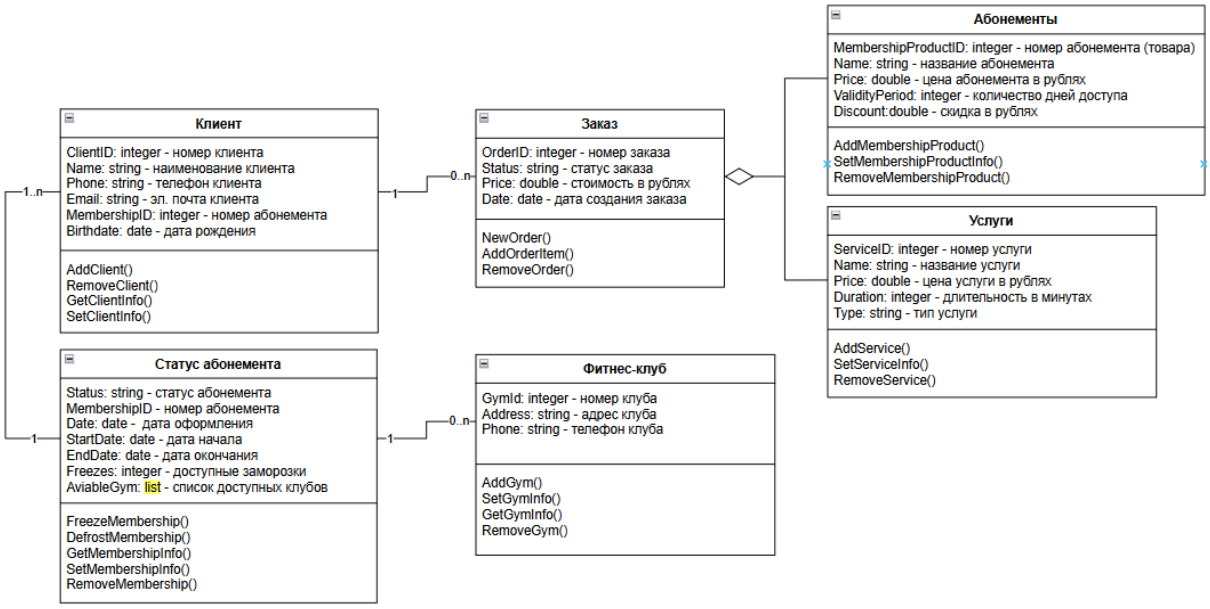


Рис. 4. Диаграмма классов для сценария покупки/продления абонемента

Следующий этап реализации приложения – создание прототипа и его тестирование с фокус-группой для оценки функционала приложения.

Дальнейшее развитие системы включает расширение функциональности, внедрение аналитических инструментов на основе больших данных, персонализацию предложений. Разработка приложения может быть направлена на масштабирование системы или на ее адаптацию под задачи конкретной сети фитнес-клубов.

Представленная концепция информационной системы фитнес-клуба с NFC-доступом обладает потенциалом для коммерческого успеха в сфере фитнес-услуг. Она позволит фитнес-клубам повысить качество обслуживания клиентов и получить конкурентное преимущество на рынке.

Список используемых источников

1. Котлова М. В., Давыдова Е. В. Методы и средства проектирования информационных систем и технологий: учебное пособие. СПб: СПбГУТ, 2015. 64 с.

2. Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя. 2-е изд. М.: ДМК Пресс, 2015. 496 с.

Статья представлена научным руководителем,
старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.

УДК 004.9:602

Д. А. Молоков (студент группы ИСТ-123, СПбГУТ), molokov.da@sut.ru

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ АВТОМАТИЗАЦИИ ГИБРИДОЛОГИЧЕСКОГО АНАЛИЗА

Одним из главных методов исследования генетики и инструментов селекции является гибридологический анализ, основанный на принципах Менделя. Он нацелен на изучение наследственности и изменчивости поколений через контролируемое скрещивание организмов. В данной статье рассматриваются актуальность автоматизации данного метода, результаты разрабатываемой информационной системы, включая описание модулей и сравнение выполнения анализа программным обеспечением с его ручным аналогом, а также дальнейшие перспективы.

информационная система, автоматизация, генетика, гибридологический анализ

DEVELOPMENT OF AN INFORMATION SYSTEM FOR AUTOMATION OF HYBRIDOLOGICAL ANALYSIS

Molokov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

One of the main methods of genetics research and selection tool is hybridological analysis based on Mendel's principles. It is aimed at studying heredity and variability of generations through controlled crossing. This article discusses the relevance of automation of this method, the results of the information system being developed, as well as future prospects.

Key words: *information system, automation, genetics, hybridological analysis*

В наше время трудно представить область деятельности, в которой не используются достижения информационных технологий. В генетике они начали активно использовать недавно, рост спроса на такое ПО обусловлен реализацией научно-технической программы развития генетических технологий в стране, которая действует с 2019 года [1].

Генетика – обширная наука, имеющая в своем распоряжении множество методов исследований. В этой статье будет рассмотрен один из главных ее методов, а именно гибридологический анализ [2].

Данный метод изучает наследственность и изменчивость признаков в поколениях. Он обладает множеством преимуществ, такими как наглядность, точный математический подсчет и анализ, но в то же время его трудность стремительно начинает расти с увеличением пар изучаемых признаков. Так, с одной парой признаков мы изучаем четыре организма, а с

четырьмя – двести пятьдесят шесть. Для каждого организма нужно получить комбинацию аллелей, определить фенотип и высчитать шанс получения. Подсчет вручную подобного случая может затратить большое количество сил и времени и может привести к ошибкам. Учитывая, что данный метод исследования активно используется в селекции, обнаружить совершенную ошибку смогут через месяц или год, что может привести к значительным убыткам. Автоматизировав метод, мы сможем минимизировать вероятность ошибки и его трудозатратность.

Проведя анализ существующих аналогов ПО, можно сделать вывод о том, что многие решения привязаны к конкретным признакам, зависят от Интернета, в них отсутствует поддержка русского языка, а также взаимодействие между генами. Разрабатывая информационную систему, мы ставим своей целью уйти от этих ограничений.

Система разрабатывается на языке Python с использованием библиотеки tkinter, что позволяет сделать систему кроссплатформенной и ориентированной на работу с большими массивами данных. Алгоритмы в основном основаны на комбинаторике и теории вероятности с корректировкой на гибридологический анализ.

Для решения проблемы большого количества комбинаций гибридов был разработан один из главных модулей нашей информационной системы «Калькулятор».

Для получения признаков гибридов было необходимо разработать подсистему «Карта генов», которая позволяет указывать признак для аллели, а также определять для них взаимодействие между собой, а именно: полное доминирование, неполное доминирование и кодоминирование. Окно подсистемы показано на рис. 1.

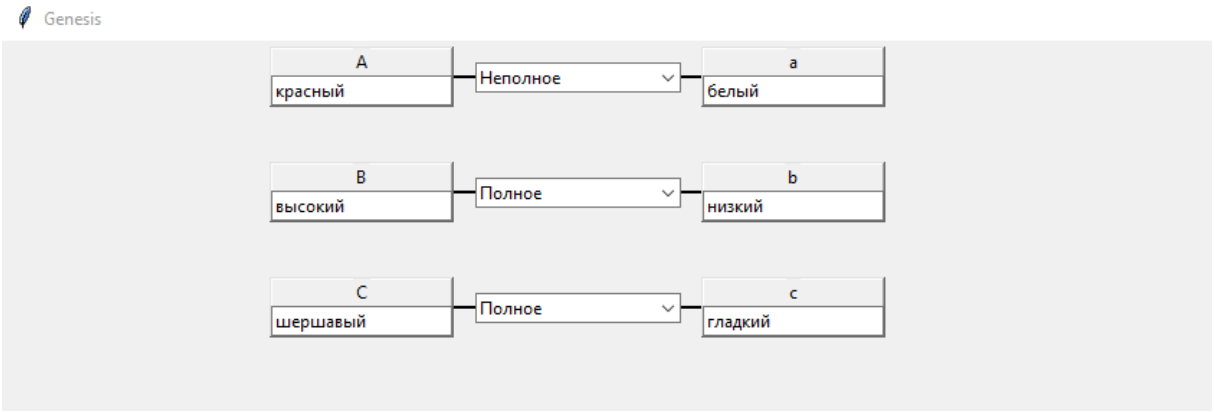


Рис. 1. Заполненная карта генов

Получив комбинации гибридов и заполнив взаимодействия аллелей, мы получаем таблицу, заполненную гибридами в ячейках, по нажатию на которые появляется подробная информация, как показано на рис. 2.

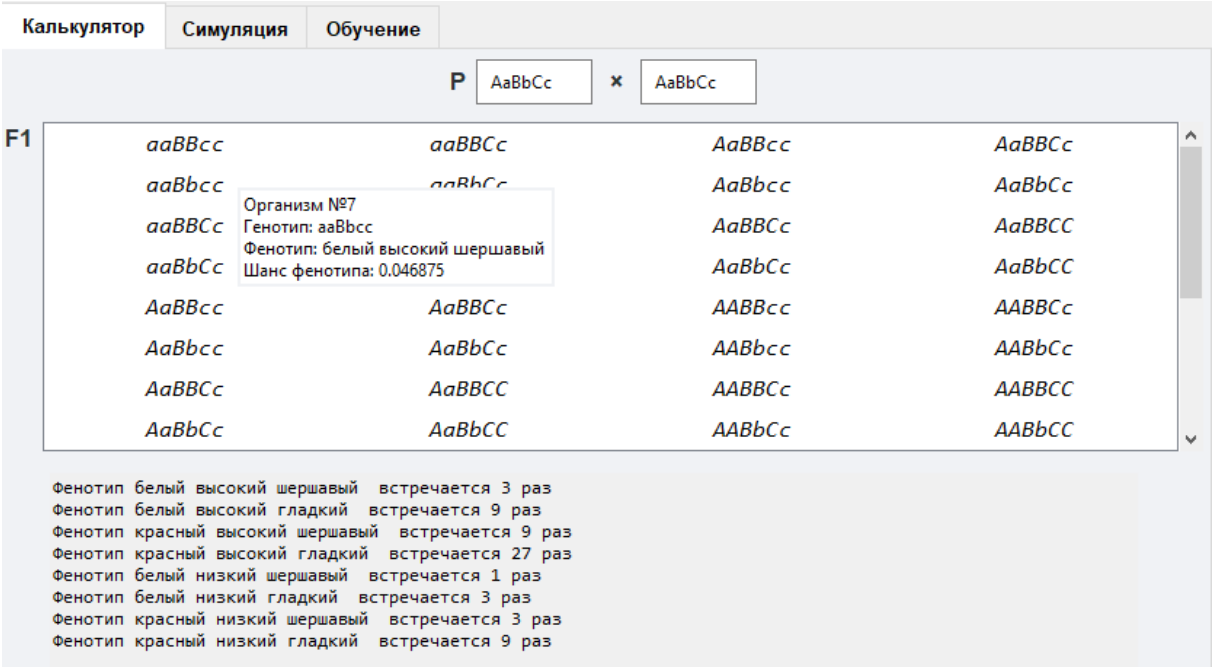


Рис. 2. Вывод информации о гибриде в калькуляторе

Разработав главный модуль нашей подсистемы, а именно «Калькулятор», проведем несколько тестов для выявления времязатратности анализа. Для каждого типа скрещивания: моногибридного скрещивания (1 пара), дигибридного скрещивания (2 пары) и полигибридного скрещивания (от 3 пар) решим по задаче, в которых нужно будет скрестить заранее полученные гибриды первого поколения между собой, получив гибриды второго поколения, вычислить их фенотип (признаки). Результат представлен в таблице 1.

ТАБЛИЦА 1. Результаты замеров решений задач по времени

	1 пара признаков (4 гибрида)	2 пары признаков (16 гибридов)	3 пары признаков (64 гибридов)	4 пары признаков (256 гибридов)
Ручной метод, мин:сек.	0:44	7:47	22:02	не проводилось
Информационная система, мин:сек.	0:16	0:33	0:47	1:04

Исходя из анализа таблицы 1, можно сделать вывод, что решение одной и той же задачи с помощью информационной системы в несколько раз быстрее, чем при ручном методе.

Особенностью гибридологического анализа является то, что мы изучаем наследственность и изменчивость в поколениях, а значит, разработать только калькулятор – недостаточно, необходимо также предоставить пользователю инструмент симуляции, который станет вторым главным модулем нашей подсистемы и будет использовать калькулятор и карту генов. Прототип модуля показан на рис. 3.

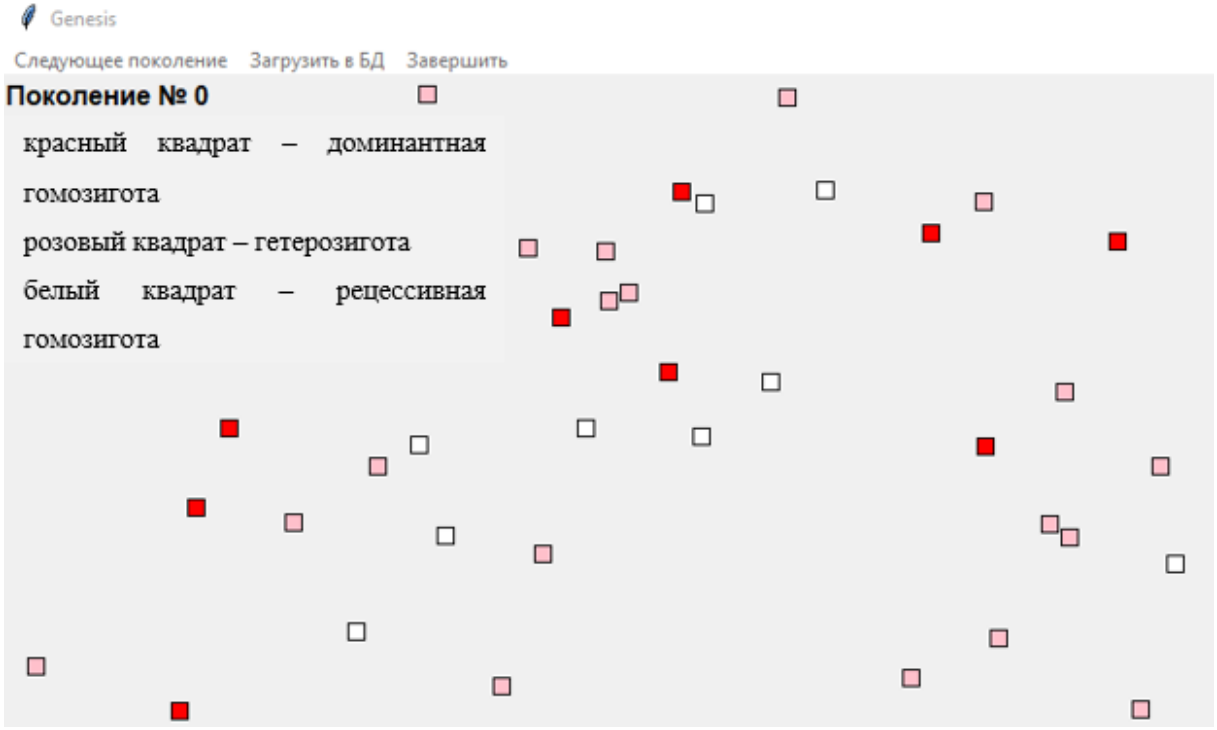


Рис. 3. Прототип симуляции

Данная информационная система обладает несколькими крупными перспективами разработки:

1. Разработка модуля «Образование». В связи с реализацией программы в настоящее время действует спрос на компетентные кадры, для обучения которых открываются новые учебные программы [3]. Реализовав данный модуль, данная система может стать не только научной, но и образовательной.

2. Карта генов требует нескольких улучшений, а именно возможность использовать индексы, которые используются при изучении полимерного взаимодействия генов, а также возможность указывать создания новых признаков из-за взаимодействия друг с другом аллелей, например, как это происходит при комплиментарном действии.

3. Модуль «Симуляция», в случае доработки, подходит для изучения генетических алгоритмов путем присвоения каждой букве генотипа его числовое значение и наблюдать за его изменением в процессе наследственности. Так это позволит изучать возможности генетических алгоритмов, например, в криптографии.

4. Если мы говорим о популяционной генетике и у нас есть модуль «Симуляция», то это открывает возможность для изучения способов автоматизации и других методов исследования генетики, такого как онтогенетического метода, в ходе которого анализируется проявление признаков во время развития организма.

5. Несомненно, гибкость программы, а именно отсутствие у нее привязки к признакам и количеству пар, выделяет данную информационную систему среди аналогов, однако возможность интеграции к уже существующим базам данных генов является важным шагом в дальнейшей разработке.

В ходе работы были разработаны два модуля и подсистема информационной системы автоматизации гибридологического анализа, которые снижают ошибки и время расчетов. Также были описаны результаты и перспективы данной информационной системы.

В дальнейшем планируется реализация описанных выше перспектив и долгосрочная поддержка проекта.

Список используемых источников

1. Указ Президента Российской Федерации от 28 ноября 2018 г. N 680 «О развитии генетических технологий в Российской Федерации».

2. Шингалов, В. А. Методы исследований в селекции и генетике сельскохозяйственных животных: краткий курс лекций для аспирантов направления подготовки 36.06.01 Ветеринария и зоотехния / В. А. Шингалов // ФГБОУ ВПО «Саратовский ГАУ». Саратов, 2015.

3. Инвестиции в будущее: как генетика стала одной из самых быстро развивающихся наук в России. URL: https://www.vedomosti.ru/esg/science_and_technology /articles/2023/04/27/972946-investitsii-v-buduschee-genetika (дата обращения 29.04.2025).

Статья представлена научным руководителем, доцентом кафедры СОД СПбГУТ, кандидатом педагогических наук Перевозником Ю. Я.

УДК 004.032.26

В. Д. Новожилова (студент группы ИКТК-12, СПбГУТ)
novozhilova.vd@sut.ru

РАЗРАБОТКА ПРИМЕРА НЕЙРОННОЙ СЕТИ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ДИАГНОСТИКИ И МОНИТОРИНГА СОСТОЯНИЯ БОЛЬНЫХ

В рамках растущей информатизации общества наблюдается все более широкое применение систем искусственного интеллекта. Одним из перспективных направлений является использование нейронных сетей для решения различных задач в области медицины. В докладе рассматривается пример нейронной сети, позволяющей осуществлять мониторинг состояния здоровья больных, в рамках развития телемедицины. Такой подход призван значительно повысить точность диагностики и позволяет врачам оперативно реагировать на изменения в состоянии пациентов.

телемедицина, нейронные сети, искусственный интеллект, архитектура нейронной сети

DEVELOPMENT OF AN EXAMPLE OF A NEURAL NETWORK FOR AUTOMATION OF DIAGNOSTIC PROCESSES AND PATIENT MONITORING

Novozhilova V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the growing informatization of society, artificial intelligence systems are increasingly being used. One promising area is the use of neural networks to solve various problems in medicine. This report examines an example of a neural network that allows for monitoring of patients' health, as part of the development of telemedicine. This approach is designed to significantly improve diagnostic accuracy and allows doctors to quickly respond to changes in patients' conditions.

telemedicine, neural networks, artificial intelligence, neural network architecture

В последние годы наблюдается внушительный рост популярности телемедицинских услуг. Одним из наиболее перспективных направлений поддержки телемедицины является использование искусственного интеллекта (ИИ) и нейронных сетей для автоматизации процессов диагностики и наблюдения за больными.

Телемедицина – это предоставление услуг здравоохранения в условиях, когда расстояние является критическим фактором, работниками здравоохранения, использующими информационно-коммуникационные технологии для обмена необходимой информацией в целях диагностики, лечения и профилактики заболеваний и травм, проведения исследований и оценок, а также для непрерывного образования медицинских работников в интересах улучшения здоровья населения и развития местных сообществ.

Нейронная сеть – это тип машинного обучения, при котором компьютерная программа имитирует работу человеческого мозга. Подобно тому, как нейроны в мозге передают сигналы друг другу, в нейросети информацией обмениваются вычислительные элементы.

В данной статье приводится пример нейронной сети для автоматизации процессов диагностики и мониторинга состояния больных сахарным диабетом 1-го типа. Для работы данной системы должно быть обеспечено наличие и взаимодействие определенных компонент:

1. Датчик измерения сахара. Датчик должен осуществлять непрерывный мониторинг (CGM), измерять уровень глюкозы в крови с заданной периодичностью и иметь модуль передачи данных (Bluetooth, Wi-Fi, GSM).

2. Клиентское устройство (промежуточное звено). В нашем случае клиентским устройством будет смартфон, собирающий данные с датчика и отправляющий данные на сервер через интернет.

3. Сервер в клинике. Принимает и хранит данные от датчиков (база данных) и обеспечивает безопасность (HTTPS, шифрование, аутентификация).

4. Нейронная сеть (аналитический модуль). На вход нейронная сеть будет получать данные об уровне сахара (временной ряд), а также дополнительные параметры (прием пищи, инсулин, физическая активность). В качестве архитектуры выбрана гибридная модель CNN + LSTM. CNN выявляет локальные паттерны (например, резкие скачки сахара после еды). LSTM обрабатывает долгосрочные зависимости (например, суточные колебания глюкозы) [1]. На выходе нейронная сеть будет выдавать прогноз возможности гипо-/гипергликемии, анализировать динамику хода заболевания и формировать рекомендации по лечению.

5. Врачебный интерфейс. Веб- или мобильное приложение для визуализации данных, а также оповещения о критических состояниях пациента.

Данная модель продемонстрирована на разработанной в рамках работы схеме (рисунок 1).

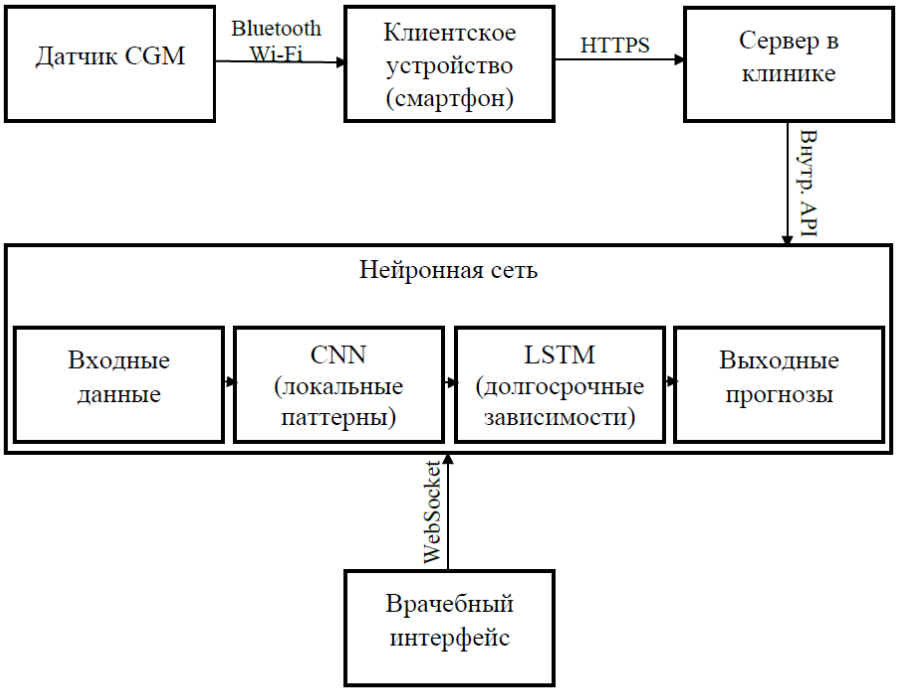


Рис. 1. Система мониторинга уровня сахара при помощи нейронной сети

Для работы данной системы была выбрана гибридная нейронная сеть CNN + LSTM. Обе архитектуры относятся к глубокому обучению и часто используются для обработки временных рядов, изображений и последовательностей. В гибридной модели CNN + LSTM они дополняют друг друга. CNN выявляет локальные паттерны (например, резкие скачки глюкозы). LSTM анализирует долгосрочные зависимости (например, суточные колебания сахара) [2].

Архитектура сверточной нейронной сети CNN содержит два основных слоя – свертка и пулинг (рисунок 2).

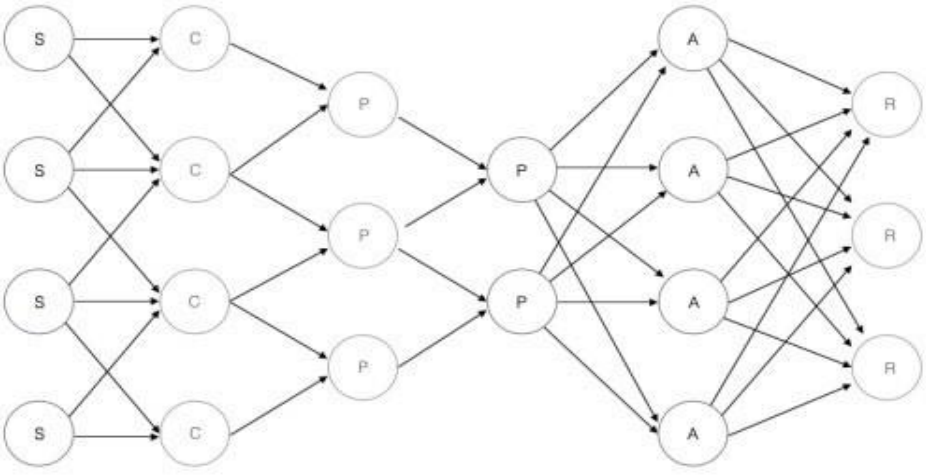


Рис. 2. Архитектура сверточной нейронной сети

Долгая краткосрочная память (Long short-term memory; LSTM) – особая разновидность архитектуры рекуррентных нейронных сетей, способная к обучению долговременным зависимостям. Рекуррентная нейронная сеть – это архитектура, похожая на сеть прямого распространения, но с возможностью учитывать последовательность данных во времени. Информация в такие сети поступает не только от предыдущих слоев, но и от себя же на предыдущей итерации (рисунок 3).

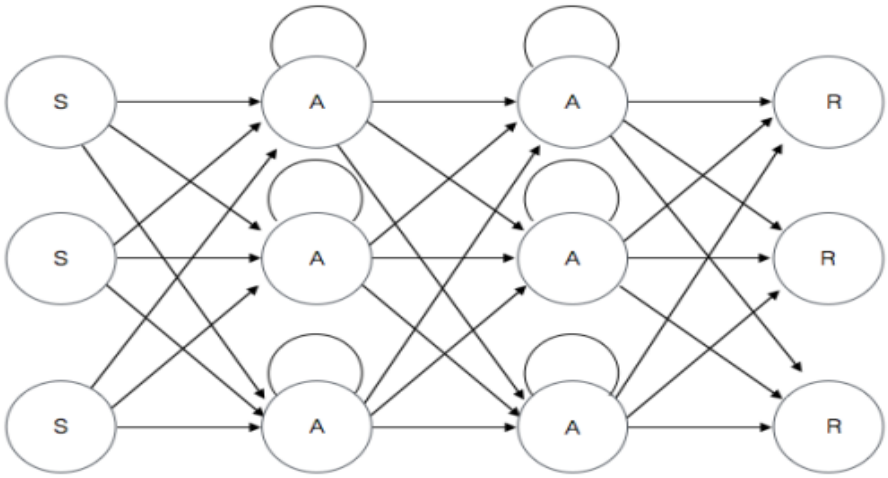


Рис. 3. Архитектура рекуррентной нейронной сети

Рассмотрим, как описанная система работает в реальном времени на примере пациента с диабетом 1 типа.

Первым этапом идет сбор данных с датчика (CGM). Датчик непрерывного мониторинга глюкозы (например, Dexcom G6 или FreeStyle Libre 3) измеряет уровень глюкозы в интерстициальной жидкости каждые 5 минут, после чего передает данные по Bluetooth на смартфон пациента (таблица 1) [3].

ТАБЛИЦА 1 – Входные данные

Время	Уровень глюкозы (ммоль/л)
08:00	5.2
08:05	5.4
08:10	6.1
…	…

Далее происходит передача данных на клиентское устройство. Приложение получает данные с датчика и добавляет контекстные данные, введенные пользователем:

08:00: Прием пищи – 40 г углеводов.

08:05: Инъекция инсулина – 5 ЕД (ультракороткий).

09:30: Физическая активность – 30 минут легкого бега.

Устройство отправляет все на сервер через HTTPS (зашифрованное соединение), после чего данные проходят обработку на сервере. Сервер в клинике принимает и хранит данные в базе (например, PostgreSQL с временными рядами), проверяет аутентификацию (только авторизованные устройства могут отправлять данные), подготавливает данные для нейронной сети.

Далее происходит анализ нейронной сетью (CNN + LSTM).

CNN (Сверточная часть):

Вход: последние 2 часа данных (24 значения по 5 минут).

Выявляет:

Резкий рост глюкозы с 5.2 до 6.1 ммоль/л после еды (фильтр CNN реагирует на производную).

Замедленный спад после инсулина (из-за физической активности).

LSTM (Долгосрочный анализ):

Вход: Данные за 24 часа + контекст (инсулин, еда, активность).

Выявляет:

Утренний феномен "рассвета" (пациент склонен к гипергликемии в 6–8 утра).

Эффект физической активности (обычно снижает сахар через 1–2 часа после нагрузки).

Кумулятивное действие инсулина (остаточный эффект прошлых инъекций).

Нейронной сетью выдает прогноз и рекомендации:

Прогноз через 1 час после пробежки (10:30):

Уровень глюкозы упадет до 3.8 ммоль/л (гипогликемия).

Рекомендации:

«Через 40 минут съесть 10 г медленных углеводов (яблоко или хлеб)».

«Следующую дозу инсулина уменьшить на 1 ЕД».

Далее данные попадают на врачебный интерфейс (рисунок 4). Веб-приложение для врача содержит дашборд с графиком глюкозы, прогнозами и событиями (еда, инсулин, активность).

При необходимости приходит оповещения:

Критическое состояние: «Пациент Иван П. – риск гипогликемии через 40 минут!» (SMS/Push-уведомление).

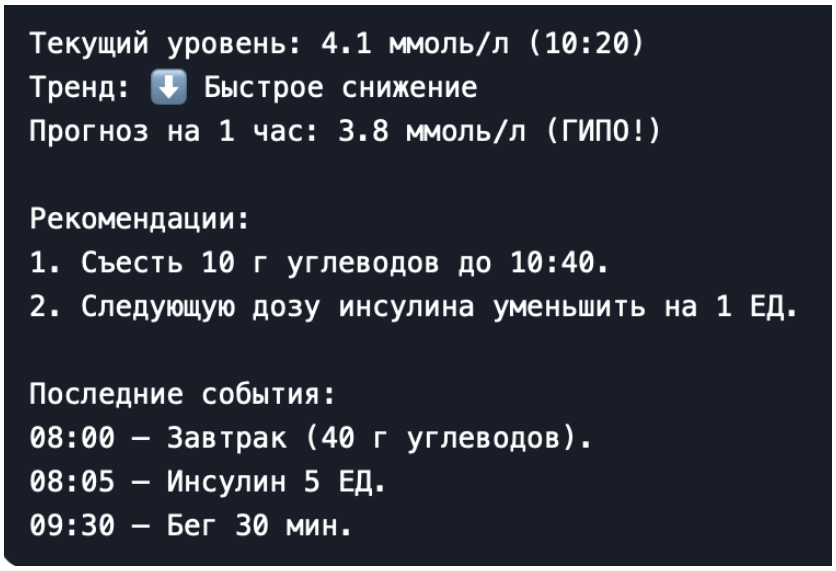


Рис. 4. Пример интерфейса

Таким образом предложенная модель нейронной сети позволяет решать задачу диагностики и мониторинга больных сахарным диабетом 1-го типа. В случае наличия инфраструктуры для сбора и анализа информации это может улучшить ситуацию по диагностированию и онлайн мониторингу здоровья в телемедицине. В дальнейшем на базе нейронных сетей можно развивать данную задачу или решать новые.

Список используемых источников

1. Горбунов А. А. Искусственный интеллект в диагностике заболеваний // Вестник новых медицинских технологий. 2019. №º3(45). URL: https://elibrary.ru/item.asp?id=36761703 (дата обращения 20.04.2025).

2. Морозова Н. П. Нейронные сети для прогнозирования динамики развития заболеваний // Онкологический журнал. 2019. №º5(15). URL: https://www.surgonco.ru/jour/article/view/505 (дата обращения 20.04.2025).

3. Мустафаев А. Г. Нейросетевая модель прогнозирования уровня глюкозы в крови у больных сахарным диабетом // Кибернетика и программирование. 2016. № 3. С. 1-5. URL: https://nbpublish.com/library_read_article.php?id=18010 (дата обращения 20.04.2025).

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

УДК 004.056.5

С. А. Рыжкова (студент группы ИСТ-212, СПбГУТ), ryzhkova.sa@sut.ru

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

В статье представлено проектирование информационной системы, предназначенной для организации и проведения анонимных электронных голосований с использованием технологии блокчейн. Обоснована необходимость применения технологии блокчейн для обеспечения неизменности, прозрачности и доверия к результатам голосования. Определены ключевые категории пользователей системы и сформулированы функциональные требования. Сформирована модульная структура системы, описаны функции основных модулей и установлены принципы их взаимодействия для обеспечения безопасности, анонимности и достоверности процесса голосования. Построены диаграммы прецедентов и классов, отражающие основные процессы и структуру системы. Предлагаемая система позволяет обеспечить защищенность данных и возможность верификации результатов каждым участником голосования.

информационная система, электронное голосование, блокчейн, анонимность, проектирование, UML

DESIGNING AN INFORMATION SYSTEM FOR ELECTRONIC VOTING BASED ON BLOCKCHAIN TECHNOLOGY

Ryzhkova S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the design of an information system for organizing and conducting anonymous electronic voting using blockchain technology. The necessity of blockchain technology application to ensure invariability, transparency and trust to the voting results is substantiated. The key categories of system users are defined and functional requirements are formulated. The modular structure of the system was formed, the functions of the main modules were described and the principles of their interaction were established to ensure security, anonymity and trustworthiness of the voting process. The diagrams of precedents and classes reflecting the main processes and structure of the system are constructed. The proposed system allows to provide data security and the possibility of verification of results by each participant of voting.

Key words: *information system, electronic voting, blockchain, anonymity, design, UML*

Современные системы электронного голосования сталкиваются с рядом ключевых проблем, которые ограничивают их применение, среди них:

недоверие со стороны общества, сложная и непонятная настройка голосований, избыточность существующих решений, сложность в обеспечении анонимности и безопасности.

Для решения указанных проблем в работе предлагается проект информационной системы VoteChain, которая основана на технологии блокчейн и позволяет обеспечить высокий уровень доверия, безопасности и прозрачности голосования. Основу архитектуры составляет децентрализованная модель хранения данных и применение криптографических алгоритмов, гарантирующих анонимность пользователей и неизменность результатов.

Технология блокчейн позволяет обеспечить неизменность и открытость результатов голосования без раскрытия данных об участниках. Все голоса записываются в распределенный реестр, защищенный от внешних и внутренних вмешательств. Использование блокчейна исключает возможность подделки или удаления уже зафиксированных голосов, что особенно важно при организации голосований. Таким образом, технология позволяет реализовать принципы доверенной среды без необходимости наличия центрального оператора [1].

В ходе анализа современных систем электронного голосования выявлены следующие общие недостатки:

- авторизация избирателя по e-mail, не обеспечивающая полной анонимности;
- ограниченные возможности гибкой настройки сценариев голосования;
- недостаточное количество тестирований систем в реальных условиях;
- слабая масштабируемость и неполное соблюдение требований безопасности.

Указанные ограничения свидетельствуют о необходимости создания более универсального и защищенного решения, способного устранить выявленные недостатки.

Основная цель разрабатываемой системы VoteChain – предоставить пользователям безопасную платформу для участия в электронных голосованиях с возможностью подтверждения достоверности результатов без раскрытия личности. Система ориентирована на использование в корпоративной и учебной среде, где важны точность, удобство и защищенность процедуры.

Ключевые пользователи системы:

- организаторы голосований, которым необходим инструмент для создания и анализа результатов опросов;
- участники голосования, желающие отправить голос и убедиться в его учете без риска деанонимизации.

Функциональные требования определяются задачами пользователей и структурированы в виде mind map (рис. 1).

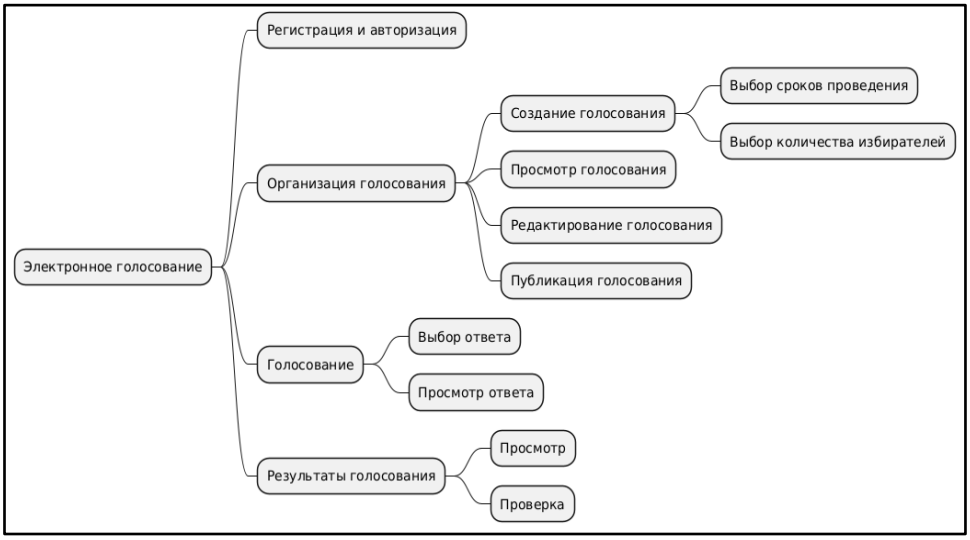


Рис. 1. Функциональные требования в виде mind map

В числе ключевых функциональных требований:

- анонимная авторизация;
- одноразовое голосование по уникальному идентификатору;
- создание, редактирование и публикация голосований;
- автоматическая и ручная остановка голосования;
- хранение и верификация голосов через блокчейн;
- визуализация результатов.

Для понимания структуры и логики работы системы составлена схема взаимодействия модулей (рис. 2).

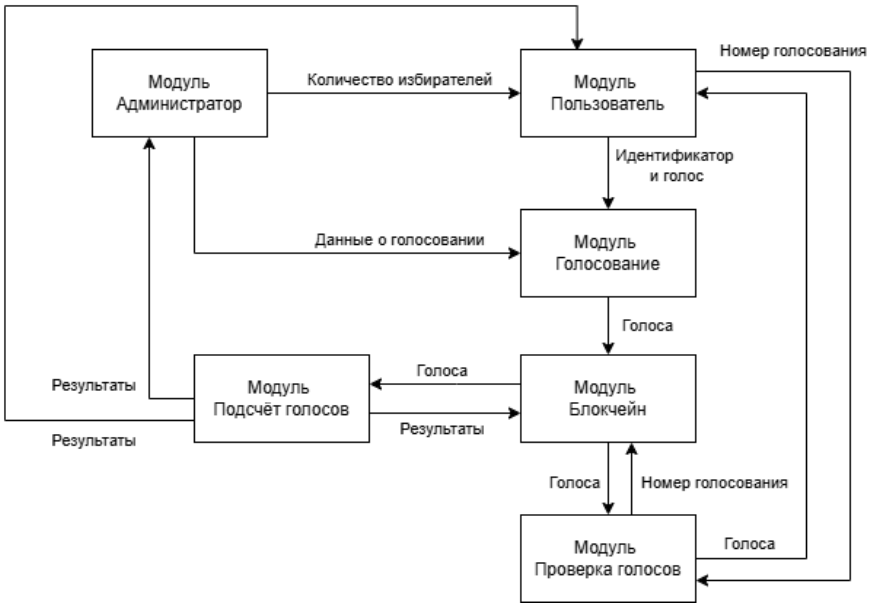


Рис. 2. Схема взаимодействия модулей системы

Ключевые модули:

- администратор – управление голосованиями и пользователями;
- пользователь – участие в голосовании, проверка голоса;
- голосование – хранение параметров и текущего состояния;
- блокчейн – фиксирование и хранение голосов;
- подсчет голосов – агрегация данных;
- проверка голосов – предоставление возможности верификации.

В рамках выбранной информационной системы выделены 3 типа акторов.

1. Гость. Права доступа: просмотр результатов голосования.

2. Участник голосования. Права доступа: просмотр результатов голосования; получение анонимного идентификатора; отправка голоса.

3. Организатор голосования. Права доступа: просмотр результатов голосования; создание, редактирование голосования; публикация и закрытие голосования.

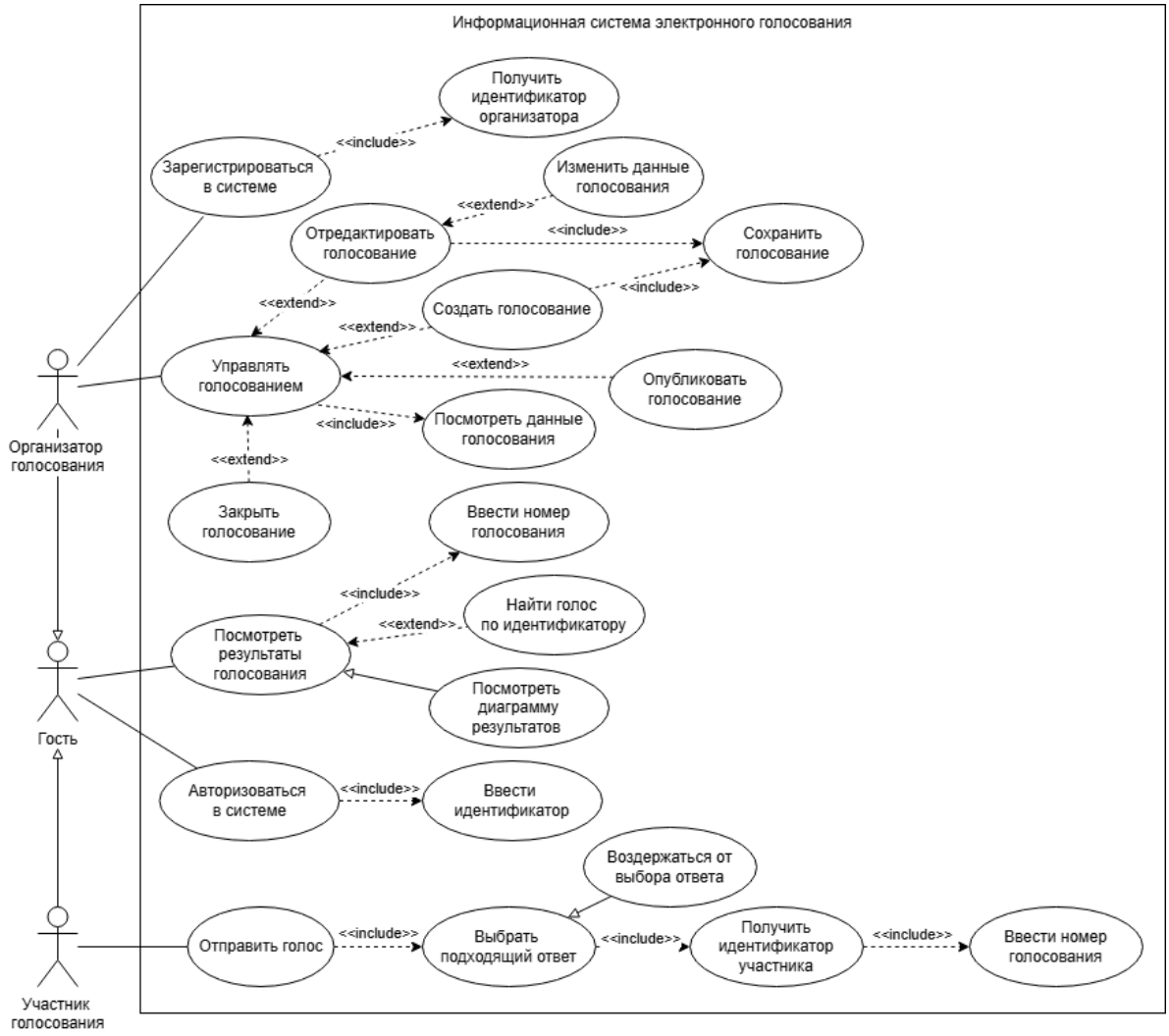


Рис. 3. Диаграмма вариантов использования системы VoteChain

Диаграммы вариантов использования и классов (рис. 3, 4) формализуют поведение акторов и внутреннюю структуру системы [2]. Они позволяют не только отразить роли пользователей и их взаимодействие с системой, но и уточнить состав и связи между основными сущностями, что упрощает реализацию и последующее масштабирование архитектуры.

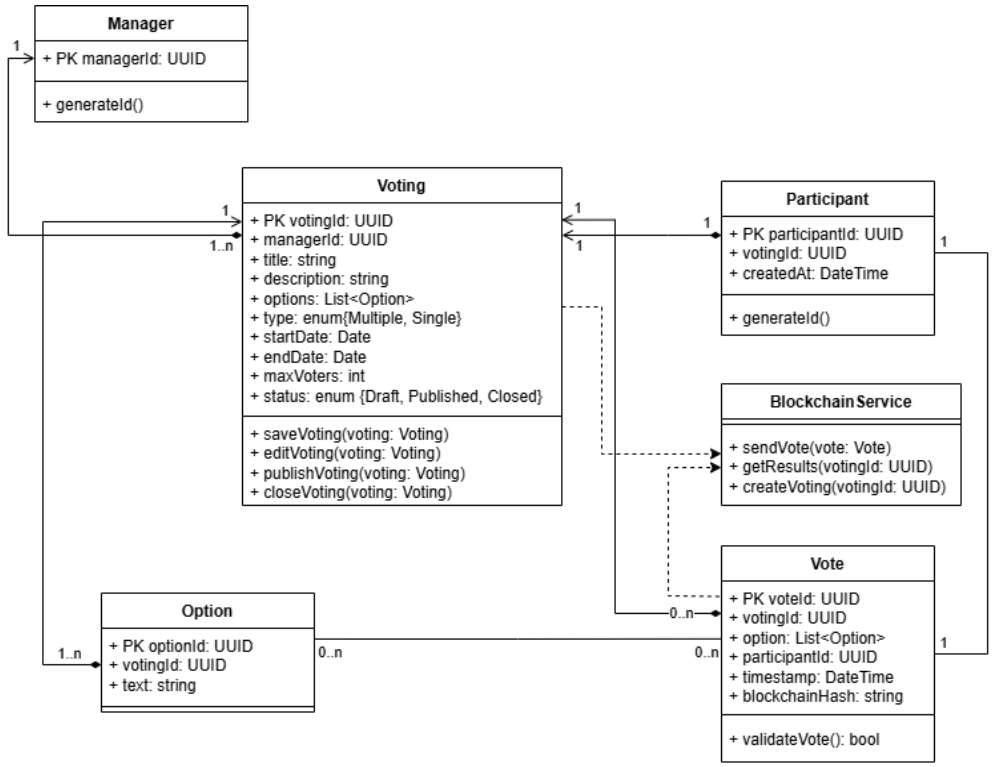


Рис. 4. Диаграмма классов системы VoteChain

Для повышения доверия к процессу голосования система VoteChain реализует возможность независимой проверки голосов каждым участником. После голосования пользователь может, используя свой анонимный идентификатор, убедиться, что его голос был корректно записан в блокчейн. Подобный механизм позволяет исключить возможность подмены или удаления голоса и делает весь процесс прозрачным без ущерба для анонимности. Такая реализация достигается за счет децентрализованного хранения данных и предоставления открытого доступа к проверке голосов без раскрытия личности избирателя.

Предложенная информационная система VoteChain предоставляет технологическую базу для проведения электронных голосований с учетом актуальных требований безопасности, анонимности и прозрачности. Использование блокчейна и модульной архитектуры позволяет обеспечить верификацию результатов, минимизировать угрозы манипуляций и повысить доверие участников.

Список используемых источников

1. Трубочкина Н. К., Поляков С. В. Система электронного голосования на основе технологии блокчейн с использованием смарт-контракта / Трубочкина Н. К., Поляков С. В. // Информационные технологии. 2019. № 2. С. 75.

2. Фаулер М. / UML. Основы, 3-е издание. Пер. с англ. СПб: СимволПлюс, 2004. 192 с., ил.

Статья представлена научным руководителем,
старшим преподавателем кафедры ИУС СПбГУТ Жарановой А. О.

УДК 004.8

Г. Д. Слезак (студент группы ИСТ-411м, СПбГУТ), slezak.gd@sut.ru

АРХИТЕКТУРА ДИНАМИЧЕСКОЙ ЭПИЗОДИЧЕСКОЙ ПАМЯТИ ДЛЯ ЯЗЫКОВЫХ МОДЕЛЕЙ НА ОСНОВЕ МУЛЬТИГРАФА СМЫСЛОВЫХ СВЯЗЕЙ

В статье представлена архитектура модуля динамической эпизодической памяти для языковых моделей, ориентированная на хранение и анализ текстовой информации. Память организована в виде мультиграфа, где узлы представляют собой эпизоды (фрагменты текста с метаданными), а ребра отражают три типа смысловых связей: семантические (эмбеддинги), ассоциативные (контекстуальные и тематические связи) и временные (последовательность появления информации). Модуль осуществляет извлечение релевантных эпизодов и выявление конфликтов между ними с помощью логического анализа на основе локальной языковой модели. Также рассматриваются способы представления эпизодов, структура графа и механизм разрешения противоречий. Предложенный подход может служить основой для разработки более гибких и интерпретируемых систем искусственного интеллекта, способных к формированию внутренней модели памяти.

динамическая память, искусственный интеллект, языковые модели, эпизодическая память, мультиграф, семантические связи, ассоциативные связи, временные связи, логический инференс, архитектура памяти, обработка текстовой информации

ARCHITECTURE OF DYNAMIC EPISODIC MEMORY FOR LANGUAGE MODELS BASED ON A MULTIGRAPH OF SEMANTIC RELATIONS

Slezak G.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the architecture of a dynamic episodic memory module for language models, focused on storing and analysing textual information. The memory is organised as a multigraph, where nodes represent episodes (text fragments with metadata), and edges reflect three types of semantic relationships: semantic (embeddings), associative (contextual and thematic relationships), and temporal (sequence of information appearance). The module extracts relevant episodes and identifies conflicts between them using logical analysis based on a local language model. Methods of representing episodes, graph structure, and conflict resolution mechanisms are also considered. The proposed approach can serve as a basis for the development of more flexible and interpretable artificial intelligence systems capable of forming an internal memory model.

Key words: *dynamic memory, artificial intelligence, language models, episodic memory, multigraph, semantic connections, associative connections, temporal connections, logical inference, memory architecture, text information processing*

Современные большие языковые модели демонстрируют впечатляющие результаты в генерации и интерпретации текста, однако ограничены фиксированной длиной контекста и неспособностью удерживать устойчивое знание о предыдущих взаимодействиях. Это приводит к противоречивости ответов при обсуждении пересекающихся или конфликтующих тем, затрудняя построение последовательного диалога и сложных рассуждений.

Современные модели частично снижают эти проблемы за счет количественного расширения (увеличения параметров, обучающих данных), но редко – за счет качественных решений, например, интеллектуального управления памятью.

Если рассматривать задачу реализации последовательного диалога с точки зрения наибольшей приближенности к диалогу с человеком, что отчасти является одной из задач, рассматриваемой науками о когнитивном искусственном интеллекте, то архитектуры, используемые в больших языковых моделях, сами по себе лишь косвенно преследуют цели приближения к человеческому интеллекту (фокусируясь на эффективности выводов ответов), и в данном вопросе обсуждения уступают другим архитектурам когнитивного ИИ, создаваемых прежде всего в соответствии с существующими теориями интеллекта.

Таким образом, имеет смысл разработка модулей памяти, которые будут динамически управлять используемым контекстом с соответствии с текущей темой диалога и обстоятельствами, что позволит, во-первых, сократить размер используемого контекста, улучшая точность ответов; во-вторых, увеличит интерпретируемость ответов благодаря ограничению области контекста, с использованием которой модель обрабатывает запрос в соответствующий момент времени; в-третьих, позволит более точно приблизиться к человеческому способу мышления в качественном смысле, что является задачей наук о когнитивном искусственном интеллекте.

Целью настоящей работы является проектирование и разработка архитектуры модуля динамической памяти для больших языковых моделей.

Объектом исследования является память в качестве компонента систем искусственного интеллекта. Предметом исследования являются архитектура и принципы организации эпизодической динамической памяти.

Существуют различные виды организации памяти в интеллектуальных системах:

1. Базы данных и знаний;
2. Латентная память в весах нейросетей;
3. Внешняя дифференцируемая память;
4. Векторная память и RAG;

5. Графовая память (knowledge graphs);

6. Гибридные подходы.

Исследования когнитивных архитектур [1, 2] указывают на ключевую роль эпизодической памяти – хранения событий, их контекста и последовательности – в формировании опыта. Большие языковые модели также нуждаются в сохранении эпизодов взаимодействий, включая их смысл, временной порядок и причинно-следственные связи.

В предлагаемой архитектуре эпизоды становятся основной единицей памяти, сохраняющей текст и метаданные (временные метки, источник и т.д.) в формате JSON. Эпизоды могут анализироваться, модифицироваться и объединяться, обеспечивая гибкое представление знаний и логико-семантическую обработку.

Архитектура реализована как мультиграф: узлы – эпизоды памяти, ребра – семантические, ассоциативные и временные связи с весами. Новые данные преобразуются в эпизоды и интегрируются в граф, что позволяет хранить информацию, анализировать ее, обнаруживать противоречия и уточнять знания.

Семантические связи определяются косинусным расстоянием между эмбеддингами, ассоциативные – по ключевым словам, временные – по порядку поступления. Такой граф облегчает поиск кластеров знаний, построение контекста и навигацию по смыслу.

Концептуальная схема структуры мультиграфа представлена на рисунке 1.

Рис. 1. Концептуальная схема структуры мультиграфа
(где x – количество совпавших ключевых слов)

Отличительной особенностью предлагаемой системы является регулярный анализ связей между эпизодами для выявления противоречий. Процесс включает:

1. Выделение локальных кластеров эпизодов, связанных ребрами с наибольшим весом (что позволяет анализировать не весь граф, а только релевантные области);

2. Семантический и логический анализ содержимого эпизодов с использованием локально запущенной LLM (Large Language Model) (например, через llama.cpp).

К основным типам выявляемых конфликтов относятся: противоречия в утверждениях, несоответствия временных и причинно-следственных связей, конфликты источников информации или уровня доверия.

При обнаружении конфликта система может выбрать один из следующих путей разрешения:

1. Автоматическое уточнение – языковая модель определяет наименее вероятный эпизод; его вес снижается или узел удаляется. При необходимости утверждения внутри эпизодов переформулируются для устранения неоднозначности.

2. Интерактивное уточнение – пользователю предлагается выбор между конфликтующими эпизодами или оценка достоверности.

3. Сохранение множественности – конфликтующие эпизоды остаются в памяти с пометкой о противоречии, что учитывается при дальнейшем обращении к данным.

Пример интерактивной работы с эпизодами представлен на рисунке 2. Визуализация графов, а также программные функции выполнены при помощи средств языка Python.

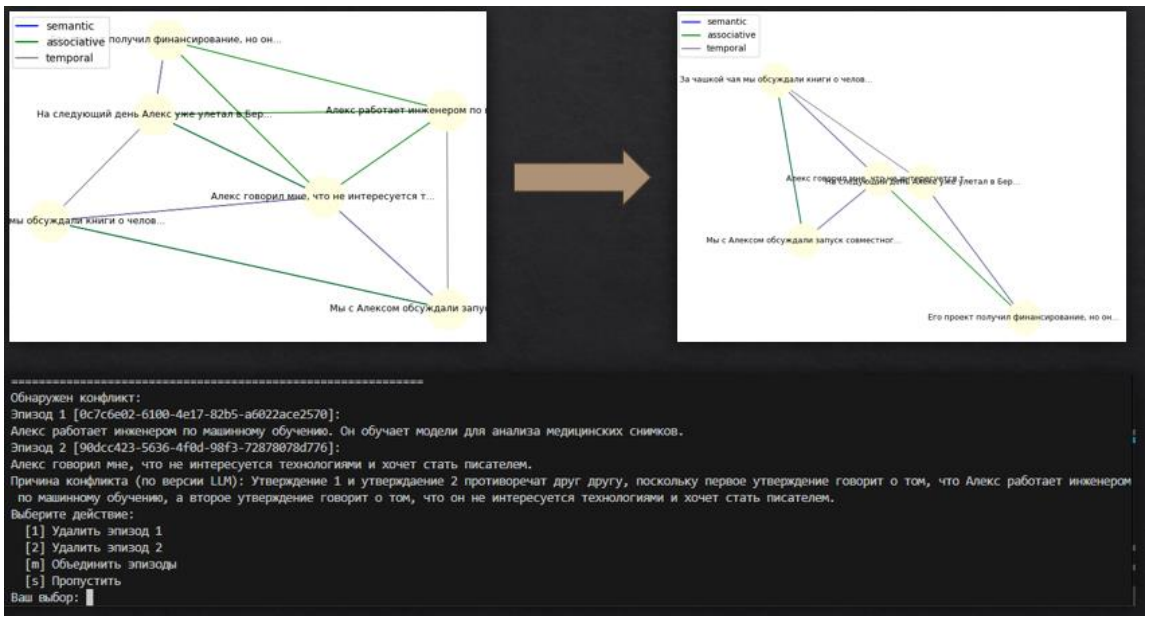


Рис. 2. Пример удаления эпизодов из памяти с визуализацией в виде графа

Предлагаемая архитектура модуля может применяться в системах поддержки принятия решений, где важно учитывать противоречивые данные и динамический контекст; в образовательных ИИ, запоминающих диалоги и отслеживающих прогресс пользователя; в когнитивных интеллектуальных

агентах и исследовательских ИИ, моделирующих поведение, близкое к человеческому; в робототехнике и автономных системах, нуждающихся в долговременной памяти; а также в диалоговых интерфейсах, где требуется поддерживать непротиворечивость утверждений.

В текущей реализации не рассмотрены способы непосредственной интеграции системы с большими языковыми моделями. Возможные подходы включают использование скрытых параметров в запросах, дообучение с LoRA (Low-Rank Adaptation), внешних контроллеров поверх LLM, обучения с подкреплением и других методов. Конкретная реализация зависит от требований системы, в которой выполняется интеграция, поэтому этот вопрос выходит за рамки данной работы, хотя его проработка планируется.

Планы дальнейшего развития системы включают:

1. Автоматизацию механизма разрешения конфликтов;
2. Интеграцию механизма «забывания», что позволит учитывать ограниченные ресурсы и моделировать динамику человеческой памяти;
3. Реализацию временной динамики (работу в реальном времени) и актуализацию эпизодов по частоте обращения;
4. Углубление логического анализа эпизодов;
5. Оптимизацию быстродействия.

Разработанная архитектура динамической эпизодической памяти позволяет моделям эффективнее управлять контекстом, обнаруживать и разрешать противоречия, а также формировать устойчивое когнитивное представление накопленных взаимодействий. Это создает основу для построения более последовательных диалогов, повышает интерпретируемость решений и приближает работу моделей к человеческому способу обработки знаний. Дальнейшее развитие системы направлено на интеграцию с LLM, улучшение логического анализа и моделирование временной динамики памяти.

Список используемых источников

1. Nuxoll A. M., Laird J. E. Extending Cognitive Architecture with Episodic Memory // Proceedings of the Twenty-Second AAAI Conference on Artificial Intelligence, July 22-26, 2007, Vancouver, British Columbia, Canada. PP. 1560-1564. URL: https://web.eecs.umich.edu/~soar/sitemaker/docs/pubs/AAAI2007_NuxollLaird_ver14%28final%29.pdf (дата обращения 03.05.2025);

2. Ménager D. Episodic Memory in a Cognitive Model // ICCBR Workshops. 2016. PP. 267-271. URL: https://ceur-ws.org/Vol-1815/paper28.pdf (дата обращения 03.05.2025).

Статья представлена научным руководителем, заведующим кафедрой ИУС, и.о. декана факультета ИТПИ СПбГУТ, кандидатом технических наук, доцентом Литвиновым В. Л.

УДК 004.032.26

И. Д. Слободчиков (студент группы ИКПИ-24, СПбГУТ),
slobodchikov.id@sut.ru

МОДИФИКАЦИЯ ТОКЕНИЗАТОРА LLM НА ПРИМЕРЕ LLAMA 3.1

В работе представлен подход к модификации токенизатора крупных языковых моделей на примере LLaMA 3.1 (8B и 70B параметров), значительно улучшающий сходимость и стабильность генерации. Специализированный токенизатор, разработанный для обработки высокоструктурированных медицинских данных, реализует декомпозицию табличной информации на категориальные компоненты с использованием особой системы специальных токенов-разделителей. Данная модификация позволяет эффективно преобразовывать высокоразмерные входные данные (более 46 тысяч признаков) в оптимальный для обработки языковыми моделями формат, снижая количество необходимых итераций обучения и повышение качества итоговых предсказаний по сравнению с базовым токенизатором. Повышение скорости сходимости достигается за счет структурирования контекстных взаимосвязей между столбцами таблицы в едином семантическом пространстве, что снижает энтропию входных данных. Для оптимизации вычислительных ресурсов применена техника Rank-Stabilized Low-Rank Adaptation (LoRA), сохраняющая преимущества улучшенной токенизации при минимальных затратах на обучение. Экспериментальные результаты показывают, что модель с 70 миллиардами параметров и модифицированным токенизатором достигает показателей BLEU 0,8405 и ROUGE-1 0,8695, что подтверждает эффективность предложенного метода токенизации для задач генерации структурированных медицинских текстов.

большие языковые модели, LLaMA 3.1, токенизация, промпт-инжиниринг, LoRA, сходимость моделей, генерация текста, нейронные сети

MODIFICATION OF THE LLM TOKENIZER: A CASE STUDY ON LLAMA 3.1

Slobodchikov I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This work presents an approach to modifying the tokenizer of large language models (LLMs), demonstrated on LLaMA 3.1 (8B and 70B parameters), which significantly improves convergence and generation stability. The specialized tokenizer, designed for processing highly structured medical data, implements the decomposition of tabular information into categorical components using a unique system of special separator tokens. This modification efficiently transforms high-dimensional input data (over 46,000 features) into an optimal format for language model processing, reducing the number of required training iterations and improving the quality of final predictions compared to the baseline tokenizer.

The accelerated convergence is achieved by structuring contextual relationships between table columns within a unified semantic space, thereby reducing input data entropy. To optimize computational resources, the Rank-Stabilized Low-Rank Adaptation (LoRA) technique was applied, preserving the benefits of enhanced tokenization with minimal training overhead.

Experimental results show that the 70-billion-parameter model with the modified tokenizer achieves BLEU-4 scores of 0.8405 and ROUGE-1 scores of 0.8695, confirming the effectiveness of the proposed tokenization method for generating structured medical texts.

Key words: *large language models, LLaMA 3.1, tokenization, prompt engineering, LoRA, model convergence, text generation, neural networks*

Развитие больших языковых моделей (LLM) в последние годы открыло новые возможности для обработки сложных данных в различных предметных областях [1]. Особое внимание исследователей привлекает применение этих технологий в медицине, где традиционные подходы часто оказываются недостаточными для работы с высокоразмерными структурированными данными [2]. В данной работе представлен альтернативный подход к модификации токенизатора крупных языковых моделей на примере LLaMA 3.1, направленный на значительное улучшение обработки медицинских данных с более чем 46 тысячами признаков [3].

1. Актуальность

Современные большие языковые модели, такие как LLaMA 3.1, демонстрируют выдающиеся результаты в обработке естественного языка, но их применение в медицинской сфере сталкивается с существенными ограничениями [1]. Основная проблема заключается в том, что стандартные токенизаторы, основанные на алгоритме Byte Pair Encoding (BPE), не приспособлены для эффективной обработки высокоструктурированных табличных данных [5]. При использовании традиционных методов токенизации происходит потеря важных структурных взаимосвязей между столбцами данных, что приводит к увеличению энтропии входных данных и снижению эффективности обучения модели [6].

2. Постановка задачи

Основная цель исследования заключается в разработке специализированного токенизатора для больших языковых моделей, способного эффективно обрабатывать высокоразмерные медицинские данные при сохранении их структурных особенностей [3]. Конкретные задачи включают:

Создание системы специальных токенов-разделителей для декомпозиции табличной информации на категориальные компоненты [4].

Валидация эффективности предложенного подхода через экспериментальную оценку качества генерации текста с использованием стандартных метрик BLEU и ROUGE [3].

3. Методы и оборудование

Экспериментальные исследования проводились на моделях LLaMA 3.1 размером 8B и 70B параметров [1]. LLaMA 3.1 представляет собой семей-

ство авторегрессивных языковых моделей с оптимизированной архитектурой трансформаторов и расширенным словарем токенизатора до 128 тысяч токенов [1]. Модели обучались с использованием высокоразмерных медицинских данных, содержащих более 46 тысяч признаков различных типов [3]. Специализированный токенизатор реализует декомпозицию табличной информации через систему специальных токенов-разделителей, аналогичных [SEP] токенам в архитектуре BERT [6].

4. Экспериментальные результаты

Экспериментальные исследования продемонстрировали значительные улучшения по всем ключевым метрикам оценки качества генерации текста и эффективности обучения [3]. Модель с 70 миллиардами параметров и модифицированным токенизатором достигла показателей BLEU 0,8405 и ROUGE-1 0,8695, что представляет существенное улучшение по сравнению с базовой версией (рис. 1) [3].

Рис. 1. Сравнение показателей качества генерации текста для модифицированного токенизатора

Для модели 8B наблюдается улучшение BLEU на 6,0 % (с 0,7936 до 0,8405) и ROUGE-1 на 5,0 % (с 0,8281 до 0,8695) [3]. В случае модели 70B улучшения составляют 4,9 % для BLEU (с 0,8014 до 0,8405) и 4,7 % для ROUGE-1 (с 0,8309 до 0,8695) [3]. Одновременно время обучения сократилось на 38,8 % и 33,9 % соответственно, что демонстрирует высокую вычислительную эффективность предложенного подхода [3]. Комплексный анализ показывает, что модифицированный токенизатор обеспечивает стабильные улучшения по всем ключевым метрикам при одновременном повышении эффективности процесса обучения [3].

5. Теоретические основы улучшений

Эффективность предложенного подхода объясняется несколькими фундаментальными теоретическими принципами [5]. Снижение энтропии входных данных через структурированную токенизацию улучшает способность модели к извлечению семантической информации из токенов [5]. Энтропия может рассматриваться как мера неопределенности в данных, и ее снижение способствует более эффективному обучению модели [6]. Специальные токены-разделители создают явные границы между различными типами медицинских данных, что позволяет модели лучше понимать контекстуальные взаимосвязи [6]. Исследования показывают, что градиент матрицы внимания кодирует взаимную информацию между токенами, и наибольшие значения этого градиента соответствуют ребрам в латентном причинном графе [6].

6. Выводы

Представленный подход к модификации токенизатора LLaMA 3.1 демонстрирует значительный потенциал для обработки высокоструктурированных медицинских данных [1]. Достигнутые улучшения в метриках качества генерации (BLEU 0,8405, ROUGE-1 0,8695) и эффективности обучения (сокращение времени на 33,9-38,8 %) открывают новые возможности для применения больших языковых моделей в медицинской практике [3]. Практическая значимость работы заключается в возможности применения разработанного подхода для улучшения качества анализа медицинских данных с использованием современных языковых моделей [1]. Сокращение времени обучения и повышение точности генерации делают предложенный метод привлекательным для практического внедрения в медицинских информационных системах [3].

Список используемых источников

1. Me-LLaMA: Foundation Large Language Models for Medical Applications. Research Square, 2024.

2. How Important Is Tokenization in French Medical Masked Language Models? arXiv, 2024.

3. Large Language Model (LLM) Evaluation Metrics – BLEU and ROUGE. ML Explained, 2023.

4. A Rank Stabilization Scaling Factor for Fine-Tuning with LoRA. arXiv, 2023.

5. Implementing A Byte Pair Encoding (BPE) Tokenizer from Scratch. Sebastian Raschka, 2025.

6. An Autonomous Framework for Layer-Wise Entropy Reduction in Neural Learning. arXiv, 2025.

Статья представлена научным руководителем, заведующим кафедрой ВМ СПбГУТ, кандидатом физико-математических наук, доцентом Плотниковым П. В.

УДК 004.021:796.015.44

В. С. Яковлева (магистрант группы ИСТ-411м, СПбГУТ),
jakovleva.vs@sut.ru

ИНТЕГРАЦИЯ IoT-УСТРОЙСТВ В ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ПОДБОРА ИНДИВИДУАЛЬНЫХ ТРЕНИРОВОК

В статье рассматривается архитектура интеллектуальной информационной системы, интегрированной с технологиями Интернета вещей (IoT), для персонализированного подбора тренировок. Подчеркивается значимость использования в реальном времени данных о физическом состоянии пользователя для динамической адаптации тренировочного процесса. Рассматриваются принципы сбора, обработки и анализа данных с фитнес-устройств, а также представлена концептуальная модель адаптивной системы, повышающей эффективность и безопасность тренировок. Приводится краткий анализ преимуществ и недостатков различных типов носимых устройств, а также обсуждаются вызовы и перспективы внедрения таких систем.

IoT, индивидуальный подход, информационные системы, фитнес, персонализация, интеллектуальные системы

INTEGRATION OF IoT DEVICES INTO INTELLIGENT SYSTEMS FOR CUSTOMIZED TRAINING

Yakovleva V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines the architecture of an intelligent information system integrated with Internet of Things (IoT) technologies for personalized workout selection. It highlights the importance of using real-time data on a user's physical condition to dynamically adapt the training process. The principles of data collection, processing, and analysis from fitness devices are discussed, and a conceptual model of an adaptive system is presented, aimed at improving the effectiveness and safety of workouts. A brief analysis of the advantages and disadvantages of various types of wearable devices is provided, along with a discussion of the challenges and prospects of implementing such systems.

***Key words**: IoT, personalized approach, information systems, fitness, personalization, intelligent systems*

Современный рынок фитнес-технологий стремительно развивается. Повсеместное использование смарт-часов, фитнес-браслетов и других носимых устройств открыло новые горизонты в сборе биометрических данных пользователей. Эти устройства, являясь частью экосистемы Интернета вещей, позволяют формировать непрерывный поток информации, описываю-

щий текущее физиологическое состояние человека. Однако, несмотря на доступность таких данных, большинство существующих информационных систем подбора тренировок либо не используют эти данные вовсе, либо обрабатывают их поверхностно, не учитывая изменения состояния пользователя в реальном времени [1-6]. Целью данной статьи является формирование архитектурного подхода к разработке интеллектуальной системы, способной анализировать данные с IoT-устройств в режиме реального времени и адаптировать тренировочный процесс с учетом полученной информации.

Обзор носимых устройств показывает, что существует значительное разнообразие как по функциональности, так и по качеству передаваемых данных. Смарт-часы и фитнес-браслеты обладают встроенными пульсометрами, акселерометрами, гироскопами и GPS-модулями. Эти устройства обеспечивают хорошую точность мониторинга сердечного ритма и двигательной активности, сохраняя при этом высокий уровень удобства в повседневном использовании. Устройства вроде умных весов дополняют картину, позволяя учитывать дополнительные параметры здоровья. Сравнительный анализ IoT-устройств приведен в таблице 1.

ТАБЛИЦА 1. Характеристики и особенности IoT-устройств для фитнеса и мониторинга состояния

Тип устройства	Точность данных	Время автономной работы	Типы собираемых данных	Функциональность	Возможность интеграции
Смарт-часы	Средняя	Среднее (1-2 дня)	Пульс, движение, сон, GPS, уведомления	Высокая	Средняя
Фитнес-браслеты	Средняя	Высокое (до 7 дней)	Пульс, движение, сон, GPS	Высокая	Высокая
Умные весы	Высокая	Высокая (питание от батареек)	Масса тела, ИМТ, состав тела	Средняя	Высокая

Архитектура системы построена на последовательной интеграции модулей сбора данных, облачного хранилища, аналитического ядра и пользовательского интерфейса. В момент сбора данных устройства синхронизируются с системой через Bluetooth, Wi-Fi или API. Сформированные потоки информации передаются на сервер, где происходит их предварительная

фильтрация и хранение. Затем данные поступают в аналитический модуль, где с помощью алгоритмов машинного обучения происходит распознавание трендов, оценка текущего состояния пользователя и прогнозирование реакций организма на различные виды нагрузки. На основании этих прогнозов система автоматически изменяет тренировочную программу, предлагая пользователю подходящий уровень интенсивности и упражнения, соответствующие его физическому состоянию. Архитектура интеллектуальной фитнес-системы с IoT-интеграцией представлена на рисунке 1.

Рис. 1. Архитектура интеллектуальной фитнес-системы с интеграцией IoT-устройств

Одним из ключевых преимуществ предложенной системы является ее способность к динамической адаптации тренировочного процесса в режиме реального времени. При поступлении данных о физиологических изменениях, например, учащенном сердечном ритме, падении вариабельности

пульса или других признаках нарастающего утомления, система оперативно анализирует текущую нагрузку и предлагает корректировки: переход в фазу восстановления, снижение интенсивности либо отмену текущей сессии для предотвращения перенапряжения. В противоположной ситуации – когда показатели организма стабильны, а уровень физической нагрузки недостаточен – система способна автоматически увеличить интенсивность тренировки, сделать упражнения более сложными или предложить дополнительный цикл. Такой адаптивный подход позволяет значительно снизить риск травмирования, повысить вовлеченность пользователя в процесс и обеспечить устойчивое, безопасное развитие физической формы.

Однако внедрение подобного рода интеллектуальных решений сопровождается рядом технологических и методологических вызовов. В первую очередь, необходимо учитывать возможные ограничения точности данных, получаемых с носимых IoT-устройств. Достоверность показаний может варьироваться в зависимости от конструктивных особенностей сенсоров, условий эксплуатации (например, плотность прилегания к телу, уровень влажности, наличие помех) и модели устройства. Во-вторых, особую значимость приобретает задача обеспечения защиты персональных данных, поскольку в процессе эксплуатации системы осуществляется сбор, хранение и передача чувствительной информации. Это требует реализации надежных механизмов шифрования, а также соответствия нормативным требованиям в области информационной безопасности. Кроме того, важным аспектом при построении такой системы является обеспечение совместимости с широким спектром устройств и программных платформ, что особенно актуально в условиях высокой фрагментированности рынка IoT-решений.

Интеграция технологий Интернета вещей в интеллектуальные системы подбора индивидуальных тренировок представляет собой перспективное направление, способное обеспечить высокий уровень персонализации тренировочного процесса. В отличие от традиционных решений, основанных на универсальных протоколах, данная система адаптируется к текущему состоянию пользователя в режиме реального времени, что значительно повышает ее эффективность. Разработанная архитектура подтверждает актуальность такого подхода и демонстрирует его потенциал для дальнейшего масштабирования и внедрения. В то же время данное направление требует проведения дополнительных исследований, направленных на повышение точности биометрических измерений, улучшение алгоритмов адаптации и развитие механизмов кроссплатформенного взаимодействия.

Список используемых источников

1. Белентьев С. А. Использование технологий и гаджетов для мониторинга физической активности и их влияние на результаты тренировок. URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologiy-i-gadzhetov-dlya-monitoringa-fizicheskoy-aktivnosti-i-ih-vliyanie-na-rezultaty-trenirovok (дата обращения 17.04.2025).

2. Wallace S. P. Аналитика данных как инструмент повышения качества тренировок с использованием умных часов и фитнес-браслетов // Sports Science Review, 2020. 198-210 p.

3. Самигуллина Е. В. Носимые устройства и технологии интернета вещей в физической культуре и спорте. URL: https://elibrary.ru/item.asp?id=43165161(дата обращения 19.04.2025).

4. Свищев А. В., Журавлев А. В. Использование IoT технологий в спорте и фитнесе. URL: https://elibrary.ru/item.asp?id=46112294 (дата обращения 19.04.2025).

5. Kostyuchenko V.F. Implementation of an individual approach in sport. URL: https://cyberleninka.ru/article/n/implementation-of-an-individual-approach-in-sport (дата обращения 22.04.2025).

6. Сидоров И. М. Проектирование информационных систем / И. М. Сидоров. М.: Издательство «Дашков и К», 2017. 240 с.

Статья представлена научным руководителем, доцентом кафедры ИУС СПбГУТ, кандидатом технических наук Раковским О. В.

КИБЕРБЕЗОПАСНОСТЬ

УДК 004.056

А. Р. Габдулина (студент группы ИБС-22, СПбГУТ), gabdulina.ar@sut.ru

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ КВАЗИБИОЛОГИЧЕСКОЙ ПАРАДИГМЫ: КОНЦЕПЦИИ, АРХИТЕКТУРА И ПОДХОДЫ К ЗАЩИТЕ

В работе представлена интеллектуальная система обнаружения вторжений, основанная на квазибиологической парадигме, имитирующей механизмы адаптации и иммунитета живых систем. Ключевым элементом архитектуры является ассимиляционная память, обеспечивающая накопление и обработку данных об угрозах с возможностью самообучения.

квазибиологическая парадигма, ассимиляционная память, ИИ, адаптивная кибербезопасность, биологически вдохновленные алгоритмы

DEVELOPMENT OF AN INTELLIGENT INTRUSION DETECTION SYSTEM BASED ON A QUASI-BIOLOGICAL PARADIGM: CONCEPTS, ARCHITECTURE, AND APPROACHES TO PROTECTION

Gabdulina A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper presents an intelligent intrusion detection system based on a quasi-biological paradigm that mimics the adaptation and immunity mechanisms of living systems. A key element of the architecture is assimilative memory, which enables the accumulation and processing of threat data with self-learning capabilities.

Key words: *quasi-biological paradigm, assimilative memory, AI, adaptive cybersecurity, biologically inspired algorithms*

В данной работе предлагается новый подход к созданию интеллектуальной системы обнаружения вторжений (СОВ), основанный на квазибиологической парадигме, вдохновленной принципами самоорганизации, адаптации и иммунитета живых систем.

Центральным компонентом архитектуры становится биологически вдохновленная система памяти, обеспечивающая накопление и структурирование знаний об угрозах. В отличие от традиционных решений, предлагаемый подход делает акцент на специализированных алгоритмах обработки информации и прозрачности принимаемых решений.

Рассмотрим мультидисциплинарный подход, объединяющий информатику, биологию, математику и кибернетику. Такой синтез позволяет создать принципиально новую модель системы безопасности, отличающуюся повышенной устойчивостью к современным киберугрозам.

I. Основы и концепции

Квазибиологическая парадигма предполагает заимствование механизмов поведения живых организмов для применения в кибербезопасности. Основные ее принципы включают саморегуляцию, способность к самоисцелению и автономное принятие решений без необходимости постоянного внешнего контроля. Среди преимуществ можно выделить устойчивость к изменениям среды и снижение влияния человеческого фактора.

Адаптивная память в данной концепции представляет собой механизм накопления, агрегации и нормализации информации. Она воспроизводит функции биологической памяти: накопление опыта, фильтрацию лишней информации, выявление закономерностей. Связь с биологией выражается в имитации процессов долговременной и кратковременной памяти и ее интеграции в когнитивные модели поведения.

Вызовы для построения интеллектуальной СОВ заключаются в необходимости обеспечения защиты от атак на ИИ, достижения высокой киберустойчивости, преодоления проблемы «черного ящика». Система должна не только выявлять аномалии, но и уметь их интерпретировать, прогнозировать и устранять без привлечения человека.

II. Архитектура и компоненты

ARMA модели в интеллектуальных системах безопасности могут анализировать сетевой трафик, выявляя подозрительные активности и предсказывая будущие атаки, основываясь на прошлых событиях.

Подобно живым организмам, они адаптируются к новым угрозам и условиям, постоянно обучаясь и повышая эффективность обнаружения. Применение моделей ARIMA в безопасности позволяет реализовать следующие ключевые функции:

1. Анализ временных рядов. Модели ARIMA анализируют временные ряды данных, что идеально подходит для анализа сетевого трафика, где данные собираются поминутно. Это позволяет выявлять аномалии и подозрительные активности, сравнивая текущее состояние системы с ожидаемым поведением.

2. Обработка больших данных. Благодаря своей архитектуре, модели ARIMA демонстрируют эффективность при представлена следующим образом. Соответственно для компонентов интеллектуальной СОВ обработка нестационарного ряда будет иметь следующий вид:

$$X_t \overset{\Delta}{\rightarrow} a_i \ + \sum_{i=1}^{p} b_i \varepsilon_{t-j} \ + \ \varepsilon_t; \qquad (1)$$

где ε_t – условно стационарный временной ряд.

Для функции времени выполнения каждого распределения параметров f(t), учитывается ее четность и выполняется ее преобразование в автокорреляционную функцию.

Если $X_t = a_i + X_{t-1} + \varepsilon_t$ допускает случайные ошибки, то во временном ряду возникает «дрейф» (см. рис. 1). Колебания отражают общее состояние обработки данных, особенно после воздействия атак, связанных с несанкционированной обработкой [1].

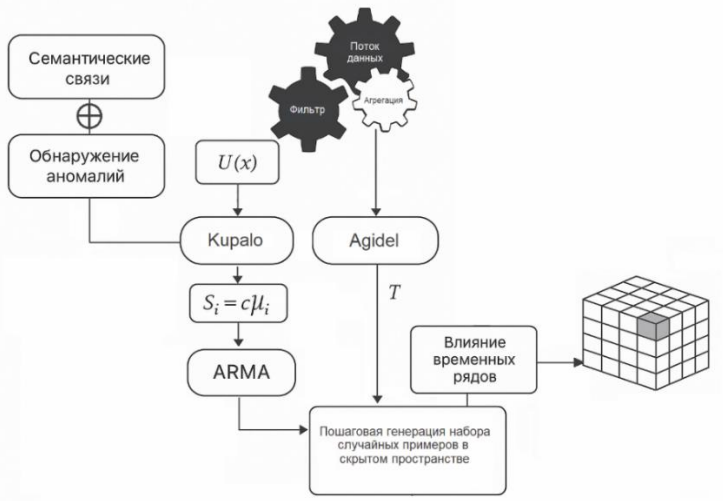


Рис. 1. Схема обработки Больших данных модулей по типу ARMA и ARIMA по отдельности с учетом накопления оценок полученных значений временных рядов

Ассимиляционная память строится на принципах репликации и кластеризации, что обеспечивает отказоустойчивость и целостность данных. Структура ассимиляционной памяти и характер наполнения ее кластеров наглядно представлены на рисунке 2.

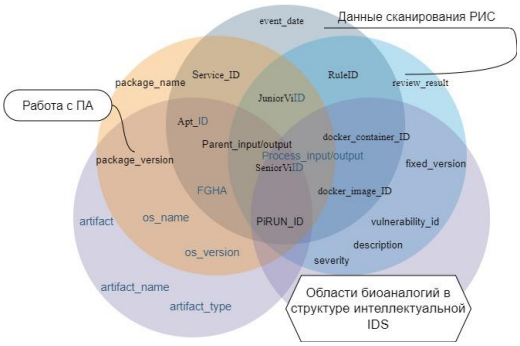


Рис. 2. Поля взаимодействия элементов и структур в системе обработки информации интеллектуальной IDS

Анализ и принятие решений осуществляется посредством нейронных сетей, машинного обучения и самоорганизующихся карт (СМК) [2]. Программные агенты (ПА) выполняют задачи распределенной обработки данных, обеспечивая взаимодействие с ассимиляционной памятью и между собой. Они способны к репликации и самостоятельному восстановлению после атак.

Для визуализации архитектуры предлагаемой системы используется рисунок 3: Влияние блоков коррекции ошибок, который демонстрирует влияние различных механизмов защиты данных на эффективность обнаружения вторжений.

Рис. 3. Влияние блоков коррекция ошибок в интеллектуальных СОВ

III. Реализация и оценка

Разработка интеллектуальной СОВ основана на масштабируемых решениях и открытых платформах, использующих библиотеки машинного обучения и анализа временных рядов. Система интегрируется со средами мониторинга через стандартизированные API [3].

Эффективность оценивается по ключевым метрикам: точность детектирования, устойчивость к угрозам, производительность и ресурсоемкость.

Особое внимание уделяется надежности восстановления после атак и стабильности под нагрузкой.

Валидация проводится путем моделирования атак в тестовой среде с последующим сравнением показателей с традиционными СОВ. Это позволяет количественно оценить преимущества квазибиологического подхода.

IV. Перспективы дальнейшего развития исследования

Перспективы развития интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы связаны с совершенствованием ее адаптивных возможностей и интеграцией с передовыми технологиями искусственного интеллекта. В современном мире, одним из приоритетов является создание систем, способных самостоятельно обучаться и адаптироваться.

Особое внимание уделяется разработке алгоритмов, позволяющих системам анализировать угрозы и корректировать свои параметры, при этом, не требуя постоянного контроля со стороны человека (AutoML) [4]. Это позволяет создать более гибкую и эффективную защиту, способную оперативно реагировать на возникающие вызовы.

V. Пример практической реализации опытного образца системы

Для проверки эффективности предложенной архитектуры разрабатывается опытный образец интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы. Опытный образец реализуется в тестовой среде, имитирующей реальные условия. Основу составляет распределенная сеть сенсоров, интегрированная с ассимиляционной памятью на базе защищенной БД с шифрованием и резервным копированием.

Нейросетевые модули обучаются на реальных и синтетических данных с применением активного обучения для повышения точности. Интеллектуальное ядро YaVi [5] управляет компонентами и адаптирует параметры в реальном времени.

Заключение

По результатам тестирования осуществляется калибровка параметров моделей и архитектуры, что позволяет уточнить подходы к балансировке нагрузки, оптимизации потребления ресурсов и повышению качества обнаружения угроз.

Таким образом, разработка опытного образца и его валидация служат основой для дальнейшей оптимизации и масштабирования интеллектуальной системы обнаружения вторжений на базе квазибиологической парадигмы, подтверждая ее перспективность и практическую применимость в условиях реальных угроз кибербезопасности. Квазибиологическая парадигма открывает новые возможности для создания гибких и самообучающихся систем кибербезопасности, способных противостоять быстро эволюционирующим угрозам.

Список используемых источников:

1. Проничев В. Д., Ушаков И. А. Автоматизированный анализ изменений в сетевых конфигурациях устройств на основе нейронных сетей // 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, 2025. С. 443-448. URL: https://www.elibrary.ru/item.asp?id = 80543725 (дата обращения 28.04.2025).

2. Штеренберг С. И. Программа автоматического машинного обучения оценки уровня безопасности моделей IDS для классификации данных // Информационная группа «elibrary.ru». URL: https://www.elibrary.ru/item.asp?id = 67983101 (дата обращения 28.04.2025).

3. Штеренберг С. И., Поляничева А. В., Алехин Р. В., Шелкоплясова П. Е. Программа мониторинга загруженности процессора и оперативной памяти вычислительного узла облачной платформы Openstack // Информационная группа «elibrary.ru». URL: https://www.elibrary.ru/item.asp?id = 80655846 (дата обращения 28.04.2025).

4. Штеренберг С. И. Программа взаимодействия с библиотекой AUTOML для тестирования нейронных сетей на уязвимости // Информационная группа «elibrary.ru». URL: http://elibrary.ru/item.asp?id = 80653530 (дата обращения 28.04.2025).

Статья представлена научным руководителем, доцентом кафедры ЗСС, заместителем декана факультета КБ по научной работе СПбГУТ, кандидатом технических наук, доцентом Штеренбергом С. И.

УДК 004.056

КВАЗИБИОЛОГИЧЕСКАЯ ПАРАДИГМА В ОРГАНИЗАЦИИ ЗАЩИЩЕННОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

П. Ю. Егорова (студент группы ИКБ-22, СПбГУТ), egorova.pu@sut.ru
Ю. В. Охлопкова (студент группы ИКБ-22, СПбГУТ), ohlopkova.uv@sut.ru

Интеллектуальная система обнаружения вторжений на основе квазибиологической парадигмы представляет собой новый подход к адаптивной киберзащите. В условиях усложняющихся атак система, сформированная из автономных компонентов, действует по принципу живого организма – каждая часть выполняет свои функции и реагирует на угрозы. За счет нейросетей и моделей, проводящих аналогию с биологическими процессами, система адаптируется к новым условиям, обучается на поступающих данных и эффективно отражает сложные киберугрозы без внешнего вмешательства

интеллектуальная система обнаружения вторжений, машинное обучение, глубокое обучение, пакетно-нейросетевые программы, защита искусственного интеллекта

QUASI-BIOLOGICAL PARADIGM IN THE ORGANIZATION OF A SECURE INTELLIGENT INTRUSION DETECTION SYSTEM

Egorova P., Ohlopkova Yu.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

An intelligent intrusion detection system based on a quasi-biological paradigm represents a new approach to adaptive cyber defense. In conditions of increasingly complex attacks, a system formed from autonomous components operates on the principle of a living organism – each part performs its own functions and reacts to threats. Due to neural networks and models that draw an analogy with biological processes, the system adapts to new conditions, learns from incoming data and effectively reflects complex cyber threats without external interference.

Key words: *intelligent intrusion detection system, machine learning, deep learning, package neural network programs, artificial intelligence protection*

Современные киберугрозы требуют от систем защиты умения быстро адаптироваться и обучаться. В условиях ускоренной цифровизации возникают принципиально новые вызовы и угрозы информационной безопасности. Прежде всего, это возрастание частоты и сложности кибератак. Традиционные методы защиты не справляются с динамически изменяющимися атаками, поскольку базируются на известных шаблонах и статичных правилах. Кроме того, стремительное развитие искусственного интеллекта (ИИ)

и технологий обработки больших данных открывает новые возможности как для атакующих, так и для защитников [1].

Сегодня злоумышленники активно используют технологии машинного обучения для автоматизации атак, поиска уязвимостей, генерации новых эксплойтов и создания убедительных сценариев социальной инженерии. В то же время защитникам информации приходится иметь дело с растущими объемами сетевого трафика и логов, которые требуют автоматизированной обработки и анализа. Именно здесь проявляется ключевое ограничение традиционных подходов – неспособность оперативно адаптироваться и самостоятельно учиться на изменяющихся условиях среды.

Эффективное решение этих проблем возможно только через синергию между научными исследованиями и практическими потребностями, что подчеркивает необходимость интеграции научных подходов в область защиты искусственного интеллекта [2].

Именно поэтому в качестве перспективного направления развития выступают интеллектуальные системы обнаружения вторжений (СОВ), построенные на принципах квазибиологической парадигмы. Подобно клеткам организма, которые выполняют свои функции, не нуждаясь в внешнем вмешательстве, компоненты интеллектуальной СОВ могут работать независимо, принимая решения на основе анализа поступающих данных. Самоорганизация и способность к адаптации этих компонентов обеспечивают эволюцию системы, где каждый элемент может обучаться на данных о предыдущих инцидентах. Это способствует устойчивому росту эффективности системы и обеспечивает ее способность своевременно адаптироваться к возникающим угрозам. Такой подход предполагает использование микросервисов, пакетно-нейросетевых программ и программных агентов как самостоятельных единиц, которые по аналогии с биологическими клетками способны самостоятельно выявлять и нейтрализовать угрозы информационной безопасности.

Этот подход основывается на нескольких ключевых принципах:

- автономность модулей: каждый модуль системы работает независимо, осуществляя обработку данных, обнаружение отклонений и принятие решений без внешнего управления;
- обучаемость: используются нейронные сети и алгоритмы глубокого обучения, позволяющие выявлять ранее неизвестные аномалии;
- распределенность: структура системы исключает наличие единой точки отказа;

● исключение человеческого фактора: минимизация роли оператора снижает вероятность человеческих ошибок и повышает надежность системы.

Применение микросервисной архитектуры и контейнеризации в сочетании с методами машинного и глубокого обучения придает системе необходимую гибкость и позволяет оперативно реагировать на изменения в характере угроз. Каждый программный компонент, реализованный в виде агента, функционирует независимо и анализирует поступающие данные с использованием нейросетевых алгоритмов. Такая организация дает возможность выявлять аномалии и потенциальные атаки в режиме реального времени. По мере накопления опыта система способна адаптироваться к ранее неизвестным сценариям и постепенно улучшать свои механизмы реагирования, что способствует ее устойчивому развитию и повышению эффективности в долгосрочной перспективе. Эти системы способны выполнять свои функции автономно, что значительно повышает скорость реакции и точность обнаружения угроз в условиях постоянно меняющихся киберугроз [3].

Центральными компонентами предлагаемой интеллектуальной СОВ являются ассимиляционная модель памяти и самоорганизующиеся карты (СОК) нейронных сетей.

Ассимиляционная память играет важную роль в интеллектуальных системах обнаружения вторжений, позволяя системе продолжать накапливать необходимые сведения о кибератаках и обеспечивать стабильную работу когнитивной сетки ИИ на протяжении длительного времени. Использование распределенной структурированной реплицируемой модели защиты ассимиляционной памяти помогает значительно снизить когнитивную нагрузку на систему и повысить точность работы.

Модели, использующие ассимиляционную память, обеспечивают надежность и устойчивость работы системы, продолжая обучаться на новых данных о кибератаках. Процесс защиты ассимиляционной памяти включает применение реплицируемых структур, что повышает устойчивость к сбоям и минимизирует потерю данных. Это позволяет интеллектуальной СОВ сохранять свою эффективность, даже при изменяющихся условиях внешней среды.

В свою очередь, добавление функций самоорганизующихся карт в интеллектуальные системы обнаружения вторжений позволяет вырабатывать квазибиологические свойства, которые способствуют повышению эффективности защиты. СОК интегрируют данные о событиях, обработанных и

структурированных для защиты ассимиляционной памяти. Эти модели способствуют выявлению аномалий, распознаванию новых типов атак и постепенному обучению системы на реальных данных [4].

Самоорганизующиеся карты оказываются особенно полезными при формировании моделей поведения систем искусственного интеллекта. Благодаря способности обобщать данные о прошлых инцидентах и оперативно вносить коррективы в текущие алгоритмы работы, СОК способствуют более точному и своевременному реагированию на потенциальные угрозы. Их интеграция в распределенные системы безопасности обеспечивает гибкость при распространении информации между компонентами и повышает устойчивость всей архитектуры к внешним воздействиям. Кроме того, они оказываются эффективным инструментом для настройки и адаптации нейросетевых структур, что позволяет минимизировать потери данных и наращивать функциональные возможности системы.

Чтобы глубже понимать, как сетевые службы реагируют на изменчивую нагрузку, исследователи применяют анализ временных рядов – в частности, модификации ARMA/ARIMA. Эти методики не просто фиксируют колебания параметров, а последовательно отслеживают их эволюцию, позволяя заранее подстроить конфигурацию под намечающиеся тенденции. Такая стратегия переводит защиту из режима «реакция после факта» в плоскость превентивного прогнозирования, а инструменты обнаружения вторжений, реализующие квазибиологический принцип, дополняют статистику механизмом непрерывного самообучения.

Работа с большими массивами данных, поступающими от сенсоров и инструментов мониторинга, требует эффективных алгоритмов анализа. Модели типа ARIMA в данном случае помогают выявлять скрытые зависимости и тренды, на основании которых система может заранее оценивать вероятность угроз. Это дает ощутимые преимущества при построении гибкой, обучающейся в реальном времени архитектуры защиты, способной адаптироваться к постоянно изменяющемуся характеру киберугроз.

Краткое описание этапов работы интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы показано на рисунке 1.

Рис. 1. Этапы работы интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы

Автономные системы, основанные на квазибиологической парадигме, обладают возможностью работать независимо, как отдельные клетки в организме. В таких системах каждый компонент, будь то микросервис или нейросетевая программа, действует как самостоятельная единица, обеспечивая гибкость и устойчивость в изменяющихся условиях, а также в отличие от традиционных систем обладает рядом важных преимуществ:

- повышенная точность обнаружения угроз: использование адаптивных нейросетевых моделей и алгоритмов глубокого обучения позволяет системе выявлять не только известные типы атак, но и ранее не встречавшиеся аномалии в поведении;
- сопротивляемость внутренним атакам: за счет децентрализованной структуры и автономной работы модулей затрудняется воздействие на всю систему при компрометации отдельных ее элементов;
- снижение влияния человеческого фактора: автоматизация рутинных процессов минимизирует риск ошибок, связанных с вмешательством оператора, и повышает оперативность реагирования на инциденты;
- гибкость и адаптивность: защитный контур быстро пересматривает рабочие алгоритмы и правила, как только меняется профиль рисков или параметры внешней среды.

Таким образом, включение квазибиологической парадигмы в архитектуру киберзащиты приводит к заметному повышению стойкости к нетипичным и комплексным инцидентам. Кроме того, подобные системы способны к постоянному самообучению и адаптации в реальном времени, что открывает новые возможности для построения гибких, автономных и самоуправляемых средств, ориентированных на долгосрочную эффективную работу в условиях динамично меняющейся информационной среды.

Список используемых источников

1. Штеренберг С. И. Методика применения в адаптивной системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода / С. И. Штеренберг // Системы управления и информационные технологии. 2016. № 1(63). С. 51-54.

2. Штеренберг С. И. Обнаружение вторжений в распределенных информационных системах на основе методов скрытого мониторинга и анализа больших данных: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени кандидата технических наук / Штеренберг Станислав Игоревич, 2018. 182 с.

3. Сахаров Д. В. Инфраструктура связи на Крайнем Севере как база для формирования единой инфосреды / Д. В. Сахаров, С. Е. Мельников, С. И. Штеренберг // Электросвязь. 2016. № 5. С. 18-20.

4. Штеренберг С. И. Установление вектора развития интеллектуальной системы обнаружения вторжений для задач защиты искусственного интеллекта / С. И. Штеренберг // Технологии информационного общества: Сборник трудов XVII Международной отраслевой научно-технической конференции, Москва, 02–03 марта 2023 года. Москва: ООО «Издательский дом Медиа паблишер», 2023. С. 113-115.

5. Методика реализации компонентов ассимиляционной памяти в среде обработки больших данных / С. И. Штеренберг, А. В. Поляничева, Д. П. Зуев, Р. Г. Шарифов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 3. С. 52-60.

Статья представлена научным руководителем, доцентом кафедры ЗСС, заместителем декана факультета КБ по научной работе СПбГУТ, кандидатом технических наук, доцентом Штеренбергом С. И.

УДК 004.725.4

Д. П. Зуев (студент группы ИКТЗ-15, СПбГУТ), zuev.dp@sut.ru

АНАЛИЗ СВОЙСТВ РАЗВЕРТЫВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ VIPNET В ОРГАНИЗАЦИИ ДЛЯ ВВЕДЕНИЯ В ЛАБОРАТОРНЫЙ КОМПЛЕКС

Статья посвящена анализу развертывания системы защиты информации ViPNet в рамках учебного лабораторного комплекса. ViPNet – отечественное сертифицированное решение для построения защищенных сетей, соответствующее требованиям законодательства в области информационной безопасности. Описаны архитектурные особенности платформы и ее компоненты, а также структура курса, охватывающего все уровни модели Open Systems Interconnection. Лабораторные работы направлены на формирование практических навыков по проектированию, установке и настройке защищенной инфраструктуры. Комплекс обеспечивает подготовку специалистов, способных внедрять системы защиты в корпоративную среду.

ViPNet, КСЗИ, безопасность, шлюз безопасности, VPN, шифрование

ANALYZING THE PROPERTIES OF DEPLOYING VIPNET SECURITY TOOLS IN AN ORGANIZATION FOR THE INTRODUCTION OF TO THE LABORATORY COMPLEX

Zuev D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the analysis of the deployment of the ViPNet information security system within the educational laboratory complex. ViPNet is a domestic certified solution for building secure networks that meets the requirements of legislation in the field of information security. The architectural features of the platform and its components are described, as well as the structure of the course covering all levels of the Open Systems Interconnection model. Laboratory work is aimed at developing practical skills in designing, installing, and configuring secure infrastructure. The complex provides training for specialists capable of implementing security systems in the corporate environment.

Key words: *ViPNet, TCB, security, network firewall, VPN, encryption*

В условиях роста кибератак защита корпоративных и критически важных систем становится приоритетом. ViPNet – комплексное отечественное решение от АО «ИнфоТеКС» для защищенных VPN-сетей поверх IP [1]. Платформа сертифицирована ФСТЭК и ФСБ, поддерживает симметричные (ГОСТ 28147-89, AES), асимметричные (ГОСТ Р 34.10-2001/2012) и хэш-

алгоритмы (ГОСТ Р 34.11-94/2012), межсетевое и персональное экранирование, туннелирование IP-пакетов и централизованное управление через ViPNet Prime.

Нормативно-правовую основу применения ViPNet составляют Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры», Приказ ФСТЭК РФ № 235 (требования к комплексным средствам защиты информации) и № 250 (сертификация межсетевых экранов) [2, 3, 4]. Согласно этим документам, применение отечественных сертифицированных КСЗИ позволяет не только обеспечить требуемый уровень защиты, но и снизить зависимость от зарубежных поставщиков в условиях санкций.

Главное архитектурное преимущество ViPNet – модульность и изоляция компонентов. Coordinator (в аппаратной и виртуальной версиях) совмещает адресацию, туннелирование, межсетевое экранирование, а также включается в себя модули IDS и DPI [5]. Client перехватывает и защищает трафик на конечных узлах. ViPNet Prime управляет построением VPN, политиками безопасности и контролем доступности.

Для формирования практических навыков по проектированию и эксплуатации комплексных систем защиты на базе ViPNet в рамках учебного процесса разработан лабораторный комплекс, привязанный к семи уровням модели OSI. Каждая лабораторная работа фокусируется на конкретном уровне и технологиях ViPNet Prime, Coordinator, Client и вспомогательных модулях. Методология обучения охватывает весь цикл проектирования защищенной сетевой инфраструктуры.

Первая работа посвящена проектированию физической инфраструктуры корпоративной ИС. Цель – сформировать понимание физического уровня модели OSI с учетом требований безопасности, отказоустойчивости и масштабируемости.

Студенты выступают в роли проектировщиков IT-инфраструктуры и на основе расшифровки встречи с заказчиком разрабатывают схему информационной системы предприятия. Необходимо учитывать потребности организации: безопасность, отказоустойчивость, масштабируемость, интеграцию ViPNet и балансировку нагрузки между сегментами сети.

Ключевыми задачами лабораторной работы являются: анализ проектных требований, составление схемы физического подключения оборудования, выбор и обоснование применения коммутаторов, источников питания,

каналов связи и модулей защиты. При проектировании необходимо обеспечить соблюдение принципов надежности (включая резервирование каналов и компонентов), масштабируемости (с поддержкой подключения новых офисов, расширения серверных мощностей и виртуализации), и безопасности (физическая защита оборудования, разделение зон доступа, межсетевые экраны, контроль трафика и идентификация).

Результатом работы должна стать оформленная схема физической структуры корпоративной сети с пояснительными подписями и возможностью ее масштабирования, как представлено на рис. 1. Дополнительно требуется подготовить обоснование проектных решений, включая ссылки на примененные стандарты, спецификации оборудования и средства защиты, в том числе интеграцию с компонентами ViPNet (Coordinator, Client, Prime). Защита работы предполагает аргументированное изложение проектных решений, их соответствие техническому заданию и нормативным требованиям в области ИБ.

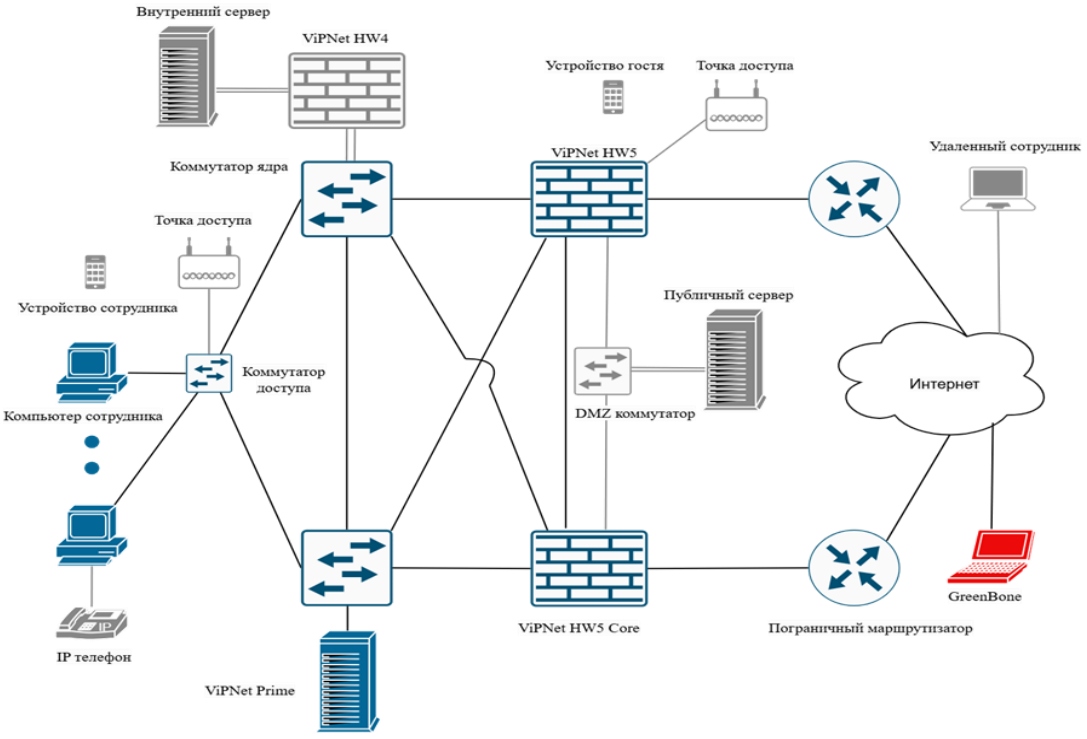


Рис. 1. Пример проекта архитектуры заказчика

Вторая лабораторная работа сосредоточена на первичном развертывании защищенной сетевой инфраструктуры с использованием операционной системы Astra Linux и базовых компонентов ViPNet. Основной целью работы является получение обучающимися практического опыта установки специализированной операционной системы и подготовки среды для последующей интеграции ViPNet в корпоративную инфраструктуру.

На начальном этапе студенты знакомятся с теоретическими аспектами установки Astra Linux и архитектурой ViPNet Prime, изучают документацию. Затем выполняется развертывание рабочих станций в виртуальной среде. Особое внимание уделяется правильной настройке сетевых адаптеров, маршрутизации и IP-адресации, что необходимо для последующего формирования единой защищенной сети.

Следующим шагом является установка программного обеспечения ViPNet Prime на подготовленную станцию, где студенты производят первичную настройку управляющего модуля.

Таким образом, данная лабораторная работа формирует у обучающихся понимание фундаментальных принципов подготовки инфраструктуры к внедрению системы защиты информации. Результатом выполнения задания является развернутая виртуальная лабораторная среда, включающая соединенные рабочие станции под управлением Astra Linux с установленным программным обеспечением ViPNet Prime, готовая к дальнейшему этапу настройки защищенных каналов и политик безопасности.

Третья лабораторная работа направлена на построение защищенной корпоративной сети на основе программно-аппаратного комплекса ViPNet. На данном этапе обучающиеся формируют системное представление о сетевом уровне модели OSI в контексте архитектуры ViPNet, изучают принципы адресации, организации взаимодействия между узлами и механизмы разграничения доступа в защищенной среде.

Основная задача лабораторной работы заключается в реализации защищенной логической структуры сети ViPNet. В процессе выполнения задания студенты создают пользователей системы, закрепляют за ними рабочие станции (хосты), назначают привязку к координатору, формируют межузловые связи. Все действия выполняются с применением интерфейса ViPNet Prime и сопровождаются генерацией справочно-ключевой информации для каждого узла. Особое внимание уделяется проверке корректности настроек разграничения прав доступа между клиентскими узлами.

Четвертая лабораторная работа посвящена исследованию программно-аппаратного комплекса ViPNet Coordinator HW 5 в аппаратном и виртуализированном исполнении. Ключевой задачей является конфигурирование межсетевого экранирования, студенты создают локальные (local), транзитные (forward), VPN-фильтры (vpn) и фильтры туннелей (tunnel), реализуя блокирующие и разрешающие правила для TCP/UDP трафика на заданных портах и диапазонах, включая стандартные порты HTTP, HTTPS,

DNS, SSH и нестандартные сервисы. Студенты исследуют журнал регистрации IP-пакетов, генерируемый службой iplircfg, анализируют логи прохождения и блокировки трафика.

Пятая лабораторная работа затрагивает три верхних уровня модели OSI: сеансовый, представления и прикладной. Их объединение в рамках одной лабораторной работы обусловлено практической целесообразностью: в реальных сетевых решениях разграничение этих уровней часто условно, и для обучения важно рассматривать их функции совместно, что соответствует модели TCP/IP, где все они сведены в единый прикладной уровень. Работа посвящена HW5 в роли NGFW и фокусируется на частичном туннелировании трафика и глубокой проверке прикладных протоколов (DPI) с использованием ViPNet Coordinator. В ее рамках развертывается топология, включающая незащищенные узлы и узлы с установленным ПО ViPNet. В работе подробно рассматриваются этапы инкапсуляции и передачи пакетов внутри сети, выполняются тесты на прохождение туннельного трафика. Также в работе осуществляется внедрение DPI-модуля HW5: загружается обширная база распознаваемых сервисов и протоколов (более 2000 наименований), формируются правила блокировки. Эффективность фильтрации проверяется попытками запуска запрещенных приложений и анализом логов блокировок. В отчете фиксируются архитектура туннеля, ключевые конфигурации ViPNet Coordinator, результаты тестов, логи DPI-фильтрации.

Таким образом, представленный лабораторный комплекс по изучению архитектуры и технологий ViPNet охватывает все уровни модели OSI и обеспечивает последовательное освоение ключевых аспектов построения, внедрения и сопровождения защищенной сетевой инфраструктуры. От проектирования физического уровня и конфигурирования сетевой топологии до анализа прикладного трафика с использованием DPI – каждая лабораторная работа формирует у обучающихся не только технические навыки, но и системное понимание принципов обеспечения информационной безопасности в условиях современных угроз. Комплексный подход, реализованный в данном курсе, позволяет не только закрепить теоретические знания, но и подготовить специалистов, способных внедрять сертифицированные средства защиты информации в реальные корпоративные и критически важные информационные системы с учетом актуальных нормативных требований и сценариев эксплуатации.

Список используемых источников

1. Кравцова В. А. Построение защищенных сетевых соединений на основе отечественного оборудования // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 702-706. EDN:EXHSYQ.

2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_220885 (дата обращения 26.04.2025).

3. Приказ от 21 декабря 2017 г. № 235 об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения 26.04.2025).

4. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» URL: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения 26.04.2025).

5. Кривец А. С. Анализ систем искусственного интеллекта применяемых для работы систем обнаружения вторжений // Технологии информационного общества XVIII Международная отраслевая научно-техническая конференция; сб. науч. ст. в 1-ом т. Москва, Московский технический университет связи и информатики. Т. 1. С. 99-101. EDN:MQZRNG.

Статья представлена научным руководителем, доцентом кафедры ЗСС, заместителем декана факультета КБ по научной работе СПбГУТ, кандидатом технических наук, доцентом Штеренбергом С. И.

УДК 621.391.6:004.056.53

Л. А. Иванова (студент группы ИКТО-28, СПбГУТ)
Н. В. Кривоносова (преподаватель, СПбГУТ)
В. Д. Сысоев (студент группы К-631, СПбГУТ), sysoyev.vd@sut.ru

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ОПТОВОЛОКОННЫХ ЛИНИЙ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ФИЗИЧЕСКИХ СВОЙСТВ СРЕДЫ

Научная работа развенчивает распространенный миф об абсолютной защищенности волоконно-оптических линий связи, демонстрируя их уязвимость к перехвату данных через физические дефекты волокна. Подробно исследуются механизмы утечки информации через дефекты и несанкционированный доступ. Особое внимание уделено современным методам обнаружения вторжений, включая OTDR-анализ и технологии мониторинга. Результаты исследования позволяют пересмотреть подходы к обеспечению безопасности ВОЛС для усовершенствования практических решений защиты информации критически важных инфраструктур.

волокно, съем информации, излучение, перехват, обнаружение НСД

SECURITY ISSUES OF FIBER-OPTIC DATA TRANSMISSION LINES BASED ON THE PHYSICAL PROPERTIES OF THE MEDIUM

Ivanova L., Krivonosova N., Sysoev V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The scientific work debunks the widespread myth about the absolute security of fiber-optic communication lines, demonstrating their vulnerability to data interception due to physical defects in the fiber. The mechanisms of information leakage through defects and unauthorized access are investigated in detail. Special attention is paid to modern intrusion detection methods, including OTDR analysis and monitoring technologies. The results of the study make it possible to review approaches to ensuring the security of ВОЛС in order to improve practical solutions for protecting information of critical infrastructures.

Key words: *fiber, information capture, radiation, interception, detection of unauthorized access*

Волоконно-оптические линии связи масштабируются большими темпами, и это повышает интерес злоумышленников к несанкционированному доступу (НСД) к передаваемой информации по волоконным световодам. Производители оптоволокна утверждают, что съем информации при передаче по ВОЛС практически невозможен. Но в действительности это не совсем так [1]. Актуальность съема информации с ВОЛС оправдана при наличии возможности принять и обработать сигнал в дешифрованный вид с

помощью SFP модуля. Например, системы последней мили, где используется оптический доступ через пассивные оптические сети (PON), обладают невысокой пропускной способностью, что позволяет без труда подобрать методы демодуляции передаваемого трафика. В отличие от высокоскоростных систем, которые используют когерентные приемопередающие устройства с применением упреждающей прямой коррекцией ошибок (FEC), что затрудняет декодирование принятого сигнала из-за неизвестности типа использованного кодирования и, как следствие, обладают высокой стоимостью когерентного оборудования. Приведенные ниже методы НСД целесообразно применять только в тех системах, которые позволяют подобрать методы декодирования принятого сигнала. Рассматривая контактный метод, подразумевается, что нарушитель, имея физический доступ к кабелю, может выполнить разделку кабеля и знает, какое именно волокно ему требуется.

1. Контактный перехват с разрывом волокна. Самым простым способом, представляется включение в линию TAP сплиттера для мониторинга оптической сети (Fiber Channel Traffic Access Point TAP). Схема включения представлена на рис. 1

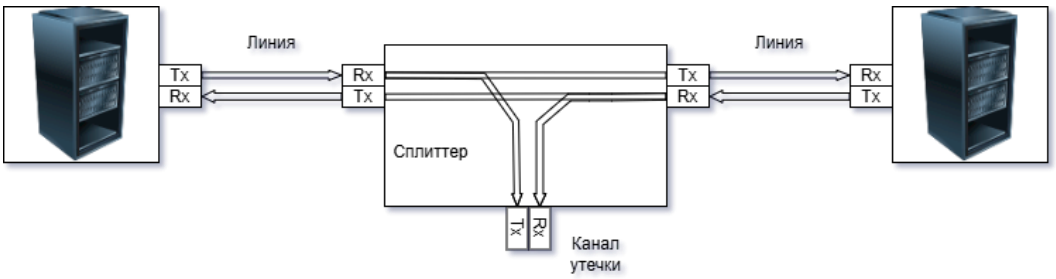


Рис. 1. Схема перехвата посредством TAP

2. Контактный перехват без разрыва. Принцип реализации этого метода заключается в механическом изгибе волокна и представлен на рис. 2. При увеличении диаметра изгиба оптического волокна (ОВ), уменьшается мощность оптического излучения, выходящего за его пределы [2] .

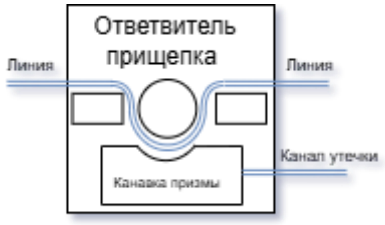


Рис. 2. Схема перехвата посредством FOD-5503

На рынке представлена прищепка FOD-5503, основное назначение которой – служебная связь между инженером и монтажником оптической

сети. Она применяется с целью консультирования монтажника о качестве выполнения сварки волокна и характеристиках оптического сигнала, но обладает существенным демаскирующим свойством – потери в линии 4 дБ для длины волны 1550 нм и 2 дБ для длины волны 1310 нм соответственно.

3. Контактный перехват на основе оптического туннелирования. После зачистки кабеля и волокна создается ответвитель. Для этого требуется достаточная длина кабеля, чтобы установить тонкую металлическую трубку с разрезом. В эту трубку помещается волокно утечки, которое затем заполняется оптическим клеем (ГОСТ 14887-80 Клеи оптические). В результате получается надежный и долговечный сплиттер от основного канала связи (рис. 3). Этот подход создает надежный, не зашумленный канал утечки на большие расстояния. Он наиболее эффективен, так как позволяет перехватить траффик с наименьшими потерями в линии, что осложняет обнаружение данного вида съема информации.

Рис. 3. Схема перехвата посредством оптического туннелирования

С точки зрения утечки информации, наиболее опасными являются оболочечные и вытекающие моды. Для доступа к такой информации достаточно иметь соответствующий тип оптического волокна и высокочувствительные фотоприемники. В качестве оптического объектива могут использоваться микролинзы или специальные системы.

Современные технологии позволяют фиксировать малейшие изменения в свойствах волокна. Спектроскопия потерь, например, улавливает даже незначительное повышение поглощения, вызванное передачей данных по свету. Анализ потенциальных каналов утечки информации помогает выявить наиболее уязвимые участки в волоконно-оптических линиях. Для реализации таких систем требуются сложные и дорогостоящие программно-аппаратные комплексы, включая машинное обучение для уменьшения ложных срабатываний, но ценность защищаемой информации может оправдать затраты.

1. Рефлектометрический метод определения каналов утечки информации в ВОЛС. Основой системы фиксации НСД является система диагностики состояния (СДС) оптического тракта (рис. 4). СДС можно построить с анализом прошедшего сигнала либо отраженного сигнала. В первой СДС на приемной части ВОЛС анализируется прошедший сигнал. При НСД происходит изменение сигнала, которое передается в блок управления ВОЛС. Основным недостатком является отсутствие информации о координате НСД [3].

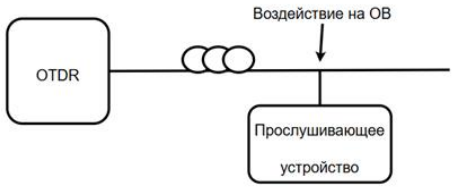


Рис. 4. Схема системы диагностики состояния оптического тракта

В исследуемое ОВ вводится мощный короткий импульс, который разрабатывает генератор импульсов и усиливает усилитель тока. Затем на этом же конце регистрируется излучение, рассеянное в обратном направлении на различных неоднородностях. Начальные рефлектограммы фиксируются при разных динамических параметрах зондирующего импульса и сравниваются с соответствующими текущими рефлектограммами. Локальное отклонение более чем на 0.1 дБ говорит о вероятности попытки НСД в этой точке линии. Съем информации с оптического волокна посредством макроизгиба сопровождается увеличением дополнительных потерь в месте подключения.

Для обнаружения механических натяжений в ОВ и участков ОВ с измененной температурой, можно использовать бриллюэновские рефлектометры, принцип работы которых основан на измерении временных зависимостей сдвига частот обратного рассеяния Мандельштама-Бриллюэна относительно частоты зондирующего оптического излучения. Рефлектограммы BOTDR (Brillouin Optical Time Domain Reflectometer) имеют хорошую чувствительность к изгибам и микроизгибам, а значит позволяют обнаружить канал утечки излучения.

При смещении частоты обратного рассеяния вследствие изменения параметров ОВ на рефлектограмме (рис. 5) будет наблюдаться спад или провал рассеянной мощности в области «подозрительных участков».

Рис. 5. Распределение спектра бриллюэновского рассеяния света в волокне

2. Обнаружение канала утечки информации из многомодового оптического волокна при помощи кремниевого фотоумножителя. Одним из наиболее распространенных способов обнаружения канала утечки информации является контроль мощности информационных сигналов, транслируемых по оптическому волокну (рис. 6). От источника оптического излучения на длине волны 650 или 850 нм в многомодовое волокно вводится свет. Он соответствует области спектральной чувствительности Si-ФЭУ (кремниевый фотоэлектронный умножитель).

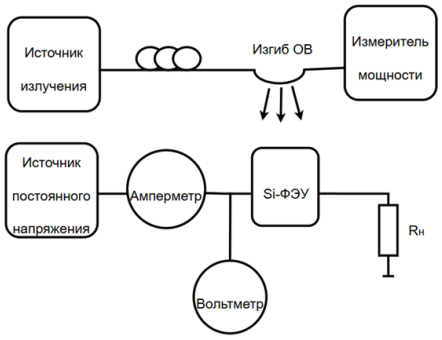


Рис. 6. Схема обнаружения КУИ с помощью кремниевого фотоэлектронного умножителя

Для передачи данных по многомодовому волокну используют излучение с длиной волны 850 нм. Для визуального поиска дефектов применяют свет с длиной волны 650 нм. К выходу волокна подключен измеритель мощности. Когда волокно изгибается, часть излучения выходит за его пределы. Это излучение улавливает Si-ФЭУ.

Результаты исследования подчеркивают необходимость пересмотра подходов к защите ВОЛС, особенно в критически важных инфраструктурах. Комбинирование методов обнаружения (OTDR, BOTDR, Si-ФЭУ) и применение интеллектуальных систем анализа данных позволят повысить уровень безопасности и минимизировать риски утечки информации. Перспективные направления защиты: развитие программно-аппаратных комплексов на основе машинного обучения для анализа рефлектограмм и минимизации ложных срабатываний, внедрение когерентных систем с FEC для высокоскоростных линий, где декодирование сигнала злоумышленниками затруд-

нено, регулярный мониторинг параметров ВОЛС (потери, спектральные изменения) для раннего выявления аномалий. Безопасность ВОЛС требует комплексного подхода, включающего как технические средства защиты, так и постоянный мониторинг состояния оптического тракта. Совершенствование методов обнаружения НСД и внедрение адаптивных систем защиты помогут обеспечить техническую защиту передачи данных.

Список используемых источников

1. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам. 1-е изд. М.: Горячая линия – Телеком, 2014. 536 с.

2. Гришачев В. В., Заболотская А. Д. Проблема информационной безопасности волоконно-оптических технологий // ФОТОНИКА Photonics Russia. 2022. Выпуск #6. С. 484-500. DOI:10.22184/1993-7296.FRos.2022.16.6.484.500

3. Рахимов Н. Р. Рефлектометрический метод определения каналов утечки информации в волоконно-оптических линиях связи // Интерэкспо Гео-Сибирь. 2010. № 5. С. 423-430.

Статья представлена научным руководителем, заведующим кафедрой ВТС DWDM СПбГУТ Марченко К. В.

УДК 004.056.5

А. В. Майоров (аспирант кафедры ЗСС, СПбГУТ), avmayorov@bk.ru

ИССЛЕДОВАНИЕ И ПОИСК АНОМАЛИЙ В ЖУРНАЛАХ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ СВОЕВРЕМЕННОГО РЕАГИРОВАНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК

Информационные системы становятся все сложнее, возрастает потребность в большем контроле за их безопасностью и состоянием. Одним из способов предотвращения киберугроз является подготовка к ним, постоянный мониторинг состояния системы, анализ журналов на предмет наличия аномальных действий в информационной системе или с ее компонентами. В данной работе рассмотрены основные шаблоны, которые возможно использовать при анализе журналов информационной системы с помощью стека ELK для своевременного обнаружения проблем безопасности или киберугроз.

ELK stack, elasticsearch, поиск аномалий, журналирование, анализ журналов

RESEARCH AND SEARCH FOR ANOMALIES IN INFORMATION SYSTEMS LOGS FOR TIMELY RESPONSE AND PREVENTION OF CYBER-ATTACKS

Mayorov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Information systems are becoming more complex, the need for more control over their safety and condition is growing. One of the ways to prevent cyber threats is to prepare for them, constantly monitor the state of the system, analyze logs for abnormal actions in the information system or with its components. This paper discusses the basic templates that can be used when analyzing information system logs using the ELK stack for timely detection of security problems or cyber threats.

Key words: *ELK stack, elasticsearch, anomaly search, logging, log analysis*

Обнаружение аномалий – ключевой инструмент современных информационных систем, позволяющий оперативно выявлять сбои или нелегитимные действия, минимизировать время простоя сервисов и риски компрометации данных. Проблемный трафик может быть вызван внешними атаками, устаревшими данными или обслуживанием, а с увеличением масштаба сети задача обнаружения аномалий усложняется. Журналы информационных систем, содержащие важные данные, широко используются для обнаружения аномалий. Однако рост сложности архитектуры систем делает построчный анализ журналов неэффективным, а использование сторонних

библиотек и модулей для реализации функционала информационной системы, увеличивает количество потенциальных проблем безопасности [1]. Увеличение объема журналов и сложность интеграции систем требуют новых подходов к анализу и устойчивости к сбоям, особенно в системах с множеством интеграций.

Для эффективного обнаружения аномалий в информационных системах необходимо использовать анализ журналов в режиме реального времени с помощью специализированного ПО, например, стека ELK (Logstash, ElasticSearch, Kibana) [2].

Современные угрозы, такие как вирусы и вредоносные программы, постоянно обновляются, чтобы обходить системы безопасности. Особенно критичны риски для доменов, связанных с пользовательскими данными и медициной, где нарушение недопустимо. Однако существующие системы предотвращения утечек данных сталкиваются с проблемой масштабируемости и неспособны своевременно обрабатывать большие объемы сетевых журналов [3]. Многие системы обнаружения аномалий обучены на устаревших данных и не способны работать с временными рядами или предоставлять оповещения в реальном времени. Их производительность в реальных условиях остается низкой, что подчеркивает необходимость улучшения подходов к кибербезопасности и разработке более эффективных решений [4].

Для обеспечения скрытого анализа журналов информационной системы требуется внешний модуль, защищенный политиками безопасности, с закрытым кодом, доступным только ограниченной группе разработчиков [5]. Этот модуль должен функционировать как «черный ящик», скрывая логику проверок, в то время как базовые проверки выполняются стандартными средствами Elastic Stack. Для анализа журналов и выявления аномалий в информационных системах и сетевом оборудовании необходимо агрегировать данные по ключевым параметрам (пользователи, время суток, тип события, геолокация, порты и т.д.) и использовать различные условия и варианты корреляции данных [6]. Таблица 1 содержит условия, по которым необходимо осуществлять анализ журналов, а также примеры промышленного использования условий в информационных системах.

ТАБЛИЦА 1. Шаблоны для анализа журналов информационных систем

Условие анализа	Промышленный пример
Объемы трафика	Неожидаемый скачок трафика на порту 443 (HTTPS) в ночное время, когда активность пользователей информационной системы минимальна. Это может указывать на DDoS-атаку или утечку данных
Подозрительные порты	Появление трафика на порту 31337, который часто используется вредоносными программами, хотя он не входит в список разрешенных портов
Необычные IP-адреса	Взаимодействие с IP-адресом из другой страны, с которой компания никогда не вела деловую активность, например, из США
Подозрительные протоколы	Использование протокола Telnet для удаленного доступа, при условии, что в компании стандартом является SSH. Это может указывать на попытку эксплуатации уязвимости
Частые неудачные попытки входа	50 неудачных попыток входа в систему с одного IP-адреса за 5 минут. Это может быть попытка брутфорса для подбора пароля
Редкая геолокация для текущей ИС	Успешный вход в систему пользователя с геолокацией, которая не соответствует местоположению сотрудника. Также это подозрительная активность, если информационная система работает только в Российской Федерации
Временные аномалии	Сетевая активность корпоративной информационной системе в 3 часа ночи, когда офис закрыт, а сотрудники не работают. Это может быть признаком несанкционированного доступа
Сетевые сканирования	IP-адрес пытается подключиться к 100 различным портам за короткий промежуток времени. Это может быть попытка сканирования сети для поиска уязвимых сервисов
Необычные шаблоны использования	Пользователь производит попытку скачать большие объемы данных с сервера, хотя обычно он работает только с небольшими файлами. Это может быть признаком утечки данных
Необычные последовательности событий	Пользователь сначала выполняет несколько неудачных попыток входа, а затем успешно входит в систему и сразу же изменяет настройки безопасности. Это может быть признаком компрометации учетной записи
Необычная частота событий	IP-адрес отправляет 1000 запросов к веб-серверу за минуту, что значительно превышает нормальную частоту запросов. Это может быть признаком атаки на веб-приложение
Различные сетевые атаки (например, DDoS)	Резкий рост трафика на веб-сервер с множества IP-адресов, что приводит к его перегрузке. Это пример DDoS-атаки
Несанкционированные изменения в конфигурации	Изменение конфигурации брандмауэра, которое открывает доступ к ранее закрытому порту. Это может быть результатом действий злоумышленника

Использование шаблонов для выявления аномалий позволяет автоматизировать процесс анализа и своевременно обнаруживать потенциальные угрозы, такие как несанкционированный доступ, сетевые атаки или сбои в работе системы. Также, необходимо предусмотреть дополнительные контуры защиты и настройки конфигураций:

● защита журналов: ограничить доступ к системным журналам, предоставляя права только администраторам. Использовать шифрование для передачи и хранения журналов, чтобы предотвратить их перехват или модификацию [7].

● мониторинг и оповещения: настроить мониторинг критически важных событий, таких как неудачные попытки входа, изменения конфигурации или сетевые сканирования. Установить пороговые значения для аномалий и настроить автоматические оповещения.

● сегментация сети: ограничить доступ к Elasticsearch и другим компонентам системы анализа, используя брандмауэры и VPN [8]. Разделить сетевые сегменты для минимизации риска распространения атак.

● обучение сотрудников: проводить регулярное обучение сотрудников по вопросам кибербезопасности. Убедиться, что администраторы понимают, как интерпретировать результаты анализа и реагировать на выявленные аномалии.

● резервное копирование: настроить регулярное резервное копирование журналов и конфигураций системы. Хранить резервные копии в защищенном месте, чтобы восстановить данные в случае атаки. Использовать методики контроля целостности файлов и подтверждения их оригинальности [9].

● Использование ML и AI: рассмотреть возможность использования машинного обучения для автоматического выявления сложных аномалий, которые трудно обнаружить с помощью статических правил.

Государственные информационные системы часто являются объектами атак злоумышленников, так как они содержат конфиденциальные данные, управляют ключевыми процессами и обеспечивают функционирование инфраструктуры, от которой зависит стабильность общества. В этом контексте анализ журналов на наличие аномалий становится не просто инструментом, а необходимым элементом защиты. Обсужденные подходы анализа журналов с использованием Elasticsearch и специализированных модулей позволяют создать эффективную систему мониторинга и выявления угроз. Своевременное обнаружение негативных событий позволяет минимизировать ущерб, предотвратить утечку данных и обеспечить бесперебойную работу системы. Практическая ценность обсужденных подходов заключается в их универсальности и адаптивности. Они могут быть применены как в небольших системах, так и в масштабных сетях с высокой степенью интеграции. Анализ журналов в реальном времени позволяет не только выявлять угрозы, но и прогнозировать потенциальные риски, что дает возможность принимать проактивные меры. В условиях, когда киберугрозы становятся все более сложными, а их последствия – более разрушительными, обсужденные подходы и шаблоны анализа журналов и выявления аномалий представляют собой не просто техническое решение, а стратегический инструмент.

Список используемых источников

1. Шариков П. И., Цветков А. Ю., Сигачева В. В., Сиротина Л. К. Исследование и алгоритм предотвращения эксплуатации уязвимостей библиотеки журналирования Log4j в информационных системах java-приложений // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 4. С. 100-106. DOI:10.46418/2079-8199_2023_4_19. EDN:BULSOH.

2. Майоров, А. В. Архитектура и программная реализация системы обнаружения компьютерных атак в корпоративных и государственных информационных системах на основе методов интеллектуального анализа // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 40-46. DOI:10.46418/2079-8199_2023_2_8. EDN:HEPDFF.

3. Ушаков И. А. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе Security Onion / И. А. Ушаков, А. В. Красов, Д. Д. У. Мулладжанов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 5-11. DOI:10.46418/2079-8199_2022_1_1. EDN:DSQOHB.

4. Майоров А. В. Модель представления Больших данных о компьютерных атаках в формате nosql / А. В. Майоров, А. В. Красов, И. А. Ушаков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47-54. DOI:10.46418/2079-8199_2023_2_9. EDN:GDZKWM.

5. Шариков П. И., Красов А. В. Исследование возможности использования java-агентов для вложения скрытого цифрового водяного знака непосредственно перед запуском java-приложения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 14-18. EDN:QQUVYX.

6. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных / А. А. Миняев, А. В. Красов, Д. В. Сахаров // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29-33. DOI:10.46418/2079-8199_2020_1_5. EDN ULHTJK.

7. Технические аспекты управления с использованием сети Интернет: Монография / А. А. Алейников, К. З. Билятдинов, А. В. Красов [и др.]. Санкт-Петербург: Центр научно-информационных технологий «Астерион», 2016. 305 с. ISBN 978-5-00045-408-4. – EDN:XGTJLL.

8. An approach for stego-insider detection based on a hybrid nosql database / I. Kotenko, K. Izrailov, A. Krasov, I. Ushakov // Journal of Sensor and Actuator Networks. 2021. Vol. 10. № 2. DOI:10.3390/jsan10020025. EDN:IKOMVS.

9. 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.

10. Шариков П. И. Методика создания и вложения цифрового водяного знака в исполняемые JAVA файлы на основе замен опкодов / П. И. Шариков, А. В. Красов, С. И. Штеренберг // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66-70. EDN:YKVPJF.

Статья представлена научным руководителем, заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Красовым А. В.

УДК 004.056

А. Д. Певзнер (студент группы ИКБ-11, СПбГУТ), pevzner.ad@sut.ru

МЕТОДИКА ОБНАРУЖЕНИЯ РАЗВЕДКИ OSINT С ИСПОЛЬЗОВАНИЕМ КОНЦЕПТА HONEYPOT ДЛЯ СБОРА ДАННЫХ

Данная статья представляет методику обнаружения разведывательных действий в открытых источниках (OSINT). Рассматривается этап разведки и действия злоумышленников в работе с открытыми источниками в сети. Предлагается концепция honeypot для обнаружения OSINT-разведки и пример ее реализации. Анализируются индикаторы активности honeypot, выявляющие разведывательные действия. Рассмотрены существующие концепты и разработки в этой сфере.

OSINT, honeypot, анализ активности, разведка, кибербезопасность, обнаружение угроз

OSINT INTELLIGENCE DETECTION TECHNIQUE USING THE HONEYPOT CONCEPT FOR DATA COLLECTION

Pevzner A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article presents a methodology for detecting intelligence activities in open sources (OSINT). The stage of intelligence and the actions of intruders in working with open sources on the network is considered. The concept of a honeypot for OSINT intelligence detection and an example of its implementation is proposed. The activity indicators of the honeypot are analyzed, revealing intelligence activities. The existing concepts and developments in this field are considered.

Key words: *OSINT, honeypot, activity analysis, intelligence, cybersecurity, threat detection*

В наше время все чаще поднимается тема информационной безопасности в компаниях, вовсю используются средства защиты от различных хакерских атак, на компьютерах установлено обновляемое антивирусное ПО, а настройке сети и ее администрированию также уделяется внимание [1-3].

Однако важно понимать, что любая хакерская атака начинается с подготовительного этапа – разведки по открытым источникам, также известном как OSINT. Отследить действия злоумышленника на этом этапе или каким-либо образом воспрепятствовать сбору информации о компании не предоставляется возможным. Собранная информация может послужить как для

планирования атаки на системы с последующей компрометацией, так и подвергнуть сотрудников компании опасности, так как под угрозой оказываются и персональные данные.

Для решения проблемы обнаружения подготовки атаки на сеть, предлагается метод, аналогичный технологии обнаружения злоумышленника в сети – honeypot (с англ. «бочонок с медом»), что по названию может намекать на что-то привлекательное, в данном случае – для злоумышленников. Работает эта технология так: к действующей сети подключается отдельное устройство (honeypot), которое содержит недостоверную информацию или информацию, к которой никто из компании не обращается. Это могут быть базы данных, пользователи с высокими привилегиями, уязвимые сетевые службы и любые другие данные, потенциально интересные атакующему. В honeypot специально внедрены уязвимости с целью склонить злоумышленника к атаке на данный узел сети. Любая активность на данном устройстве, кроме процесса установки, является крайне подозрительной и свидетельствует об сканировании, проникновении, или попытки взлома сети. Такие данные отправляются на анализ сотрудникам отдела информационной безопасности для анализа и реагирования на проникновение. В качестве «узла» в OSINT-honeypot могут использоваться сканируемые открытые источники.

Для реализации разработки требуется построить систему, в которой из ловушек будет собираться информация, обрабатываться, поступать в базу данных, из которой сервис анализа производит выборку для последующего предоставления результатов аналитикам данных и уведомлений о сканировании открытых источников (рис. 1).

Данные, которые возможно получить из ловушек:

- адреса электронной почты – приходящие письма, адресаты, содержание писем для анализа;
- страница авторизации, перейти на которые можно будет только при сканировании страниц сайта – попытки авторизации
- страницы в соцсетях, которые содержат личную информацию «сотрудника» компании, которую можно использовать для подбора паролей – попытки входа, заявки в друзья, личные сообщения, просмотры и лайки постов;
- группы в соцсетях с ссылками на конференции без аутентификации, конфиденциальная информация – заявки на вступление в группу, просмотры, вход на конференцию.

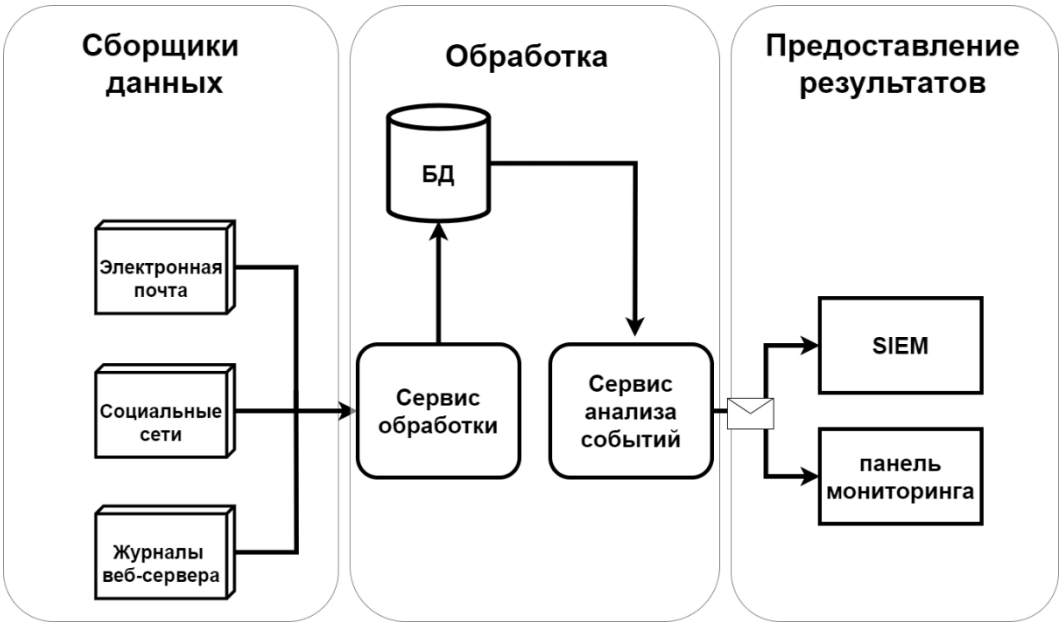


Рис. 1. Схема компонентов системы OSINT-honeypot

С помощью данных, полученной из OSINT-honeypot специалисты реагирования на инциденты информационной безопасности смогут собрать больше информации о злоумышленниках и понять, насколько они подготовлены к атаке, сколько устройств у них может быть задействовано и их IP-адреса.

Данная разработка имеет некоторые недостатки. Во-первых, проект требует дальнейшей доработки и внедрения в соответствии со структурой и задачами компании, что увеличивает количество расходов на обеспечение защиты. Во-вторых, так же, как и с сетевыми honeypot, злоумышленники смогут определить, является ли информация достоверной и научиться обходить их.

Несмотря на это, применение OSINT-honeypot позволит узнать, что злоумышленник планирует произвести атаку на объект что дает защитникам больше времени на реагирование и позволяет определить характер атаки, сбор данных для дальнейшего анализа уязвимостей источников, находящихся в открытом доступе.

На данный момент времени, завершенных проектов, посвященных созданию программ, инструментов и систем для анализа разведывательных действий по открытым источникам не существует, однако, идеи и концепты существуют. Так, например, на конференции Black Hat USA 2020, был представлен проект, доказывающий осуществимость концепции (Proof of Concept) – OSINT honeypot Manuka: модульный проект с открытым исход-

ным кодом, развернутый в Docker. В данном проекте реализовано получение уведомлений о подписке и добавлении в друзья в соцсетях Facebook и LinkedIn. Для работы данного проекта требуется настройка Google Cloud и Gmail. Однако, данная реализация не может быть рекомендуема к применению в отечественных организациях, так как имеет привязку к зарубежной компании Google и ее системам, а Facebook и LinkedIn заблокированы на территории РФ. Проект затронул тему противостояния разведке на уровне открытых источников, но не получил дальнейшего развития после конференции в 2020 году.

В ближайшее время разработка OSINT-honeypot получит свою реализацию, которая поможет организациям и предприятиям в противостоянии кибератакам, а также в исследовании рисков открытых источников. По результатам реализации можно будет собрать индикаторы активности злоумышленников и провести оценку собранных данных.

В результате разработана архитектура системы OSINT-honeypot и обоснована перспектива использования концепции honeypot для проактивного обнаружения и предотвращения потенциальных угроз, возникающих в результате разведки по открытым источникам.

Список используемых источников

1. GitHub – spaceraccoon/manuka: A modular OSINT honeypot for blue teamers. URL: github.com/spaceraccoon/manuka/tree/master (дата обращения 07.01.2025).

2. Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. № 4. Том 14. С. 362-377 DOI:10.21638/11702/spbu10.2018.409. EDN:YSGVZR.

3. Красов А В, Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm. Телекоммуникации и Транспорт. 2018. № 10. Том 12. С. 36-40 DOI:10.24411/2072-8735-2018-10154 EDN:YMWVOX.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Браницким А. А.

УДК 004.056

А. Д. Певзнер (студент группы ИКБ-11, СПбГУТ), pevzner.ad@sut.ru

РАЗРАБОТКА HONEYPOT-СИСТЕМЫ ДЛЯ ОБНАРУЖЕНИЯ ФИШИНГОВЫХ АТАК И РАЗВЕДЫВАТЕЛЬНЫХ ДЕЙСТВИЙ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

В современном мире повсеместно распространены социальные сети, которые злоумышленники используют для сбора данных о компаниях и частных лицах, чтобы найти уязвимые места для осуществления целевой атаки. В качестве проактивного метода защиты от такой атаки разрабатываются специализированные honeypot-системы, которые отслеживают подозрительную активность пользователей сети на предмет признаков, указывающих на подготовку атак на компанию, а также на факты фишинговой атаки. В данной статье рассматривается пример реализации и применения такой системы.

honeypot, разведка по открытым источникам, социальные сети, социальная инженерия, фишинговые атаки, целевые атаки

DEVELOPMENT OF A HONEYPOT SYSTEM FOR DETECTING PHISHING ATTACKS AND OPEN SOURCE INTELLIGENCE ACTIVITIES

Pevzner A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, social networks are ubiquitous, which attackers use to collect data about companies and individuals in order to find vulnerabilities for a targeted attack. As a proactive method of protection against such attack, a specialized honeypot systems have been developed which monitor the suspicious activity of network users for signs indicating the preparation of attacks on the company, as well as the facts of a phishing attack. The paper discusses an example of implementing and applying such a system.

Key words: *honeypot, open-source intelligence, social networks, social engineering, phishing attacks, targeted attacks*

В условиях увеличения числа киберугроз, обусловленных повсеместным внедрением информационных технологий, обеспечение информационной безопасности организаций и частных лиц становится задачей первостепенной важности. Одними из наиболее распространенных и опасных киберугроз являются фишинговые атаки. Им часто предшествует разведывательная деятельность, осуществляемая посредством открытых источников (OSINT), с целью сбора информации о потенциальных жертвах. Фишинговые атаки, основанные на социальной инженерии, позволяют

злоумышленникам получать конфиденциальную информацию, такую как логины, пароли и финансовые данные, посредством обмана и манипуляций. Разведывательные действия по открытым источникам, в свою очередь, используются для сбора информации о потенциальных жертвах, инфраструктуре и уязвимостях, что является подготовительным этапом для проведения более сложных и целенаправленных атак.

В отличие от фишинговых атак, противодействие OSINT-активности представляет собой более сложную задачу. Существующие методы защиты от разведки по открытым источникам в основном сводятся к контролю информации, публикуемой организацией или частным лицом в открытом доступе. Это включает в себя политики информационной безопасности, обучение персонала основам «цифровой гигиены», использование инструментов для мониторинга упоминаний организации в сети Интернет, а также применение техник обфускации и внедрения дезинформирующих источников информации для затруднения сбора достоверной информации. Однако, данные методы часто не позволяют полностью предотвратить сбор информации злоумышленниками, так как значительная часть данных, необходимых для проведения OSINT-разведки, может быть получена из сторонних источников, контролировать которые невозможно.

Для обнаружения разведывательных действий возможно использование инструментов для обеспечения проактивной защиты и сбора данных для дальнейших действий специалистами информационной информации. В основе реализации данной разработки лежит концепт honeypot. В каноничном представлении, honeypot представляет из себя узел сети, используемый для приманивания злоумышленников, он содержит в себе полезную информацию и является уязвимым для взлома объектом. Он не является полноценной частью сети и используется только как приманка, а любое взаимодействие с ним злоумышленников передается в систему мониторинга событий. Сам honeypot не является инструментом противодействия атакам, но его использование позволяет более подробно изучить действия злоумышленника, а также помогает в выработке проактивного реагирования на инциденты.

Для расширения возможностей по раннему обнаружению атак предлагается применить методы, аналогичные honeypot, для обнаружения разведывательных действий по открытым источникам.

Разработанный программный прототип имеет модульную архитектуру и состоит из сборщика данных, базы данных и системы анализа. Рассмотрим один из модулей honeypot-системы, предназначенный для поиска следов

разведки и социоинженерных атак в социальных сетях. В данной реализации ловушками выступают группы и личные страницы соцсети «ВКонтакте». Для сбора и анализа информации из социальной сети использовался API, описанный в официальной документации для разработчиков [1], а для автоматизации взаимодействия используется библиотека vk_api [2]. Структурная схема полученной системы приведена на рис. 1.

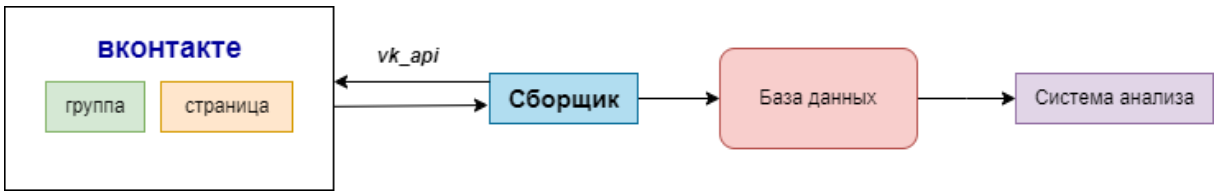


Рис. 1. Структурная схема honeypot-системы

Ключевую роль в этой системе играет сборщик. Он получает путем запросов к API к «ВКонтакте» получает из ловушек данные и отправляет в базу данных следующую информацию:

1. Группы и личные страницы:

- заявки в друзья/группу: id группы/страницы, id пользователя, время заявки, сообщение на вступление;
- личные сообщения: id пользователя, время, текст сообщения.

2. Посты/изображения в галерее:

- комментарии: id поста, id пользователя, текст комментария, время добавления комментария, ветка ответа;
- просмотры: количество;
- лайки: id поста, id пользователя.

Пример собранных данных приведен на рис. 2.

id	comment_id	from_id	date	text
1	32		2020-05-26 12:34:13	

Рис. 2. Пример таблицы в базе данных sqlite

На основе изменения этих данных система анализа отслеживает параметры потенциальных злоумышленников на предмет наличия аномальной активности с их стороны. С этой целью используется граничное обнаружение (пороговый анализ): когда на нескольких источниках в базу поступают данные об увеличении количества просмотров, это может рассматриваться как проведение разведки на социальные сети. Данные о заявках, коммента-

риях, лайках и сообщениях являются более активными действиями злоумышленников, что требует анализа подозрительных пользователей сети на предмет фишинговых атак и их подготовки к целевым атакам, а также позволяет больше собрать информации о злоумышленниках.

Для сбора тестовых данных были использованы 2 страницы и 3 группы: одна закрытая, для сбора заявок, две – открытые.

Контекст «ловушек»: страницы поставщика Кроликовой Н. И. и менеджера Остапова М. В. компании по производству рыболовных крючков «ForPhishing», на которых по 10 и 5 постов на странице соответственно. В первой группе «B» 21 пост для клиентов и 5 изображений в галерее она предназначена для обратной связи с клиентами, содержит обсуждения, отзывы, комментарии. Во второй группе «C» 11 содержательных постов для сотрудников, со ссылками на конференции и личными данными компании и клиентов. В группе «D» постов нет, так как она занимается только сбором запросов.

Далее смоделируем со стороны пользователя Иванова И. И. разведывательную деятельность для получения данных. На рис. 3 представлен соответствующий ей график активности.

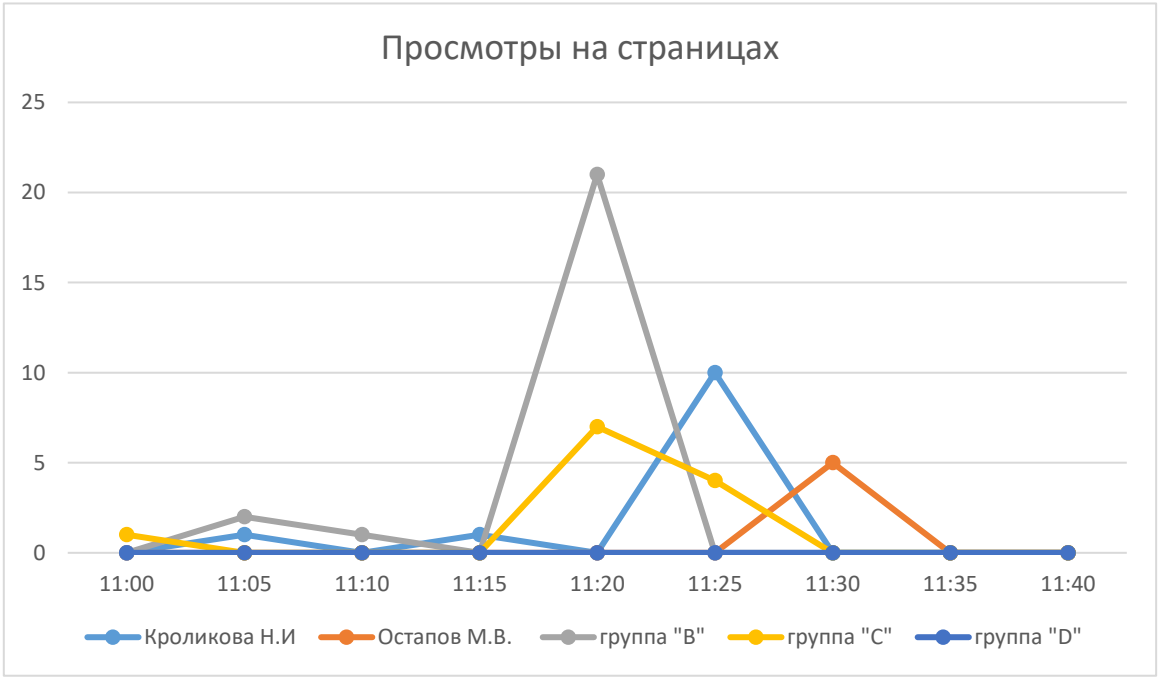


Рис. 3. График аномальной активности

По собранной в течение сорока минут статистике можно увидеть, что на временном промежутке 11:15-11:35 были просмотрены все посты в связанных группах и страницах, а в группе «D» получена информация о заявке

в группу «D» от «сотрудника компании» Иванова И.И., из чего можно сделать вывод, что по данным источникам проводилась разведка.

Развертывание honeypot-системы для выявления OSINT-активности сопряжено с рядом преимуществ и ограничений, требующих тщательного анализа. К преимуществам следует отнести возможность раннего обнаружения разведывательных действий, направленных на агрегацию информации об организации из открытых источников, что обеспечивает временной ресурс для реализации контрмер. Кроме того, система позволяет осуществлять сбор данных о потенциальных злоумышленниках, что в конечном итоге, приводит к усилению общего уровня осведомленности в области кибербезопасности внутри организации и формированию проактивной стратегии защиты. Вместе с тем, необходимо учитывать и ограничения, присущие данному подходу. Реализация honeypot-системы требует подробного планирования и конфигурирования с целью минимизации ложных срабатываний и обеспечения сбора релевантных данных. Существует также риск обнаружения honeypot злоумышленником, что может повлечь за собой компрометацию системы и ее использование в качестве вектора атаки. Следовательно, обеспечение конспиративности honeypot и соблюдение принципов безопасности представляются критически важными.

В дальнейшем будут собираться реальные данные, в том числе и по фишинговым атакам. Разработанный прототип состоит из нескольких модулей, таких как почта, ссылки на открытые внутренние ресурсы и веб-сайты, на которых, по аналогии с социальными сетями, можно получать данные о разведывательных действиях. В последующем планируется выполнить сбор статистики по ведению разведки, сбор данных о злоумышленниках и организациях, готовящих атаки на компании. Планируется расширение функциональности разработанной honeypot-системы за счет интеграции с другими средствами защиты информации и масштабирования до уровня распределенной сети ловушек. Примером реализации подобного подхода является [3], где рассматриваются вопросы масштабирования honeypot-решений для корпоративных сетей.

В результате проведенной работы реализован прототип системы обнаружения разведки по открытым источникам путем мониторинга страниц социальной сети. На основе анализа данных, полученных при помощи данной системы, были зарегистрированы следы разведки по открытым источникам.

Список используемых источников

1. Документация VK для разработчиков URL: https://dev.vk.com (дата обращения 20.04.2025).

2. Документация vk_api. URL: https://vk-api.readthedocs.io (дата обращения 20.04.2025).

3. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях. // Труды учебных заведений связи. 2019. № 3. Том 5. С. 86-97. DOI:10.31854/1813-324X-2019-5-3-86-97 EDN:VDCCKM.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Браницким А. А.

УДК 004.896

В. А. Страйстар (магистрант группы ИКТБ-48м, СПбГУТ),
straistar.va@sut.ru

ОЦЕНКА УСТОЙЧИВОСТИ АВТОКОДИРОВЩИКА ДЛЯ ОБНАРУЖЕНИЯ ИНСАЙДЕРОВ К АТАКАМ НА ДАННЫЕ

В данной работе будет исследована устойчивость автокодировщика, который применяется для обнаружения так называемых инсайдеров к различным типам атак на данные. Был проведен анализ непосредственного влияния искаженных данных на качество детектирования аномалий. Результат показывает, что стандартный автокодировщик уязвим к целенаправленным атакам типа evasion. Полученные выводы имеют важное значение для повышения надежности систем информационной безопасности, основанных на машинном обучении. Исследование подчеркивает актуальность изучения устойчивости моделей к состязательным атакам и предлагает направления для дальнейших работ в этой области.

автокодировщик, инсайдерские угрозы, CSV-данные, атаки на данные, poisoning-атаки, evasion-атаки

ASSESSING THE RESILIENCE OF AN AUTOENCODER FOR INSIDER DETECTION TO DATA ATTACKS

Straystar V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In this study, we will investigate the robustness of an autoencoder that is used to detect so-called insiders with different types of data attacks. Direct data on the quality of anomaly detection was analyzed. The result shows that the standard autoencoder is vulnerable to targeted evasion attacks. The findings are important for improving the reliability of machine learning-based information security systems. The study highlights the relevance of studying the resilience of models to adversarial attacks and suggests directions for further work in this area.

Key words: *autoencoder, insider threats, CSV data, data attacks, poisoning attacks, evasion attacks*

Актуальность

В современных условиях цифровой трансформации проблема защиты корпоративных данных от внутренних угроз приобретает особую значимость [1]. CSV-файлы, являясь одним из наиболее распространенных форматов хранения и передачи структурированных данных, представляют собой критически важный элемент информационной инфраструктуры

предприятий. Однако именно их повсеместное использование и относительная простота формата делают CSV-данные уязвимыми для различных видов злонамеренных воздействий.

Введение

Автокодировщик, применяемый для выявления аномалий в поведении пользователей, обрабатывает данные в CSV-формате, что создает дополнительные векторы для потенциальных атак. Проводимое исследование направлено на заполнение существующего пробела в области оценки и повышения устойчивости автоэнкодеров при работе с CSV-данными, что позволит разработать более надежные системы обнаружения инсайдерских угроз.

Целью данной работы является оценка устойчивости автокодировщика к двум ключевым типам адверсариальных атак – poisoning-атакам на этапе обучения и evasion-атакам на этапе эксплуатации – применительно к задаче обнаружения инсайдерских угроз в структурированных данных.

Поставленные задачи:

- создание примеров реализуемых атак;
- обучение модели на чистых данных, затем обучение на уже «отравленных» данных;
- оценить изменение точности модели, изменение ее предсказаний, а также изменение порогового значения после реализации атак;
- сделать выводы об устойчивости данной модели к реализуемым атакам.

Краткое описание используемой модели

LSTM автокодировщик обучается и принимает на вход предварительно извлеченные данные из набора r5.2 для инсайдерских тестов CERT. Ввиду малого числа подтвержденных инсайдерских инцидентов в исходном датасете, эти образцы были изъяты из обучающей выборки и использованы только для финального тестирования модели.

Разницу между входом x и выходом x' модели можно пометить как $d(x, x')$. Решение, является ли пользователь инсайдеров применяется на основе порогового значения δ. Образец считается аномальным в соответствии с правилами определения:

$$x \rightarrow \text{"normal"}\ if\ d(x, x') \leq \delta$$

$$x \rightarrow \text{"anomaly"}\ if\ d(x, x') > \delta$$

После обучения модели использовалось пороговое значение, равное δ = 71.01.

Пороговая ошибка рассчитывалась с помощью метрики MAE (Mean Absolute Error) – средней абсолютной ошибки, которая применяется для оценки точности прогнозов модели. MAE определяется как среднее арифметическое абсолютных отклонений между предсказанными и фактическими значениями [2]. Чем меньше значение MAE, тем выше точность модели. Формула для расчета MAE выглядит следующим образом:

$$MAE = \frac{1}{N}|y_i - y_i'|, \quad (1)$$

где N – количество наблюдений, y_i – предсказанное значение, y_i' – истинное значение.

Распределение ошибки выглядит следующим образом (рисунок 1):

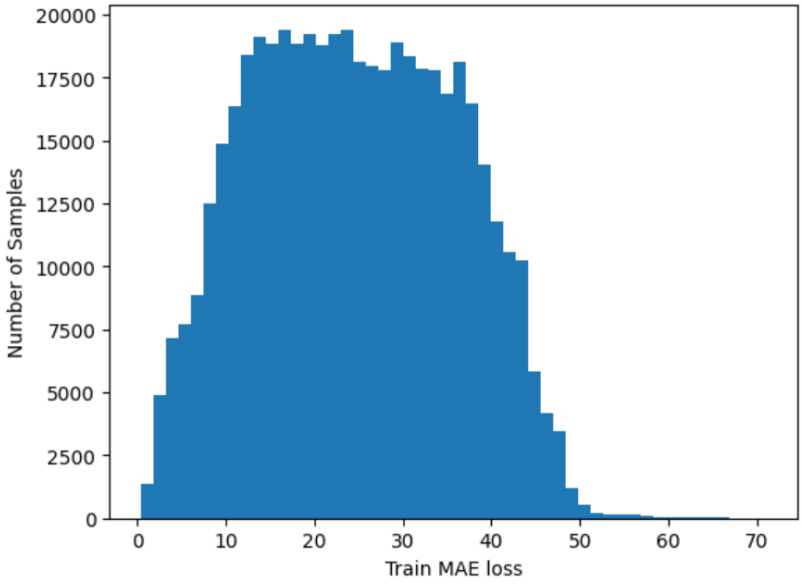


Рис. 1. График MAE до атаки

Реализация атак на данные

В данной работе будет воспроизведены адверсариальные атаки на датасет. Адверсариальные атаки – это целенаправленные злонамеренные действия, направленные на ухудшение качества данных или обман машинного обучения.

Типы адверсариальных атак, воспроизведенных в данной работе:

1. Poisoning-атаки (атаки «отравления»). Внесение искаженных или вредоносных данных на этапе обучения модели.

2. Evasion-атаки (атаки «уклонения»). Манипуляции с входными данными на этапе инференса (во время работы модели).

3. Отравление данных (Poisoning-атака) – намеренное внесение изменений в обучающую выборку, чтобы добиться определенного поведения модели во время исполнения при корректном поведении во время валидации [3]. Все данные изменяются на заданный в коде вектор. Формула может быть записана в векторной или поэлементной форме, в зависимости от размерности данных.

$$x_{poisoning} = x + \Delta x, \quad (2)$$

где $x_{poisoning}$ – возмущенный (модифицированный) пример, x – исходный вектор/тензор, Δx – заранее заданное смещение.

Формула применяется поэлементно к каждому признаку:

$$x_{poisoning}[i,j] = x[i,j] + \Delta x[i,j], \forall_i \in \{1,\dots,N\}, j \in \{1,\dots 14\} \quad (3)$$

В данном случае был использован следующий вектор:

$$\Delta x = [\begin{matrix}-0.05,-0.04,-0.03,-0.02,-0.01,0.00,\\ 0.01,0.02,0.03,0.04,0.05,0.06,0.07,0.08\end{matrix}]^T$$

Далее обучение модели запускается заново уже на измененном датасете. После обучения модели пороговое значение изменилось, после отравления данных для обучения оно стало равным $\delta \approx 72.1$.

Распределение ошибки выглядит следующим образом (рисунок 2):

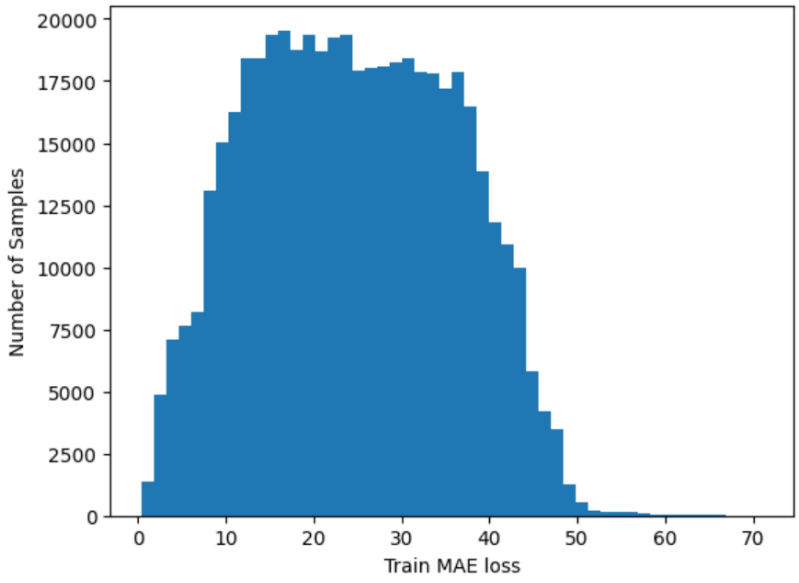


Рис. 2. График MAE после реализации атаки

Evasion-атака основана на методах, которые изменяют входные данные, чтобы обмануть модель [4]. С помощью метода numpy.random.uniform() мы можем получить случайные выборки из равномерного распределения и вернуть случайные выборки в виде массива numpy. Все данные изменялись в диапазоне от –0.7 до 0.7 от исходного числа. Формула для данного метода генерации адверсариальных примеров может быть записана следующим образом:

$$x_{evasion} = x + \Delta x, \quad (4)$$

где $x_{evasion}$ – адверсариальный пример, x – исходный экземпляр данных, Δx – случайный шум, генерируемый из равномерного распределения.

Математически шум можно выразить как:

$$\Delta x \sim U(-\epsilon, \epsilon), \quad (5)$$

где ϵ – параметр, ограничивающий максимальную величину возмущения.

В данном случае ϵ = 0,7.

Далее используется метод для предсказания значений при подаче данных, преобразованных при помощи атаки. Также заранее были зафиксированы значения, предсказанные до реализации атаки. Задача заключается в сравнении двух полученных массивов, метод, осуществляющий эту задачу на выходе, дал значение «False», что говорит о несовпадении полученных значений до атаки и после. Следующим этапам был написан метод, на выходе которого был получен результат совпадения массивов в процентах, составил он 4,8 %.

Результаты

В данном разделе представлены выводы по работе системы тестирования модели автокодировщика на уязвимость к атакам на входные данные и на данные, используемые для обучения.

Атака на данные обучающей выборки показала изменение порогового значения на 1 единицу, что соответствует 1,4 %. В данном случае можно указать на слабую эффективность атаки. Система проявила достаточную устойчивость, ведь порог, после которого автокодировщик признает образец аномальным, почти не изменился. Для увеличения эффективности атаки необходимо учитывать специфику модели.

Адверсариальная атака на входные данные продемонстрировала изменение точности на 4,8 %, что свидетельствует о том, что даже незначительные изменения во входных данных могут существенно повлиять на результаты классификации. Это подчеркивает потребность в разработке методов защиты, которые могут повысить устойчивость модели к подобным атакам.

Список используемых источников:

1. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных: специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность": диссертация на соискание ученой степени кандидата технических наук. СПб., 2020. 215 с. EDN: ISTTII.

2. Базилевский М. П. Оптимизационная задача построения линейных регрессий с минимальной величиной средней абсолютной ошибки на тестовых выборках // Моделирование и анализ данных. 2024. Т. 14. № 4. С. 91-103.

3. Tian Z. et al. A comprehensive survey on poisoning attacks and countermeasures in machine learning //ACM Computing Surveys. 2022. Т. 55. № 8. С. 1-35.

4. Biggio B. et al. Evasion attacks against machine learning at test time //Machine learning and knowledge discovery in databases: European conference, ECML pKDD 2013, Prague, Czech Republic, September 23-27, 2013, proceedings, part III 13. Springer Berlin Heidelberg, 2013. С. 387-402.

Статья представлена научным руководителем, и.о. заведующего кафедрой ИБКС, доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом Ушаковым И. А.

УДК 004.75-004.054

А. Ю. Строило (студент группы ИКТЗ-16, СПбГУТ), stroilo.au@sut.ru

АНАЛИЗ КРИТЕРИЕВ ОЦЕНКИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

Распределенные системы хранения данных все чаще используются для надежного и масштабируемого хранения информации. В данной работе рассматриваются ключевые критерии оценки качества их функционирования: максимальная пропускная способность, IOPS, доступность системы, отклик системы и механизм хранения данных на уровне объектов. Анализ этих параметров позволяет выработать рекомендации по выбору и сравнению систем хранения в зависимости от требований к производительности, отказоустойчивости и архитектурной гибкости. Работа носит обзорный характер и может служить основой для дальнейших исследований и практической реализации решений.

распределенная система хранения данных, критерии эффективности

ANALYSIS OF QUALITY ASSESSMENT CRITERIA OPERATION OF A DISTRIBUTED DATA STORAGE SYSTEM

Stroilo A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Distributed storage systems are increasingly being used for reliable and scalable information storage. This paper discusses the key criteria for evaluating the quality of their operation: maximum throughput, IOPS, system availability, system response, and the mechanism for storing data at the object level. The analysis of these parameters makes it possible to develop recommendations for the selection and comparison of storage systems, depending on the requirements for performance, fault tolerance and architectural flexibility. The work is of an overview nature and can serve as a basis for further research and practical implementation of solutions.

Key words: *distributed data storage system, performance criteria*

Распределенные системы хранения данных (РСХД) все глубже интегрируются в инфраструктуру современных информационных технологий, обеспечивая надежное и масштабируемое хранение больших объемов информации. При их проектировании и эксплуатации ключевое значение приобретает оценка качества функционирования, поскольку именно от этого зависят эффективность, отказоустойчивость и экономическая

целесообразность решения [1]. На практике выбор подходящей архитектуры РСХД требует тщательного анализа множества технических и эксплуатационных параметров.

В настоящее время при организации систем хранения применяются различные подходы – от типовых коммерческих решений до разработанных с учетом специфики архитектур. Каждый из них предъявляет свои требования к производительности, доступности и гибкости. Однако независимо от реализации, оценка эффективности всегда строится на основе определенного набора критериев, позволяющих структурировать процесс анализа и объективно сравнить различные системы.

Основными критериями, характеризующими качество функционирования распределенной системы хранения данных, являются: максимальная пропускная способность, IOPS, доступность системы, отклик системы и механизм хранения данных на уровне объектов (Object Storage). Эти характеристики позволяют получить всестороннее представление как о производительности системы под нагрузкой, так и о ее устойчивости, скорости реакции и архитектурной гибкости.

Максимальная пропускная способность является одним из ключевых показателей производительности распределенной системы хранения данных. Он определяет предельное количество данных, которое система способна обработать или передать за единицу времени [1]. Этот параметр напрямую влияет на эффективность функционирования системы, особенно в условиях высокой нагрузки.

Пропускная способность зависит от архитектуры системы, сетевых протоколов, характеристик носителей и уровня параллелизма. Измеряется она обычно в мегабитах в секунду (Мбит/с). На практике ее оценивают с помощью тестовых утилит, таких как netperf или Iometer.

Важность данного критерия особенно велика в высоконагруженных системах – облачных хранилищах, платформах для обработки больших данных и сервисах потокового вещания.

IOPS (Input/Output Operations Per Second) – это важный метрический показатель, характеризующий производительность распределенной системы хранения данных. Он отражает количество операций ввода-вывода, которые система способна выполнить за одну секунду. Данный параметр особенно значим при оценке скорости обработки запросов на чтение и запись, что напрямую влияет на общее быстродействие системы.

Значение IOPS зависит от множества факторов: типа носителей (HDD или SSD), архитектуры хранилища, алгоритмов кэширования и степени параллелизма. Высокий уровень IOPS указывает на способность системы эффективно справляться с интенсивными нагрузками, что критично для систем баз данных, облачных платформ и сервисов с высокой частотой обращений.

Таким образом, IOPS является одной из ключевых характеристик, на основании которой оценивается производительность и надежность современных решений в области распределенного хранения данных.

Доступность системы является одним из ключевых критериев оценки качества функционирования распределенной системы хранения данных. Под данным параметром понимается способность системы отвечать на запросы пользователей в любой момент времени и обеспечивать непрерывность предоставления услуг [1].

В процессе работы каждое обращение пользователя к системе запускает ряд процедур на сервере, направленных на обработку запроса и выдачу результата. Однако, как и в любом техническом механизме, возможны сбои – аппаратные неисправности, сетевые ошибки или программные конфликты, которые могут привести к временной или полной недоступности системы.

Доступность данных зависит от готовности элементов системы хранения к предоставлению хранящихся в ней баз данных. Этот показатель может быть оценен на основе коэффициентов доступности g соответствующих элементов хранилища [2]:

$$g = \frac{t_p}{t_p + t_b}, \quad (1)$$

где t_p – время регулярной работы системы, в течение которого запрашиваемые записи данных должны предоставляться с установленной эффективностью, t_b – время, в течение которого запрошенные записи данных были недоступны.

Высокая доступность достигается за счет использования механизмов резервирования, отказоустойчивости, автоматического восстановления и балансировки нагрузки между узлами. Особо высокие требования к данному критерию предъявляются в финансовых системах, облачных сервисах и платформах реального времени, где даже кратковременные простои могут привести к существенным последствиям.

Отклик системы – это один из важнейших критериев оценки производительности РСХД. Он характеризует время, которое проходит с момента отправки запроса пользователем до получения результата на стороне сервера [1]. Данный параметр напрямую влияет на восприятие скорости работы системы и удобства ее использования.

Отклик системы обычно измеряется в миллисекундах или секундах. Чем ниже значение этого показателя, тем быстрее система реагирует на входящие запросы. Однако при чрезмерно высокой нагрузке время отклика может возрасти до критических значений, что может привести к ошибкам типа Timeout.

Данный критерий особенно важен для систем, где требуется оперативная обработка данных – например, веб-сервисы, облачные хранилища и интерактивные приложения. Оптимизация времени отклика обеспечивается за счет эффективной балансировки нагрузки, кэширования данных и улучшения сетевых взаимодействий между узлами.

Механизм хранения данных на уровне объектов – важная характеристика распределенных систем хранения. Он предусматривает представление информации в виде объектов, включающих данные, уникальный идентификатор и метаданные [3]. Такая структура обеспечивает гибкость управления и удобство работы с большими объемами неструктурированных данных. За счет абстракции от низкоуровневых операций снижается сложность администрирования, исключается необходимость ручной настройки RAID-массивов и контроля фрагментации дисков. Объектное хранилище поддерживает горизонтальное масштабирование, что делает его популярным в облачных средах и системах хранения архивов, видео, логов и резервных копий. Вместе с тем, механизм может уступать другим типам хранения по скорости случайного доступа и уровню согласованности. Однако эти ограничения часто допустимы ради масштабируемости и экономической эффективности.

Для наглядного представления процесса оценки качества функционирования РСХД предлагается блок-схема на рис. 1. Она демонстрирует последовательность шагов, необходимых для комплексного анализа системы на основе ключевых критериев.

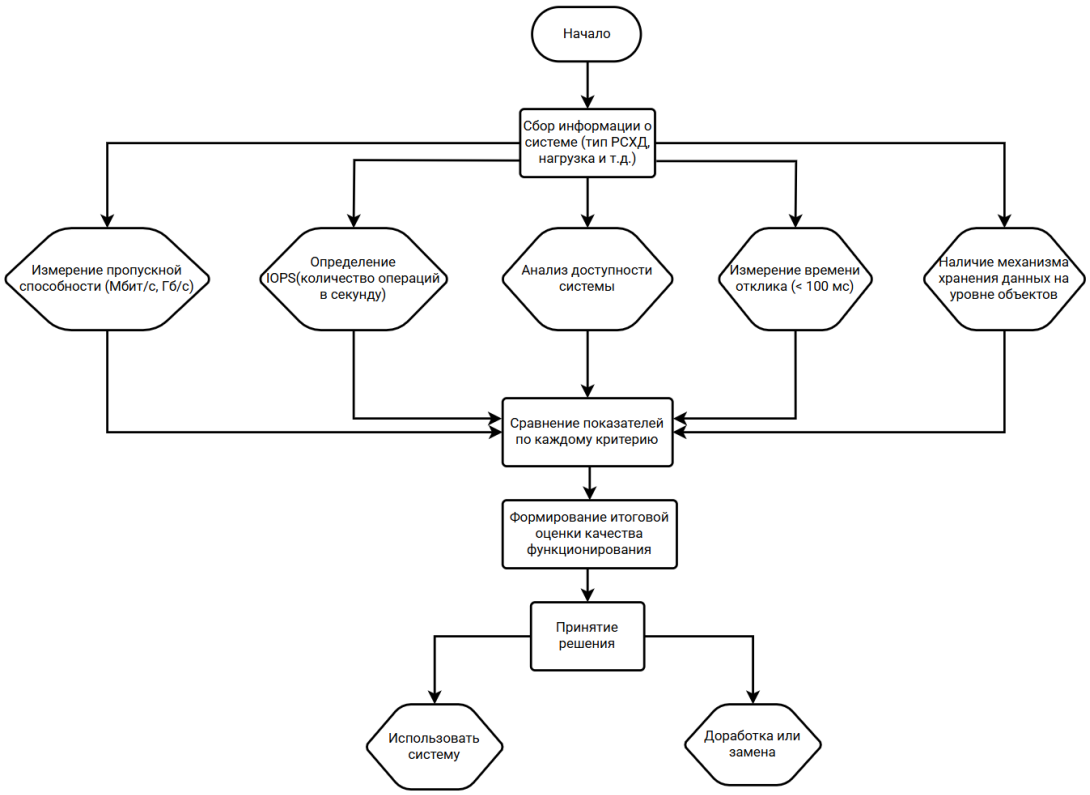


Рис. 1. Алгоритм оценки качества функционирования РСХД

На рис. 1 показано, что алгоритм начинается с собирания информации о системе, включая ее архитектуру, тип хранимых данных, масштаб и предполагаемую нагрузку. Далее выполняются измерения по каждому критерию:

1. Измерение пропускной способности – определяется скорость передачи данных в Мбит/с или ГБ/с;

2. Определение IOPS – вычисляется количество операций чтения/записи за секунду;

3. Анализ доступности системы – оценивается время безотказной работы системы с использованием формулы (1);

4. Измерение времени отклика – проверяется скорость реакции системы на запросы, с целевым значением менее 100 миллисекунд;

5. Проверка наличия механизма хранения данных на уровне объектов.

После выполнения всех измерений производится сравнение показателей по каждому критерию, что позволяет сформировать итоговую оценку качества функционирования системы. На основании полученных результатов принимается решение об использовании, доработке или замене системы.

Анализ критериев оценки качества распределенных систем хранения данных показывает, что их эффективность определяется совокупностью па-

раметров: пропускной способностью, IOPS, доступностью, временем отклика и реализацией объектного хранилища. Эти характеристики позволяют оценить производительность, надежность и гибкость системы.

Выбор решения зависит от специфики задач: в высоконагруженных системах важны скорость и пропускная способность, в критически важных – доступность и согласованность. При этом данные параметры тесно взаимосвязаны, и их баланс влияет на устойчивость и экономическую эффективность системы.

Для построения модели, соответствующей конкретным требованиям, необходимо провести серию экспериментов с различными конфигурациями. Это позволит выявить зависимости между параметрами и обоснованно выбрать оптимальное решение.

Список используемых источников

1. Костюков А. А. Критерии и средства оценки качества функционирования распределенной системы обработки информации / А. А. Костюков // Перспективы развития информационных технологий. 2016. № 28. С. 11-16. EDN:VOLJJZ.

2. Басыров А. Г., Кошель И. Н., Абраменков В. В. Алгоритмы оценивания показателей качества функционирования распределенной системы хранения конфиденциальных данных // Интеллектуальные технологии на транспорте. 2024. № 2 (38). С. 13–19. DOI:10.20295/2413-2527-2024-238-13-19

3. Мазур Э. М. Распределенные системы хранения данных: анализ, классификация и выбор / Э. М. Мазур // Перспективы развития информационных технологий. 2015. № 26. С. 33-60. EDN:UZQENL.

4. Таненбаум Э. Распределенные системы. Принципы и парадигмы. СПб.: Питер, 2003. ISBN: 5-272-00053-6.

Статья представлена научным руководителем, старшим преподавателем кафедры ЗСС СПбГУТ Цветковым А. Ю.

СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ И ЭКОНОМИКА ДАННЫХ

УДК 94(47).084.3:323.28:343.1

А. Б. Гехт (к.и.н., доцент, заведующий кафедрой истории и регионоведения, заместитель декана факультета СТЭД по научной работе СПбГУТ)
П. К. Гаврилова (студент группы ЗР-42, СПбГУТ), gavrilova.pk@sut.ru

ДЕЛО ТУХАЧЕВСКОГО: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВЕРСИЙ О ВОЕННОМ ЗАГОВОРЕ И ПОЛИТИЧЕСКОЙ ПРОВОКАЦИИ В КОНТЕКСТЕ 1930-х ГОДОВ

Дело Михаила Тухачевского, а также других высших военачальников СССР, которые были обвинены в «Военно-фашистском заговоре» в июне 1937 году, является одним из самых спорных и неоднозначных эпизодов сталинских репрессий. Данный процесс стал символом «Большого террора», а также не только лишил Советский Союз талантливых и опытных военачальников перед грядущей Второй мировой войной, но и открыто показал глубинные механизмы политических чисток, в которых реальность смешивалась с мифом, а факты – с пропагандой.

репрессии, заговор Тухачевского, Сталинский режим, фальсификация, реабилитация

THE TUKHACHEVSKY CASE: A COMPARATIVE ANALYSIS OF VERSIONS OF MILITARY CONSPIRACY AND POLITICAL PROVOCATION IN THE CONTEXT OF THE REPRESSIONS OF THE 1930s

Geht A., Gavrilova P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The case of Mikhail Tukhachevsky, as well as other top military leaders of the USSR, who were accused of a "Military fascist conspiracy" in June 1937, is one of the most controversial and controversial episodes of Stalinist repression. This process became a symbol of the "Great Terror", and not only deprived the Soviet Union of talented and experienced military leaders before the coming World War II, but also openly revealed the deep mechanisms of political cleansing, in which reality was mixed with myth, and facts with propaganda.

Key words: *repression, Tukhachevsky conspiracy, Stalin's regime, falsification, rehabilitation*

Даже сейчас продолжаются споры в кругу историков о том, был ли реален заговор Тухачевского и действительно ли маршал СССР хотел свергнуть уже сложившийся на тот момент сталинский режим, или же это все было тщательно спланированной провокацией, направленной на устранение неугодных для вождя лиц? С одной стороны, обвинения опирались на «признания» подследственных, полученные под пытками, и сомнительные документы, часть которых, как предполагается, могла быть сфабрикована зарубежными спецслужбами. С другой – конфликты внутри военной элиты, критика сталинской стратегии и опасения вождя перед потерей контроля создавали почву для веры в существование «врагов народа».

Чтобы приблизиться к пониманию истины, рассмотрим аргументы в пользу того, что Тухачевский действительно являлся участником заговора и что дело было сфабриковано. Перейдем к аргументам в пользу первого суждения.

Во-первых, Тухачевский, будучи харизматичным военачальником, имел значительное влияние в армии, а также политические амбиции [1]. Его разногласия со Сталиным по вопросам военной доктрины трактуются как основа конфликта с руководством СССР. Но не стоит забывать, что Тухачевский никогда не стремился попасть в политическую сферу, он лишь хотел служить в армии.

Во-вторых, в 1920-30-х годах Тухачевский участвовал в сотрудничестве с Германией, а также контактировал с военными кругами Великобритании, включая визиты на маневры Вермахта. Эти связи рассматриваются, как потенциальный канал для координации действий против сталинского режима [1-4].

В-третьих, на процессе 1937 года подсудимые «признались» в организации заговора, поэтому многие архивные материалы, где фигурируют якобы планы военного переворота, также приводятся в аргумент за существование заговора против сталинского режима [1].

Теперь перейдем к альтернативной и наиболее популярной точке зрения, где дело против Тухачевского было сфабриковано.

Начнем с того, что заключенные подвергались избиениям, чтобы следователи смогли получить их признания [3, 4, 5]. Известный английский ис-

торик, профессор Лондонского университета Д. Рейфилд, в 2008 году опубликовал работу «Сталин и его подручные», которое было основано на глубоком анализе личности И. В. Сталина. В своей работе он утверждал, что на изображении признания М. Н. Тухачевского присутствуют бурые пятна, которые судебно-медицинская экспертиза идентифицировала как пятна крови. Безусловно это не дает точных сведений о том, что Тухачевского избивали, но и никак не опровергает его [3]. Следует также отметить, что заключение по результатам графологического анализа рукописных показаний М. Н. Тухачевского показало, что скорее всего человек, написавший этот документ, находился в некоем необычном состоянии, например, под воздействием лекарственных препаратов [3, 5, 6], что также может свидетельствовать о применении насилия в сторону Тухачевского.

Также 2 июня 1937 г. Сталин выступил с докладом, в котором говорилось об «… изменниках Родины…», но официальное судебное слушание было назначено только на 11 июня. Это говорит о том, что результаты слушания были известны заранее, еще до его проведения. Да и стоит упомянуть, что на слушании у подсудимых даже не было адвокатов и была представлена лишь сторона обвинения [3, 4].

Также свидетель суда над Тухачевским, С. М. Буденный, и сам считал маршала СССР невиновным и говорил, что во время слушания Михаил Николаевич «…при чтении обвинительного заключения и при показании всех других подсудимых качал головой…», что также может являться свидетельством в его невиновности [3].

Последним аргументом является реабилитация в 1957 году Тухачевского и других фигурантов дела как жертв фальсификаций, связанная с деятельностью Н. С. Хрущева [3, 4].

Таким образом, дело против М. Н. Тухачевского было сфабриковано. Все доказательства, приводимые против этого, имеют свои контраргументы. Доказательства указывают на то, что НКВД создало ложное дело для устранения неугодных военачальников. Мотивы Тухачевского не исключают его критического отношения к сталинской политике, но нет данных, что это переросло в организованный заговор. Сталин использовал дело для профилактики любых форм оппозиции и укрепления личной власти перед надвигающейся войной.

Список используемых источников

1. Минаков С. Т. 1937. Заговор был. М.: Историческая литература, 2015. 180 с. ISBN 978-5-9876-5432-1.

2. Кантор Ю. В. Война и мир Михаила Тухачевского. М.: АСТ, 2008. 320 с.

3. Тереняк А. М. Сталинские репрессии против военных 30-х годов: дело маршала Тухачевского // CyberLeninka. 2023. URL: https://cyberleninka.ru/article/n/stalinskie-repressii-protiv-voennyh-30-h-godov-delo-marshala-tuhachevskogo (дата обращения 12.04.2025).

4. Котельников К. Сталинские репрессии против военных 30-х годов: дело маршала Тухачевского // Diletant.media. 2022. URL: https://diletant.media/articles/45310426/ (дата обращения 10.04.2025).

5. Минушкина Е. Дело Тухачевского: неразрешенные вопросы // Diletant.media. 2024. URL: https://diletant.media/articles/41243955/ (дата обращения 15.04.2025).

6. Рейфилд Д. Сталин и его подручные / пер. с англ. И. В. Петрова. М.: КоЛибри, 2020. 720 с. ISBN 978-5-389-12345-6.

УДК 327.5

А. Б. Гехт (к.и.н., доцент, заведующий кафедрой истории и регионоведения, заместитель декана факультета СТЭД по научной работе СПбГУТ)
А. И. Капуков (студент группы ЗР-41м, СПБГУТ) zamyatin.rd@sut.ru

ПРОБЛЕМА ОБРАЗОВАНИЯ ТИХООКЕАНСКОГО НАТО: ЯПОНИЯ, ТАЙВАНЬ, ЮЖНАЯ КОРЕЯ И СИНГАПУР

В условиях возрастающей геополитической нестабильности и усиления конкуренции в Азиатско-Тихоокеанском регионе, вопрос о формировании новых форматов сотрудничества в сфере безопасности становится все более актуальным. Одним из наиболее обсуждаемых сценариев является возможность создания так называемого "Тихоокеанского НАТО" – военного альянса, объединяющего Японию, Тайвань, Южную Корею и Сингапур. Эта концепция, вызывающая повышенный интерес у экспертов и политиков, рассматривается как потенциальный инструмент сдерживания Китая и обеспечения стабильности в регионе.

Азиатско-тихоокеанский регион, Тихоокеанское НАТО, Китай, Япония, Тайвань, Южная Корея, Сингапур

THE PROBLEM OF THE FORMATION OF THE PACIFIC NATO: JAPAN, TAIWAN, SOUTH KOREA AND SINGAPORE

Geht A., Kapukov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of increasing geopolitical instability and increasing competition in the Asia-Pacific region, the issue of forming new formats of cooperation in the field of security is becoming increasingly relevant. One of the most discussed scenarios is the possibility of creating a so–called "Pacific NATO" – a military alliance uniting Japan, Taiwan, South Korea and Singapore. This concept, which is of great interest to experts and politicians, is seen as a potential tool to contain China and ensure stability in the region.

***Key words**: Asia-Pacific region, Pacific NATO, China, Japan, Taiwan, South Korea, Singapore*

Исторически в Тихоокеанском регионе не было института обеспечения безопасности, такого как НАТО. Все можно объяснить особенностями холодной войны и специфичности расстановки сил Восточной Азии. Таким образом, Манильский пакт, который просуществовал с 1955 по 1977 года, не смог помочь в решении задач по борьбе с национально-освободительными движениями в Южной и Юго-Восточной Азии и, в конце концов, был распущен.

После победы в войне во Вьетнаме в Азиатско-Тихоокеанском регионе практически пятьдесят лет народы находится в мире. Правда, происходили

конфликты в третьей Индокитайской войне, включающих серию вооруженных конфликтов между Китаем, Лаосом, Вьетнамом и Кампучией (Камбоджей).

Тем не менее, наличие в Тихоокеанском регионе большого количества игроков с отличным военным потенциалом могут повлечь за собой прямые конфликты, огромные материальные потери и человеческие жертвы, что, в очередной раз показывает, как идея образования азиатского НАТО рискует оказать колоссальное воздействие на ряд мер по безопасности [1].

История

Японский премьер-министр Сигэру Исиба начал высказываться о создании Азиатского НАТО еще до вступления в должность. 10 сентября 2024 года, после вступления на пост лидера правящей Либерально-демократической партии, в своей речи в Гудзоновском институте в сентябре того же года Исиба отмечал, что главная цель организации – это обеспечение безопасности в Азии и конфронтация с Китаем, и главное из этого противостояния – недопущение завоевания острова Тайвань. Основа данного проекта – это создание так называемой коалиции демократии, способствующей к сдерживанию Китая, так как Япония очень ограничена материально и законодательно и таким образом не может увеличить свой силовой потенциал. Однако в октябре 2024 года Сигеру Исиба занял пост премьер-министра Японии и уже через месяц после вступления в должность старался избегать упоминания о создании Азиатского НАТО [2].

При наличии мирной конституции, японское общество всегда испытывало глубокое уважение перед авиацией, флотом и вообще перед армией в целом. Даже сам премьер-министр Исиба славится среди политиков как милитарист. Но в последнее время граждане Японии испытывают некоторые сомнения по поводу военного направления страны. Кроме того, тезисы некоторых политиков, пытающихся протолкнуть высказывания об украинском конфликте и опасениях в реакционных кругах такой же ситуации в Азии, также не получили особой поддержки хотя и повлияли на политику страны в сфере военной стратегии [3].

В этом случае Сигеру Исиба не стал упоминать на своем выступлении в парламенте о ядерном сдерживании совместно с Соединенными Штатами, видимо, причина в том, что подобные идеи противоречат законам и приоритетам страны. Уже в ноябре на мероприятии АСЕАН представители Японии

начали говорить о том, что создание такой защитной организации по подобию НАТО – вопрос не одного дня, и рекомендовали отложить решение данного вопроса на неопределенное время.

Однако в стране относительно длительное время идут разногласия по реализации Азиатского НАТО в целях обороны Японии и безопасности Азиатско-Тихоокеанского региона в целом [4].

В данном контексте высказывание о создании Азиатского НАТО имеет под собой определенную почву, хотя созданная оппозиция военно-политического союза может действовать в собственных интересах, поэтому данная идея имеет вероятность ограничить Японию в развитии международного сотрудничества в мировом сообществе.

Еще одним щекотливым моментом может стать отношения стран к КНР, так как страны Тихоокеанского региона не согласны принимать Китай как потенциального противника. В данном случае стратегия Японии в связи с национальной безопасностью страны преподносит Китай, как огромный вызов для Японии [5]. В то же время Сигеру Исиба высказывается одновременно о сдерживании Китая и о выгодном партнерстве на всех уровнях, представляя общность интересов между странами.

Кроме вышеупомянутого момента, проблемой для Японии может являться неопределенность в продвижении и успешности карьеры Сигеру Исиба в кресле премьера, так как впереди предстоящие выборы, а для Либерально-демократической партии любыми средствами необходимо удержать свои позиции в правительстве. Таким образом, внешняя политика Японии, скорее всего, будет находиться в состоянии лабильности для сохранения приоритетов партии [6].

Трельяжная беседка вместо велосипедного колеса

В последние годы Соединенные Штаты сильно ускорили процессы по сотрудничеству со своими союзниками в Тихоокеанском регионе, такими как Япония, Южная Корея, Новая Зеландия, Австралия. Сегодня рассмотрение безопасности некоторым образом отличается от системы ступицы и спиц, что была сформирована после Второй мировой войны в преддверии новых концепций усложнения связи между странами-союзниками. Известный политолог Виктор Ча описал стратегию, возникающую в Тихоокеанском регионе, как лоскутное одеяло, состоящую из военных союзов, созданных из региональных организаций и связанных с этим отношений.

Как известно из стратегии 2022 года, в Вашингтоне придерживаются созданной решетчатой стратегии в виде взаимосвязей партнеров напоминающей ажурную сетку. В Вашингтоне сфокусировались на AUKUS и QUAD для формирования основного подхода в стратегическом пространстве. В данную программу входит Кэмп-Дэвидское соглашение с Сеулом и, соответственно, Токио, заключенное в августе 2023 года, и первый американо-японско-филиппинский саммит с одновременным соглашением о партнерстве с Вьетнамом.

Некоторая склонность Соединенных Штатов к созданию различных стратегий сотрудничества, а не одной организованной стратегии было названо «минилатерализмом», рассматривается как образование небольших форматов по безопасности, направленных в основном на сдерживание Китая [7]. Но что примечательно, Вашингтон никогда не афишировал, к чему именно в системе безопасности отдает предпочтение, одновременно подчеркивая предрасположенность к порядку, согласованному в правилах. Сообразно высказываниям госсекретаря Блинкена, советника по нацбезопасности Дж. Салливана и министра обороны Остина, уже можно говорить не о двойственных договорах, а о взаимных пересекающихся отношениях и обязательствах между партнерами.

Скорее всего, такая тактика может в дальнейшем быть использована в разных областях. В октябре 2024 года посол Соединенных Штатов в Японии Р. Эмануэль высказался в пользу экономической коалиции по подобию НАТО. Он же указал, что для обороны необходим аналог Ст. 5 устава НАТО. В такой ситуации, в случае экономической атаки на одного из стран участниц остальные участники будут вынуждены оказать посильную помощь [8, 9].

Так можно предположить, что идеологи США считают модель НАТО, созданную в 1949 году, рабочим вариантом в современном мире, так как в то время СССР считался для Европы с подачи США наиболее опасным, чем сами штаты. Правда, сейчас Китай не представляет военной угрозы для Тихоокеанского региона, так как страны Азии рассматривают Китай, как партнера, нежели опасного конкурента. И даже существующие разногласия между некоторыми из стран не мешают развивать многополярные связи, выгодные всем сторонам и воздерживаются от прямых притязаний.

В сфере навязывания идеологии от КНР не происходит никакого нагнетания и навязывания другим странам. Более того, Коммунистическая партия Китая (КПК) считает, что нужно развивать собственную экономику и государство в целом, не экспортируя коммунистические идеи [10]. К тому же

еще и министр иностранных дел Индии высказался против идеи по созданию блока НАТО в Тихоокеанском регионе. В его поддержку выступил и премьер-министр Австралии Э. Албаниз, высказав общую точку зрения о непринятии данной системы коллективной безопасности.

Эксперты считают, что идея создания подобной системы, как НАТО в Азии, не будет осуществлена, но Япония предпримет попытку к модернизации собственной армии для противостояния угрозам, поступающим извне. Китайские же исследователи более чем уверены, что создание НАТО в Азиатско-Тихоокеанском регионе будет являться шагом назад, развивающим противостояние наподобие противостояния холодной войны.

По причине нежелания Токио нагнетать ситуацию, полагают китайские ученые, все разговоры о многосторонней организации в сфере военно-политической безопасности в АТР все же будут отложены на неопределенный срок.

Список используемых источников

1. Симония Н. А. Новый мировой порядок: от биполярности к многополюсности / Н. А. Симония, А. В. Торкунов // Polis: Journal of Political Studies. 2015. № 3. С. 27-37.

2. Азиатский НАТО // Рувики: энциклопедия. URL: https://ru.ruwiki.ru/wiki/Азиатский_НАТО (дата обращения 10.05.2025).

3. Никитин А. И. Перспективы военно-политической интеграции в Азии. Быть ли "азиатской НАТО"? // Мировая экономика и международные отношения. 2022. Т. 66, № 8. С. 5–15.

4. Smith J. Geopolitical Implications of a Pacific NATO // Journal of Strategic Studies. 2023. № 46(2). PP. 250-275. DOI:10.1080/01402390.2022.XXXXXXXX.

5. Tanaka H. Taiheiyo no anzen hosho kyoryoku no tenbo [Prospects for Security Cooperation in the Pacific] // Kokusai Mondai. 2022. № 701. PP. 15-32.

6. Губин А. Союз неспасения: идея «азиатского НАТО» одинаково вредна для всех стран АТР Андрей Губин // Российский совет по международным делам (РСМД): – URL: https://russiancouncil.ru/analytics-and-comments/analytics/soyuz-nespaseniya-ideya-aziatskogo-nato-odinakovo-vredna-dlya-vsekh-stran-atr/ (дата обращения 11.05.2025).

7. Ratner E. Rebalancing to Asia with an insecure China // The Washington Quarterly. 2013. Vol. 36, Issue 2. PP. 21-38. Mode of access: https://csis.org/ files/publication/TWQ_13Spring_Ratner.pdf (дата обращения – 06.08.2025.)

8. Шаклеина Т. А. «Дилемма Америки» в формировании современного мирового порядка // Междунар. процессы. 2019. Т. 17, № 4(59). С. 36–48. https://doi.org/10.17994/IT.2019.17.4.59.3 (дата обращения 11.05.2025).

9. Антонов Р. А. Внешнеполитическая стратегия правящих элит США в XXI веке \ Р. А. Антонов, Изв. Сарат. ун-та. Нов. сер. Сер.: Социология. Политология. 2023. Т. 23, вып. 3 350.

10. Roy D.U.S. – China relations: Stop striving for «trust» // The Diplomat. 2013. 7 June. Mode of access: http://thediplomat.com/2013/06/u-s-china-relations-stopstriving-for-trust/ (дата обращения – 01.08.2025.)

УДК 327.51

А. В. Голланд (студент группы ЗР-11, СПбГУТ), golland.av@sut.ru

ВОЕННО-ПОЛИТИЧЕСКОЕ ВЗАИМОДЕЙСТВИЕ США И РЕСПУБЛИКИ КОРЕЯ В ПЕРВОЙ ЧЕТВЕРТИ XXI в.

Взаимоотношения между Соединенными Штатами Америки и Республикой Корея имеют долгую и обширную историю, однако с двухтысячных годов они вступили в новую фазу. Наступление нового тысячелетия ознаменовало собой период обострения экономических, политических и социальных проблем в Азиатско-Тихоокеанском регионе. Это потребовало создания новых альянсов для их решения. На примере союза между Соединенными Штатами и Кореей можно проследить эволюцию международных отношений в данном регионе. В данной работе приводится анализ динамики американо-южнокорейских взаимоотношений.

США, Южная Корея, КНДР, международные отношения, НАТО, ядерная безопасность

THE MILITARY AND POLITICAL COOPERATION BETWEEN THE UNITED STATES OF AMERICA AND THE REPUBLIC OF KOREA IN THE FIRST QUARTER OF THE XXI CENTURY

Golland A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The relationship between the United States and the Republic of Korea has a long and extensive history, but it has entered a new phase since the turn of the millennium. The advent of the new millennium marked a period of heightened economic, political and social challenges in the Asia-Pacific region. This necessitated the establishment of novel alliances to address these issues. The alliance between the United States and Korea provides a pertinent case study in the evolution of international relations in this region.

Key words: *USA, South Korea, North Korea, foreign relations, NATO, nuclear security*

Республика Корея и США являются одними из главных акторов влияния в Азиатско-Тихоокеанском регионе. Их взаимодействие отражается на политико-экономической обстановке во всей Северо-Восточной Азии. В связи с нарастанием политической напряженности, в регионе сформировались две «оси безопасности» – Вашингтон-Сеул-Токио и Москва-Пекин-Пхеньян. Сотрудничество внутри них за последнюю четверть века сформировало новый политический облик Северо-Восточной Азии. В данной статье рассмотрены основные аспекты взаимодействия США и Республики Корея в период 2000-2025 гг.

Актуальность исследования обусловлена рядом факторов, имеющих глобальное и региональное значение. Данный период характеризуется значительными геополитическими изменениями в Азиатско-Тихоокеанском регионе. Они включают в себя изменение экономической обстановки, усиление влияния Китайской Народной Республики и ядерную угрозу со стороны Корейской Народной Демократической Республики. Необходима оценка эволюции двусторонних отношений на фоне изменения геополитической обстановки в мире и новых вызовов современности. Также сотрудничество между США и Республикой Корея является ключевым элементом системы коллективной безопасности во всей Северо-Восточной Азии и оказывает существенное влияние на глобальную стабильность. Исследование данной темы позволит лучше понять динамику региональной безопасности, а также дать оценку возможным путям ее развития.

Целями данной работы является описание теоретических аспектов взаимодействия США и Республики Корея, а также анализ конкретных примеров.

Американо-корейское взаимодействие имеет длинную историю. Еще в 1882 между США и государством Чосон был заключен Договор о мире, дружбе, торговле и навигации (Treaty of Peace, Amity, Commerce and Navigation). Однако, двустороннее сотрудничество государств, такими какими мы их знаем сейчас, началось с 1949 г, когда правительство США официально признало Южную Корею единственным легитимным государством на полуострове и установило дипломатические отношения.

Это также сыграло роль в корейской войне 1950-1953 гг. Экономическая, материальная и политическая поддержка от США южнокорейской армии привела к относительной нормализации обстановки на полуострове и заключении перемирия. В год окончания войны был подписан договор о взаимной обороне, между двумя государствами [1].

Договор о взаимной обороне предполагает, что в случае угрозы безопасности одной из стран, государства имеют право консультироваться друг с другом, а также совместно реализовывать меры по защите суверенитета. Также, в Статье 4 закрепляется право нахождения американских вооруженных сил на территории Республики Корея: «Республика Корея гарантирует, а Соединенные Штаты Америки подтверждают свое согласие с правом размещения сухопутных, воздушных и морских сил США на территории Республики Корея и вблизи нее, как это будет определено по взаимному соглашению». В последней статье документа указано, что несмотря на то, что

данный договор является бессрочным, любое из государств может расторгнуть его, предупредив вторую сторону об этом за год. Соглашение 1953 г., с небольшими дополнениями действует до сих пор. На данный момент этот документ является основным в военно-политическом взаимодействии между США и Кореей, последующие акты явно или косвенно опираются на него [2].

Основными аспектами военно-политического взаимодействия США и Республики Корея в первой четверти XXI в. являлись ядерная безопасность; политика в отношении третьих государств; а также сотрудничество в рамках космических исследований, кибербезопасности и инновационных технологий. Большинство из реализовывались в рамках программы «Основной союзник вне НАТО» [3].

Республика Корея с 1987 г. является страной-участницей программы «Основной союзник вне НАТО» (Major non-NATO ally). Помимо того, что данный статус «является сильным символом тесных отношений, которые Соединенные Штаты разделяют со странами, и демонстрирует глубокое уважение к дружбе со странами, которым он предоставлен», он также предоставляет государствам-участницам значительные привилегии. Такие, как участие в совместных операциях и исследованиях, доступ к военной технике США за рубежом, приоритет на распределение «военных излишков», разрешение на использование американской материальной помощи для покупки или аренды определенного оборонного оборудования и др. [3]. Совместно с соглашением 1953 г., это ставит Республику Корея в один ряд с другими странами Северо-Атлантического договора.

Активное развитие отношений продолжилось в XXI в. В «Совместном видение альянса» от 2009 г. упоминаются планы на расширение сотрудничества США и Кореи в том числе в военной и ядерной безопасности. За последующие 15 лет был подписан ряд важных соглашений по сотрудничеству, две индивидуальные программы партнерства, Республика Корея стала членом центра киберзащиты НАТО, совершено несколько совместных гуманитарных миссий, а также расширены уже существующие проекты. Во всех соглашениях тем или иным образом фигурирует Корейская Народно-Демократическая Республика, что позволяет сделать вывод о том, что самым главным аспектом сотрудничества остается противодействие северокорейской угрозе [4]. Несмотря на то, что существуют прямые опасения относительно безопасности на корейском полуострове, необходимо

упомянуть, что иногда данная причина является скорее предлогом для проведения совместных военных мероприятий и усиления американского влияния в регионе. Большое развитие отношения получили во время президенства Юн Сок Еля, поддерживающего проамериканский курс внешней политики.

На данный момент, основными документами, регулирующими военно-политическое взаимодействие между двумя государствами, являются Mutual Defense Treaty Between the United States and the Republic of Korea (1953), Joint vision for the alliance of the United States of America and the Republic of Korea (2009), Status of forces agreement (SOFA) (2011), Basic exchange and cooperation agreement concerning geospatial intelligence (2011), Joint Statement from the Governments of the United States of America and the Republic of Korea at the United States-Republic of Korea Civil Space Dialogue (2025), Закон о военной службе (병역법) (1994), Рамочный план оборонной реформы 2014–2030 (국방개혁 기본계획) (2006).

Несмотря на, казалось бы, благотворное сотрудничество двух государств, в их взаимоотношениях имеются спорные моменты. Одним из них является стратегия относительно КНР. Китайско-корейские отношения на протяжении долгого времени демонстрировали стабильный рост, однако с каждым годом все большее значение в них играет американский фактор. Стремление США к доминированию в АТР приводит к ситуации, в которой Корея становится все более зависима от Западных партнеров [5]. Это приводит к внутриполитическим спорам относительно необходимости проведения активной проамериканской политики.

Другим фактором является формирования «Индо-Тихоокеанского аналога НАТО», в который также включают Японию. Сложные исторические взаимоотношения двух стран сказываются на современной политической обстановке. Между Японией и Кореей сохраняются территориальные споры относительно статуса о. Токто или о. Такэсима, а также неурегулированные вопросы относительно компенсаций жертвам войны. По опросам 2014 г., 79 % корейцев высказывали негативное мнение относительно Японии. Все это, а также «торговые войны» между государствами не дают возможности проводить слаженные совместные действия в рамках трехстороннего сотрудничества с США.

Все это привело к явлению, которое получило название «ситуативный антиамериканизм». Данное движение проявляется критикой только отдельных аспектов политики или действий США. Во многом, его рассвет пришелся на начало 2000-х гг., когда происходило расширение американских военных баз на территории Кореи, а также отмечался значительный спад межкорейской напряженности, в связи с шестисторонними переговорами. На данный момент антиамериканские настроения поднимаются в рамках предвыборных компаний, во время досрочных выборов президента Кореи.

Таким образом, сотрудничество США и Южной Кореи остается важной составляющей политической обстановки в Северо-Восточной Азии. Хотя вызовы со стороны КНДР, Китая и внутренние политические различия усложняют взаимодействие, альянс сохраняет стратегическую важность для обеих сторон.

Список используемых источников и литературы:

1. Садаков Д. А. Политика США в отношении государств Корейского полуострова в 1953–1980 гг.: автореф. дис. д-р. ист. наук: 5.6.2. - Екатеринбург, 2025. 47 с.

2. Basic Documents Volumes I and II. «Mutual Defense Treaty Between the United States and the Republic of Korea» (01.10.1953). Washington, DC: Department of State Publication 6446. 1957. 2 с.

3. Ланцова И. С. Государства Корейского полуострова в международных отношениях (конец XX - начало XX вв.) / под науч. ред. Б. А. Ширяева. СПб.: СПбГУ, 2013. 247 с.

4. Мишин В. Ю., Болдырев В.Е. Корейский полуостров: проблемы ядерной безопасности и их влияние на экономическую интеграцию // Ойкумена. Регионоведческие исследования. 2015. № 2. С. 121-127.

5. Фархетдинова Э. Т. Современное геополитическое положение Республики Корея: на стыке интересов США и КНР // Конфликтология / nota bene. 2023. № 1. DOI: 10.7256/2454-0617.2023.1.37776 EDN:AWSJZX URL: https;//nbpublish.com'Hbrary_read_article.php?id=37776 (дата обращения 30.04.2025).

УДК 004.67

Р. И. Зарипов (к.фил.н., докторант ВУ имени князя Александра Невского)
Н. Р. Стрельников (курсант ВКА имени А.Ф. Можайского), vka@mil.ru

КОЛИЧЕСТВЕННЫЙ АНАЛИЗ ВЛИЯНИЯ ФАСЦИНАТИВНЫХ ЭЛЕМЕНТОВ НА ВОВЛЕЧЕННОСТЬ АУДИТОРИИ В РОССИЙСКИХ TELEGRAM-КАНАЛАХ

В условиях интенсивного распространения информации в медиапространстве активно используются инструменты фасцинации, способствующие привлечению внимания аудитории к контенту, в том числе манипулятивному. Исследования показывают, что пользователи чаще взаимодействуют с сообщениями, обладающими высокой социально-политической значимостью и резонансностью или содержащими интригующие заголовки и другие приемы аттракции. Однако остается недостаточно изученным, как конкретные фасцинативные элементы (эмодзи, маркеры срочности) влияют на вовлеченность аудитории. В данной работе исследуется зависимость реакции пользователей на новостные посты в Telegram (30 популярных каналов из категории "новости") от наличия в них фасцинативных элементов, таких как восклицательные эмодзи, маркеры и т.д.

количественный анализ, фасцинация, Telegram, матрица корреляции, вовлеченность пользователей, новости

QUANTITATIVE ANALYSIS OF THE EFFECT OF FASCINATIVE ELEMENTS ON AUDIENCE ENGAGEMENT IN RUSSIAN TELEGRAM CHANNELS

Zaripov R.[1], Strelnikov N.[2]
[1]Military University named after Prince Alexander Nevsky
[2]A. F. Mozhaysky Military Space Academy

In the context of the intensive dissemination of information in the media space, fascination tools are actively used to attract the audience's attention to content, including manipulative content. Research shows that users are more likely to interact with messages that have high socio-political significance and resonance or contain intriguing headlines and other attraction techniques. However, it remains poorly understood how specific fascinative elements (emojis, urgency markers) affect audience engagement. This paper examines the dependence of users' reactions to news posts in Telegram (30 popular channels from the "news" category) it depends on the presence of fascinative elements in them, such as exclamation emojis, markers, etc.

Key words: *quantitative analysis, fascination, Telegram, correlation matrix, user engagement, news*

В современных условиях скоростной передачи огромных объемов информации возникает актуальная необходимость контроля и фильтрации контента. Проблема усложняется стремлением распространителей любыми

способами привлечь внимание читателей. Медиапоток новостей, представляющий собой наиболее активную форму распространения информации, часто содержит инструменты фасцинации, способствующие аттракции аудитории и создающие условия для подавления ее критического мышления. Это соответствует тому, что «в общей массе людей лишь 15–25 % способны критически анализировать предъявляемую им информацию, а порядка 75 % достаточно легко поддаются внушению» [1].

В результате проведенного в конце 2023 года фасцинативного эксперимента [2] установлена следующая закономерность: «Фасцинация как коммуникативный феномен реализует механизм психологического заражения (самопроекции) адресата, способствует возникновению его когнитивного интереса и повышает уровень его доверия к сообщению, придавая убедительность последнему при условии уместности и соразмерности эмоционально окрашенных (фасцинативных) элементов и их подкрепления рациональной аргументацией». Под фасцинацией понимается такое воздействие сигнала как языковой, так и неязыковой природы, при котором адресат испытывает какую-либо эмоциональную реакцию определенной степени заряженности, длительности и интенсивности, что кратковременно или на более длительный период переводит восприятие и понимание информации в иррациональную, чувственно-эмоциональную плоскость.

Процедуры указанного эксперимента предусматривали непрямое (скрытое) качественно-количественное эмпирическое исследование методом анкетирования, в котором приняли участие 133 человека в возрасте от 17 до 64 лет из числа студентов, курсантов, офицеров и гражданского персонала Военного университета имени князя Александра Невского Министерства обороны Российской Федерации [там же].

Данный анализ является продолжением исследования на основе более глобальной выборки данных с целью подтверждения или корректировки полученных результатов и определения направлений дальнейшей работы. Исходя из этого, было принято решение о проведении количественного анализа с целью выявления зависимости между применением фасцинативных элементов (эмодзи, маркеров срочности) в новостных Telegram-каналах и реакцией аудитории (просмотры, репосты, комментарии, эмодзи-реакции). Для исследования был создан датасет, содержащий 30 популярных Telegram-каналов российского сегмента из категории «Новости и СМИ». Каналы отличаются независимостью от определенной тематики новостной повестки. Данный фактор важен для ис-

ключения влияния субъективно-личностной заинтересованности пользователей к определенной теме. В каждом канале была проведена выборка поликодовых и вербальных постов, которые содержат непустые строки в описании, составивших базу данных из 1.133.088 новостных постов.

В качестве инструмента проведения анализа был выбран язык программирования Python и его возможности для анализа данных и обработки естественного языка (библиотеки Matplotlib, NumPy, Pandas, Scikit-Learn, Pymorphy3, NLTK, Emoji).

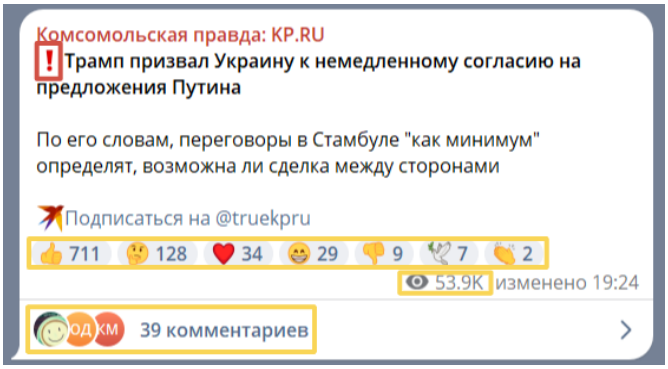


Рис. 1. Пример новостного поста с выделенными метриками для анализа

В результате проведенного анализа была получена матрица корреляции по коэффициенту Пирсона, представленная на рисунке 2.

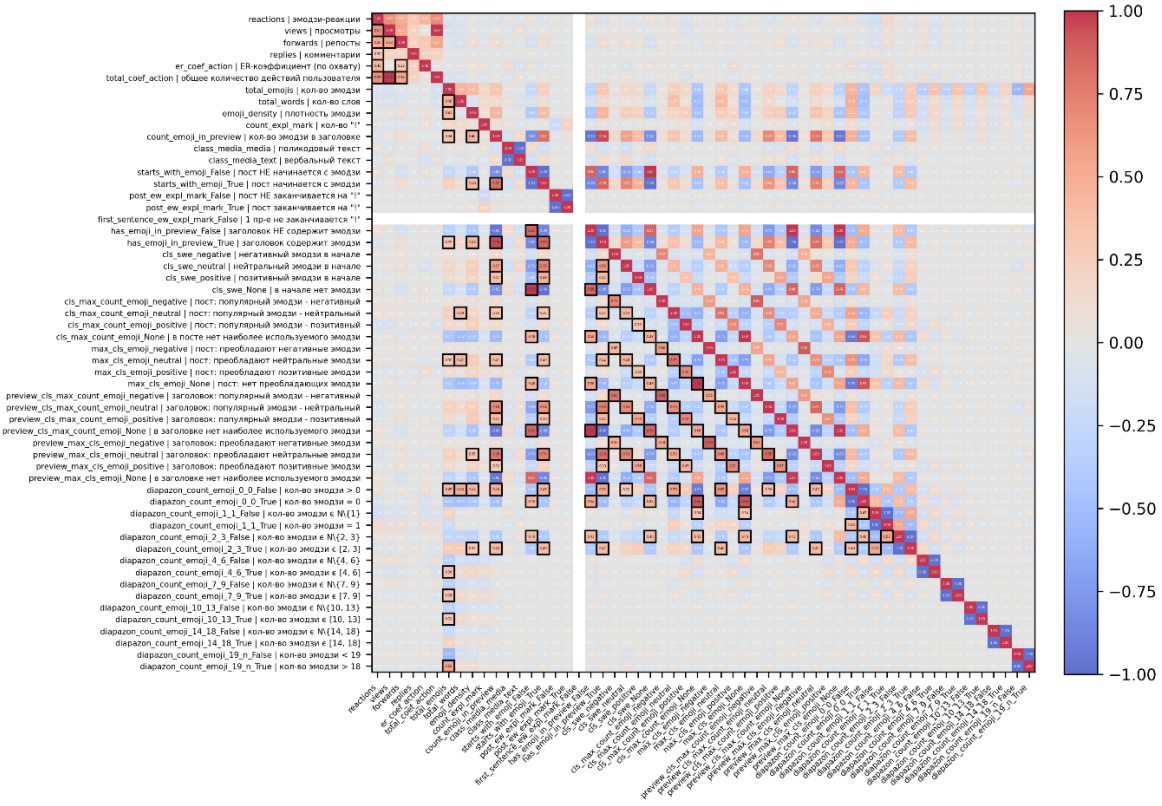


Рис.2. Полотно с отображением матрицы и коэффициентами умеренной и сильной корреляции

В рамках анализа полученных результатов были сделаны выводы и составлена таблица 1.

ТАБЛИЦА 1. Результат анализа наиболее значимых коэффициентов корреляции

Метрика 1	Метрика 2	|r|	Примечание
Общие закономерности			
«пост НЕ начинается с эмодзи»	«в начале нет эмодзи»	1,0	Если пост не начинается с эмодзи, то в нем гарантированно нет эмодзи в начале
Метрика 1	Метрика 2	|r|	Примечание
«просмотры»	«общее количество действий пользователя»	1,0	Высокие просмотры всегда связаны с большим количеством эмодзи-реакций, репостов и комментариев
Эмодзи в заголовке			
«заголовок содержит эмодзи»	«заголовок: преобладают нейтральные эмодзи»	0,83	Если в заголовке есть эмодзи, то они чаще всего нейтральные
«количество эмодзи в заголовке»	«заголовок содержат эмодзи»	0,96	Количество эмодзи напрямую влияет на наличие эмодзи в заголовке
«заголовок содержит эмодзи»	«пост начинается с эмодзи»	0,86	Посты, которые имеют в заголовке эмодзи чаще содержат их в самом начале
Наполнение эмоциональной окраской текста с помощью эмодзи			
«пост: популярный эмодзи – негативный»	«заголовок: популярный эмодзи – негативный»	0,89	Если в посте популярен негативный эмодзи, то и в заголовке он тоже будет частым. Аналогичные метрики, связанные с «позитивными» эмодзи, демонстрируют |r|=0,72
«негативный эмодзи в начале»	«заголовок: популярный эмодзи – негативный»	0,80	Преобладание негативного эмодзи в заголовке поста сильно связано с негативным эмодзи в начале поста
«заголовок: популярный эмодзи – нейтральный»	«заголовок: преобладают нейтральные эмодзи»	0,85	Наличие нейтрального эмодзи как самого популярного в посте влияет на преобладание нейтральных эмодзи во всем посте
«нейтральный эмодзи в начале»	«заголовок: преобладают нейтральные эмодзи»	0,73	Наличие нейтрального эмодзи в начале поста (первым символом) влияет на преобладание нейтральных эмодзи в заголовке
Влияние на вовлеченность			
«эмодзи-реакции»	«просмотры»	0,67	Посты с эмодзи-реакциями чаще получают просмотры
«просмотры»	«репосты»	0,53	Репосты коррелируют с просмотрами. Но слабее зависят от ER-коэффициента (показатель интереса, проявленного к контенту со стороны всех пользователей) – 0,32

Проведенный анализ позволяет сделать следующие выводы. Аудитория предрасположена совершать действия, демонстрирующие вовлеченность (выбирать эмодзи-реакции, пересылать пост и комментировать). Причем с ростом количества просмотров количество данных действий также увеличивается. Эмодзи в заголовке чаще нейтральные и имеют положение первого символа поста (даже если их несколько, один из них скорее всего стоит в начале). В структуре новостных постов сохраняется стилистика и эмоциональная окрашенность всего поста (тональность эмодзи заголовка и всего поста совпадает). Наличие негативного эмодзи, как наиболее встречающегося в посте, указывает на его положение первым символом, что может говорить о том, что негативные эмодзи принято использовать в начале поста, не перегружая остальной текст и не отвлекая внимание читателей от изначально проявленного (первым символом) негатива. Данный факт подтверждается тем, что нейтральные (например: ★, ✈, →) (а в иных случаях и негативные, позитивные) эмодзи используются в изоляции от других тональностей для того, чтобы сохранять настроение читателя. Действия пользователей (репосты, комментарии, эмодзи-реакции и просмотры), характеризующие вовлеченность аудитории, коррелируют между собой. И при этом значительно хуже зависят от посторонних факторов. Значительнее оказывается то, что вызванный интерес у читателя к новостному посту, способствует репосту другому пользователю и отметке эмодзи-реакцией этого поста. Наличие в посте количества эмодзи в диапазоне от 2 до 3 чаще указывает на нейтральную тональность заголовка. При этом повышение количества эмодзи в посте отвлекает внимание пользователей и вызывает недоверие к контенту (эффект контрфасцинации).

В заключение отметим, что наличие результатов проведенного анализа способствует выявлению основных закономерностей применения эмодзи для привлечения внимания и усиления определенной тональности текста. Однако для полного выявления влияния фасцинации на вовлеченность аудитории необходимо дополнить эксперимент комплексным анализом фасцинации вербального, контекстуального и универсального характера и рассмотреть все показатели в совокупности и в контрасте. Предполагается, что анализ всех аспектов воздействия на реципиента с применением фасцинативных сигналов различного уровня позволит получить результаты, более точно отражающие реальные условия.

Список используемых источников

1. Информационно-психологическое противоборство в войне: история, методология, практика: учебник для курсантов и студентов вузов / А. Г. Караяни, Ю. П. Зинченко. Москва: МГУ, 2007. 172 с.

2. Зарипов, Р. И. Фасцинативный эксперимент: замысел, содержание, результаты / Р. И. Зарипов. // Политическая лингвистика. 2024. № 2 (104). С. 66-84.

3. Комсомольская правда: KP.RU // Telegram. URL: https://t.me/truekpru (дата обращения 26.04.2024).

УДК 330.47

А. И. Клюев (студент группы ЭМ-22, СПбГУТ), kluev.ai@sut.ru
А. С. Павлова (студент группы ЭМ-22, СПбГУТ), pavlova1.as@sut.ru

ВЛИЯНИЕ НЕЙРОМАРКЕТИНГА НА ДИНАМИКУ ПРОДАЖ РОССИЙСКИХ КОМПАНИЙ

В статье рассматривается развитие нейромаркетинга в России как междисциплинарного подхода, направленного на изучение подсознательных реакций потребителей. Анализируются успешные кейсы внедрения технологий в компаниях (Сбербанк, «Билайн», Тинькофф), где использование нейромаркетинга позволило повысить конверсию, улучшить пользовательский опыт и увеличить продажи. Акцентируется внимание на необходимости интеграции нейронаучных методов в маркетинговые стратегии для повышения эффективности взаимодействия с клиентом, а также на вызовах, ограничивающих массовое распространение подхода: высокой стоимости исследований, этических вопросах и адаптации методов к локальным рынкам. Статья подчеркивает, что нейромаркетинг становится ключевым инструментом для повышения конкурентоспособности бизнеса в условиях цифровой трансформации экономики.

нейромаркетинг, UX-исследования, геймификация, NUDGE, поведенческий маркетинг, психографика, динамика продаж

THE IMPACT OF NEUROMARKETING ON THE SALES DYNAMICS OF RUSSIAN COMPANIES

Klyuev A., Pavlova A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article examines the development of neuromarketing in Russia as an interdisciplinary approach aimed at studying the subconscious reactions of consumers. Successful case studies of technology implementation at companies (Sberbank, Beeline, Tinkoff) are analyzed, where the use of neuromarketing has increased conversion, improved user experience, and increased sales. The article focuses on the need to integrate neuroscientific methods into marketing strategies to improve customer engagement, as well as on the challenges that limit the widespread adoption of this approach: the high cost of research, ethical issues, and the adaptation of methods to local markets. The article emphasizes that neuromarketing is becoming a key tool for enhancing business competitiveness in the context of digital economic transformation.

Key words: *neuromarketing, UX research, gamification, NUDGE, behavioral marketing, psychographics, sales dynamics*

Нейромаркетинг – междисциплинарная область, объединяющая нейробиологию, психологию и маркетинг, направленная на изучение подсозна-

тельных реакций потребителей для прогнозирования и управления их поведением. Основная гипотеза нейромаркетинга заключается в том, что до 90 % решений о покупке принимаются на бессознательном уровне (Zaltman, 2003), что делает традиционные методы (опросы, фокус-группы) недостаточно точными из-за когнитивных искажений.

Ключевая цель нейромаркетинга – выявление паттернов мозговой активности, эмоций и физиологических реакций, связанных с восприятием брендов, рекламы или продуктов. [1]

На сегодняшний день рынок нейромаркетинга России представлен пятью лабораториями:

1. NEUROTREND.
2. Nielsen.
3. Лаборатория Мозга.
4. Центр прикладной нейроэкономики и поведенческих исследований CNBR.
5. Z&G Branding [2].

Данные лаборатории проводят нейромаркетинговые исследования с помощью электроэнцефалографии (ЭЭГ), функциональной магнитно-резонансная томографии (фМРТ), айтрекинга (отслеживание движений глаз), биометрических датчиков (например, GSR (кожно-гальваническая реакция), частота сердечных сокращений и дыхания, ФЭГ (фациальная электрография), анализа эмоций с помощью ПО (например, Microsoft Azure Emotion API), а также комбинированных методов (опросы + нейроданные) [3].

Динамика развития рынка нейромаркетинга в России представлена на рис. 1 (составлено автором на основе [2]).

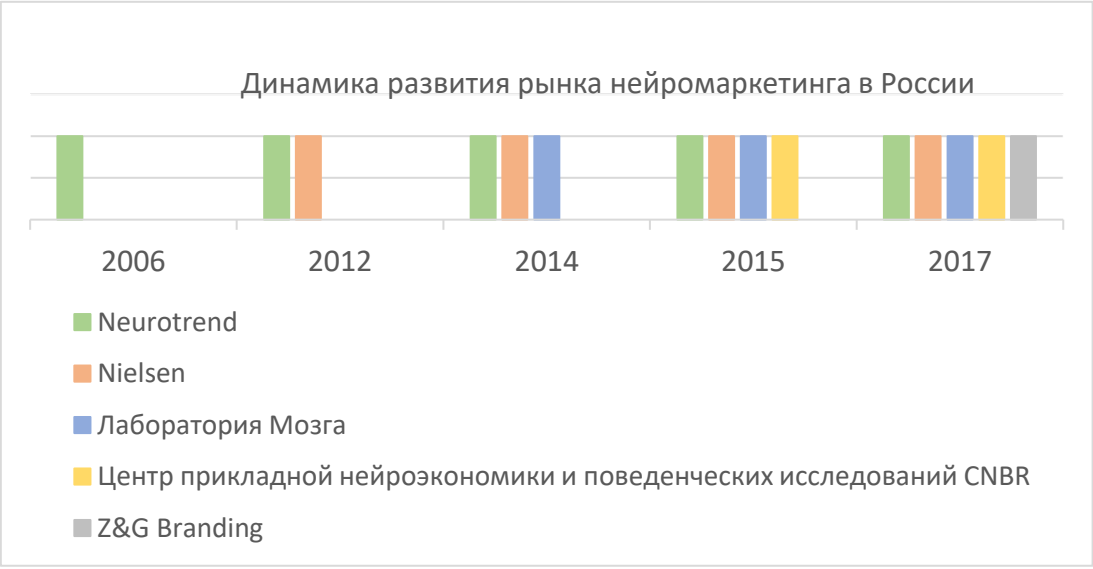


Рис. 1. Динамика развития рынка нейромаркетинга в России

В России нейромаркетинг набирает обороты, хотя часто его называют иначе, используя термины вроде UX-исследований, геймификации, NUDGE, поведенческого маркетинга, психографики или анализа данных о поведении.

Крупнейшие компании, такие как банки, телеком-операторы, организации розничной торговли, производства и IT-компании, активно применяют нейромаркетинговые исследования и смежные методы. Основные направления работы включают в себя анализ эмоциональных реакций потребителей (психографика), исследования пользовательского опыта (UX) и применение специализированных инструментов нейромаркетинга. Чтобы лучше понимать своих клиентов, многие лидеры рынка открывают собственные лаборатории, специализирующиеся на нейромаркетинге и UX. Так, Сбербанк использует психографический анализ для выстраивания эффективной коммуникации с клиентами, что стало основой для развития их клиентского бизнеса. Внедрение технологий анализа поведения в социальных сетях позволило Сбербанку в 2017 году сэкономить 50 миллионов долларов, о чем сообщил Герман Греф на Всемирном экономическом форуме в Давосе.

Андрей Кислов, основатель FasTest и бывший CEO Brain Company, подтверждает, что крупные корпорации из банковской сферы, FMCG, IT, телекоммуникаций и ритейла активно используют нейромаркетинг. Среди них такие компании, как «Альфа-Банк», «Газпромбанк» и Mail.ru Group. Однако, А. Кислов утверждает: «Нейромаркетинг позволяет получить более точную информацию непосредственно из мозга респондента, а такие услуги достаточно дорогие и по-своему экзотические для применения в ежедневной практике». Основатель FasTest добавляет: «Нейромаркетинг – это инструмент, которым можно пользоваться для решения каких-то конкретных задач, но не каждый день. Поэтому подобные исследования в России пока не очень востребованы».

Владимир Жолобов, директор Z&G.Branding, подтверждает популярность нейромаркетинговых исследований: «Билайн» использует айтрекинг, Borjomi Russia и «Черкизово» проводят комплексные нейромаркетинговые исследования своих рекламных роликов. В компании Z&G. Branding для крупного производителя специй проводили тестирование старой и новой упаковки и делали сравнение с конкурентами».

Для своего мобильного приложения «Альфа-Банк» провел нейромаркетинговое исследование. Мария Гончарова, руководитель центра развития электронных продуктов и сервисов для розничных клиентов «Альфа-

Банка», пояснила: «Мы определяли факторы UX и UI дизайна, которые негативно влияют на впечатления новых клиентов при первом использовании приложения». Целью исследования было выявить возможности для улучшения приложения, используя объективные данные о пользователях. В ходе исследования были определены сценарии, вызывающие у пользователей когнитивную нагрузку и негативные эмоции, что негативно сказывается на вероятности повторного использования приложения. В результате банк получил возможность сосредоточиться на системных улучшениях, а не только на локальных изменениях.

Согласно результатам исследования Mail.Ru Group, посвященного игре «Planet of Heroes», для проекта были сформулированы конкретные предложения по оптимизации. К ним относится: минимизация элементов, не способствующих вовлеченности игрока, исключение излишне навязчивых компонентов, сокращение диалоговых сцен, увеличение времени проведения дуэлей, а также точечное добавление музыкального сопровождения. Параллельно компания Mail.Ru Group приступила к применению нейромаркетинговых технологий для оценки эффективности своих рекламных роликов. [4, 5].

Использование подходов нейромаркетинга привело к росту продаж кредитных продуктов в Сбербанке на 30 %. В то же время улучшенная таргетированная реклама и кастомизация UX/UI-интерфейса мобильного приложения способствовали росту удержания и вовлечения клиентов.

Благодаря нейромаркетинговым исследованиям, по результатам которых была проведена оптимизация и кастомизация UX/UI-интерфейсов сайта и мобильного приложения, Т-Банк смог увеличить количество открытых счетов на 25 %.

Компания «Л'Этуаль» зафиксировала рост продаж на 20 % в течение трех месяцев после внедрения новых PR-стратегий и изменения дизайна упаковки. Благодаря визуальному анализу дизайна, компания «Л'Этуаль» смогла повысить привлекательность продукции, выявив ключевые факторы, которые вызывают положительные эмоции у целевой аудитории.

Компания «Билайн» смогла добиться 30 % роста конверсии за три месяца, когда запустила новый тарифный план, использующий айтрекинг и ЭЭГ [4].

Демонстрация увеличения конверсии после внедрения инструментов нейромаркетинга в российских компаниях представлена на рисунке 2 (составлен автором на основе [4]).

Рис. 2. Демонстрация увеличения конверсии после внедрения нейромаркетинговых инструментов в российских компаниях

Российский рынок нейромаркетинга демонстрирует уверенный рост и все более широкое применение в различных отраслях, включая банковский сектор и телекоммуникации. Несмотря на то, что сами технологии и методики часто маскируются, их влияние на бизнес-процессы становится все более явным. Ярким примером является Сбербанк, который благодаря внедрению психографического анализа и поведенческих моделей достиг существенной экономии и повышения эффективности.

Успешный опыт таких компаний, как «Альфа-Банк», «Билайн», «Тинькофф», «Л’Этуаль» и Mail.ru Group, подтверждает потенциал нейромаркетинга в увеличении конверсии, росте продаж, улучшении пользовательского опыта и повышении лояльности клиентов.

Тем не менее, высокая стоимость, сложность технологий и этические вопросы, связанные с воздействием на психику потребителей, пока ограничивают его применение нишевыми проектами или задачами, требующими глубокого анализа поведения аудитории.

Список используемых источников

1. Аузана А. А., Колесова В. П., Герасименко В. В., Тутова Л. А. Инновационное развитие экономики России: междисциплинарное взаимодействие. Седьмая международная научная конференция; Москва, МГУ имени М. В. Ломоносова, экономический факультет, 2014. 680 с.

2. Развитие нейромаркетинга в России // cyberleninka.ru. URL: https://cyberleninka.ru/article/n/razvitie-neyromarketinga-v-rossii (дата обращения 25.04.2025).

3. Тенденции и перспективы нейромаркетинга в построении бренда// Апни. URL: https://apni.ru/article/6081-tendenczii-i-perspektivy-nejromarketinga-v-postroenii-brenda (дата обращения 21.04.2025).

4. Кто в России занимается нейромаркетингом и кому можно доверить свои исследования // рубейс. URL: https://rb.ru/longread/neuromarketing-companies/ (дата обращения 25.04.2025).

5. Нейромаркетинг и его применение в российском бизнесе // vc.ru. URL: https://vc.ru/marketing/1166148-neiromarketing-i-ego-primenenie-v-rossiiskom-biznese (дата обращения 25.04.2025).

Статья представлена научным руководителем, и. о. заведующего кафедрой ЭД СПбГУТ, кандидатом экономических наук, доцентом Калимуллиной О. В.

УДК 338.47

В. В. Макаров (д.э.н., профессор, профессор кафедры экономики данных СПбГУТ)
А. А. Симонова (студентка группы БИМ-41з, СПбГУТ), simonova.aa@sut.ru

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ИЗМЕНЕНИЕ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ

Искусственный интеллект (ИИ) стал ключевым драйвером трансформации бизнес-процессов в России, оптимизируя рутинные операции, улучшая аналитику и персонализацию услуг. В докладе анализируются кейсы внедрения ИИ в российских компаниях (Сбер, Ozon, Т-Банк), выделяются ключевые тренды, а также барьеры. На основе данных исследований доказывается, что ИИ повышает эффективность бизнеса, но требует адаптации управленческих моделей. К тому же, при внедрении ИИ компании сталкиваются с различными ограничениями.

искусственный интеллект, бизнес-процессы, автоматизация, цифровая трансформация

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CHANGING A COMPANY'S BUSINESS PROCESS

Makarov V., Simonova A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Artificial intelligence (AI) has become a key driver of the transformation of business processes in Russia, optimizing routine operations, improving analytics and personalization of services. The report analyzes the cases of AI implementation in Russian companies (Sber, Ozon, T-Bank), highlights key trends, as well as barriers. Based on these studies, it is proved that AI improves business efficiency, but requires adaptation of management models. In addition, companies face various limitations when implementing AI.

Key words: *artificial intelligence, business processes, automation, digital transformation*

Цифровая трансформация экономики делает искусственный интеллект ключевым инструментом перестройки бизнес-процессов. Актуальность исследования обусловлена необходимостью адаптации предприятий к новым технологическим реалиям, где конкурентоспособность зависит от скорости внедрения инноваций. ИИ оптимизирует рутинные операции, снижая затраты [1, 2]. Как отмечает Зенкина Е. В., цифровые технологии, включая ИИ, становятся основой для повышения эффективности управления бизнес-

процессами, особенно на малых и средних предприятиях, где автоматизация критически важна для сохранения конкурентоспособности [1].

Внедрение ИИ позволяет решать комплексные задачи: от прогнозирования спроса до автоматизации производства. Однако между крупными компаниями и малым бизнесом сохраняется «цифровой разрыв» из-за нехватки ресурсов и экспертизы. Это усиливает неравенство в доступе к технологиям, требуя адаптивных стратегий интеграции ИИ [3, 4]. Башаратьян М. М. подчеркивает, что российские промышленные предприятия отстают от зарубежных конкурентов в цифровизации, что создает угрозы экономической безопасности и снижает устойчивость развития [4].

В рамках исследования будут изучены теоретические основы искусственного интеллекта, изучен опыт российских компаний во внедрении искусственного интеллекта, выявлены факторы успешной интеграции ИИ, будут сформированы советы по успешной интеграции ИИ в бизнес-процессы.

Данное исследование включает разносторонние методы:

1. Теоретические методы:

- системный анализ научной литературы, нормативных документов и кейсов внедрения ИИ;
- сравнительный анализ подходов к цифровизации бизнес-процессов в компаниях разного масштаба и отраслей.

2. Эмпирические методы:

- кейс-стади предприятий, успешно интегрировавших ИИ, для выявления лучших практик и проблем.

3. Синтетические методы:

- разработка рекомендаций на основе синтеза теоретических выводов и эмпирических данных;
- оценка экономической и управленческой целесообразности предложенных решений с помощью SWOT-анализа.

В таблице 1 представлены примеры бизнес-процессов, которые могут быть автоматизированы с помощью искусственного интеллекта. Для составления таблицы были проанализированы реальные кейсы российских компаний.

ТАБЛИЦА 1. Примеры внедрения ИИ в бизнес-процессы

Бизнес-процесс	Что может ИИ	Пример внедрения	Эффект
Управление данными	Анализ больших данных, прогнозирование трендов	Сбер: ИИ-алгоритмы для аналлиза транзакций	Ускорение обработки данных
Маркетинг	Персонализация рекламы, генерация контента	Ozon: создание описаний товаров с помощью YandexGPT	Рост конверсии
Продажи	Чат-боты для клиентов, прогнозирование спроса	Т-Банк: ИИ-ассистент для обработки заявок	Снижение загрузки колл-центра
Логистика	Оптимизация маршрутов, управление запасами	Wildberries: прогнозирование поставок	Сокращение логистических затрат
Финансы	Кредитный скоринг, обнаружение мошенничества	Альфа-Банк: ИИ-скоринг	Снижение рисков
HR	Подбор кандидатов	hh.ru: ИИ-фильтрация резюме	Ускорение подбора персонала
Клиентский сервис	Голосовые ассистенты	МТС: голосовой робот поддержки	Уменьшение времени ответа

Изученная литература описывает данные кейсы как кейсы успешной интеграции искусственного интеллекта. Однако, в различных источниках упоминаются и проблемы [5], с которыми сталкиваются компании при интеграции ИИ, они представлены в таблице 2.

ТАБЛИЦА 2. Проблемы внедрения ИИ в бизнес-процессы

Проблема	Описание
Кадровый дефицит	Нехватка специалистов, высокая стоимость оплаты их труда
Технологические барьеры	Нехватка вычислительных мощностей, многие системы не адаптированы для российской специфики
Организационные и стратегические ошибки	Интеграция ИИ в нестратегические процессы, что мешает их масштабированию; “галлюцинирование” нейронных сетей
Регуляторные и этические риски	Нехватка правового регулирования, безопасность данных, предвзятость программы (например, при подборе персонала)
Отраслевая специфика	Не учтена отраслевая специфика (в логистике, ритейле и т.д.)

Данная работа демонстрирует, что ИИ – это не будущее, а настоящая реальность российского бизнеса, требующая адаптации управленческих моделей и инвестиций в кадры. Исследование направлено на решение актуальной проблемы трансформации бизнес-процессов предприятий под влиянием технологий искусственного интеллекта. В работе поставлена цель, для достижения которой решались задачи анализа теоретических основ, оценки практических кейсов, разработки адаптивных стратегий и рекомендаций по минимизации рисков.

Список используемых источников

1. Зенкина Е. В. Стратегии и методы цифровой трансформации бизнеса и их использование в процессах управления компаниями // Наука и искусство управления. 2023. № 1. С. 10–25. DOI:10.28995/2782-2222-2023-1-10-25.

2. Guru. Стратегия цифровой трансформации: Полное руководство для бизнес-руководителей. 2025. URL: https://www.getguru.com/ru/reference/digital-transformation-strategy (дата обращения 24.04.2025).

3. Башаратьян М. М. Цифровизация как источник обеспечения устойчивого развития российской промышленности в условиях инновационной экономики // Экономический журнал. 2023. URL: https://1economic.ru/lib/113453.

4. 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.

5. Куприяновский В. П. и др. Принятие решений в цифровой экономике: Опыт Великобритании // International Journal of Open Information Technologies. 2017. № 4. С. 63–73.

УДК 330.47

Д. А. Пантелеев (студент группы ЭМ-22, СПбГУТ), panteleev.da@sut.ru
А. А. Шумельная (студент группы ЭМ-22, СПбГУТ)

АНАЛИЗ ТРАНСФОРМАЦИИ ЭКОСИСТЕМЫ ПАО «МТС»

В статье рассматривается трансформация ПАО «МТС» из телекоммуникационной компании в одну из ведущих цифровых экосистем России. Исследуются стратегия и ключевые направления экосистемы, анализируются финансовые и операционные показатели компании. Акцентируется внимание на необходимости повышения жизненного цикла взаимодействия с клиентом для увеличения эффективности и конкурентоспособности компаний. Отражены структурные изменения, включая переход к холдинговой модели управления и консолидацию нетелекоммуникационных бизнесов.

цифровая экосистема, платформа, цифровые сервисы, трансформация, развитие, стратегия

ANALYSIS OF THE TRANSFORMATION OF THE PJSC MTS ECOSYSTEM

Panteleev D., Shumelnaya A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article examines the transformation of PJSC MTS from a telecommunications company into one of Russia's leading digital ecosystems. The article examines the ecosystem's strategy and key areas, and analyzes the company's financial and operational performance. It emphasizes the need to enhance the customer interaction lifecycle to increase efficiency and competitiveness. Structural changes are reflected, including the transition to a holding management model and the consolidation of non-telecommunications businesses.

***Key words**: digital ecosystem, platform, digital services, transformation, development, strategy*

В последние годы наблюдается тенденция к смещению приоритетов крупных компаний от оказания узкоспециализированных услуг к формированию многофункциональных цифровых платформ. Данное направление развития обусловлено необходимостью удержания клиента и повышения жизненного цикла взаимодействия с ним. Ключевым элементом такого подхода становится экосистема – бесшовная цифровая среда, объединяющая сервисы, которые представлены на различных сегментах рынка, вокруг одной компании.

С 2019 года МТС последовательно реализует стратегию CLV 2.0 (Customer Lifetime Value 2.0), проходя трансформацию от компании, предо-

ставляющей телекоммуникационные услуги, до одной из ведущих цифровых экосистем в России. В соответствии с данной стратегией компания стремится увеличить время взаимодействия клиентов с брендом посредством разнообразных цифровых продуктов и услуг [1].

С 2021 по 2023 гг. инвестирование в разработку и развитие экосистемных продуктов обрело огромные масштабы, что неминуемо отразилось на финансовых и операционных показателях компании (рис. 1, 2).

Рис. 1. Общая выручка и чистая прибыль МТС в млрд. руб. за 2021-2023гг. [2]

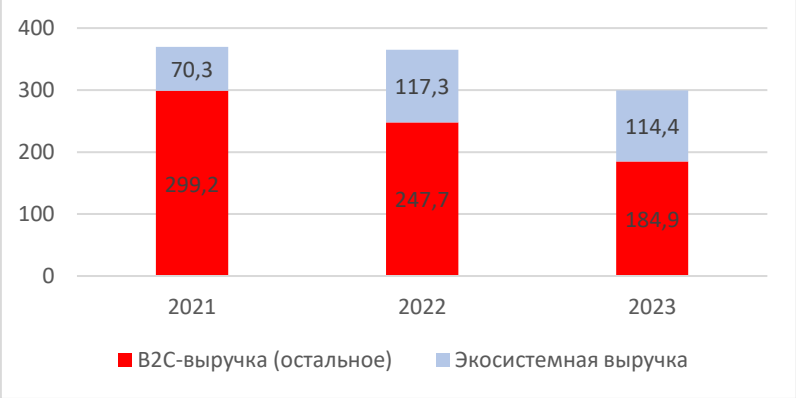


Рис. 2. Доля экосистемной выручки МТС в общей B2C-выручке 2021, 2022, 2023 гг. [2]

К 2023 г. экосистема МТС значительно расширила линейку самостоятельных, но взаимосвязанных цифровых сервисов, сгруппированных по следующим направлениям:

- Телеком – основной бизнес компании. Включает мобильную связь, домашний интернет и цифровое телевидение, а также обеспечивает широкую клиентскую базу.
- Финансовые технологии – «МТС Банк», «МТС Pay», «МТС Все страховки», фокус на цифровом банкинге и финансовых сервисах.
- Медиа и развлечения – онлайн-кинотеатр «KION», видеоплатформа «Nuum», «МТС Музыка», «МТС Fog Play» для облачного гейминга, онлайн-библиотека «Строки» и сервис по продаже билетов «МТС Live».

● Мобильность и транспорт – сервис для аренды самокатов и велосипедов «Юрент».

● IT-направления – МТС Digital, МТС AI, МТС Big Data и CloudMTS.

Одним из приоритетных векторов экосистемного развития МТС стало медиа-направление. Основные акценты были сделаны на:

● трансформацию онлайн-кинотеатра «KION» в полноценный развлекательный медиасервис;

● существенное увеличение аудитории и рост ее вовлеченности;

● применение технологий Big Data для персонализации интерфейса и улучшения алгоритмов рекомендаций.

Так, аудитория «KION» к концу 2023 года достигла 7,6 миллиона пользователей, что на 15 % выше, чем в 2022 году, а общее количество просмотров контента на платформе превысило 750 миллионов. Подобные действия привели к увеличению выручки МТС Медиа на 18,3 % по сравнению с 2022 годом [3].

Также компания добилась значительных успехов в развитии нового продукта «МТС Travel», благодаря ряду решений, таких как: AI-подбор туров, расширение базы отелей включая эксклюзивные варианты размещений, рассрочку под 0 % при оплате через «МТС Банк» и специальную опцию для экономии на мобильной связи за границей. Таким образом, сервис для бронирования отелей стал одним из самых быстрорастущих сервисов экосистемы за счет синергии с другими продуктами компании.

В 2023 году ПАО «МТС» продемонстрировала наибольшую активность среди российских B2C-экосистем, выступив лидером по приобретению и запуску новых сервисов, тем самым укрепив свои позиции как одной из крупнейших российских экосистем.

По итогам года все ключевые направления экосистемы продемонстрировали устойчивую положительную динамику, что свидетельствует о высоком спросе со стороны пользователей и подтверждает актуальность выбранной стратегии трансформации компании в цифровую экосистему с широкой линейкой сервисов (рис. 3).

В конце 2024 года компания МТС заявила о переходе к холдинговой структуре, тем самым продолжив трансформацию бизнеса. Нетелекоммуникационные бизнесы теперь сосредоточены под управлением нового юридического лица – «Экосистема МТС». Все IT-направления группы объединяются под брендом МТС Web Services (MWS).

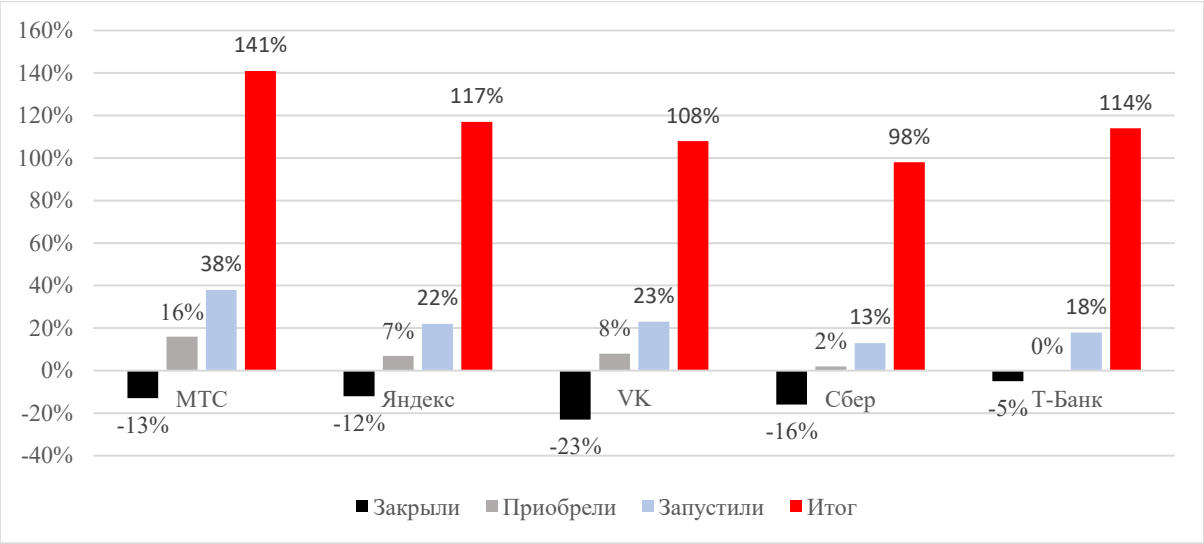


Рис. 3. Динамика наполнения экосистем в 2022–2023 гг.
(изменение в % от общего числа сервисов на начало 2022 г.) [2]

Переход на холдинговую структуру является естественным этапом для зрелой экосистемы, так как появляется возможность привлечь внешнее финансирование проведя IPO. МТС готовит к размещению на бирже компании «AdTech» и «Юрент», поскольку уже имеет положительный опыт привлечения денежных средств через публичное размещение акций «МТС-Банка» на Московской бирже, которое принесло 11,5 миллиарда рублей [4].

В 2024 году ПАО «МТС» продемонстрировала значительный прогресс в развитии своей цифровой экосистемы, количество клиентов выросло на 16 % по сравнению с предыдущим годом и достигло 17,5 миллионов человек, а количество клиентов, использующих четыре или более продуктов экосистемы, увеличилось на 30 % (рис. 4). Экосистемная выручка, тем временем, возросла на 22 % [5].

Также МТС в 2024 году приняла решение о прекращении развития неэффективных направлений, таких как: «МТС Авто», «МТС Умный Дом» и видеосервис «Nuum» [10]. Данные проекты пришлось закрыть по причине их низкой рентабельности, ограниченного потенциала роста и несоответствия выбранной стратегии. Компания сосредоточилась на сокращении долга и перераспределении инвестиций в более перспективные направления.

МТС ожидает, что к 2026 году доля выручки от нетелекоммуникационных сегментов превысит 50 %, а общая выручка компании достигнет 1 триллиона рублей к 2027 году. Рост экосистемной клиентской базы, которая достигла 17,5 миллиона клиентов, свидетельствует о положительной динамике развития экосистемы [10].

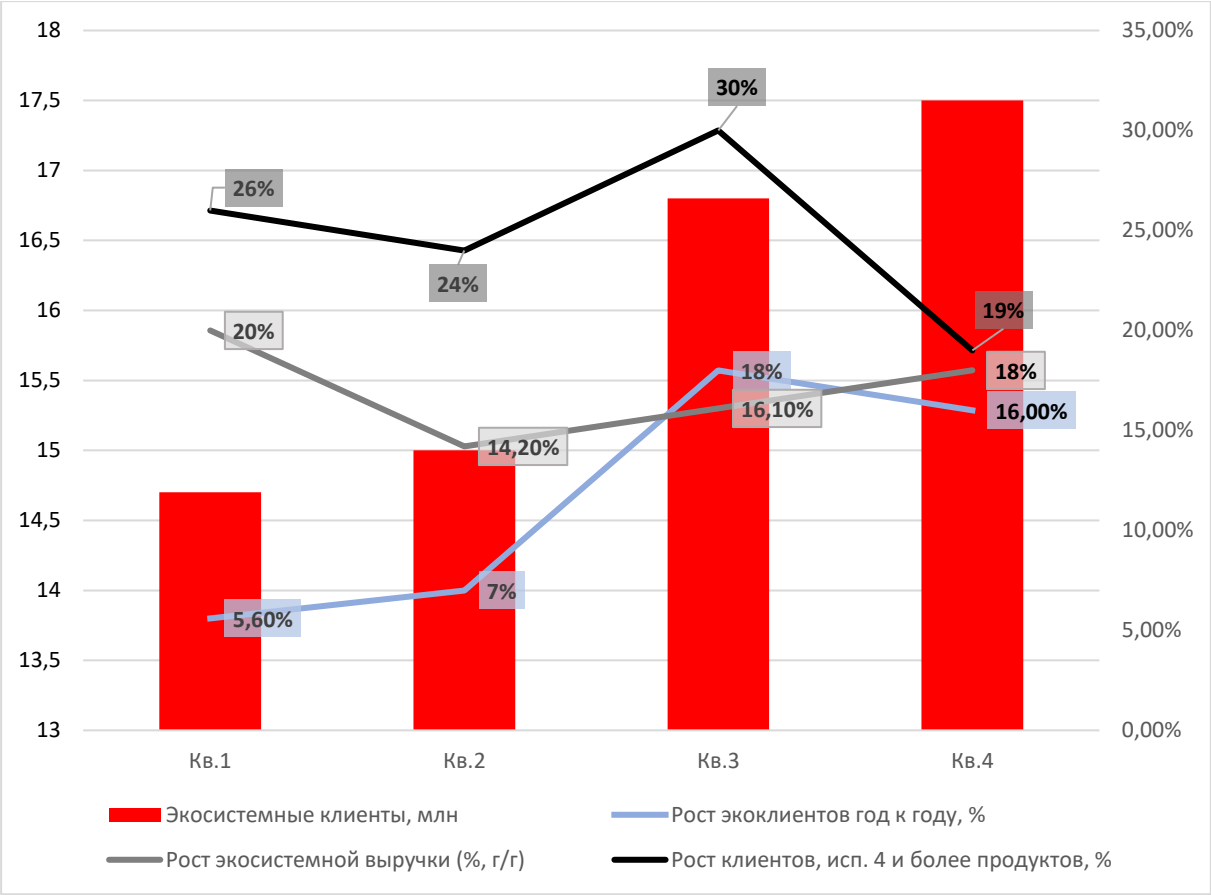


Рис. 4. Рост экосистемы МТС в 2024 году, г/г [6, 7, 8, 9]

Таким образом, ПАО «МТС» демонстрирует последовательную реализацию стратегии трансформации в мультисервисную цифровую экосистему с акцентом на развитие и капитализацию новых бизнес-направлений, что способствует укреплению позиций компании на рынке и созданию дополнительной акционерной стоимости.

Список используемых источников

1. ПАО «МТС». Годовой отчет за 2022 год // URL: https://ar2022.mts.ru/obzor-transformaczii-ekosistemy/nasha-strategiya/ (дата обращения 24.04.2025).

2. Яндекс.Диск. Файл // URL: https://disk.yandex.ru/i/xKCz-_rGNKJM1Q (дата обращения 24.04.2025).

3. ПАО «МТС». Годовой отчет за 2023 год // URL: https://ar2023.mts.ru/ (дата обращения 24.04.2025).

4. РБК. МТС выделит экосистемные активы в отдельные структуры // URL: https://www.rbc.ru/finances/26/04/2024/662b4b549a7947fdb75f9695 (дата обращения 24.04.2025).

5. ПАО «МТС». Финансовые и операционные результаты группы МТС за III квартал 2024 года // URL: https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2024-11-19/finansovye-i-operacionnye-rezultaty-gruppy-mts-za-3-kvartal-2024 (дата обращения 24.04.2025).

6. ПАО «МТС». Презентация финансовых результатов за I квартал 2024 года // URL: https://static.ssl.mts.ru/mts_rf/contents/10610/MTS_Q1_2024_Presentation.pdf (дата обращения 25.04.2025).

7. ПАО «МТС». Презентация финансовых результатов за II квартал 2024 года // URL: https://static.ssl.mts.ru/mts_rf/contents/10610/MTS_Q2_2024_Presentation_1109.pdf (дата обращения 25.04.2025).

8. ПАО «МТС». Наша стратегия. Годовой отчет за 2024 год // URL: https://ar2024.mts.ru/ekosistema-mts-vektory-i-rezultaty-razvitiya/nasha-strategiya/ (дата обращения 25.04.2025).

9. ПАО «МТС». Презентация финансовых результатов за III квартал 2024 года // URL: https://static.ssl.mts.ru/mts_rf/contents/10610/MTS_Q3_2024_Presentation_1910.pdf (дата обращения 25.04.2025).

10. ПАО «МТС». Презентация финансовых результатов за IV квартал 2024 года URL: https://static.ssl.mts.ru/mts_rf/contents/10610/MTS_Q4_2024_Presentation.pdf (дата обращения 25.04.2025).

Статья представлена научным руководителем, заведующим кафедрой ЭД СПбГУТ, кандидатом экономических наук, доцентом Калимуллиной О. В.

УДК 330.47

Я. В. Платонова (студент группы ЭМ-21, СПбГУТ), platonova.yv@sut.ru
Д. С. Суздалов (студент группы ЭМ-21, СПбГУТ), suzdalov.ds@sut.ru

ПРЕИМУЩЕСТВА И ОПАСНОСТИ ПРОГРАММ ЛОЯЛЬНОСТИ СТРАХОВЫХ КОМПАНИЙ

Актуальность темы определяется потребностью в совершенствовании нормативно-правовой базы страхового рынка в части стимулирования лояльности клиентов. Активное использование программ лояльности в страховании требует тщательного анализа преимуществ и рисков для поиска баланса между маркетинговыми инициативами страховщиков и защитой интересов потребителей от недобросовестных практик и поддержания финансовой устойчивости страховых компаний.

В условиях усиления конкуренции страховщики вынуждены бороться за клиентов, интегрируясь в экосистемы с банками (например, «Сбер», «Альфа»), медицинскими сервисами (например, «РЕСО»), и активно разрабатывать новые стратегии для долгосрочного удержания клиентов, применять демпинг тарифов, акции и кешбэк. Анализ популярных страховых компаний показал, что практически все компании уже имеют простые программы лояльности: кешбэк или бонусы. В докладе рассмотрены цели программ лояльности, приведена их классификация и показаны преимущества для стэйкхолдеров. Проанализированы негативные моменты для страхователей и угрозы для страхового бизнеса в целом, их возможные последствия и рекомендации по их предотвращению или снижению.

***Key words**: страховые компании, программы лояльности, бонусные программы, навязывание потребностей*

ADVANTAGES AND RISKS OF INSURANCE COMPANY LOYALTY PROGRAMS

Platonova Ya., Suzdalov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The relevance of this topic is determined by the need to improve the insurance market's regulatory framework for stimulating customer loyalty. The active use of loyalty programs in insurance requires a thorough analysis of the benefits and risks to find a balance between insurers' marketing initiatives and protecting consumers from unfair practices and maintaining the financial stability of insurance companies. In an increasingly competitive environment, insurers are forced to compete for customers by integrating into ecosystems with banks (e.g., Sber, Alfa) and medical services (e.g., RESO), and actively developing new strategies for long-term customer retention, including rate dumping, promotions, and cashback. An analysis of popular insurance companies revealed that almost all already have simple loyalty programs, such as cashback or bonuses. The report examines the objectives of loyalty programs, classifies them, and highlights the benefits for stakeholders. It also analyzes the negative impacts on policyholders and threats to the insurance industry as a whole, their potential consequences, and offers recommendations for preventing or mitigating them.

Insurance companies, loyalty programs, bonus programs, demand-driven behavior

Страхование, являясь одним из ключевых сегментов финансового рынка, призвано обеспечить защиту интересов граждан, предприятий и организаций от разнообразных рисков. Как механизм передачи риска финансовых потерь, страхование гарантирует юридическим и физическим лицам в случае наступления страхового случая материальную компенсацию, приносит пользу страхователям и обществу в целом и положительно влияет на социально-экономическую стабильность в государстве.

В настоящее время страховой рынок, как и другие финансовые виды деятельности, претерпевает значительные изменения. Цифровая трансформация экономики нашей страны и внедрение технологий безусловно оказывают влияние на отрасль страхования. Система регулирования вынуждена обновляться, чтобы соответствовать изменениям рынка и поддерживать финансовую стабильность.

Сегодня страховые агенты уже не обходят жителей домов в поисках желающих застраховаться. Страхование все больше переходит в онлайн формат, продажу полисов через банковские каналы, делая доступным и удобным заключение договоров страхования. Возросшая конкуренция среди страховщиков вынуждает их активно внедрять бонусные программы, скидки, кэшбеки для привлечения и удержания клиентов. Программы лояльности для потребителей, с одной стороны, усиливают их активность, но с другой стороны, создают угрозы для страхователей и усиливают их риски. Задачи регулятора в страховании – найти баланс между стимулированием лояльности клиентов и не допустить навязывания услуг, создать нормативную базу для защиты прав страховщиков и застрахованных лиц, обеспечить контроль за финансовой устойчивостью страховых компаний и стабильность страхового рынка в целом.

В последнее время прослеживается тенденция к созданию экосистем, выгодных и для страховых компаний – больше возможностей для роста и повышения прибыли, и для клиентов – удобство, экономия времени и персонализация услуг.

В условиях усиления конкуренции страховщики вынуждены бороться за клиентов, интегрируясь в экосистемы с банками (например, «Сбер», «Альфа»), медицинскими сервисами (например, «РЕСО»), и активно разрабатывать новые стратегии для долгосрочного удержания клиентов, применять демпинг тарифов, акции и кешбэк. Анализ популярных страховых компаний показал, что практически все компании уже имеют простые программы лояльности: кешбэк или бонусы.

Под кешбэком (от англ. cash back) принято понимать разновидность бонусной программы, когда часть потраченной суммы возвращается клиенту. Анализ рынка показывает, что в настоящее время страховые компании активно используют разнообразные программы с кешбэком (табл. 1).

Таблица 1. Примеры программ лояльности страховых компаний «Кешбэк»

Компания	Программа лояльности «Кешбэк»
Ренессанс Страхование	20 % при оплате каско картой «Мир» Максимальная сумма кешбэка 10000 руб.
АльфаСтрахование	Сервис лояльности Апельсин – при оплате «Апельсинками» до 50% стоимости полиса с покупок в Перекрестке и Пятерочке повышенный кешбэка на продукты питания в этих магазинах
АльфаСтрахование	Кешбэк 10% от стоимости полиса реальными деньгами полиса каско для аккуратных водителей Кешбэк до 50% от стоимости полиса ОСАГО
Т-банк	30% на ОСАГО и Каско (акция закончилась 31 марта, но еще можно получить 10%)
Совкомбанк страхование	Накопительное страхование жизни с кешбэком 25% от взноса
РенессансЖизнь	44 % от страхового взноса по договору страхования
Ингосстрах Банк	Накопительное страхование жизни «Копи с кешбэком» 35 %
Ингосстрах Банк	Программа лояльности «Cashback» для держателей банковских карт АО Ингосстрах Банк с разным вознаграждением в зависимости вида карты за покупки по картам
Банки.ру	Кешбэк до 50 % при оформлении полиса ипотечного страхования (предложение доступно до 24 февраля 2025 г.). Размер кешбэка зависит от банка, в которой оформлена ипотека
Банки.ру	Кешбэк до 100 % при оформлении полиса в Сбербанке на 2-й год

Одним из наиболее эффективных инструментов получения конкурентных преимуществ являются программы лояльности бренда – маркетинговые механизмы, направленные на мотивацию потребителей к новым и повторным покупкам через систему поощрений и вознаграждений.

Программы лояльности помимо скидок могут предоставлять разнообразные бонусы или иные формы вознаграждения, которые зависят от вида программы. На сегодня существует обширная линейка программ лояльности [1] (рис. 1). Однако их общая цель заключается в удержании клиентов за счет укреплении доверия и повышении интереса потенциальных потребителей к продуктам и услугам компании.

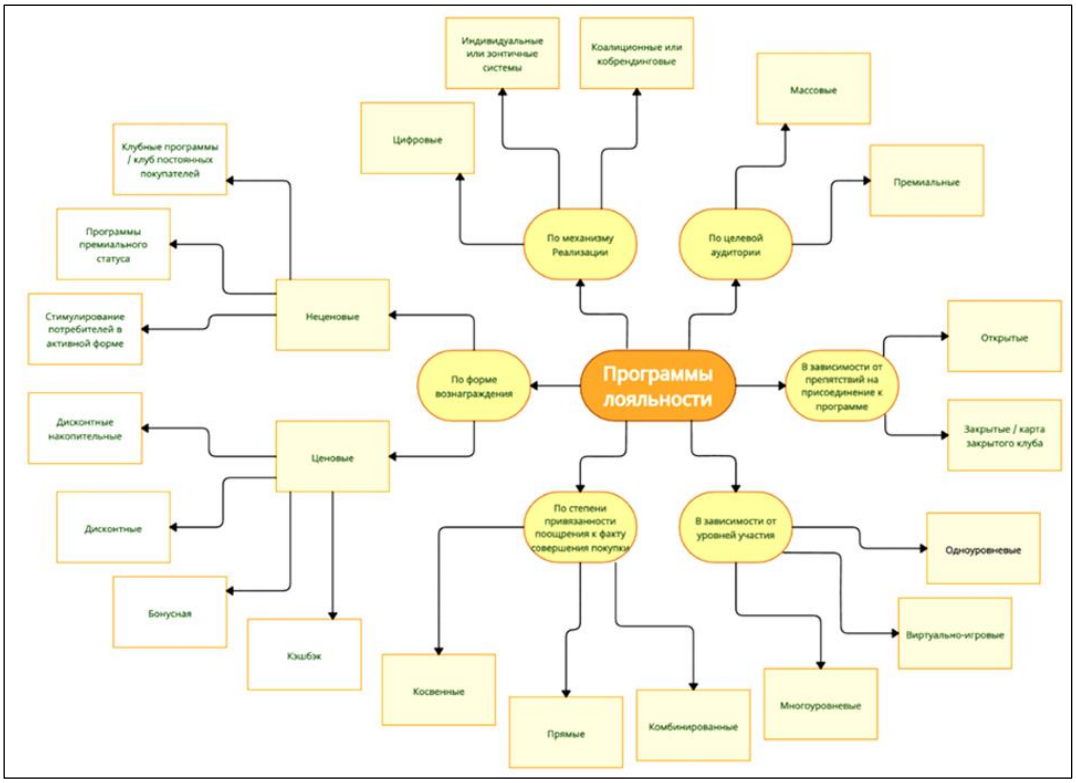


Рис. 1. Классификация программ лояльности

Компании могут выбирать для себя разные виды программ лояльности с возможностью дифференцировать преимущества для разных стейкхолдеров. Общим для всех видов программ лояльности является сбор данных о клиенте (так как они требуют регистрации) и формирование портрета клиента, что помогает компаниям лучше понимать своих клиентов и дает возможность персонализировать предложения.

Цели программ лояльности: снизить отток существующих и привлечь новых клиентов; снизить операционные издержки; повысить удовлетворенность клиентов и сформировать позитивное отношение к страховой компании; повысить узнаваемость бренда и выделиться среди конкурентов. Считается, что для страховых компаний лояльно настроенные клиенты менее чувствительны к цене, и они выгоднее за счет снижения затрат на привлечение новых клиентов [2].

При разработке и реализации программ лояльности следует учитывать не только преимущества, но и возможные негативные моменты для страхователей и угрозы для страхового бизнеса. Исследования компании Cap Gemini показали, что 89 % отзывов в соцсетях о программах лояльности являются негативными [3], что свидетельствует о несоответствии программ лояльности ожиданиям клиентов и требует вмешательства государства.

Мы считаем, что государственное регулирование программ лояльности в сфере страхования должно быть обязательным, чтобы не допустить злоупотреблений со стороны страховщиков и нарушения прав страхователей. Высокий процент негативных отзывов, фишинговые атаки и другие мошеннические схемы в онлайн-страховании, жалобы клиентов на обман с кешбэком [4], утечка персональных данных (свежий пример: в январе 2025 г. утечка уникальных адресов электронной почты и номеров телефонов 0,5 млн клиентов в «АльфаСтрахование-Жизнь»), мисселинг (продажа страховых продуктов под видом других финансовых услуг (например, ИСЖ под видом вклада) подчеркивают необходимость регулирования программ лояльности.

Но где заканчивается лояльность и начинается навязывание потребностей? Граница между этими понятиями проходит там, где интересы компании начинают превалировать над интересами клиента, когда мотивация к покупке перестает быть добровольной и осознанной. Различия данных явлений показаны в таблице 2.

Таблица 2. Сравнение признаков программы лояльности и навязывания потребностей

Программа лояльности	Навязанные услуги
Добровольность участия: клиент сам принимает решение – участвовать в программе или нет	Давление на клиента: использование агрессивных продаж, психологического давления со стороны продавцов, которые вызывают чувство срочности или страха упустить выгоду
Прозрачность условий: все условия программы четко прописаны: клиент понимает, что ему нужно сделать для получения «бонуса»	Скрытые условия: непрозрачные или замаскированные под выгодные предложения, чтобы ввести клиента в заблуждение
Ценность для клиента: бонусы и скидки действительно представляют ценность для клиента, а не являются формальностью	Манипуляция потребностями: компания создает у клиента ощущение дефицита или необходимость купить товар/услугу, даже если изначально клиент этого не планировал

Таким образом, перед Центробанком стоит важная задача – стимулировать конкуренцию и программы лояльности, направленные на удовлетворение реальных потребностей клиентов, и не допустить манипулирования потребностями клиентов ради увеличения прибыли страховых компаний любой ценой.

Цели регулирования программ лояльности: обеспечение честности, прозрачности и защиты интересов страхователей и контроль финансовой устойчивости страховщиков. Регулирование должно гарантировать добросовестное поведение на рынке страхования. Центробанк сформулировал 8 принципов добросовестного поведения на финансовом рынке: честность, справедливость, прозрачность, забота, безопасность, профессионализм, ответственность и целостность [5].

Итак, мы рассмотрели очевидные преимущества и проанализировали возможные риски и угрозы программ лояльности для всех участников рынка страхования, их возможные последствия и рекомендации по их предотвращению или снижению.

Обосновали необходимость регулирования таких программ в страховой деятельности. Именно регулятор должен найти тонкую грань между стимулированием лояльности и защитой от навязывания услуг, чтобы обеспечить стабильность, конкуренцию и доверие к страховой системе.

Список используемых источников

1. Калинина А. Е. Специфика программ лояльности, ее виды, оценка эффективности / А. Е. Калинина // Границы возможного в рекламном и PR-креативе: Сб. материалов Пятой Всероссийской (национальной) научно–практической конференции, Орел, 27 октября 2023 года. Орел: Российская академия народного хозяйства и государственной службы при Президенте РФ, 2024. С. 78-83.

2. Программы лояльности как неотъемлемая часть современного маркетинга. URL: https://cyberleninka.ru/article/n/programmy-loyalnosti-kak-neotemlemaya-chast-sovremennogo-marketinga (дата обращения 16.04.2025).

3. EcommerceCEO. The beginner’s guide to customer loyalty programs. URL: https://www.ecommerceceo.com/customer-loyalty-programs/ (дата обращения 16.04.2025).

4. Банки.ру. Обманули с кэшбэком за ОСАГО – отзыв о ВТБ от "user-413511703921". URL: https://www.banki.ru/services/responses/bank/response/11738567/ (дата обращения 17.04.2025).

5. Центральный Банк России. Методические рекомендации Банка России по применению основных принципов добросовестного поведения на финансовом рынке. URL: https://www.cbr.ru/Crosscut/LawActs/File/9969 (дата обращения 17.04.2025).

Статья представлена научным руководителем, доцентом кафедры ЭД СПбГУТ, кандидатом экономических наук Егоровой М. А.

УДК 687.016

Д. Е. Хитова (студент группы РСО-34 СПбГУТ), khitova.de@sut.ru

УСТОЙЧИВАЯ МОДА В ЭПОХУ ПЕРЕПРОИЗВОДСТВА

Решение проблемы экологического кризиса зависит от многих факторов. Мода стоит в числе самых масштабных сфер человеческой деятельности, которая обладает большим количеством отходов, вредящих всей экосистеме и здоровью человека. Устойчивая мода – новое явление, способное более осознанно подходить к потреблению и производству товаров, заботясь при этом об экологии, условиях труда рабочих и здоровье человека.

устойчивая мода, экология, перепроизводство, кризис

SUSTAINABLE FASHION IN THE ERA OF OVERPRODUCTION

Khitova D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The solution to the environmental crisis depends on many factors. Fashion is one of the largest areas of human activity, generating large amounts of waste that harms the entire ecosystem and human health. Sustainable fashion is a new phenomenon that enables a more conscious approach to the consumption and production of goods, while also taking care of the environment, working conditions, and human health.

Key words: *sustainable fashion, ecology, overproduction, crisis*

XXI век – время, когда игнорирование проблем мирового масштаба просто невозможно. Мода всегда являлась и будет оставаться частью жизни человека. Одежда – это инструмент, с помощью которого можно донести до мира о своих чувствах, позициях, амбициях и взглядах. Люди склонны показывать свою индивидуальность через одежду, которую они носят, комбинируют между собой или создают. В погоне за уникальность, которую предлагают потребителям бренды, и с развитием технологий производства появился fast fashion или «быстрая мода». Тренды в социальных медиаплатформах сменяются с огромной скоростью. Рекламные кампании психологически воздействуют на людей, убеждая их, что следование каждому тренду и новинкам сможет сделать их уникальными. Но это вовсе не так. Быстрая мода лишь порождает перепроизводство, эксплуатацию труда и низкокачественную одежду с целью угодить потребителю.

По данным на февраль 2025 года, индустрия моды ежегодно производит около 92 миллионов тонн текстильных отходов на планете. По информации исследования Lamoda, проведенного совместно с аналитическим агентством А2 в 2023 году, мужчины воспринимают покупку одежды как базовую необходимость и готовы тратить на это до 30 тыс. рублей в год, женщины – до 100 тыс. рублей. При этом, по данным исследования, большинство россиян (31%) обновляют гардероб раз в сезон, еще 21% делают это каждый месяц. Доступность и возможность выбора – это хорошо, но это не отменяет того факта, что потребление любого продукта должно оставаться осознанным [1].

Перепроизводство, равно как и перепотребление, стало разрушать границы системы нормального прагматического производства одежды. Люксовые бренды не раз были обвинены обществом в уничтожении своей же продукции в целях сохранения эксклюзивности бренда. Британский люксовый бренд Burberry сжег вещи из прошлых коллекций на 36,5 миллиона долларов, чтобы изделия не попадали в руки «не тех людей». Таким же методом сохранения имиджа пользуется французский бренд Louis Vuiton, сжигая свои сумки, а не продавая их за более низкую цену. Представители бренда объясняют, что продукцию бренда должны покупать все за одинаково высокую цену.

Термин «устойчивая мода» появился в 1987 году в докладе Комиссии ООН по окружающей среде и развитию, известной как Комиссия Брунтланн, названной так по имени министра окружающей среды Норвегии Харлем Брунтланн. Ключевая идея устойчивого развития по Брунтланн основывается на балансе ресурсов между поколениями и экономическом росте, не приводящем к деградации окружающей среды. Однако только в начале XXI века в России начались исследования устойчивой моды, интерпретируемой как развитие с учетом текущих потребностей, не ставящее под угрозу ориентиры будущих поколений. С тех пор у представителей модной индустрии появилась цель: «Удовлетворить потребности сегодняшнего дня, не лишая будущие поколения возможности удовлетворить их собственные потребности» [2].

Явление устойчивой моды можно рассматривать с точки зрения разных подходов. В концепции **экологического подхода** устойчивая мода сосредоточивается на основных этапах производства одежды. То есть дизайнеры стараются сделать продукт экологичным на протяжении всего его жизненного цикла, начиная от задумки и производства, заканчивая утилизацией.

Исследователи Д. Шен, Дж. Ричардс, Ф. Лю выделяют восемь измерений устойчивой моды: ресайклинг, органическая продукция, винтаж/секонд-хенд, местное производство, кастомизация продукции, сертификация fair trade, vegan и hand-made-товары. В данном списке исследователи выделяют веганскую моду, так как она также является частью экологического подхода. На сегодняшний день понятие веганство обширно и понимается, как отказ от любого использования животных в производстве и употреблении. Борцы за права животных и веганы проводят кампании против использования животных в модной индустрии еще с конца 1800-х годов. На данный момент существуют специальные веганские товарные знаки и маркировки, которыми обозначаются товары брендов, производящих продукцию, которая не содержит компоненты животного происхождения [2].

По сути, данный подход направлен создание такой моды, которая отвечала бы запросам покупателей: была уникальной и с широким ассортиментом для выбора. И при этом мода должна оставаться справедливой по отношению к окружающей среде: экологичное производство, щадящая транспортировка товара и возможность для утилизации.

Существует также и **социальный подход** к изучению и исследованию устойчивой моды. Понятие быстрая мода породила эксплуатацию труда: за широким выбором товаров, который, кажется, необходим людям, стоит неэффективное и опасное для рабочих производство товаров с низким качеством. Большая часть одежды массмаркетов отшивается в бедных странах или странах с дешевой рабочей силой. Производители требуют работать людей за несколько долларов в день по двенадцать часов в сутки, находясь при этом в нечеловеческих условиях труда. Быстрое производство увеличило количество случаев гибели людей на рабочем месте. Один случай произошел в Бангладеш в Rana Plaza, где располагалось несколько швейных предприятий. Работники швейного цеха не были эвакуированы из-за обнаружения крупных трещин на фасаде здания, вследствие чего погибло более тысячи людей. С тех пор немногое изменилось в модной индустрии, и быстрая мода с желанием производителей получить больше прибыли, продолжают расширять токсичное производство и эксплуатацию труда. Безусловно, покупатели не всегда видят обратную сторону модной индустрии и не всегда понимают цену, которую приходится отдать, чтобы другие люди чувствовали себя лучше. По этой причине важна осведомленность потребителей о реальном процессе производства, чтобы больше людей стали более осознанно относится к покупке той или иной одежды. Осознанное или

устойчивое потребление характеризуется приобретением качественно созданной, экологичной продукции, которая не вредит окружающей среде и рабочим [1].

Существует также и **культурологический подход** в трактовке явления устойчивой моды. В рамках этого подхода устойчивая мода понимается, как символическое выражение нашей эпохи XXI века. Если вспомнить историю моды, то в разные времена мода всегда отражала мысли и жизнь всего общества. XVIII в. – век пышности платьев, огромного разнообразия тканей и фурнитур, тогда мода была целым искусством, ведь на изготовление платья могло уйти несколько месяцев ручной работы. Конец XIX и начало XX века олицетворяли бунт феминисток, которые старались добиться своих гражданских прав. Этот бунт отражался и в моде того времени: более свободные формы одежды, аскетичность в деталях, не было чрезмерной пышности и блеска бриллиантов, ведь тогда женщины хотели доказать, что не являются лишь украшением мужчины. Они тоже могут постоять за себя, могут понимать точные науки и могут занимать те же должности, что и мужчины. Первая и вторая мировые войны существенно изменило и саму моду: из-за нехватки тканей и материалов, люди с большей бережностью старались сохранить свои вещи, даже несмотря на то, что они не были модными [1].

Поэтому и сейчас устойчивая мода или осознанное потребление – это отражение нашего времени. Времени перепроизводства, времени перепотребления, времени перенасыщения информации, времени «быстрой» жизни. Сторонники устойчивой моды уже создают общество людей, которые хотят оставаться модными, но при этом не вредить природе. Общий интерес в защите окружающей среде подвигает людей и дальше развивать явление устойчивой моды, делясь своими мыслями и взглядами с другими и показывая своим примером, как можно жить.

Воспитательный подход подразумевает образование для устойчивого развития, что влечет за собой не только трансформацию образовательных систем, но и подготовку граждан к получению новых знаний. Для средних образовательных учреждений нужно вводить дисциплины, касающиеся экологии в целом, ведь подрастающим поколениям придется бороться с экологическим кризисом. Введение в образ жизни экологичных привычек, таких как: использование многоразовых бахил и пакетов, сортировка мусора (пластика, стекла, макулатуры), сдача ненужной одежды на благотворительность или переработку побудит людей больше обращать внимание на состояние нашего окружающего мира и на явление устойчивой моды. Согласно

образовательной методологии, увеличение уровня осведомленности о устойчивом развитии благоприятно сказывается на установках и действиях, связанных с экологическими практиками в моде [1].

Устойчивая мода – это явление, которое будет стремительно развиваться в будущем. Будет увеличиваться использование органических, переработанных и биоразлагаемых материалов. Технологии, такие как синтетические волокна из растительных источников или переработанного пластика, станут более распространенными. Модные бренды будут все чаще переходить к модели, основанной на повторном использовании и переработке. Это включает в себя программы возврата одежды, аренду и обмен вещей, что позволит снизить количество отходов. Устойчивость будет включать не только экологические аспекты, но и социальные. Бренды будут уделять внимание условиям труда своих работников, справедливой оплате и поддержке местных сообществ.

Таким образом, категория устойчивости стала значимой в современных исследованиях моды, которым присущ междисциплинарный характер, сочетание академических и прикладных элементов, поэтому ученые задействовали теоретические и методологические ресурсы различных дисциплин. Устойчивая мода подразумевает лучшую осведомленность дизайнеров, покупателей, розничных продавцов и потребителей о влиянии продукции на работников, сообщества и экосистемы.

Список используемых источников

1. Теория моды: одежда, тело, культура / Под ред. Валери Стил, Музей Института технологий моды (Нью-Йорк). Москва: Изд-во Новое Литературное Обозрение, 2023. Вып. 73. 331 с.

2. Кручинина Д. Д. Устойчивая мода в современном научном дискурсе: исследовательские подходы // // Общество: философия, история, культура. 2023. № 6. С. 188–193.

Статья представлена научным руководителем, доцентом кафедры СПН СПбГУТ, кандидатом философских наук, доцентом Астафьевой-Румянцевой И. Е.

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
Корректура
Д. Н. Яшугин
Дизайн логотипа Г. И. Юрьев
Подписано в печать 10.10.2025
Объем 19 усл.-печ. л.

Объединенная редакция рецензируемых научных изданий СПбГУТ
193232 СПб., пр. Большевиков, 22, корп. 1

СПбГУТ)))