СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ | SIBERIAN FEDERAL UNIVERSITY

ПРОСПЕКТ СВОБОДНЫЙ - 2025

Материалы XXI Международной научной конференции студентов, аспирантов и молодых учёных

Электронное издание
в 4 частях
Часть IV

Технические науки
Институт космических и информационных технологий

2025

Красноярск

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ | SIBERIAN FEDERAL UNIVERSITY

PROSPECT SVOBODNY - 2025

Proceedings of the XXI International Scientific Conference
for undergraduate, postgraduate, PhD students
and early career researchers

Electronic publication
in 4 parts
Part IV

Technical sciences
School of Space and Information Technology

2025

Krasnoyarsk

Министерство науки и высшего образования Российской Федерации
Сибирский федеральный университет

ПРОСПЕКТ СВОБОДНЫЙ – 2025

Материалы XXI Международной научной конференции
студентов, аспирантов и молодых ученых

Электронное издание
в 4 частях
Часть IV

Технические науки
Институт космических и инофрмационных технологий

Красноярск
21–26 апреля 2025 г.

УДК 001.891(03)
ББК 72.5
П827

Ответственные за выпуск: Брежнев Руслан Владимирович
Губанов Алексей Константинович
Чижов Илья Алексеевич

В том числе члены Студенческого научного сообщества Сибирского федерального университета:

Гусева Маргарита Сергеевна

П827 **Проспект Свободный – 2025**: материалы XXI Международной научной конференции студентов, аспирантов и молодых ученых. Красноярск, 21–26 апреля 2025 г. [Электронный ресурс] / отв. за вып. Р. В. Брежнев, А. К. Губанов, И. А. Чижов, М. С. Гусева – Электрон. дан. (6,9 Mb). – Красноярск: Сиб. федер. ун-т, 2025. – 263 с. – Систем. требования: PC не ниже класса Pentium I; 128 Mb RAM; Windows 98/XP/7/8/10; Adobe Reader V8.0 и выше. – Загл. с экрана.

ISBN 978-5-7638-5173-1 (часть 4)
ISBN 978-5-7638-5169-4

Представлены результаты научно-исследовательской работы студентов, аспирантов и молодых ученых. Материалы публикуются в авторской редакции.

Предназначены для студентов различных направлений и специальностей, аспирантов, научных работников и преподавателей.

УДК 001.891(03)
ББК 72.5

ISBN 978-5-7638-5173-1 (часть 4)
ISBN 978-5-7638-5169-4

© Оформление. Сибирский федеральный университет, 2025

Ministry of Science and Higher Education of Russian Federation
Siberian Federal University

PROSPECT SVOBODNY – 2025

Proceedings of the XXI International Scientific Conference
for undergraduate, postgraduate, PhD students and early
career researchers

Electronic publication
in 4 parts
Part IV

Technical sciences
School of Space and Information Technology

Krasnoyarsk
April 21 – 26, 2025

UDC 001.891(03)
LBC 72.5
П827

Responsible for edition: Ruslan V. Brezhnev
Aleksey K. Gubanov
Ilya. A Chizhov

Members of the Siberian Federal University Research Students' Union:

Margarita S. Guseva

П827 **Prospect Svobodny – 2025**: proceedings of the XXI International Scientific Conference for undergraduate, postgraduate, PhD students and early career researchers. Krasnoyarsk, April 21–26, 2025 [Electronic resource] / edit. R. V. Brezhnev, A. K. Gubanov, I. A. Chizhov, M. S. Guseva – Electronic data (6,9 Mb). – Krasnoyarsk: SibFU, 2025. – 263 p.
– Hardware re-quirements: PC Pentium I or higher; 128 Mb RAM; Windows 98/XP/7/8/10; Adobe Reader V8.0 or higher.
ISBN 978-5-7638-5170-0 (part 1)
ISBN 978-5-7638-5169-4

The proceedings include results of research by undergraduate, postgraduate, PhD students and early career researchers. The proceeding papers are published in the author's edition.

The edition is aimed at students of different specializations, PhD students, scholars and university professors.

UDC 001.891(03)
LBC 72.5

ISBN 978-5-7638-5170-0 (part 1)
ISBN 978-5-7638-5169-4

© Design. Siberian Federal University, 2025

СОДЕРЖАНИЕ

Информатика и вычислительная техника 7
Информационная безопасность 51
Прикладная математика, математическое моделирование 108
Прикладная лингвистика 150
Системный анализ, управление и программная инженерия 195

Информатика и вычислительная техника

УДК 004.622+004.42

ИСПОЛЬЗОВАНИЕ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ ДЛЯ ПРЕПРОЦЕССИНГА БИОЛОГИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Г. Ю. Аникутин[1]
Научный руководитель Д. А. Кузьмин[1]
Кандидат технических наук, заведующий кафедрой высокопроизводительных вычислений

[1]*Сибирский федеральный университет*

За последние годы исследования в области анализа последовательностей ДНК развиваются крайне быстро. Стоимость секвенирования генов снижается, позволяя получать всё больше информации, однако из этого следует и увеличение объёма данных, которые необходимо обработать. При работе с геномом необходимо решать проблемы, связанные с колоссальным объёмом данных и сложными вычислениями. В связи с этим актуальной является тема предварительной обработки (или препроцессинга) данных, которая облегчает и повышает точность анализа. Работа с данными последовательностей хорошо поддаётся распараллеливанию и использованию многопоточности, это будет рассмотрено далее.

Биологические последовательности – это линейные представления молекулярных структур, к ним относятся ДНК, РНК и белки. Последовательность ДНК состоит из нуклеотидов четырёх видов, комбинации из которых составляют биологическую информацию. Данные записывают в виде последовательности ASCII-символов в файлах текстового формата (например, FASTQ), каждый символ соответствует одному из нуклеотидов. Однако объём получаемых данных колоссален – например, в рамках проекта «Геном человека» [1] описано более 3,2 млрд пар оснований. Кроме того, данные, получаемые при секвенировании, могут быть далеки от идеального состояния, и для их анализа необходима предварительная обработка.

Предварительная обработка данных или препроцессинг – это метод интеллектуального анализа данных, при котором необработанные данные преобразуются в понятную структуру, это критически важный этап в любой работе с генами, повышающий точность и достоверность результатов. Сбор данных несёт определённые погрешности, поэтому сырые данные зашумлены, имеют ошибки секвенирования, некачественные участки с низкой достоверностью, технические артефакты. Из-за длины молекулы ДНК её невозможно обрабатывать целиком, секвенаторы разрезают ДНК на фрагменты, называемые ридами, и это может породить новые проблемы, дубликаты и избыточность, некоторые риды могут иметь низкое качество или слишком маленькую длину, работа с этим – также задача препроцессинга.

© Аникутин Г. Ю., 2025

Для подобного формата данных и задач, которые нужно решить при их обработке, хорошо подходят параллельные вычисления. При параллельных вычислениях одновременно используется несколько вычислительных устройств, каждое из которых выполняет свою часть вычислений параллельно с другими, задача делится на несколько частей и решается
с помощью нескольких процессоров. Для этого могут использоваться графические процессоры (GPU), которые имеют большое количество ядер, что позволяет проводить вычисления на каждом из них, значительно ускоряя процесс вычислений по сравнению с обычными процессорами (CPU). Параллелизм можно организовать на уровне данных и на уровне инструкций, при этом все варианты хорошо применимы для обработки данных последовательностей.

Среди многочисленных процедур предварительной обработки последовательности можно выделить основные, такие как контроль качества и фильтрация последовательностей. Контроль качества используется для выбора ридов из набора данных, соответствующих показателям качества. Фильтрация уменьшает количество ридов, снижая вычислительные затраты. Предварительная обработка последовательности генома часто распараллеливается на уровне данных, поскольку практически нет необ-ходимости обмениваться данными между этими задачами.

Можно рассмотреть такие примеры, как Fastp, PRINSEQ++, Parabricks.

Fastp – это многопоточный инструмент, предложенный Ченом и соавторами [2] в 2018 г. Это один из самых популярных, быстрых и универсальных инструментов для препроцессинга FASTQ-данных. Он может выполнять контроль качества, также обрезку адаптера и фильтрацию качества ридов. Инструмент написан на C++ и поддерживает многопоточность на CPU, с его помощью можно отсеивать короткие и низкокачественные риды, исправлять ошибки с перекрытием пар и удалять дубликаты из данных.

PRINSEQ++ – это приложение контроля качества и предварительной обработки последовательностей, реализованное на основе популярного инструмента prinseq-lite [3], поддерживает фильтрацию ридов, обрезку и переформатирование последовательностей для улучшения их анализа. Инструмент разработан Канту и соавторами [4], работает как инструмент командной строки, специализируется на фильтрации, очистке, обрезке и обобщённой статистике FASTQ-файлов, написан на C++, поддерживает многопоточность на многоядерных CPU.

Parabricks – это коммерческий фреймворк от NVIDIA [5], предназначенный для работы в биоинформатике. Его возможности включают GPU-оптимизированные версии популярных инструментов, таких как BWA-MEM, занимающийся выравниванием ридов по референтному гену, GATK BQSR, MarkDuplicates, позволяющий находить и помечать PCR-дубликаты, BaseRecalibrator, ApplyBQSR, выполняющие калибровку качества оснований (Base Quality Score Recalibration – BQSR). Также предполагается совместимость

с другими инструментами для работы с последовательностями и ускорение вычислений в 10–100 раз по сравнению с вычислениями на CPU.

Подводя итоги, можно сказать, что препроцессинг биологических последовательностей – это важнейший этап в анализе геномных данных, обеспечивающий высокое качество и надёжность результатов. Современные объёмы данных, получаемые при секвенировании, требуют применения высокопроизводительных вычислительных решений. Использование многопоточности позволяет значительно ускорить препроцессинг и делает возможным анализ больших наборов данных в разумные сроки; кроме того, использование графических процессоров (GPU) показывает наибольшую эффективность и значительно ускоряет процесс.

Список литературы

1. Human Genome Project Fact Sheet. URL: genome.gov/about-genomics/educational-resources/fact-sheets/human-genome-project.

2. Chen S. Fastp: an ULTRA-FAST All-in-one FASTQ Preprocessor / S. Chen et al. // Bioinformatics. 2018. Vol. 34. No. 17. Pp. 1 884–1 890.

3. Schmieder R. Quality Control and Preprocessing of Metagenomic Datasets / R. Schmieder, R. Edwards // Bioinformatics. 2011. Vol. 27. No. 6. Pp. 863–864.

4. Cantu V. A. PRINSEQ++, a Multi-threaded Tool for Fast and Efficient Quality Control and Preprocessing of Sequencing Datasets / V. A. Cantu, J. Sadural, R. Edwards. 2019.

5. Clara for Genomics // NVIDIA. URL: nvidia.com/en-us/clara/genomics.

УДК 004.454:004.056.53:004.7

ПРЕДВАРИТЕЛЬНЫЕ ЭТАПЫ АЛГОРИТМА АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ АБОНЕНТСКИХ ТЕРМИНАЛОВ В СЕТИ СПУТНИКОВОЙ СВЯЗИ

Д. А. Баталов[1]
Научный руководитель И. Н. Рыженко[1]
Кандидат технических наук, старший преподаватель

[1]Сибирский федеральный университет

В рамках современного цифрового мира обеспечение безопасности систем связи, особенно в контексте спутниковых технологий, становится ключевым фактором для обеспечения целостности данных и бесперебойной работы устройств. Разработка элементов системы безопасности для системы спутниковой связи, включающей в себя меры аутентификации, защиты и управления доступом, а также процедуры входа абонентских

© Баталов Д. А., 2025

терминалов (АТ) в сеть, играет значимую роль в безопасности передачи информации.

В отчёте центра исследования безопасности Лаборатории Касперского под названием «Обзор угроз для IoT-устройств в 2023 г.» утверждается, что проблема недостаточной защищённости устройств Интернета вещей характерна не только для пользовательского рынка, но и для промышленных систем Интернета вещей. Подобные системы могут содержать тривиальные уязвимости, а рекомендованные разработчиками настройки – быть небезопасными [1]. Данные утверждения актуальны и для систем спутниковой связи гражданского назначения, в которых было выявлено два главных вектора атак, используемых злоумышленниками для нарушения целостности прошивки устройств.

1. Физический доступ и модификация прошивки:

– использование USB для обновления – злоумышленник может использовать физический доступ к устройству для замены оригинальной прошивки на поддельную;

– программирование NAND/eMMC-чипа памяти – путём прямого доступа к чипу памяти злоумышленник может изменить прошивку, внедрив вредоносный код.

2. Man-in-the-Middle-атака через сеть:

– перехват запросов на обновление прошивки – злоумышленник, получив доступ к сети, к которой подключено устройство, может перехватить запрос устройства на обновление прошивки;

– отправка поддельной прошивки – посредством MITM-атаки злоумышленник отправляет фальшивую, «отравленную» прошивку, выдавая себя за подлинный сервер обновлений.

Данные атаки способны либо остановить функционирование системы спутниковой связи, либо нарушить конфиденциальность информации, передающейся в такой системе. Таким образом, обеспечение цепочки доверия при загрузке образов прошивок АТ систем спутниковой связи является важным этапом при реализации входа АТ в сеть спутниковой связи с частотно-временным разделением ресурса (MF-TDMA).

Для решения указанной проблемы были выполнены следующие задачи, направленные на обеспечение защиты АТ от несанкционированной замены программного обеспечения.

Был проведён анализ защищённых криптографических ускорителей различных производителей. Анализ включал в себя пять устройств, которые сравнивались по параметрам: поддерживаемые криптографические алгоритмы, алгоритмы формирования ключа, токи потребления (в спящем режиме и максимальный ток), наличие и битность уникального идентификационного номера и шина взаимодействия. По результатам анализа была выбрана для применения криптомикросхема ATSHA204A.

Для обеспечения готовности криптомикросхемы с системой на кристалле AT с учётом особенностей спящего режима микросхемы было разработано IP-ядро ПЛИС, позволяющее с точностью до 2,5 мкс манипулировать питанием микросхемы.

С учётом вышеприведённого изменения управления питанием криптомикросхемы были введены изменения в драйвер данной микросхемы, входящий в состав ядра Linux.

Был проведён харденинг ядра ОС Linux абонентских станций, т. е. процесс настройки опций компиляции ядра ОС с целью отключения опций, позволяющих эксплуатировать уязвимости ядра. Действия по настройке опций можно условно разделить на четыре вида [2; 3]:

1) добавление опций, реализующих защиту от определённого вида угроз (например, защита от аппаратных уязвимостей Spectre [4]);

2) отключение опций, для которых были найдены методы, позволяющие эксплуатировать уязвимости (например, поддержка /dev/mem – файла символьного устройства, представляющего образ памяти);

3) включение опций, повышающих общее состояние защищённости ядра (например, опция PAGE_POISONING, которая перезаписывает страницы памяти паттерном при их освобождении);

4) отключение опций, отвечающих за неиспользуемые возможности ядра.

Был разработан алгоритм верификации образов ПО AT (рис. 1, 2), который состоит из трёх основных этапов:

– предварительный этап заключается в создании основного секретного ключа MainKey, его записи в микросхему ATSHA204A в зону OTP на каждом пользовательском устройстве и последующей блокировке;

– первый этап выполняется при разработке новой версии ПО на стороне компании-разработчика;

– второй этап выполняется при обновлении на конечном устройстве.

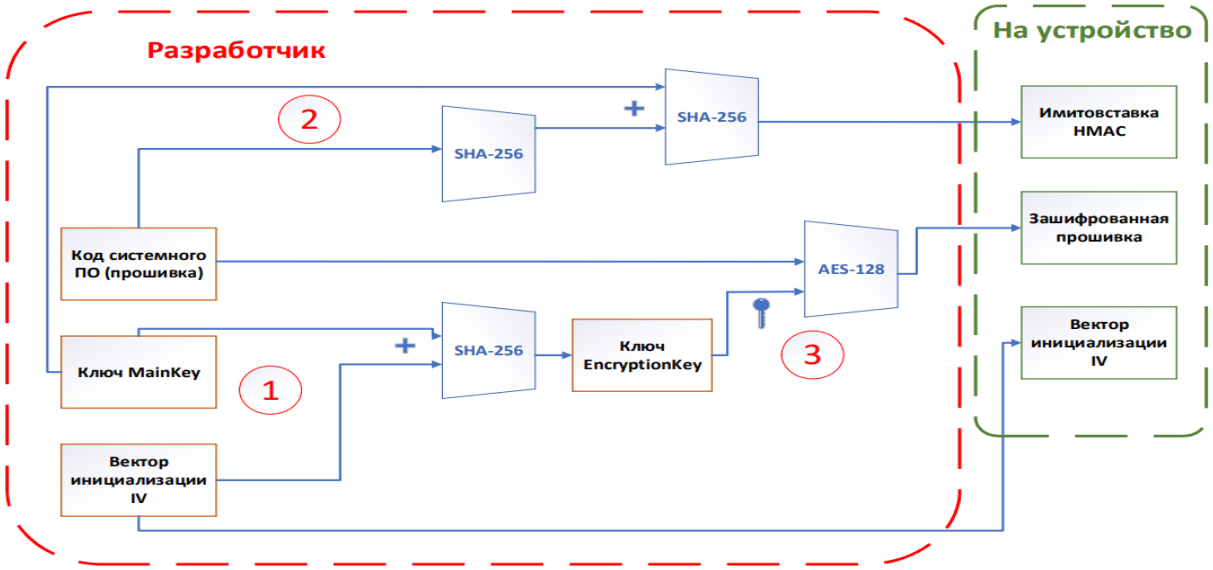


Рисунок 1. Схема первого этапа алгоритма

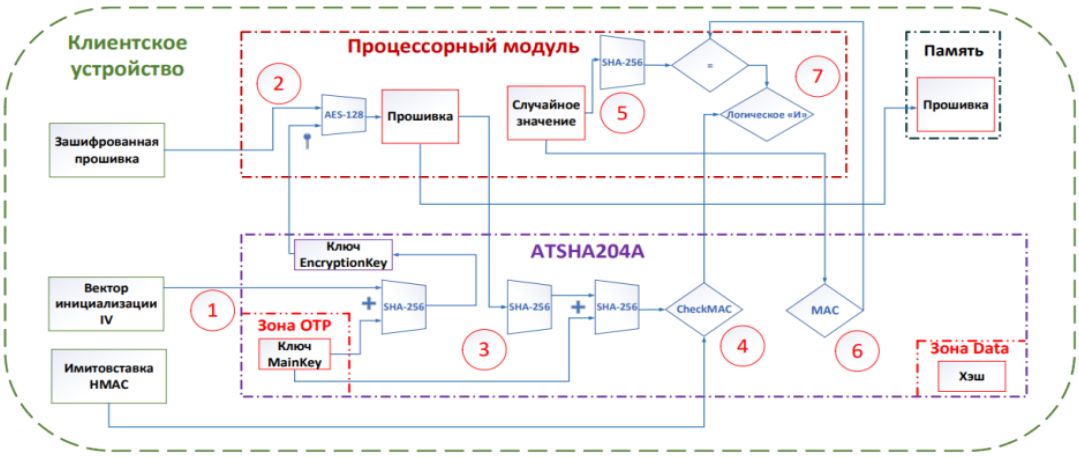


Рисунок 2. Схема первого этапа алгоритма

Таким образом, в ходе данной работы было приведено описание комплексного решения предварительных этапов алгоритма входа абонентских терминалов в сети спутниковой связи, позволяющего успешно и безопасно реализовать алгоритм входа АТ в сеть.

Список литературы

1. Обзор угроз для IoT-устройств в 2023 г. // SECURELIST by Kaspersky. URL: securelist.ru/iot-threat-report-2023/108088.

2. Securing your Linux Configuration (Kernel Hardening) // Tymesys. URL: timesys.com/security/securing-your-linux-configuration-kernel-hardening.

3. Рекомендации по безопасной настройке операционных систем Linux: метод. документ от 25.12.2022 // ФСТЭК России. URL: fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty.

4. Spectre Attacks: Exploiting Speculative Execution. URL: meltdownattack.com.

УДК 004.89+004.93

АКТУАЛЬНОСТЬ И ВЫЗОВЫ ON-DEVICE-МЕТОДОВ РАСПОЗНАВАНИЯ ЛИЦ НА УСТРОЙСТВАХ С ОГРАНИЧЕННЫМИ РЕСУРСАМИ

А. А. Горбацевич[1]
Научный руководитель Д. А. Кузьмин[1]
Кандидат технических наук, заведующий кафедрой высокопроизводительных вычислений

[1]*Сибирский федеральный университет*

Современные мобильные устройства Интернета вещей (IoT) характеризуются ограниченными вычислительными ресурсами, энергопотреблением и памятью. В то же время растёт спрос на применение в

© Горбацевич А. А., 2025

таких системах алгоритмов машинного обучения, в частности системы распознавания лиц [1; 2]. On-device – это подход, при котором обработка данных и вычисления выполняются на конечном устройстве, без передачи исходных данных внешним сервисам.

Этот подход позволяет обеспечить высокий уровень защиты персональных данных, что особенно важно в условиях, когда государства всё больше ужесточают нормативы сбора и хранения данных [3; 4]. Отсутствие необходимости в передаче данных является особо важным обстоятельством для ситуаций, когда нет возможности использовать интернет-соединение (закрытые или удалённые территории, наличие только спутникового интернета).

Но несмотря на отсутствие передачи личных данных третьим лицам, подход on-device-распознавания лиц всё же имеет серьёзные проблемы приватности доступа и безопасности [5]. Существуют такие атаки, позволяющие обмануть систему и получить доступ к закрытой информации, – например, face-spoofing. Злоумышленники используют фотографии, видео или 3D-маски для обхода системы аутентификации. Для защиты от такого типа атак необходимо внедрение механизмов liveness detection, способных отличить «живое» лицо от статичного изображения или видео [6; 7]. Получается, что несмотря на очевидные преимущества, on-device-метод требует комплексного подхода к обеспечению безопасности и приватности, что, в свою очередь, требует постоянного совершенствования технологий противодействия угрозам и алгоритмов работы.

При проектировании и создании системы распознавания лиц на малопроизводительных устройствах существует множество ограничивающих факторов. Основным из них является проблема ограниченности в доступных объёмах памяти и вычислительных ресурсах конечной системы. Другим фактором является проблема окружения, в котором применяется система. К этому относятся проблемы освещения, положения устройства в пространстве, выражения лица или используемая людьми одежда, частично или полностью закрывающая «точки интереса» лица. Для работы на низкопроизводительных устройствах была сделана модель EdgeFace [8] – это гибрид, объединяющий скорость работы свёрточных нейронных сетей и точность трансформеров. Другим вариантом может служить MobileFaceNets [9] – эта модель свёрточной нейронной сети с лёгкой архитектурой содержит менее 1 млн параметров и разработана специально для работы на мобильных и встроенных устройствах. Стоит также отметить SqueezeFacePoseNet [10] – адаптацию легковесной модели SqueezeNet для обеспечения распознавания лиц независимо от позы человека, что, как было отмечено выше, является одной из проблем окружения работы конечного устройства. Как видно, решения существуют, однако выбор подходящего всё ещё является сложной задачей, к которой необходимо подходить исходя из контекста применения системы.

Будущее on-device-распознавания лиц видится автором перспективным благодаря работе множества исследователей, направленной на дальнейшее снижение вычислительной нагрузки и повышение точности работы моделей

для применения в условиях ограниченных ресурсов. Современные модели демонстрируют, что легковесные архитектуры могут обеспечивать высокую производительность при сохранении низкого энергопотребления и небольшого объёма памяти, что особенно важно для мобильных устройств и IoT-систем. Перспективным направлением развития является также интеграция с федеративным обучением [11], благодаря которому можно объединить опыт работы множества устройств (например, в рамках одного предприятия) без компрометации персональных данных. Эти инновации, наряду с дальнейшим развитием специализированного аппаратного обеспечения (LiDAR- и ИК-камеры для определения «живости»; внешние ускорители нейронных вычислений), позволят обеспечить высокую адаптивность, устойчивость и масштабируемость систем распознавания лиц, что откроет новые возможности для их применения в самых различных областях – от контроля доступа (автономные СКУД) до интеллектуальных домашних устройств (Intranet of Things).

В заключение хочется сказать, что on-device-распознавание лиц является актуальным направлением в условиях необходимости обработки данных на устройствах с ограниченными ресурсами. Данный подход усиливает конфиденциальность, снижает задержки и сокращает расходы на инфраструктуру облачных вычислений. И хотя много где уже используется данный подход, не стоит забывать о необходимости совершенствования методов оптимизаций моделей и их адаптации к изменяющимся условиям использования.

Список литературы

1. Меньшикова Е. Распознай меня, если сможешь: могут ли системы распознавания лиц определить, что мы чувствуем на самом деле / Е. Меньшикова. URL: news.itmo.ru/ru/news/8691.

2. Аналитика МТС: растёт спрос на камеры с системой распознавания лиц. URL: telecomdaily.ru/news/2024/06/05/analitika-mts-rastet-spros.

3. Ужесточение ответственности за нарушение 152-ФЗ: разбор изменений в области защиты персональных данных // Хабр. URL: habr.com/ ru/companies/ussc/articles/865676.

4. Ужесточение правил защиты персональных данных на территории РФ в 2025 г. // Хабр. URL: habr.com/ru/companies/cloud4y/articles/882114.

5. Facial Recognition Technology and Privacy Concerns // ISACA. URL: isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns.

6. Blog I. What is Liveness Detection? A Complete Guide. URL: incognia.com/the-authentication-reference/what-is-liveness-detection.

7. Chakraborty S. An Overview of Face Liveness Detection / S. Chakraborty, D. Das. 2014.

8. George A. EdgeFace: Efficient Face Recognition Model for Edge Devices / A. George et al. 2024.

9. Chen S. MobileFaceNets: Efficient CNNs for Accurate Real-Time Face Verification on Mobile Devices / S. Chen. 2018.

10. Alonso-Fernandez F. SqueezeFacePoseNet: Lightweight Face Verification across Different Poses for Mobile Platforms / F. Alonso-Fernandez. 2025.

11. Solomon E. Federated Learning Method for Preserving Privacy in Face Recognition System / E. Solomon, A. Woubie. 2024.

УДК 004.415.26

ГЕНЕРАТОР C++ КОДА НА ОСНОВЕ РУССКОЯЗЫЧНОГО АЛГОРИТМИЧЕСКОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ

И. А. Заболотский[1]
Научный руководитель Д. А. Кузьмин[1]
Кандидат технических наук, заведующий кафедрой высокопроизводительных вычислений
Научный руководительС. А. Бронов[1]
Доктор технических наук, профессор

[1]*Сибирский федеральный университет*

При желании начать карьеру разработчика программного обеспечения нередко возникает вопрос «с чего начать изучение программирования?», и у многих начинающих разработчиков появляются проблемы с пониманием синтаксиса языка (каким образом объявлять переменные, когда нужно ставить кавычки или скобки). Также большинство языков программирования основаны на английском языке, что создаёт дополнительные трудности в овладении базовыми конструкциями. Для тех, кто не владеет английским языком, будет легче начать знакомство с языком программирования, основанном на кириллице и алгоритмическом псевдокоде, с которым ученики знакомятся на уроках информатики, с необходимым минимумом логических конструкций и синтаксических символов.

Для упрощения обучения программированию была создана программа [1], состоящая из синтаксического анализатора [2] и генератора кода [3] на *C++*. Основная цель состоит в том, чтобы позволить пользователям писать код программы на упрощённом, удобном для пользователя русском алгоритмическом языке с последующим преобразованием его в корректный код на *C++*. Программа поддерживает базовые конструкции языка *C++* (пользовательские функции, структуры данных, циклы, условия, ввод и вывод текста), а также элементы объектно ориентированного программирования (ООП) [4], включая структуры, классы, разные степени защиты переменных.

Синтаксический анализатор способен распознавать и переводить пользовательский синтаксис, что позволяет пользователям писать интуитивно понятные или зависящие от предметной области команды, которые переводятся

© Заболотский И. А., 2025

на *C++*. На вход программы подаётся файл с кодом на основе русского языка, после чего программа генерирует код на *C++* и выводит его в новый файл, который далее может компилироваться обычным образом (рис. 1).

```
включить потоквхвых
включить вектор
включить алгоритм

функц главная
цел яблоки = 5
цел груши = 4

ввод яблоки

вектор : цел Массив

Массив.в_конец(5)
Массив.в_конец(2)
Массив.в_конец(10)
Массив.в_начало(12)

сортировка Массив
если яблоки > 5 И груши < 8 то яблоки = 8
пока яблоки < 10 то яблоки++;
цикл и=0 и<10 и++ яблоки += и
структура точка
    цел в
    цел г
закр_структуры
союз данные
    цел д
    вещ е
закр_союза
класс мойкласс
публичная:
    цел целоепублич
защищенная:
    символ символзащ
частная:
    строка часстрока
закр_класса

перстроки
печать яблоки
вернуть 0
```

а

```
#include <iostream>
#include <vector>
#include <algorithm>
int main() {
    int __abloki = 5;
    int _gru_hi = 4;
std::cin>>__abloki;
    std::vector<int> _Massiv;
    _Massiv.push_back(5);
    _Massiv.push_back(2);
    _Massiv.push_back(10);
    _Massiv.insert(_Massiv.begin(), 12);
    std::sort(_Massiv.begin(), _Massiv.end());
    if (__abloki > 5 && _gru_hi < 8 ) {
        __abloki = 8;
    }
    while (__abloki < 10 ) {
        __abloki++;
    }
    for (int _i=0; _i<10; _i++) {
        __abloki += _i;
    }
struct _to_cka {
    int _v;
    int _g;
};
union _dann_ye {
    int _d;
    float _e;
};
class _moyklass {
    int _celoepubli_c;
    char _simvolza_j;
    std::string __casstroka;
};
std::cout << std::endl;
std::cout<<__abloki;
return 0;
}
```

б

Рисунок 1. Пример работы программы – генератора кода:
а – на разработанном языке; б – после генерирования кода на C++

Разработанный алгоритмический псевдокод предназначен прежде всего для упрощения обучения программированию.

Обучение процессу алгоритмизации упрощается за счёт того, что всё внимание уделяется математической сущности операций, их последовательности и взаимосвязи. Все особенности синтаксиса языка *C++* «знает» разработанный генератор кода.

Обучение процессу кодирования заключается в том, что для любого алгоритма можно сразу получить корректную запись на *C++* и изучить особенности её синтаксиса без обращения к справочникам и учебникам. При этом можно изучать, как изменение алгоритма отражается на коде.

Программа может использоваться для быстрого прототипирования кода, когда разработчики хотят быстро создавать прототипы своих программ и

тестировать свои идеи без написания подробного кода на *C++*. Программа может быть основой для создания предметно-ориентированных языков *DSL* (domain-specific language), где пользователи могут писать код на языке, адаптированном к конкретной предметной области или задаче, и преобразовывать его в *C++*. Разработанная программа устраняет разрыв между упрощённым псевдокодом и полнофункциональными программами на *C++*.

Алгоритмический язык может быть использован как компилируемый, так и интерпретируемый. Планируется доработка программы для работы с ассемблером – соответственно, это будет полноценный компилируемый язык.

Список литературы

1. Интерпретатор алгоритмических команд в C++: свидетельство о государственной регистрации программы для ЭВМ № 2024686933 / С. А. Бронов, Д. Д. Кривова, И. А. Заболотский ; правообладатель ФГАОУ ВО «Сибирский федеральный университет» (RU). № 2024686702; заявл. 13.11.2024; зарегистрировано в Реестре программ для ЭВМ 13.11.2024; Бюллетень № 11/2024.

2. Grune D. Parsing Techniques: a Practical Guide / D. Grune, C. J. H. Jacobs. Springer, 2008.

3. Herrington J. Code Generation in Action / J. Herrington. 2003.

4. Gamma E. Design Patterns: Elements of Reusable Object-oriented Software / E. Gamma, R. Helm, R. Johnson et al. Addison-Wesley, 1994.

УДК 004.94

БЛОЧНО-МОДУЛЬНЫЙ ПРИНЦИП КАК ОСНОВА УЧЕБНО-НАУЧНОЙ СИСТЕМЫ МОДЕЛИРОВАНИЯ

А. В. Зазнобина[1]
Научный руководитель – С. А. Бронов[1]
Доктор технических наук, профессор

[1]*Сибирский федеральный университет*

Системы моделирования являются основой систем автоматизированного проектирования. Поэтому обучение разработке подобных систем целесообразно предусмотреть в образовательных программах бакалавров, специалистов и магистров. Но в настоящее время отсутствуют какие-либо методические материалы по разработке систем моделирования. В данной работе рассмотрено решение задачи создания научно-учебной системы моделирования с открытым кодом.

Система моделирования строится с использованием общепринятого блочно-модульного принципа. Предполагается, что моделируемый объект

© Зазнобина А. В., 2025

разделяется на блоки, соответствующие составным частям объекта, а затем выходы одних модулей соединяются с входами других модулей.

Например, электропривод постоянного тока, используемый в качестве примера в разработанной учебно-научной системе моделирования, может быть представлен в виде системы из нескольких блоков с взаимными связями различной физической природы (рис. 1).

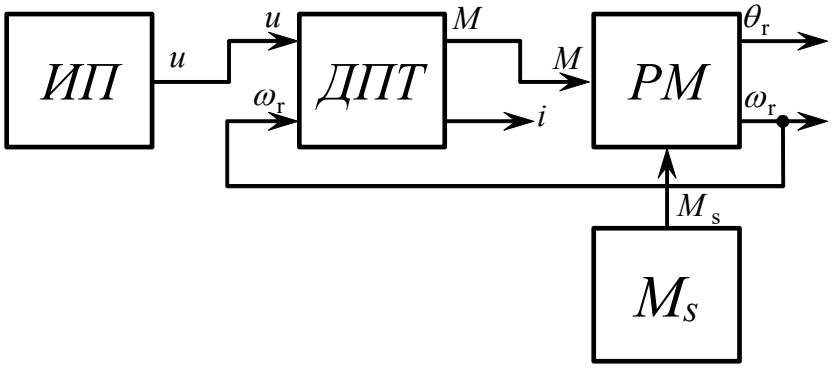


Рисунок 1. Структурная схема модели электропривода
в качестве примера исследуемого объекта: ИП – источник питания; ДПТ – двигатель постоянного тока; РМ – рабочий механизм; Ms – момент сопротивления нагрузки

Каждый блок в системе на рисунке 1 имеет собственную модель в виде системы дифференциально-алгебраических уравнений. Выход каждого блока с соответствующей переменной является входом каких-то последующих блоков или всего электропривода в целом: u – напряжение якорной обмотки двигателя; M – электромагнитный момент; i – ток якорной обмотки двигателя; ω_r – угловая скорость вала двигателя; θ_r – угол поворота вала двигателя.

Система моделирования должна быть универсальной, т. е. обеспечивать возможность расчёта процессов в различных объектах при различном сочетании блоков, входных и выходных переменных. Эти связи можно устанавливать вручную, но предпочтительнее делать это автоматически.

Для этого в системе моделирования предусмотрены два режима работы: режим инициализации и режим расчёта.

Разработана унифицированная форма программной модели в виде подпрограммы-функции, разделённая на две части. В первой части, которая связана с режимом инициализации, задаются имена входных и выходных переменных (например, скорость, угол поворота, напряжение и т. д.), а также их условные символические обозначения. Во второй части, предназначенной для режима расчёта, записываются математические выражения.

Моделируемый объект представляется в виде списка программных моделей, каждая из которых соответствует некоторому устройству (блоку).

Работа системы моделирования начинается с запуска её в режиме инициализации (рис. 2). В этом режиме просматривается список используемых моделей и по очереди вызываются соответствующие подпрограммы-функции. В каждой модели обрабатывается только часть, относящаяся

к режиму инициализации, и заполняются два массива имён переменных – входных и выходных. После окончания просмотра всех моделей массивы имён входных и выходных переменных сравниваются и по совпадению имён определяются сочетания «вход – выход» для всех блоков.

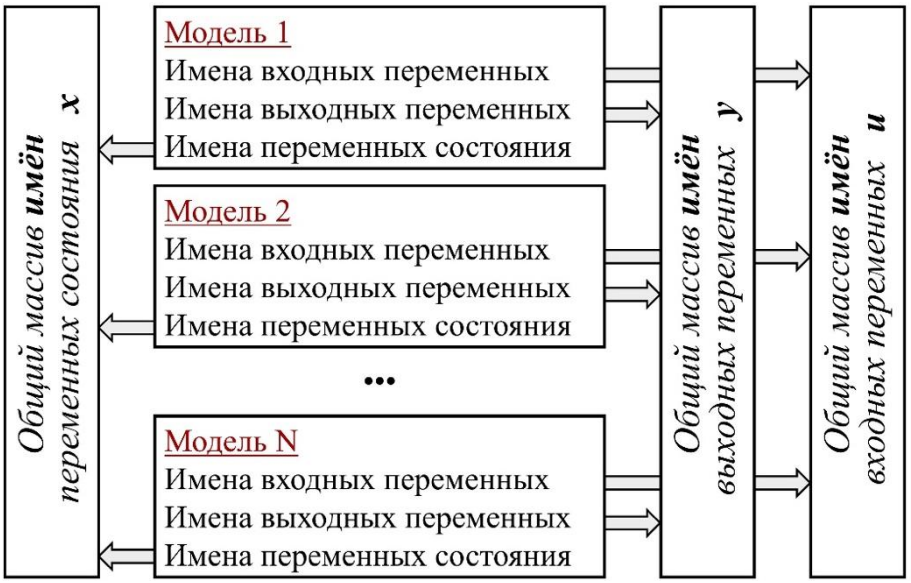


Рисунок 2. Структурная схема системы моделирования в режиме инициализации

Затем запускается режим расчёта. В этом режиме обрабатывается вторая часть подпрограмм-функций с записанными математическими моделями. В результате рассчитываются значения производных всех переменных и значения входных переменных, которые помещаются в соответствующие два массива. Они передаются в подпрограмму-функцию, реализующую метод численного интегрирования для расчёта новых значений переменных [1]. Таким образом выполняется процесс моделирования для заданного интервала времени (рис. 3).

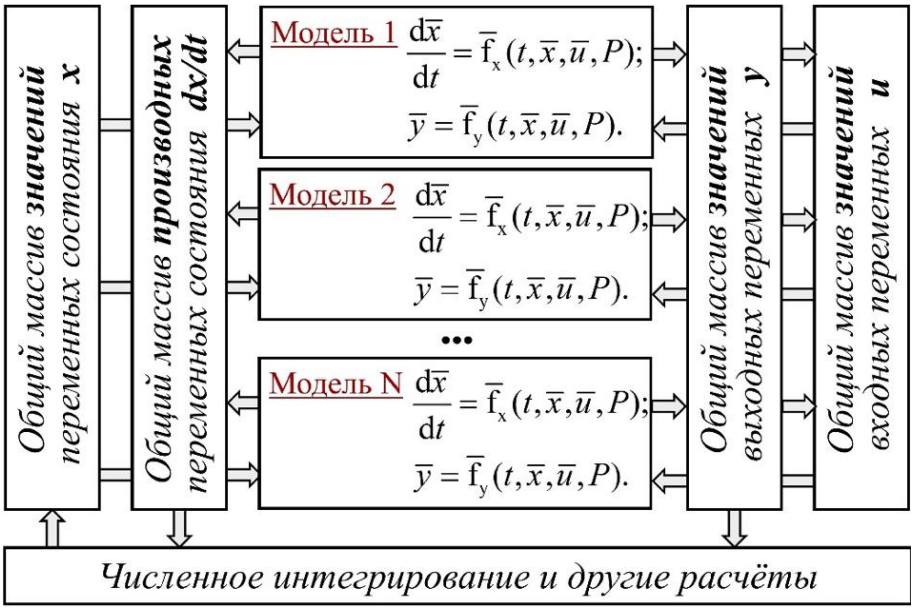


Рисунок 3. Структурная схема системы моделирования в режиме расчёта

Результаты расчёта в виде таблицы записываются в файл. При этом формируется шапка таблицы с обозначениями рассчитанных переменных.

Имеется возможность в процессе моделирования остановить вычисления и изменить состав блоков. Тогда снова запускается режим инициализации и устанавливаются новые связи между блоками, а затем выполняется переход в режим расчёта и моделирование продолжается. Это позволяет моделировать системы с переменной структурой, например, в неожиданно возникающих аварийных режимах работы объекта.

На данном этапе создания системы моделирования разработаны алгоритмы, реализованные в программе *MathCAD*14 для упрощения их отладки. В дальнейшем они будут реализованы на различных языках программирования: *C++*, *C#* и др. Такой подход демонстрирует алгоритмическую сущность систем моделирования без привязки к конкретным языкам.

Список литературы

1. Процедуры численного интегрирования для библиотеки методов системы моделирования динамических объектов: свидетельство о государственной регистрации программы для ЭВМ № 2023683924 / С. А. Бронов, Д. Д. Кривова, И. А. Заболотский, А. В. Зазнобина, Д. В. Лукьянов; правообладатель ФГАОУ ВО «Сибирский федеральный университет» (RU). № 2023683761; заявл. 13.11.2023; зарегистрировано в Реестре программ для ЭВМ 13.11.2023; Бюллетень № 11/2023.

УДК 004.722.45

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРИЁМНИКА БОРТОВОГО МАЯКА КОСМИЧЕСКОГО АППАРАТА

К. А. Иванникова[1]
Научный руководитель Е. С. Бывшев[1, 2]
старший преподаватель
Научный руководитель А. А. Комаров[2]

[1]*Сибирский федеральный университет*

[2]*АО «НПП «Радиосвязь»*

Современные космические аппараты (КА) оснащаются бортовыми маяками, которые играют ключевую роль в навигации, управлении и мониторинге состояния системы. Приёмник бортового маяка используется для получения сигналов от бортового ретрансляционного комплекса, установленного на КА. Благодаря ему можно определить местоположение КА,

© Иванникова К. А., 2025

получить информацию о его состоянии и настройках, а также обеспечить навигацию в сложных условиях.

Бортовой маяк работает как радиопередатчик, который периодически отправляет короткие сообщения, содержащие информацию о КА. В данной работе скорость передачи символов в радиоканале – 50 бит/с, период повторения сообщения – 4 с, метод модуляции – частотная модуляция с девиацией ±10 кГц.

В рамках настоящей работы разработана модель приёмника бортового маяка КА, которая декодирует следующую информацию:

– идентификатор КА;

– идентификатор способа работы программы;

– скорость работы программы.

На рисунке 1 представлена модель приёмника.

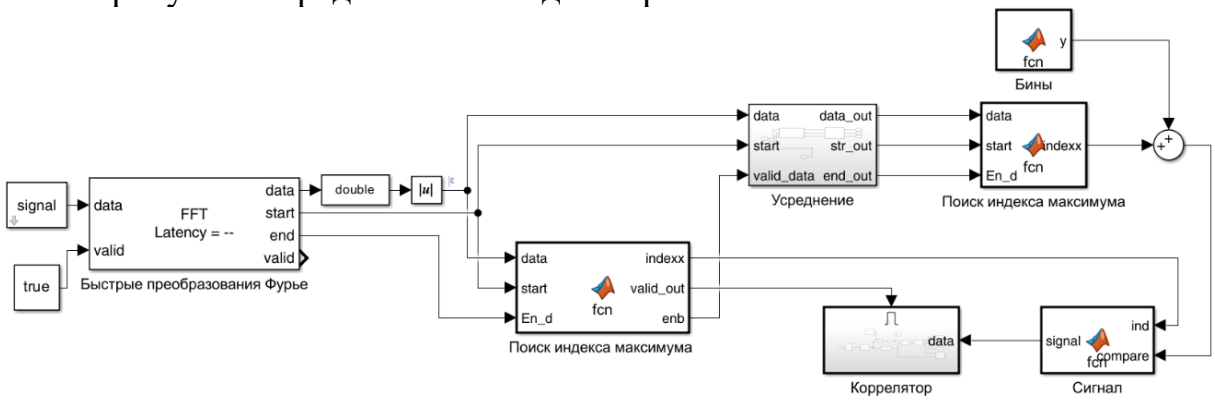


Рисунок 1. Общая модель приёмника бортового маяка

Сигнал поступает на блок быстрого преобразования Фурье (БПФ). После этого полученный сигнал поступает на блок поиска индекса максимума. В нём написан скрипт на языке *MatLab* для поиска максимального значения в отчёте и нахождения индекса этого максимального элемента. Это необходимо для определения частотной расстройки и компенсации эффекта Доплера. Т. к. скорость движения неизвестна, приёмник оценивает доплеровский сдвиг по принятому сигналу, усредняя результаты за некоторое время, измеряется мгновенный сдвиг частоты для каждого фрагмента.

Параллельно с этим данные с выхода блока *FFT* поступают на блок усреднения. Он состоит из функции, на которую подаётся сигнал начала отчёта БПФ для того, чтобы посчитать 50 отчётов БПФ. На выходе функция выдаёт 1, когда накапливается 50 отчётов, и 0 во всех остальных случаях. Этот блок используется для уменьшения дисперсии шума.

Далее сигнал вновь проходит через поиск индекса максимума и к этому индексу суммируется 10 кГц для нахождения порога, по которому будет декодирован сигнал.

После этого сигнал преобразуется в 0 и 1 и поступает на блок коррелятора. Т. к. структура передаваемого сообщения имеет заданный вид, по преамбуле находится начало сигнала; место идентификатора КА и дополнительная информация также заранее известны и записаны в двоичной

системе счисления. Происходит перевод из двоичной в десятичную систему и вывод информации на экран. На рисунке 2 показан блок определения номера КА.

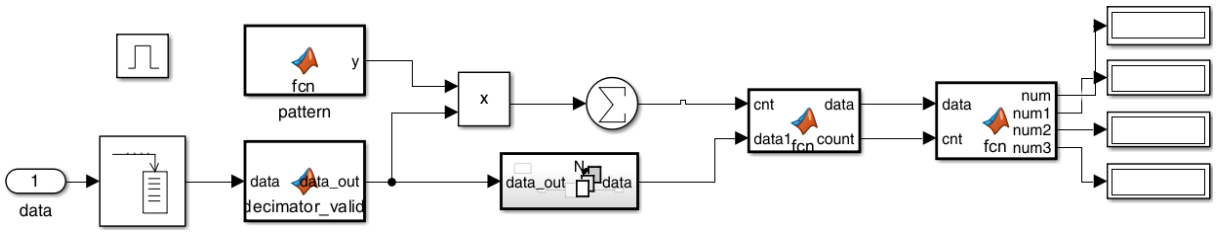


Рисунок 2. Блок определения номера КА

Данная математическая модель разрабатывалась под стандарты единой системы средств связи третьего поколения, т. к. она предназначена не только для приёма данных, но и их обработки.

В дальнейшем планируется перевести данную модель в формат с фиксированной точкой для генерации *HDL*-кода (*hardware description language*) и прошивки данной модели в плату для использования в реальной жизни.

Список литературы

1. Романов Д. А. Измеритель мощности сигнала бортового маяка для спутниковых систем связи, использующихся в наведении и автосопровождении / Д. А. Романов, П. В. Луферчик, А. А. Комаров и др. // Системы связи и радионавигации. 2024. С. 64.

УДК 004.7

О ПРОЕКТИРОВАНИИ МНОГОФУНКЦИОНАЛЬНОЙ СИСТЕМЫ МОНИТОРИНГА ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ СОСТОЯНИЯ КОРПОРАТИВНОЙ СЕТИ БЮДЖЕТНОЙ ОРГАНИЗАЦИИ

С. Е. Корнев[1]
Научный руководитель Ф. А. Казаков[1]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

В современных условиях эффективное функционирование любой организации, в т. ч. бюджетной, неразрывно связано со стабильной и эффективной работой её корпоративной сети [1]. Отдельные государственные учреждения управляют собственными центрами обработки данных и предоставляют широкий спектр сервисов на территориально распределённых объектах. При этом действующие системы мониторинга, собирающие данные о

© Корнев С. Е., 2025

доступности сетевого оборудования и общем трафике, уже не отвечают возрастающим требованиям к управлению и контролю сетевой инфраструктуры. Так, администраторы сети не могут оперативно либо не способны вовсе решать нестандартные проблемы сети и её пользователей.

Необходима многофункциональная система мониторинга (МСМ), способная не только отслеживать базовые параметры, но и анализировать качественные характеристики трафика, потребление ресурсов отдельными пользователями, а также предоставлять гибкие возможности расширения [4]. В статье на основе корпоративной сети конкретного государственного учреждения рассматривается проектирование такой системы с учётом ограничений, характерных для бюджетных организаций.

Текущая система мониторинга корпоративной сети основана на использовании базовых метрик, получаемых по протоколу *SNMP* (*Simple Network Management Protocol*) [2]. Такой подход позволяет получать информацию о доступности оборудования через механизмы опроса (*polling*) и уведомлений (*traps*), а также собирать агрегированные данные о загрузке сетевых интерфейсов. Основной недостаток текущей системы – ограниченный набор собираемых данных. Для эффективного управления сетью требуется более глубокий анализ трафика, включая адреса источников и назначения, объём трафика, потребляемый каждым пользователем, характеристики передаваемых пакетов (например, типы протоколов). Кроме того, система должна быть масштабируемой, позволяющей легко добавлять новые метрики и контролируемые элементы сети. Важным аспектом является и визуализация данных, предоставляющая администраторам наглядное представление о состоянии сети и потенциальных проблемах.

При проектировании МСМ корпоративной сети государственного учреждения следует принимать во внимание характерные особенности существующей инфраструктуры и специфику внутренних процессов [5].

Корпоративная сеть государственного учреждения имеет сложную сегментированную структуру, где каждый сегмент характеризуется уникальной топологической организацией [3]. Важной особенностью является неоднородность сетевой инфраструктуры, обусловленная поэтапным развёртыванием сегментов в разные временные периоды. В результате такого исторически сложившегося подхода к формированию сети инфраструктура представляет собой конгломерат разнотипного оборудования с неоднородным функциональным потенциалом и различными характеристиками.

В связи с этим МСМ предлагается строить на модульной архитектуре [7], обеспечивающей гибкость и масштабируемость, параллельно с текущей системой мониторинга. Центральный элемент – сервер сбора и анализа данных, на котором развёрнута база данных для хранения информации и программное обеспечение для обработки и визуализации. С целью сбора данных оптимально использовать агенты, устанавливаемые на рабочих станциях пользователей, а также важно произвести соответствующую настройку сетевого оборудования. Агенты будут собирать информацию

о трафике, использовании ресурсов и других параметрах, передавая её на центральный сервер.

При выборе технологического стека для реализации МСМ необходимо учитывать ряд специфических требований, характерных для бюджетных организаций: непрерывность работы (система должна функционировать 24/7 без существенных простоев, а все обновления и модификации должны производиться без прерывания мониторинга); простота эксплуатации; соответствие требованиям федерального законодательства (использование программного обеспечения, включённого в Реестр отечественного ПО, либо свободного ПО с открытым исходным кодом); экономическая эффективность; масштабируемость.

Предлагаемый технологический стек включает такие элементы [6]:

– система сбора потоковой статистики – nProbe (открытый исходный код) или отечественный аналог для сбора данных NetFlow/sFlow/NetStream;

– система мониторинга доступности – Zabbix или Prometheus (открытый исходный код) для базового мониторинга по ICMP и SNMP;

– хранилище данных – ClickHouse (открытый исходный код российской разработки) для долгосрочного хранения и аналитики временных рядов;

– аналитический движок – Apache Spark или Arenadata Streaming (российская альтернатива) для обработки потоковых данных;

– система визуализации – Grafana (открытый исходный код) или отечественные аналоги, такие как Диасофт Дашборд;

– интеграционная шина – Apache Kafka или RabbitMQ для обеспечения надёжного обмена сообщениями между компонентами.

Использование компонентов с открытым исходным кодом не только отвечает требованиям импортозамещения, но и обеспечивает возможность адаптации системы под специфические потребности конкретной организации [6].

Предложенная МСМ предоставит государственному учреждению оптимальный инструмент для управления и оценки состояния своей корпоративной сети [7]. Расширенный набор собираемых данных, гибкость и масштабируемость, а также экономичность делают её привлекательным решением для организаций с ограниченными ресурсами. Дальнейшее развитие МСМ может включать интеграцию с системами безопасности, автоматизацию реагирования на инциденты и использование технологий машинного обучения для прогнозирования и предотвращения проблем.

Изложенный подход позволяет оптимизировать работу системы мониторинга корпоративной сети без дополнительных финансовых затрат, сохраняя экономическую эффективность внедряемых изменений при одновременном повышении качества обслуживания сети [1; 7].

Список литературы

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы /

В. Г. Олифер, Н. А. Олифер. СПб.: Питер, 2023. 1 008 с.

2. Сорокин А. А. Автоматизированная информационная система комплексного мониторинга телекоммуникационной сети / А. А. Сорокин, А. Г. Тарасов, С. П. Королев // Системы и средства информатики. 2014. Т. 24. № 3. С. 176–191.

3. Шмыков Н. С. Анализ сетевого трафика в корпоративной сети / Н. С. Шмыков // Студент-Наука: матер. всеросс. НПК. Воронеж: ВГТУ, 2022. С. 90–92.

4. Рудзейт О. Ю. Обзор инструментов мониторинга и анализа сетевого трафика / О. Ю. Рудзейт, Ю. В. Добржинский // Современная наука и молодые учёные: матер. 15-й междунар. НПК. Пенза: Наука и Просвещение, 2024. С. 20–23.

5. Зверев А. А. Особенности использования систем мониторинга в государственных учреждениях / А. А. Зверев, И. П. Карпов // Информационные технологии в государственном управлении. 2024. № 2. С. 112–119.

6. Проничев А. В. Применение открытого программного обеспечения в системах мониторинга: российский опыт / А. В. Проничев, О. И. Лисов // Открытые системы. СУБД. 2023. № 3. С. 45–51.

7. Горелик С. Л. Разработка масштабируемых систем мониторинга сетевой инфраструктуры / С. Л. Горелик, С. В. Белов // Прикладная информатика. 2024. № 1. С. 78–85.

УДК 004.89

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ ПОБОЧНЫХ ЭФФЕКТОВ ПОЛИПРАГМАЗИИ

С. А. Котов, С. Ю. Пичковская[1]
Научный руководитель О. В. Непомнящий[1]
Кандидат технических наук, заведующий кафедрой вычислительной техники

[1]*Сибирский федеральный университет*

Одновременное назначение нескольких лекарственных препаратов (полипрагмазия) приводит к неожиданным и нежелательным взаимодействиям, которые трудно предсказать традиционными методами. В связи с этим особую актуальность приобретает использование искусственного интеллекта (ИИ), способного анализировать большие объёмы медицинских данных и выявлять скрытые закономерности [1; 2].

На сегодняшний день в прогнозировании побочных эффектов активно применяются различные методы машинного обучения, такие как

© Котов С. А., Пичковская С. Ю., 2025

регрессионные модели (логистическая регрессия, *LASSO* и *Ridge*-регрессия), деревья решений, случайные леса и нейронные сети. Особенно перспективными считаются графовые нейронные сети (*GNN*), которые эффективно моделируют сложные лекарственные взаимодействия. Тем не менее большинство упомянутых подходов требуют значительных вычислительных ресурсов и имеют ограничения в интерпретации получаемых результатов, что затрудняет их внедрение в клиническую практику [3].

Для повышения эффективности предложенного подхода был проведён дополнительный анализ, который позволил оценить влияние отдельных компонентов модели на итоговые результаты. В частности, изучалось воздействие метода главных компонент (*PCA*) на точность и стабильность прогнозов. Было выявлено, что применение PCA позволяет сократить размерность признакового пространства примерно на 40 % без существенной потери информации. Это ускоряет процесс обучения моделей и улучшает обобщающую способность нейронной сети [4].

Также была проведена оценка чувствительности модели к изменениям объёма и качества исходных данных. Результаты показали, что предложенная модель устойчива к небольшим колебаниям в данных и сохраняет высокие показатели точности и AUC-ROC, что подчёркивает её пригодность для применения в реальных клинических условиях, где данные часто бывают неполными или неоднородными.

Особое внимание уделено интерпретируемости модели. Введение регрессионного анализа на финальном этапе обработки данных позволило повысить не только точность предсказаний, но и прозрачность принимаемых решений.

Это особенно важно для врачей, которым необходимо понимать, по каким критериям модель выносит предположения о возможных побочных эффектах.

Отдельно был рассмотрен вопрос масштабируемости предлагаемого решения. Было установлено, что модель хорошо масштабируется при увеличении объёма данных, не теряя в производительности. Тестирование на более крупных наборах данных подтвердило, что увеличение количества обучающих примеров положительно влияет на качество и устойчивость прогнозов.

Тестирование предложенного подхода проводилось на открытых базах данных TwoSides и DrugBank. Предлагаемая модель продемонстрировала высокую точность и стабильность, превосходя традиционные методы по таким метрикам, как Accuracy, AUC-ROC и F-мера. Сравнительные результаты различных методов представлены в таблице.

Таким образом, проведённый анализ подтвердил высокую практическую значимость разработанного подхода и возможность его эффективного использования в медицинских информационных системах для предотвращения побочных эффектов при полипрагмазии.

Таблица 1

Сравнительные результаты различных методов

Метод	*Accuracy*	*AUC-ROC*	*F*-мера
Логистическая регрессия	0,78	0,81	0,76
Случайный лес	0,83	0,85	0,82
GNN	0,88	0,90	0,87
Предлагаемая модель	0,93	0,95	0,92

Разработанный подход на основе комбинации методов искусственного интеллекта продемонстрировал высокую эффективность в прогнозировании побочных эффектов при полипрагмазии. Использование PCA позволило сократить размерность данных, а ансамбли нейронных сетей значительно повысили точность прогноза. Предлагаемая модель может быть рекомендована для интеграции в информационные системы медицинских учреждений для улучшения качества медицинской помощи.

Список литературы

1. Schölkopf B. Empirical Inference: Festschrift in Honor of Vladimir N. Vapnik / B. Schölkopf, Z. Luo, V. Vovk. Springer, 2013. 306 p.

2. Zitnik M. Graph Convolutional Networks / M. Zitnik, M. Agrawal, J. Leskovec // Bioinformatics. 2018.

3. Rendle S. Factorization Machines / S. Rendle // ACM Transactions on Intelligent Systems and Technology. 2012.

4. Vilar S. Detection of Drug Interactions / S. Vilar // Briefings in Bioinformatics. 2018.

УДК 004.42:81'33

СЕРВЕРНАЯ ЧАСТЬ МИКРОСЕРВИСА ДЛЯ УПРАВЛЕНИЯ УЧЁТНЫМИ ЗАПИСЯМИ В ОРГАНИЗАЦИИ

М. И. Краев[1]

Научный руководитель Л. И. Покидышева[1]

Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

В современном мире, где бизнес-среда уже долгое время опирается на информационные технологии, эффективное управление учётными записями пользователей становится ключевым аспектом успешного функционирования организаций и предоставления услуг. Развитие микросервисной архитектуры в разработке программного обеспечения, в свою очередь, позволяет создавать гибкие и масштабируемые решения, способные обеспечить оптимальное управление учётными данными.

© Краев М. И., 2025

Целью данной работы является разработка серверной части микросервиса для управления учётными записями в организации.

Актуальность работы обуславливается следующим. В организации ООО «Сиб-ИТ» разрабатывается информационная система, нацеленная на упрощение ведения бизнес-процессов, связанных с охранной деятельностью. В настоящее время у пользователей нет возможности самостоятельно менять пароли для своих учётных записей. Чтобы выполнить эту процедуру, они вынуждены обращаться к специальному сотруднику – администратору учётных записей, который должен самостоятельно обновлять информацию в базе данных. Кроме того, этому сотруднику приходится вручную создавать новые учётные записи и настраивать им права доступа к различным модулям системы. Этот процесс отнимает много времени и сопряжён с риском ошибок или утечки конфиденциальных данных.

В связи с этим было принято решение о необходимости внедрения в систему специализированного микросервиса, который обеспечит безопасность учётных данных пользователей, повысит эффективность управления ими и будет отвечать требованиям к масштабируемости системы.

На рынке программного обеспечения существует немало готовых решений для управления учётными записями. Они называются IdM (Identity Management). В нынешнее время IdM-системы становятся всё более востребованными как инструмент централизованного контроля над учётными записями и правами пользователей в корпоративных средах.

При исследовании существующих решений были проанализированы следующие продукты: 1IDM [1], Avanpost IDM [2], ОТР.УСБ, Ankey IDM.

В таблице представлены результаты анализа.

Таблица 1

Сравнительный анализ аналогов

Продукт	**Портал пользо-вателя**	**Управление жизненным циклом учётных записей**	**Управление правами доступа**	**Анализ рисков компрометации данных**	**Интеграция через *REST***
1*IDM*	Нет	Да	Да	Нет	Нет
Avanpost IDM	Нет	Да	Да	Да	Да
ОТР.УСБ	Нет	Да	Да	Нет	Да
Ankey IDM	Нет	Да	Да	Нет	Да
ООО «Сиб-ИТ»	Да	Да	Да	Да	Да

В ходе анализа существующих решений было установлено, что больше всего установленным требованиям соответствует *Avanpost IDM*. Однако, в этой системе отсутствует портал пользователя, который является неотъемлемым базовым функционалом. Кроме того, руководство организации посчитало, что данный продукт имеет излишний функционал, что способно затруднить его внедрение и эксплуатацию.

В связи с этим было принято решение о разработке собственного микросервиса, который будет отвечать всем необходимым критериям и будет сразу внедрён в существующую информационную систему.

Анализ аналогов позволил выставить функциональные требования к разрабатываемому микросервису:

– интеграция через REST [3] по причине гибкости и широкой поддержки данного протокола;

– наличие портала пользователя, в котором он сможет сменить пароль и перейти в модули через меню;

– функционал для управления жизненным циклом учётных записей;

– возможность управления правами доступа;

– обеспечение автоматизации и безопасности процессов управления учётными записями.

Для разработки серверной части микросервиса для управления учётными записями использовались следующие технологии: Golang – компилируемый многопоточный язык программирования от Google с открытым исходным кодом; PostgreSQL – объектно-реляционная система управления базами данных с открытым исходным кодом; REST – архитектурный стиль взаимодействия между клиентом и сервером.

Для создания микросервиса управления учётными записями пользователей было решено следовать принципам микросервисной архитектуры. На рисунке представлена структурная схема решения, которая включает в себя:

– клиентскую часть, через которую пользователь может обращаться к серверной части модуля;

– службу авторизации, через которую пользователь входит в аккаунт и получает токен для дальнейших запросов на сервер;

– базу данных, в которой хранится вся информация об учётных записях;

– микросервис для управления аккаунтами, в котором происходит обработка запросов клиента.

Рисунок 1. Архитектура системы

Управление доступом к микросервису осуществляется следующим образом. Пользователь проходит аутентификацию, отправляя учётные данные на сервер. При успешной проверке генерируется токен с данными (логин, роль, права доступа). После авторизации интерфейс модуля адаптируется под роль

пользователя. Доступ к данным контролируется через токен (проверка прав на чтение/запись), а также на уровне БД – через групповые роли и *RLS* (ограничение видимости строк) [4]. Дополнительно ведётся журнал событий для мониторинга активности и безопасности.

Итак, разработанная серверная часть микросервиса для управления учётными записями была успешно интегрирована в информационную систему организации. Её реализация оптимизирует процессы администрирования аккаунтов и предоставляет пользователям удобный личный кабинет с полным набором необходимых функций.

Список литературы

1. 1IDM: система управления учётными записями. 2023. URL: 1idm.ru.

2. Avanpost IDM: система управления учётными записями. 2021. URL: avanpost.ru/products/avanpost-idm.

3. Проектирование веб-API RESTFUL // Microsoft Learn. 2022. URL: learn.microsoft.com/ru-ru/azure/architecture/best-practices/api-design.

4. RLS // Microsoft Learn. 2023. URL: learn.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16.

УДК 004

СИСТЕМА АНАЛИТИКИ МЕДИЦИНСКИХ ДАННЫХ

С. А. Ману[1]

Научный руководитель Д. А. Кузьмин[1]

Кандидат технических наук, заведующий кафедрой высокопроизводительных вычислений

[1]*Сибирский федеральный университет*

Актуальность эффективного использования данных в области медицинской реабилитации постоянно возрастает, особенно в связи с необходимостью повышения точности и персонализации лечебных мероприятий. Особую значимость приобретает проблема реабилитации пациентов, перенёсших инсульт и другие тяжёлые заболевания. Ежегодно в Российской Федерации регистрируется около 450 тыс. новых случаев инсультов, что значительно увеличивает спрос на эффективные реабилитационные решения.

Использование аналитической системы позволяет агрегировать и анализировать большие объёмы данных о взаимодействии пользователей с медицинским программно-аппаратным комплексом *SensoRehab* в режиме реального времени. Медицинской компании, которая принимает решения на

© Ману С. А., 2025

основе аналитики данных, такая система даёт возможность отслеживать эффективность создания и внедрения новых решений в свой продукт.

Аналитическая система состоит из трёх ключевых компонентов: интерфейса сбора пользовательских данных, аналитического модуля и инструментов визуализации.

Интерфейс сбора пользовательских данных обеспечивает оперативный сбор информации о действиях пользователей как с клиентской части приложения, когда необходимо собрать информацию о поведенческом паттерне пользователя, так и с серверной части приложения, где находятся обезличенные результаты реабилитации. Аналитический модуль отвечает за выявление поведенческих паттернов на основе сравнения тех данных, что система получает с клиентской части приложения, с теми данными, которые система получает с серверной части приложения. Инструменты визуализации представляют результаты анализа в виде агрегированных таблиц, различных графиков и отчётов.

Преимуществами использования аналитической системы в медицинской реабилитации на основе программно-аппаратного комплекса *SensoRehab* являются:

– возможность оперативного отслеживания эффективности применения оборудования;

– выявление поведенческих паттернов пользователей для дальнейшего повышения эффективности и работоспособности приложения;

– минимизация субъективных ошибок за счёт автоматизированного анализа данных;

– улучшение качества медицинской помощи путём персонализации лечебных методик;

– возможность проводить детальный анализ и прогнозирование эффективности реабилитационных мероприятий на основе полученных данных;

– оптимизация сбора обратной связи от пользователей при реализации нового функционала комплекса *SensoRehab*.

Аналитическая система обеспечивает достоверную оценку уже реализованного функционала и показывает точность прогноза эффективности создаваемых реабилитационных мероприятий. Анализ осуществлялся на пациентах с различными медицинскими диагнозами, в разнообразных условиях применения оборудования.

На текущий момент технология уже интегрирована с медицинским программно-аппаратным комплексом *SensoRehab*; разработаны и успешно применяются специализированные методы сбора, агрегации и аналитики данных, которые повышают точность и эффективность принятия решений по дальнейшей разработке видов реабилитации после инсульта и других неврологических заболеваний и удовлетворяют растущий спрос на персонализированные медицинские решения.

Список литературы

1. Панов А. И. Использование аналитики больших данных в здравоохранении / А. И. Панов // Экономика и качество систем связи. 2023. URL: cyberleninka.ru/article/n/ispolzovanie-analitiki-bolshih-dannyh.

2. Проблемы и перспективы информационных технологий в здравоохранении России: современные реалии // Физическая и реабилитационная медицина. URL: journals.eco-vector.com/2658-6843/article/110384/pdf_2.

3. Amplitude Documentation. URL: amplitude.com.

4. Davenport T. Competing on Analytics: the New Science of Winning / T. Davenport, J. Harris. Boston, USA: Harvard Business Review Press, 2017. 256 p.

УДК 004.31

КОМПЛЕКС ТЕСТИРОВАНИЯ ОДНОКРИСТАЛЬНОГО ВЫЧИСЛИТЕЛЯ ДЛЯ ПОДАВЛЕНИЯ РЕВЕРБЕРАЦИОННЫХ ПОМЕХ

Д. О. Непомнящий, А. А. Чаругин[1]
Научный руководитель Р. В. Брежнев[1]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

При создании приборов обработки низкочастотных сигналов, в т. ч. звуковоспроизводящих устройств, медицинского и научно-исследовательского оборудования, особое внимание уделяется разработке эффективных систем подавления реверберационных помех [1]. При этом хорошие результаты получают посредством методов адаптивной фильтрации. Например, используют подходы, основанные на алгоритмах *LMS*, *NLMS*, *FDAF* [2].

Для повышения эффективности было предложено комбинированное решение, включающее применение адаптивного алгоритма и нейронной сети [3]. Такой подход, в отличие от известных, позволяет не только значительно снизить основной эхо-сигнал, но и избавиться от остаточного эха.

Результаты моделирования адаптивного фильтра, создания моделей нейронных сетей и комплексной совместной отработки комбинированного фильтра в режимах компьютерного моделирования позволили перейти к практической реализации вычислителя на базе программируемой логической интегральной схемы (ПЛИС) [3]. Однако, для лабораторного тестирования требуется создание рабочего места инженера-исследователя, предназначенного для натурной отработки получаемых аппаратных и программных решений.

© Непомнящий Д. О., Чаругин А. А., 2025

Основной задачей комплекса является формирование двухканального аудиосигнала, стробируемого цифровым импульсом (рис. 1).

По одному из каналов передаётся основной сигнал, а по-другому – сгенерированный сигнал помехи. При этом сигналы подаются фрагментами согласно разработанной методике обучения и тестирования адаптивного фильтра и нейронной сети, входящей в состав вычислителя (рис. 2). Каждый фрагмент стробируется цифровым сигналом для обеспечения синхронизации, в т. ч. при отработке функционирования входных каскадов аналого-цифрового (АЦП) и выходных каскадов цифро-аналогового преобразователей (ЦАП).

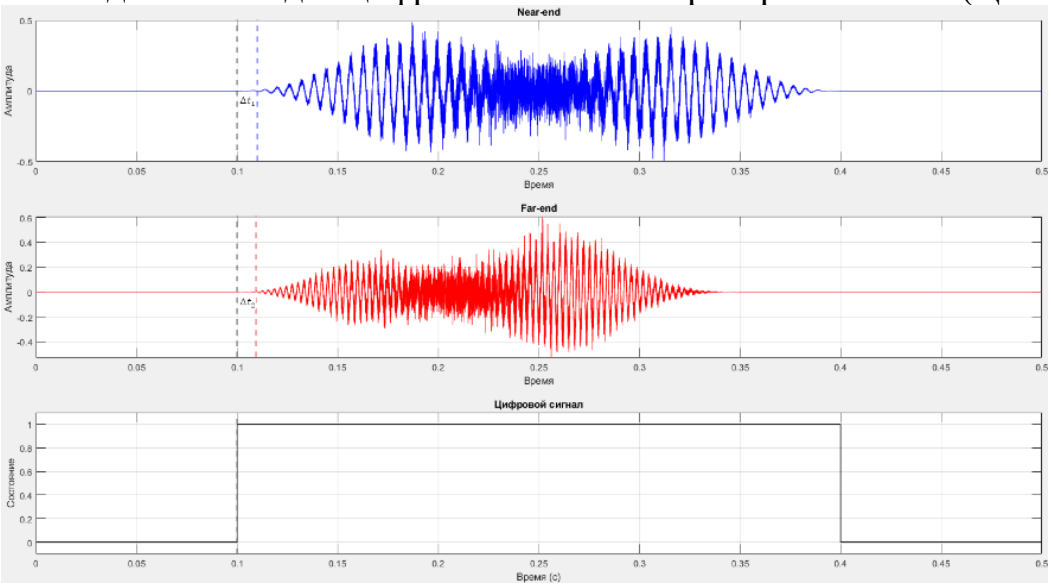


Рисунок 1. Временная диаграмма генерируемых сигналов

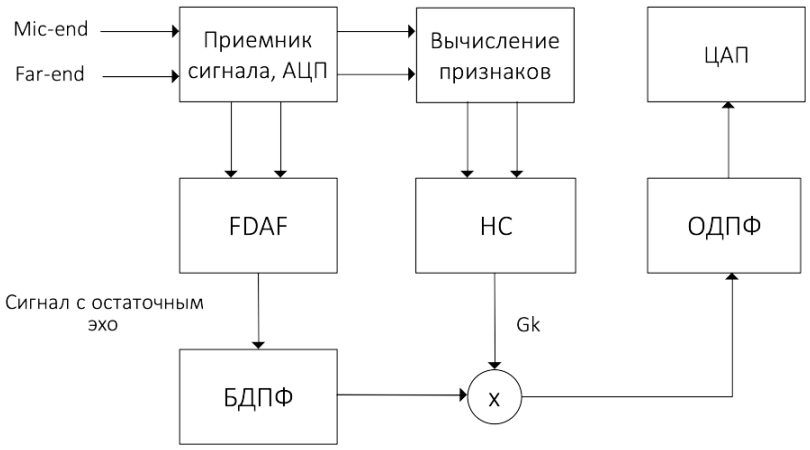


Рисунок 2. Архитектура комбинированного фильтра

Сигнал с микрофона Mic-end и сигнал «дальнего конца» Far-end поступают на приёмник аналогового сигнала и проходят аналогово-цифровое преобразование. Далее цифровые сигналы передаются в модуль подавления эха, функционирующий на основе алгоритма адаптивной фильтрации, который позволяет адаптировать коэффициенты фильтра в зависимости от изменяющихся условий сигнала в частотной области. В результате работы адаптивного фильтра выполняется подавление основного эха. При этом в выходном сигнале, как правило, присутствует остаточное эхо.

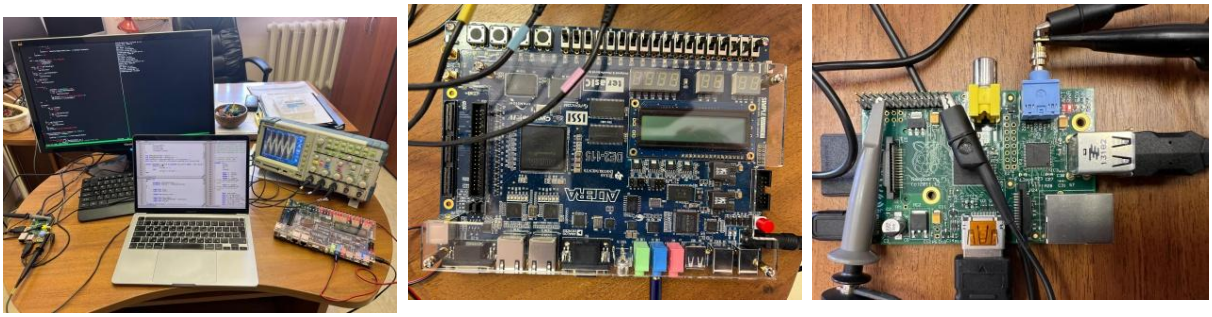
На следующем этапе используется предварительно обученная нейронная сеть, которая позволяет компенсировать остаточный эхо-сигнал. На рекуррентную нейронную сеть покадрово поступают признаки, рассчитываемые для сигнала Far-end и микрофонного сигнала Mic-end. На выходе нейронной сети формируются коэффициенты предсказания значений Gk для подавления остаточного эхо-сигнала путём изменения соответствующих полос его частотного диапазона.

Далее для сигнала, прошедшего этап подавления эха с помощью адаптивного фильтра и содержащего остаточное эхо, выполняется вычисление спектра с помощью алгоритма быстрого преобразования Фурье. Полученный спектр проходит разбивку на 22 частотных диапазона, соответствующих шкале Барка, которые корректируются на коэффициенты Gk.

Далее над обработанным таким образом спектром производится операция обратного преобразования Фурье, результатом которой является сигнал во временной области с изменённым частотным диапазоном остаточного эхо.

При реализации стенда для тестирования фильтра в качестве формирователя тестовых сигналов и сигналов управления используется мини-компьютер Raspberry Pi первого поколения, имеющий в своём составе звуковую карту с 3.5-jack стереовыходом. Такой подход позволяет применять готовые драйверы для устройств вывода информации и файловую систему для подготовки и хранения данных в виде аудиофрагментов заданной частоты воспроизведения и формата. Программная оболочка реализуется посредством интерпретируемого языка программирования Golang и функционирует под управлением операционной системы Debian Linux, что обеспечивает использование системных потоков. Для вывода аудиосигналов используется звуковая подсистема Alsa. Также в состав испытательного комплекса входят: отладочная плата Intel-Altera DE115 с ПЛИС и аудиокодером, персональный компьютер, два монитора, цифровой четырёхканальный осциллограф с функцией записи и хранения данных, вспомогательное оборудование.

На рисунке 3 представлены результаты создания лабораторного комплекса инженера-исследователя.



а *б* *в*

Рисунок 3. Комплекс тестирования однокристального вычислителя:
а – общий вид лабораторного комплекса; б – плата ПЛИС цифрового фильтра;
в – плата генератора тестовых сигналов

Предложен комбинированный метод подавления реверберационных помех, суть которого заключается в использовании адаптивного фильтра *FDAF* и предварительно обученной рекуррентной нейронной сети. Результаты моделирования позволили перейти к практической реализации метода в виде однокристального вычислителя – фильтра подавления реверберационных помех. Цифровая часть фильтра реализуется посредством ПЛИС. При этом для тестирования разработанной системы в лабораторных условиях создан комплекс инженера-исследователя, включающий необходимый комплект оборудования и разработанное программное обеспечение.

Список литературы

1. Вартанян И. А. Физиология сенсорных систем: Руководство И. А. Вартанян. СПб.: Лань, 2006. 224 с.

2. Bensouda M. Y. Improved Fast NLMS Algorithm based on Variable Forgetting Factor Technique for Acoustic Echo Cancellation / M. Y. Bensouda, A. Benallal // 8th International Conference on Image and Signal Processing and their Applications (ISPA). Biskra, Algeria, 2024. Pp. 1–6.

3. Медведев М. С. Метод подавления остаточного эха на основе адаптивного фильтра и технологии машинного обучения / М. С. Медведев, А. Г. Хантимиров, Д. О. Непомнящий и др. // Радиотехника. 2024. Т. 78. № 12. С. 31–40.

УДК 004.42:81'33

Клиент-серверное веб-приложение виртуального MIDI-контроллера

К. А. Падерин[1]
Научный руководитель Л. И. Покидышева[1]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

Многие музыканты, использующие компьютер для обработки звука музыкальных инструментов, сталкиваются с необходимостью оперативно изменять параметры эффектов, изменяющих звуковой сигнал, прямо во время игры. Традиционно для этого применяются физические *MIDI*-контроллеры и педали, но у них есть существенные ограничения в виде высокой стоимости, громоздкости и необходимости музыканту отвлекаться на управление во время игры. Актуальность данной работы заключается в необходимости разработки программного решения, которое предоставит возможность автоматизировать процесс управления музыкальным программным обеспечением (ПО) посредством записи и дальнейшего воспроизведения *MIDI-CC*-сообщений [1].

© Падерин К. А., 2025

При исследовании рынка ПО для автоматизации звуковых эффектов были проанализированы следующие популярные цифровые аудиостанции: *FL Studio*, *Reaper*, *Ableton Live*, *Bitwig Studio*, *Cubase*. Наиболее детальному сравнению подверглись *FL Studio* и *Reaper* как наиболее релевантные аналоги (табл.).

Таблица 1

Сравнение аналогов

Название	**Автоматизация**	**Требует установки**	**Специализированное решение**	**Гибкая автоматизация**
FL Studio	+	–	–	+
Reaper	+	–	–	+
Разрабатываемое решение	+	+	+	+

Анализ показал, что существующие решения обеспечивают автоматизацию, но в рамках комплексных решений все анализируемые программы требуют установки на устройство пользователя, а также, что разобранные решения предоставляют удобный интерфейс автоматизации в виде графиков.

В ходе анализа аналогов были выставлены требования к разрабатываемому решению. Реализация решения должна быть в виде веб-приложения для обеспечения кроссплатформенности и хранения данных пользователя в облаке, а также обладать интуитивной системой автоматизации на основе линейных графиков.

Клиентская часть разработана с использованием библиотеки React.js [2]. Визуализация графиков автоматизации реализована посредством библиотеки Echarts [3], предоставляющей возможность создавать гибкие графики. Для создания серверной части использовался фреймворк ASP.Net Web API [4]. Для работы с базой данных использовалось объектно-реляционное отображение Entity Framework Core [5].

Приложение реализовано по клиент-серверной модели с поддержкой *MIDI*. Веб-клиент выполняет две основные функции: передачу *MIDI*-команд через *Web MIDI API* и взаимодействие с сервером через *REST API*. Сервер обрабатывает запросы, выполняет бизнес-логику и управляет данными, используя СУБД и облачное хранилище.

Ключевая особенность – виртуальный *MIDI*-порт, эмулирующий физический контроллер и обеспечивающий совместимость с аудиопрограммами.

На рисунках 1, 2 показаны окна пресета и графиков автоматизации.

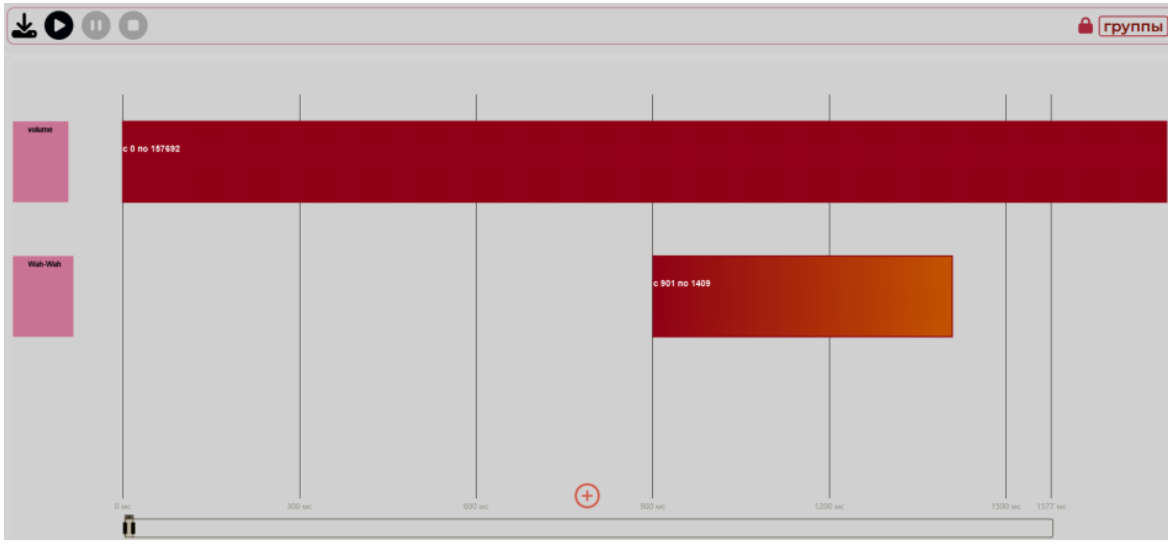


Рисунок 1. Схема пресета

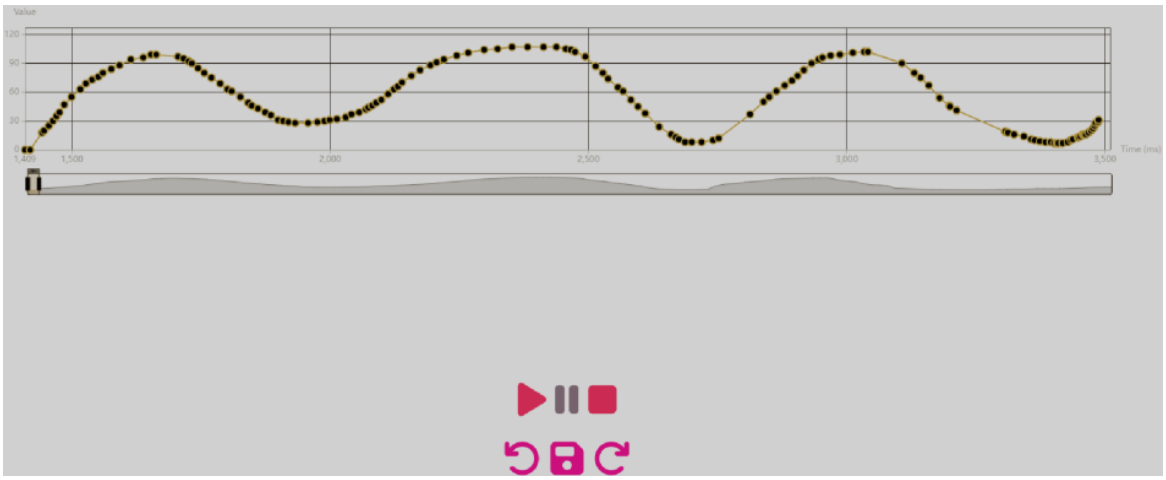


Рисунок 2. Схема графика автоматизации

В окне пресета происходит конфигурация автоматизации через элементы управления (розовые прямоугольники на рис. 1). Красные прямоугольники определяют в себе графики автоматизации (рис. 2). Двигая прямоугольники вдоль горизонтальной временной оси, можно изменять время начала срабатывания графиков автоматизации. Графики автоматизации (рис. 2) позволяют визуально контролировать динамику параметров (громкость, эффекты) с точностью до миллисекунд.

Таким образом, разработанное веб-приложение решает ключевые проблемы современных музыкантов, предлагая доступную альтернативу дорогостоящим физическим *MIDI*-контроллерам. Реализованная система сочетает преимущества специализированного решения для автоматизации с кроссплатформенностью веб-технологий. Приложение успешно устраняет недостатки существующих решений, предлагая музыкантам гибкий инструмент для творчества без необходимости использования дополнительного оборудования.

Список литературы

1. Что такое MIDI-события и зачем они нужны // Samesound. 2017. URL:

samesound.ru/prod/70572-midi-messages-explain.

2. Документация // React.js 2023. URL: react.dev/blog/2023/03/16/ introducing-react-dev.

3. Документация // Echarts. 2021. URL: echarts.apache.org/option.html.

4. Руководство по ASP.NET Core 8 // Metanit. 2024. URL: metanit.com/ sharp/aspnet6.

5. Документация Entity Framework Core // Microsoft Learn. 2023. URL: learn.microsoft.com/ru-ru/ef/core.

УДК 004.722.45

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПАРАМЕТРОВ АНАЛИЗА ЧАСТОТНОГО РЕСУРСА НА ДЕТЕКТИРОВАНИЕ СИГНАЛОВ

И. В. Петров[1, 2], А. В. Архипов[2]
Научный руководитель Е. С. Бывшев[1]
старший преподаватель
Научный руководитель А. А. Комаров[2]

[1]Сибирский федеральный университет

[2]АО «НПП «Радиосвязь»

При реализации децентрализованной системы связи с многостанционным доступом с частотным разделением возникает потребность в определении занятости частотного ресурса. Одним из решений является спектральный анализ сигнала. Такой подход подразумевает использование быстрого преобразования Фурье (БПФ), накопление отсчётов и детекцию по уровню. Настоящая работа посвящена определению влияния параметров модели анализатора частотного ресурса на точность детектирования [1].

В данной работе рассматривается *OQPSK*-сигнал с информационной скоростью 9,6 кГц, сглаживающий фактор формирующего фильтра – 90 %, минимальное отношение «сигнал – шум» – 2 дБ. Система связи включает 50 полнодуплексных каналов и работает в энергоэффективном режиме. Блок БПФ принимает отсчёты с частотой 1,024 МГц.

На результат БПФ влияет вид оконной функции и интервал накопления (длина БПФ и количество усредняемых спектров). Для корректной работы алгоритма разрешающая способность БПФ должна минимизировать перекрытие защитных интервалов сигналами при максимальном *SNR* (*signal-to-noise ratio*) системы приблизительно 20 дБ [1]. В таблице приведено отклонение уровня энергии в защитном интервале от средней энергии шума для нескольких оконных функций различной длины.

© Петров И. В., Архипов А. В., 2025

Таблица 1

Отклонение энергии в защитном интервале от энергии шума с разной разрешающей способностью и оконной функцией при *SNR* 20 дБ

Оконная функция	Разность средней энергии в защитных диапазонах и средней энергии шума, дБ			
	БПФ – 256	БПФ – 512	БПФ – 1 024	БПФ – 2 048
Прямоугольное окно	3,9353	1,1797	0,3262	0,1654
Окно *flat-top*	4,6732	4,6556	1,5064	0,3364
Окно Ханна	4,1378	1,6060	0,2549	0,0642
Окно Хэмминга	4,3062	2,2132	0,3956	0,0174
Окно Блэкмана	4,2709	1,7785	0,2988	0,0075
Окно Чебышева	3,6222	0,8397	0,1034	0,0149

Значения, превосходящие минимальное отношение «сигнал – шум» системы, говорят об увеличении вероятности пропущенного детектирования (Probability miss detection – Pmd) сигналов с низкой энергетикой при наличии мощных сигналов. Таким образом, длина БПФ 256 и менее далее рассматриваться не будет.

По результатам экспериментов для оценки влияния вида оконной функции были построены кривые вероятности пропущенного детектирования от вероятности ложного детектирования (Probability false alarm – Pfa), представленные на рисунке 1, при одинаковом интервале накопления 16 мс.

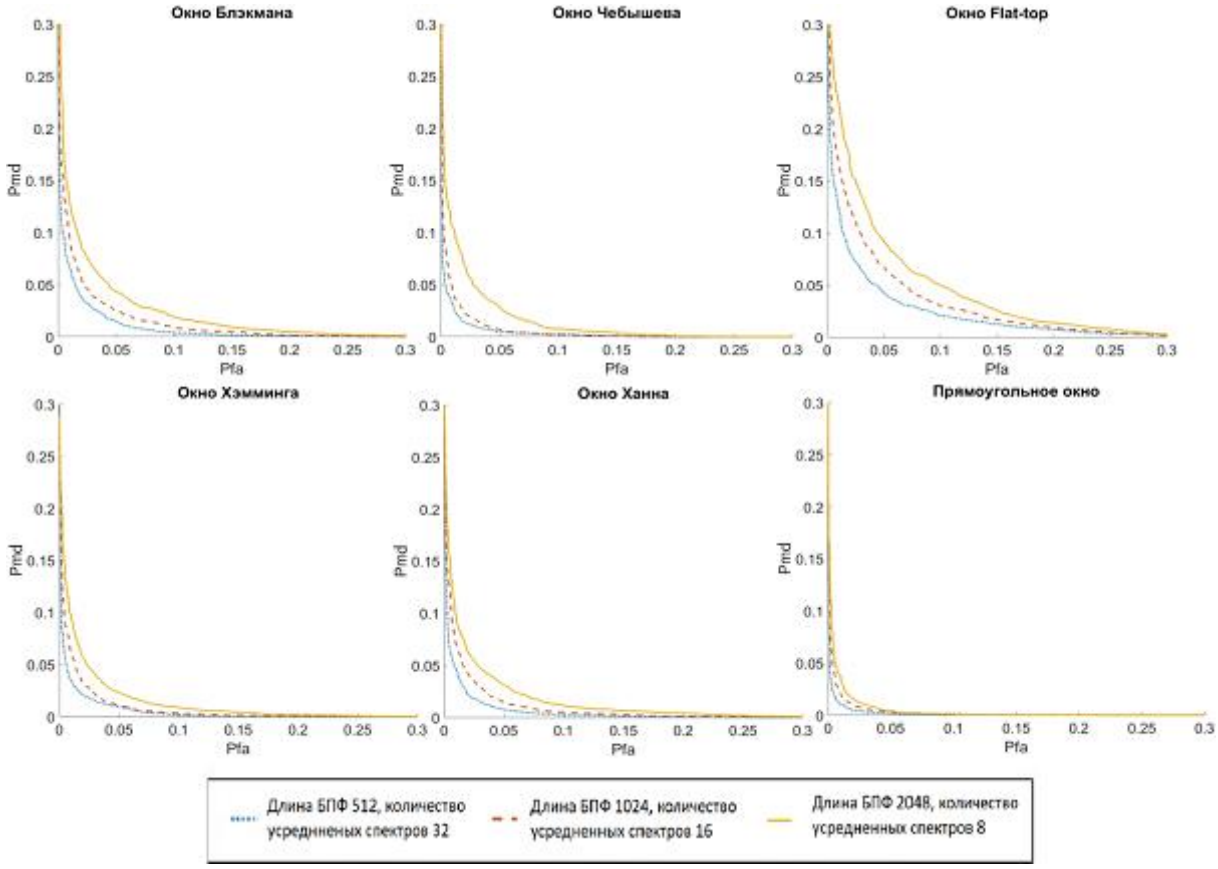


Рисунок 1. Графики оценки влияния оконных функций и разрешающей способности на качество детектирования при SNR 2 дБ

Прямоугольное окно обладает наибольшей избирательностью, что оказывает положительное влияние на качество детектирования. Боковые лепестки, являющиеся главным недостатком данного окна, не оказывают влияния на защитные интервалы ввиду низкой энергетики сигнала. Таким образом, наилучшее качество детектирования установлено при прямоугольном окне. Также уменьшение дисперсии посредством усреднения большего количества спектров показало лучшие результаты по сравнению с увеличением разрешающей способности БПФ.

На рисунке 2 представлены графики оценки влияния интервала накопления на качество детектирования.

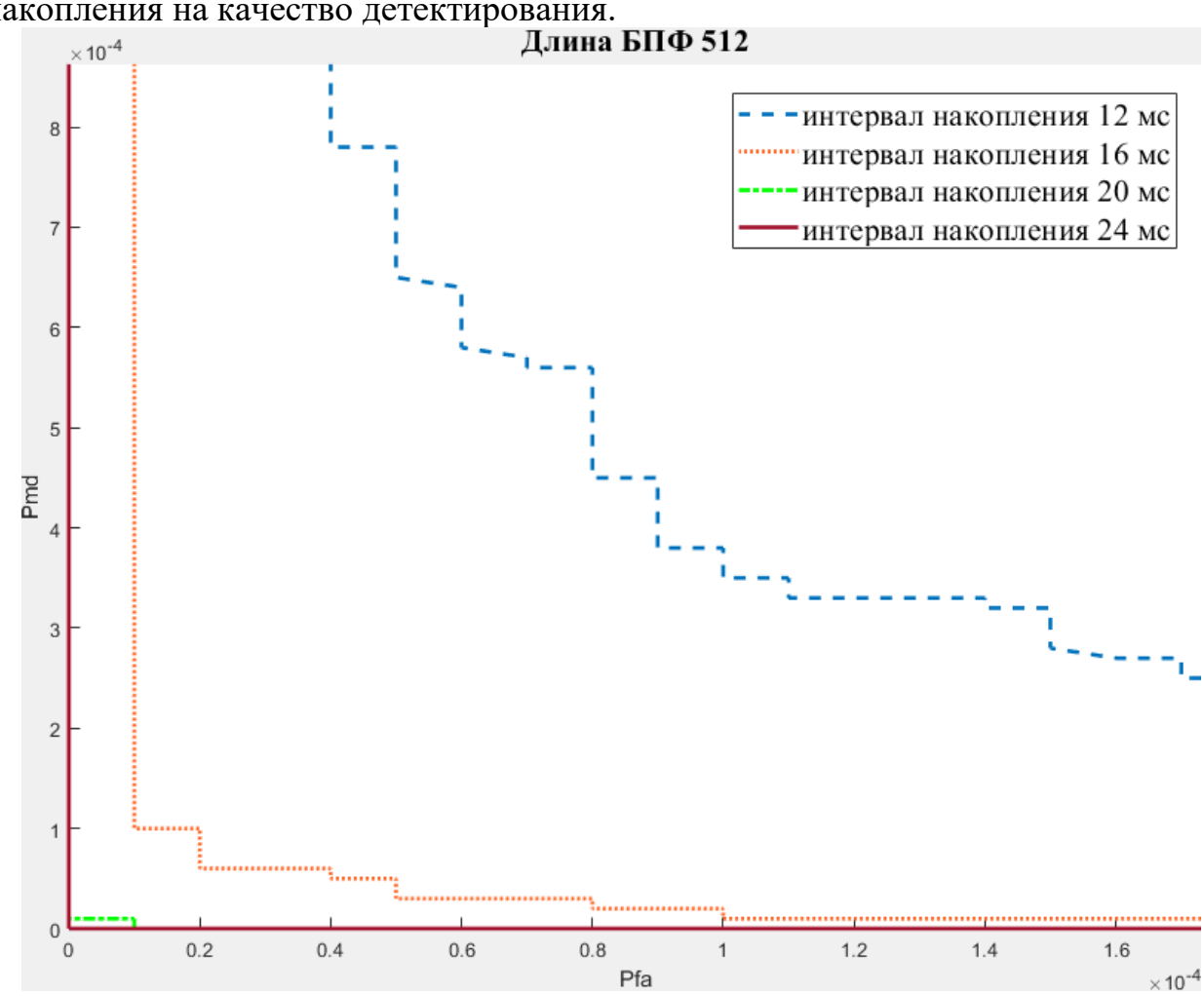


Рисунок 2. Графики оценки влияния интервала накопления
на качество детектирования при SNR 2 дБ

Таким образом, при интервале накопления от 24 мс вероятность ошибки не превышает 10*e*–5, что удовлетворяет требованиям точности детектирования сигналов данной системы.

В результате выполнения данной работы было установлено, что длина БПФ должна быть не менее 512, вид окна – прямоугольное окно, уменьшение дисперсии важнее увеличения разрешающей способности БПФ, достаточный интервал накопления – 24 мс. Аппаратная реализация модели с такими

параметрами не требует большого количества вычислительных ресурсов и обеспечивает достаточно точные результаты за короткий промежуток времени.

Список литературы

1. Петров И. В. Анализ частотного ресурса бортового ретранслятора для систем связи с множественным частотным доступом / И. В. Петров, П. В. Луферчик, А. А. Комаров и др. // Системы связи и радионавигации. 2024. С. 61.

УДК 004.94

КОРРЕКЦИЯ ОШИБОК В ИНЕРЦИАЛЬНЫХ НАВИГАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

А. А. Сиротинин [1, 2]
Научный руководитель – Д. В. Капулин[1]
Кандидат технических наук, директор Института космических и информационных технологий

[1]*Сибирский федеральный университет*

[2]*АО «НПП «Радиосвязь»*

На сегодняшний день инерциальные навигационные системы (ИНС) широко используются для решения задач навигации. Они обеспечивают высокоскоростные навигационные решения без необходимости в навигационных сигналах от внешних источников. Однако с течением времени точность работы ИНС ухудшается из-за накопления интегральных ошибок, возникающих в процессе работы, что связано с систематическими и случайными погрешностями показаний датчиков [1].

Для повышения эффективности работы ИНС разрабатываются различные методы и подходы, направленные на снижение влияния погрешностей и корректировку ошибок. К таким подходам относятся комплексирование ИНС с неавтономными навигационными системами, такими как глобальные спутниковые навигационные системы (ГСНС), а также применение различных алгоритмов фильтрации [2]. Тем не менее эти методы имеют свои ограничения и не позволяют полностью исключить ошибки навигации.

С развитием технологий нейросетей и машинного обучения активно появляются методы коррекции ошибок, основанные на применении методов глубокого обучения, являющихся подмножеством машинного обучения и использующих многослойные самообучающиеся нейронные сети.

Искусственные нейронные сети (*Artificial Neural Network*, *ANN*) представляют собой программную реализацию математической модели

© Сиротинин А. А., 2025

биологических нейронных сетей. Они не обладают заранее заданным алгоритмом работы и могут обучаться на основе входных данных.

В ряде исследований [3–4] были предложены алгоритмы, использующие *ANN* для коррекции погрешностей и комплексирования данных с инерциальных датчиков, что существенно повышает общую точность работы ИНС.

Рекуррентные нейронные сети (*RNN*) представляют собой разновидность *ANN*, характеризующуюся направленными обратными связями между элементами внутренней структуры и наличием внутреннего состояния. В отличие от традиционных нейронных сетей, *RNN* способны учитывать информацию, поступающую из предыдущих состояний, что делает их полезными для анализа последовательных данных, таких как текст, геномы, речь и временные ряды. В некоторых исследованиях предложено использовать *RNN* на базе структуры прямого распространения, которая использует последовательную информацию от предыдущих отсчётов [5].

Нейронные сети долгой краткосрочной памяти (*Long Short-Term Memory*, *LSTM*) представляют собой разновидность *RNN*, способную обучаться долговременным зависимостям. Алгоритмы *LSTM* могут быть использованы для компенсации погрешностей датчиков и их комплексирования. Например, в работе [6] была представлена *LSTM*-сеть для комплексирования данных визуальной одометрии и дешёвых инерциальных измерительных модулей.

Кроме того, *LSTM* может быть эффективно использована для уменьшения шумов, возникающих в инерциальных датчиках. В исследовании [7] был предложен метод моделирования ошибок с применением *LSTM* для выявления случайных погрешностей в гироскопах. Экспериментальные результаты показали, что однослойная *LSTM*-сеть может уменьшить стандартное отклонение на 42,4 % и ошибку ориентации на 52,0 %.

Управляемый рекуррентный блок (*Gated Recurrent Unit*, *GRU*) – это ещё одна разновидность *RNN*, схожая с *LSTM*, но предназначенная для упрощения и ускорения обучения при сохранении эффективности *LSTM*. В работе [8] демонстрируется использование *GRU* для подавления шумов гироскопа. *GRU* отличается от *LSTM* меньшим количеством компонентов, что способствует более высокой скорости обучения и лучшей производительности для определённых задач.

В исследовании [9] предложены гибридные архитектуры, комбинирующие *LSTM* и *GRU*. Сравнение их эффективности с методами, использующими только *LSTM* или *GRU*, показало, что гибридные *LSTM-GRU*-методы позволяют снизить ошибки определения ориентации на 72 %.

Таким образом, современные методы коррекции ошибок инерциальных навигационных систем на основе глубокого обучения значительно повышают их эффективность. Для достижения наилучших результатов эти методы могут быть эффективно интегрированы с традиционными методами коррекции или с другими подходами машинного обучения и нейросетями.

Список литературы

1. Wei W. SINS/SRS/GNS Autonomous Integrated Navigation System based on Spectral Redshift Velocity Measurements / W. Wei, Z. Gao, S. Gao et al. // Sensors. 2018. Vol. 18. No. 4. P. 1 145.

2. Strachan V. F. Inertial Measurement Technology in the Satellite Navigation Environment / V. F. Strachan // The Journal of Navigation. 2000. Vol. 53. Pp. 247–260.

3. Choi A. Single Inertial Sensor-based Neural Networks to Estimate COM-COP Inclination Angle during Walking / A. Choi, H. Jung, J. H. Mun // Sensors. 2019. Vol. 19. P. 2 974.

4. Chen H. Improving Inertial Sensor by Reducing Errors using Deep Learning Methodology / H. Chen, P. Aggarwal, T. M. Taha et al. // Proceedings of the NAECON 2018-IEEE National Aerospace and Electronics Conference. Dayton, USA, 2018. Pp. 197–202.

5. Subathra B. Recurrent Neuro Fuzzy and Fuzzy Neural Hybrid Networks: a Review / B. Subathra, T. K. Radhakrishnan // Instrumentation Science & Technology. 2012. Vol. 40. Pp. 29–50.

6. Chen C. Deep Neural Network based Inertial Odometry using Low-cost Inertial Measurement Units / C. Chen, C. X. Lu, J. Wahlström et al. // IEEE Transactions on Mobile Computing. 2021. Vol. 20. Pp. 1 351–1 364.

7. Jiang C. A MEMS IMU De-noising Method using Long Short Term Memory Recurrent Neural Networks (LSTM-RNN) / C. Jiang, S. Chen, Y. Chen et al. // Sensors. 2018. Vol. 18. P. 3 470.

8. Cho K. Learning Phrase Representations using RNN Encoder-decoder for Statistical Machine Translation / K. Cho, B. Van Merriënboer, C. Gulcehre et al. // arXiv Preprint. arXiv:1406.1078, 2014.

9. Jiang C. A Mixed Deep Recurrent Neural Network for MEMS Gyroscope Noise Suppressing / C. Jiang, Y. Chen, S. Chen et al. // Electronics. 2019. Vol. 8. P. 181.

УДК 004.42:81'33

Серверная часть платформы кадрового агентства

Е. В. Слукина[1]
Научный руководитель – Л. И. Покидышева[1]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

В условиях современного рынка, характеризующегося высокой конкуренцией и постоянными изменениями, кадровые агентства играют ключевую роль в обеспечении организаций квалифицированными специа-

© Слукина Е. В., 2025

листами. Эффективное управление процессами подбора и размещения персонала требует не только глубокого понимания потребностей клиентов, но и надёжной технологической инфраструктуры. Разработка серверной части платформы кадрового агентства становится важным шагом к оптимизации этих процессов, позволяя автоматизировать рутинные задачи, улучшить взаимодействие с клиентами и кандидатами, а также обеспечить безопасность и масштабируемость системы.

Целью данной работы является разработка серверной части платформы кадрового агентства.

Актуальность работы обуславливается следующими факторами. В организации ООО «Сиб-ИТ» разрабатывается платформа кадрового агентства, нацеленная на оптимизацию процессов подбора и управления персоналом. На данный момент пользователи сталкиваются с рядом трудностей: отсутствие единой базы данных по кандидатам и вакансиям, а также недостаточная автоматизация процессов обработки резюме и взаимодействия с кандидатами. В результате *HR*-специалистам приходится тратить значительное время на ручное введение данных и анализ информации, что увеличивает вероятность ошибок и снижает общую продуктивность работы.

В связи с этим было принято решение о необходимости разработки интегрированной платформы, которая обеспечит автоматизацию бизнес-процессов, связанных с подбором кадров, улучшит взаимодействие между кандидатами и работодателями, а также позволит проводить более глубокий анализ эффективности мероприятий по подбору персонала.

На сегодняшний день существует множество платформ, предлагающих услуги по подбору персонала.

При исследовании существующих решений были проанализированы следующие продукты: Поток Рекрутмент [1], *FriendWork Recruiter* [2], Воронка найма [3].

В таблице представлены результаты анализа.

Таблица 1

Сравнительный анализ аналогов

Продукт	**База данных вакансий**	**Администрирование**	**Воронка подбора персонала**	**Многопользовательский доступ**	**Управление обратной связью**
Поток Рекрутмент	Да	Да	Да	Да	Нет
FriendWork Recruiter	Да	Да	Да	Да	Нет
Воронка найма	Нет	Да	Да	Да	Нет
ООО «Сиб-ИТ»	Да	Да	Да	Да	Да

После сравнения аналогов приходим к выводу, что не существует системы, которая обладает ключевыми требованиями к продукту. Принято решение о проектировании продукта, который удовлетворит всем требованиям.

Для разработки серверной части платформы кадрового агентства использовались следующие технологии: Golang [4] – компилируемый многопоточный язык программирования от Google с открытым исходным кодом; PostgreSQL [5] – объектно-реляционная система управления базами данных с открытым исходным кодом; REST [6] – архитектурный стиль взаимодействия между клиентом и сервером.

Для создания платформы кадрового агентства было решено следовать принципам микросервисной архитектуры. На рисунке представлена структурная схема решения, которая включает в себя:

– клиентскую часть, через которую пользователь может обращаться к серверной части модуля;

– службу авторизации, через которую пользователь входит в аккаунт и получает токен для дальнейших запросов на сервер;

– базу данных, в которой хранится вся информация;

– микросервис кадрового агентства, в котором происходит обработка запросов клиента.

Рисунок 1. Архитектура системы

Управление доступом к микросервису осуществляется следующим образом. Пользователь проходит аутентификацию, отправляя учётные данные на сервер. При успешной проверке генерируется токен с данными (логин, роль, права доступа). После авторизации интерфейс модуля адаптируется под роль пользователя. Доступ к данным контролируется через токен (проверка прав на чтение/запись), а также на уровне БД – через групповые роли и *RLS* (ограничение видимости строк) [7]. Дополнительно ведётся журнал событий для мониторинга активности и безопасности.

Итак, разработанная серверная часть платформы кадрового агентства была успешно интегрирована в информационную систему организации, которая позволяет оптимизировать бизнес-процессы, связанные с поиском, отбором и трудоустройством кандидатов.

Список литературы

1. Поток Рекрутмент: система автоматизации HR-процессов. 2025. URL: potok.io.

2. FriendWork Recruiter: система для автоматизации рекрутинга. 2025.

URL: friend.work.

3. Воронка найма // Контур: HR-сервис для автоматизации подбора персонала. 2025. URL: kontur.ru/lp/hr-funnel.

4. Go: the Go Programming Language. 2025. URL: go.dev.

5. PostgreSQL: Open Source Database. 2025. URL: postgresql.org.

6. Проектирование веб-API RESTFUL // Microsoft Learn. 2022. URL: learn.microsoft.com/ru-ru/azure/architecture/best-practices/api-design.

7. RLS // Microsoft Learn. 2023. URL: learn.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16.

УДК 004.3

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МОДЕЛЕЙ АВТОНОМНОГО ВОЖДЕНИЯ ЗА СЧЁТ ИНТЕГРАЦИИ СЕМАНТИЧЕСКОГО ЛИДАРА

М. К. Тихонов[1]

Научный руководитель – О. В. Непомнящий[1]

Кандидат технических наук, заведующий кафедрой вычислительной техники

[1]*Сибирский федеральный университет*

Беспилотные автомобили полагаются на сложные системы датчиков для восприятия окружающей среды, и среди них лидар играет одну из ключевых ролей благодаря своей способности создавать высокоточные трёхмерные карты. Однако традиционные лидары имеют серьёзное ограничение: они фиксируют только расстояние до объектов, не определяя их природу. Например, такой лидар не может отличить пешехода, стоящего у обочины, от припаркованного автомобиля или дорожного знака. Для решения данной проблемы в беспилотных системах используют комбинацию лидара и камер. Камеры дополняют лидарные данные, позволяя не только определять положение объектов, но и распознавать их природу. Такая интеграция повышает точность восприятия, что критически важно для безопасного и эффективного автономного вождения [1].

Семантический лидар представляет собой технологию, которая объединяет данные традиционного лидара и семантической камеры, чтобы создать трёхмерную карту окружающей среды, где каждый объект не только локализован в пространстве, но и классифицирован по своему типу [2].

Процесс создания семантического лидара начинается с синхронизации данных, поступающих от лидара и семантической камеры. Эти устройства точно откалиброваны, чтобы их показания соответствовали друг другу во времени и пространстве. Далее данные лидара, представляющие собой облако точек с координатами (x, y, z), совмещаются с изображениями от семантической

© Тихонов М. К., 2025

камеры. Это достигается путём проецирования: каждая точка из облака лидара сопоставляется с определённым пикселем на изображении камеры, который уже имеет семантическую метку. Например, если точка лидара находится на расстоянии 5 м и соответствует пикселю, помеченному как «пешеход», эта точка получает такую же метку. Для этого используются методы компьютерного зрения и геометрические преобразования, учитывающие положение и ориентацию датчиков относительно друг друга. В результате получается трёхмерная карта, где каждая точка содержит не только пространственные координаты, но и информацию о типе объекта [3].

В рамках настоящего исследования были разработаны модели управления беспилотным автомобилем. Эти модели, построенные на алгоритмах глубокого обучения с подкреплением PPO (Proximal Policy Optimization) [4] и SAC (Soft Actor-Critic) [5] из библиотеки Stable-Baselines3 [6], получили названия MainPPO и MainSAC. Модели используют широкий набор датчиков: четыре RGB-камеры, четыре семантические камеры, вид с высоты птичьего полёта, традиционный лидар и семантический лидар. Главная задача системы – успешно пройти маршрут из пункта А в пункт Б в симуляторе CARLA, преодолевая 24 различных сценария дорожного движения, представленных разработчиками симулятора. Итоговая оценка вождения формируется на основе трёх ключевых показателей из таблицы лидеров [7].

1. Driving Score: R_iP_i – основная метрика таблицы лидеров, служащая произведением между показателями завершения маршрута и штрафами за нарушения, где R_i – процент выполнения i-го маршрута и P_i – штраф за нарушение i-го маршрута.

2. Route Completion: процент пройденного агентом расстояния от общего пути.

3. Infraction penalty: $P_i = \prod_j p_j^{\#\text{infractions}_j}$ – в таблице лидеров отслеживается несколько типов нарушений, и эта метрика объединяет все эти нарушения, совершённые агентом, в виде геометрического ряда. Агенты начинают с идеальной базовой оценки 1,0, которая уменьшается при каждом типе нарушения.

Результаты оценки моделей до и после применения семантического лидара представлены в таблицах 1 и 2 соответственно.

Таблица 1

Показатели до применения семантического лидара

Ранг	Модель	*Driving Score*	*Route Completion*	*Infraction Penalty*
1	*ReasonNet*	79,95	89,89	0,89
2	*InterFuser*	76,18	88,23	0,84
3	*TCP*	75,14	85,63	0,87
4	*MainSAC*	74,11	84,72	0,83
5	*MainPPO*	73,56	83,12	0,79

Таблица 2

Показатели после применения семантического лидара

Ранг	Модель	*Driving Score*	*Route Completion*	*Infraction Penalty*
1	*ReasonNet*	79,95	89,89	0,89
2	*MainSAC*	76,84	88,91	0,86
3	*InterFuser*	76,18	88,23	0,84
4	*MainPPO*	75,62	86,25	0,85
5	*TCP*	75,14	85,63	0,87

Рассмотрим полученные результаты более подробно. До применения семантического лидара в рейтинге лидировала модель ReasonNet с Driving Score 79,95, Route Completion 89,89 % и Infraction Penalty 0,89, за ней следовали InterFuser (76,18; 88,23 %; 0,84), TCP (75,14; 85,63 %; 0,87), MainSAC (74,11; 84,72 %; 0,83) и MainPPO (73,56; 83,12 %; 0,79). После внедрения семантического лидара позиции изменились: ReasonNet осталась на первом месте, но MainSAC поднялась на второе место (76,84; 88,91 %; 0,86), обойдя InterFuser, которая сместилась на третье место. Модель MainPPO заняла четвёртое место (75,62; 86,25 %; 0,85), обогнав TCP, которая стала пятой. Это показывает, что семантический лидар сильно повлиял на модели MainSAC и MainPPO, подняв их в рейтинге за счёт улучшения восприятия.

Применение семантического лидара при разработке моделей автономного вождения, как показывает настоящее исследование, значительно повышает их оценку вождения. Объединяя данные традиционного лидара и семантической камеры, эта технология создаёт трёхмерную карту с классифицированными объектами, что улучшает восприятие окружающей среды и позволяет принимать более точные решения.

Список литературы

1. Hirz M. Sensor and Object Recognition Technologies for Self-driving Cars / M. Hirz, B. Walzel // Computer-aided Design and Applications. 2018. Vol. 15. No. 4. Pp. 501–508.

2. Behley J. Semantickitti: a Dataset for Semantic Scene Understanding of Lidar Sequences / J. Behley et al. // Proceedings of the IEEE/CVF International Conference on Computer Vision. 2019. Pp. 9 297–9 307.

3. Ma W. C. Exploiting Sparse Semantic HD Maps for Self-driving Vehicle Localization / W. C. Ma et al. // IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2019. Pp. 5 304–5 311.

4. Schulman J. Proximal Policy Optimization Algorithms / J. Schulman et al. // arXiv preprint arXiv:1707.06347. 2017.

5. Haarnoja T. Soft Actor-critic: Off-policy Maximum Entropy Deep Reinforcement Learning with a Stochastic Actor / T. Haarnoja et al. // International Conference on Machine Learning. PMLR, 2018. Pp. 1 861–1 870.

6. Raffin A. Stable-baselines3: Reliable Reinforcement Learning Implementations / A. Raffin et al. // Journal of Machine Learning Research. 2021.

Vol. 22. No. 268. Pp. 1–8.

7. Evaluation Criteria for the Leaderboard 1.0. URL: leaderboard.carla.org/evaluation_v1_0.

Информационная безопасность

УДК 004.056+004.9+658.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ ОРГАНИЗАЦИЙ К ПРОТИВОДЕЙСТВИЮ CYBER KILL CHAIN

С. В. Андреева, Т. С. Котоманов, К. Е. Манакова[1]
Научный руководитель В. Б. Туговиков[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

Cyber Kill Chain (цепочка кибератак) представляет собой модель, описывающую процесс осуществления целевой кибератаки. Каждый этап этой цепочки предоставляет возможности для противодействия угрозам. В докладе проводится сравнительный анализ подходов к противодействию Cyber Kill Chain в различных типах организаций: государственной корпорации, крупном коммерческом учреждении и у ведущих разработчиков технологий в сфере информационной безопасности.

Актуальность темы определяется постоянным ростом числа и сложности кибератак, направленных на различные секторы экономики. Современные угрозы, такие как целевые атаки, становятся всё более изощрёнными, и для успешной защиты важно понимать каждый этап кибератаки и соответствующим образом разрабатывать защитные меры. Модель Cyber Kill Chain, предложенная Lockheed Martin, предоставляет чёткую структуру для анализа и предотвращения таких атак, что делает её полезным инструментом для построения стратегии киберзащиты в различных организациях. Учитывая, что организации различного масштаба сталкиваются с разными угрозами, подходы к защите от кибератак могут значительно различаться. Полезность исследования заключается в том, что оно позволяет не только классифицировать и понять уязвимости различных типов организаций, но и выработать на основе этого эффективные меры защиты.

Госкорпорация «Росатом» реализует комплексный подход к защите от киберугроз, основанный на многоуровневой системе безопасности. В рамках IT-инфраструктуры используются средства защиты от несанкционированного доступа для операционных систем Windows и Linux, защищённые каналы связи, виртуализация, а также системы мониторинга интернет-угроз. Организация обладает лицензиями ФСТЭК, ФСБ и Министерства обороны, что подтверждает соответствие строгим стандартам информационной безопасности. Особое внимание уделяется защите от инсайдеров и внешних угроз, включая фишинг и целевые атаки. Кроме того, в «Росатоме» действует центр «Атомзащитаинформ», который занимается разработкой методологий защиты, сертификацией средств безопасности и аудитом эффективности мер защиты. Для противодействия атакам

© Андреева С. В., Котоманов Т. С., Манакова К. Е., 2025

в «Атомзащитаинформ» применяются такие инструменты, как статические и динамические анализаторы кода (Svace, Crusher), системы анализа защищённости (Сканер-ВС), а также специализированные решения для защиты критической инфраструктуры. Регулярное обновление ПО, обучение сотрудников и внедрение передовых технологий обеспечивают высокий уровень кибербезопасности в организации.

ООО «Лента» как крупная розничная сеть с развитой IT-инфраструктурой использует многоуровневую защиту от киберугроз. Основу безопасности составляют технические решения: защищённые серверы на OpenBSD/FreeBSD, прокси-сервисы QRATOR для фильтрации трафика и защиты от DDoS-атак, строгий контроль доступа через брандмауэры. Сетевой периметр защищён системой обнаружения и блокировки сканирования, что подтверждается реакцией на агрессивные nmap-сканирования. FTP-ресурсы доступны только для внутреннего использования. Компания контролирует конфиденциальность данных сотрудников, информация о которых отсутствует в соцсетях и СМИ. Для борьбы с фишингом внедрена фильтрация писем и обучение персонала. Данные защищены с помощью HashiCorp Vault, который хранит пароли, API-ключи и сертификаты. Компания соблюдает PCI DSS и ФЗ-152. Бизнес-процессы защищены через Power BI и Qlik View с использованием TLS, подписанных сертификатов и автоматического разграничения доступа по ролям.

Positive Technologies как ведущий эксперт в области информационной безопасности применяет комплексный подход к противодействию киберугрозам, сочетающий собственные технологические разработки с глубокой экспертизой, а используемые ими операционные системы включают различные версии Windows, Linux. Компания использует многоуровневую систему защиты, включающую продукты собственной разработки: MaxPatrol для мониторинга уязвимостей и соответствия стандартам, PT Application Firewall для защиты веб-приложений, PT Network Attack Discovery для обнаружения сложных сетевых атак. Специализированные исследовательские центры PT ESC и PT SWARM занимаются анализом действий хакерских группировок и выявлением уязвимостей нулевого дня в популярных продуктах. Системы мониторинга PT SIEM и песочница PT Sandbox обеспечивают оперативное выявление и анализ угроз. Важным элементом стратегии является обучение – ежегодный форум Positive Hack Days и специализированные курсы PT Expert повышают квалификацию специалистов. Компания обладает необходимыми лицензиями ФСТЭК и ФСБ, её решения сертифицированы для использования в критически важных отраслях. Positive Technologies делает акцент на инновационных разработках и адаптивных методах защиты, что позволяет эффективно противостоять киберугрозам, одновременно предлагая клиентам готовые решения для обеспечения информационной безопасности.

Как можно заметить из всего вышеперечисленного, каждая из организаций адаптирует стратегии защиты в соответствии со своими потребностями и спецификой. Государственная корпорация «Росатом» применяет многоуровневую защиту с мониторингом угроз и специализированными решениями для критической инфраструктуры, включая центр «Атомзащитаинформ», при поддержке лицензий ФСТЭК, ФСБ и Минобороны. Крупная коммерческая организация ООО «Лента» делает акцент на защите сетевого периметра, сегментации сети, фильтрации трафика и обучении сотрудников, соблюдая стандарты PCI DSS и ФЗ-152. Вендор информационной безопасности Positive Technologies сочетает собственные технологические разработки, такие как MaxPatrol и PT Application Firewall, с глубокой экспертизой, включая анализ уязвимостей нулевого дня и проведение обучающих мероприятий.

Анализ показал, что подходы к защите от Cyber Kill Chain различаются: государственные структуры ориентированы на всеобъемлющую защиту, коммерческие организации – на устойчивость бизнес-процессов, а вендоры – на инновации и адаптивные решения. Также стоит отметить, что несмотря на внедрение технических мер защиты, слабым звеном в противодействии фишингу остаётся персонал, поэтому все организации должны регулярно проводить обучение сотрудников, повышая их осведомлённость о современных методах социальной инженерии и киберугрозах.

Список литературы

1. Yadav T. Technical Aspects of Cyber Kill Chain / T. Yadav, A. M. Rao // International Symposium on Security in Computing and Communication. Cham: Springer International Publishing, 2015. Pp. 438–452.

2. Котенко И. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров // Вопросы кибербезопасности. 2022. № 4 (50). С. 52–79.

3. Росатом. URL: rosatom.ru/index.html.

4. Центр анализа и защиты информации. URL: цази.рф/main.

5. Positive Technologies. URL: ptsecurity.com/ru-ru.

6. ТехРадар ООО «Лента». URL: lenta.tech/radar.

УДК 004.732.056.5

ИЗМЕНЕНИЕ ПАРАДИГМЫ СЕТЕВОЙ БЕЗОПАСНОСТИ: РОЛЬ КОНЦЕПЦИИ НУЛЕВОГО ДОВЕРИЯ В КОРПОРАТИВНЫХ СИСТЕМАХ

А. О. Варыгина[1]
Научный руководитель М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

С появлением новых тенденций в современном мире, таких как дистанционная работа, облачные хранилища, приложения, базы данных и платформы как услуги (DBaaS, PaaS, SaaS) понятие периметра корпоративных сетей становится всё более расплывчатым. Увеличение ресурсов, передача задач провайдерам, территориальные распределения офисов и данных увеличивают поверхность атаки. Корпоративные сети становятся всё более уязвимыми к кибератакам и утечкам конфиденциальных данных.

Становится очевидным, что старый подход к построению сетей перестаёт быть достаточно надёжным. На смену ему Джоном Киндервагом была предложена концепция нулевого доверия (Zero Trust), главная идея которой заключается в том, что никто и ничто не является доверенным по умолчанию. Все действия пользователя проверяются и авторизуются для доступа к ресурсам. Этот подход становится всё более популярным в условиях роста угроз информационной безопасности и необходимости защиты корпоративных данных от несанкционированного доступа.

Принцип нулевого доверия представляет собой стратегию, направленную на снижение рисков и повышение уровня безопасности информационных систем, обеспечивая защиту как от внутренних, так и от внешних угроз. Внедрение данного принципа является важным шагом в создании безопасных сетей и защите конфиденциальной информации от злоумышленников. Основной целью такого подхода является обеспечение защиты организации от разнообразных угроз.

Ключевым элементом принципа нулевого доверия является необходимость постоянной проверки подлинности пользователей и устройств при каждом запросе на доступ к ресурсам. Данный подход обеспечивает дополнительный уровень защиты, предотвращая потенциальные нарушения работы сети и несанкционированный доступ к конфиденциальным данным. В рамках данной концепции также предполагается отсутствие доверия к сетевым устройствам, которые могут быть скомпрометированы или использованы в рамках кибератак. Следовательно, все устройства должны находиться под

© Варыгина А. О., 2025

постоянным контролем и проверяться на наличие уязвимостей или несанкционированных действий, что дополнительно укрепляет общую безопасность инфраструктуры.

Принцип нулевого доверия способствует созданию более безопасной и надёжной сетевой инфраструктуры, что, в свою очередь, обеспечивает защиту данных и предотвращает инциденты безопасности. Однако было выявлено, что такой подход существенно снижает мотивацию сотрудников как со стороны поддержания защиты информации, так и при развитии их профессиональных навыков. Основная проблема заключается в том, что работодатели больше заинтересованы в усиленном надзоре над сотрудниками, чем в самих механизмах разграничения доступа и корректной настройке политик. Такой гиперфокус вызывает у сотрудников снижение доверия к работодателю [1].

В построении сетей с нулевым доверием проектируется полный цикл аутентификации и авторизации пользователей. Подходы к организации аутентификации зависят от возможностей и приоритетов каждой компании.

Аутентификация в концепции нулевого доверия применяется с использованием криптографии и программно-определяемого периметра. Также, как правило, используется несколько факторов аутентификации. Всё это предоставляет высокий уровень безопасности и надёжности системы. Однако, эти методы не защищают конфиденциальные данные пользователей.

Для сохранения конфиденциальности было предложено новое решение, сочетающее в себе цифровую подпись и аутентификацию, соответствующую концепции нулевого доверия через протокол Kerberos. Метод основан на модели UDVS и получил название TUDVS, где T – traceable. Принципиальным отличием является наличие алгоритма отслеживания на сервере аудита [2].

Отдельно стоит рассмотреть биометрию. Она считается самым надёжным способом аутентификации, т. к. биометрические данные уникальны и всегда находятся при пользователе. Однако внедрение биометрии связано с техническими трудностями, высокими затратами на оборудование и требованиями по защите данных. Взамен классической биометрии была предложена веб-биометрия, которая проверяет поведенческие и когнитивные паттерны в браузере, к которым относятся: мониторинг измерения количества кликов, сопоставление скорости набора текста на клавиатуре, скорость сканирования файлов [3].

Программно-определяемый периметр (SDP) является ключевым компонентом модели нулевого доверия. Эта модель обеспечивает динамическое создание защищённого доступа к ресурсам, скрывая приложения и серверы от неавторизованных пользователей. Доступ предоставляется только после успешной аутентификации пользователя и проверки контекста его запроса.

Для усиления контроля применяется микросегментирование, позволяющее детально отслеживать трафик каждого пользователя и управлять его правами доступа к ресурсам [4].

Дальнейшее развитие этой концепции предполагает интеграцию программно-определяемого периметра (SDP) с программно-определяемой сетью (SDN). Такое объединение решает две важные задачи: обеспечивает гибкое и динамичное развёртывание сетевой инфраструктуры и повышает безопасность сети, в частности защищая её от атак типа «отказ в обслуживании» (DDoS) [5].

Указанные методы обеспечивают высокую эффективность в выявлении аномалий, оперативную реакцию на угрозы и автоматизацию анализа данных. Однако их внедрению сопутствуют высокие затраты на установку и поддержку, а также риск ложных срабатываний, когда безопасные действия могут быть ошибочно восприняты как угрозы. Проблемой может стать использование устаревшего оборудования или программного обеспечения, несовместимого с новыми технологиями.

Кроме микросегментации и программно-определяемого периметра, архитектура, реализующая принцип нулевого доверия, может включать иные современные подходы: контроль доступа на основе контекста, многофакторная аутентификация, поведенческая аналитика, управление привилегиями, оркестровка безопасности, мониторинг в режиме реального времени. Эти подходы помогают создать многослойную защиту, повышая безопасность инфраструктуры и уменьшая риски, связанные с кибератаками.

Вместе с тем внедрение принципа нулевого доверия сопряжено с рядом трудностей, которые могут усложнить переход на эту парадигму безопасности. К ним можно отнести: комплексность архитектурных изменений, изменение менталитета и культуры безопасности, высокую стоимость внедрения и поддержки, необходимость глубокой сегментации сети, совместимость с унаследованными системами, трудоёмкую настройку и управление политиками, проблемы с производительностью.

Концепция нулевого доверия (Zero Trust) находится на стадии активного развития и эволюции, и её будущее обещает значительные изменения в подходе к обеспечению безопасности цифровых систем. Перспективы развития данной концепции связаны с расширением функциональности, увеличением масштабируемости и интеграции с другими современными технологиями.

С развитием технологий ИИ и машинного обучения концепция нулевого доверия станет ещё более автоматизированной и интеллектуальной. ИИ поможет анализировать поведение пользователей и устройств в реальном времени, прогнозировать угрозы и адаптивно реагировать на изменения в среде, что позволит значительно сократить время на обнаружение и устранение инцидентов.

Будут развиваться методы биометрической аутентификации, поведенческой аналитики и проверки контекста доступа. Такие меры помогут сделать процесс входа в систему безопасным и удобным для пользователей, уменьшив при этом вероятность компрометации учётных данных.

С увеличением числа мобильных устройств и объёма удалённой работы нулевое доверие должно становиться всё более гибким и адаптированным к

разным сценариям использования. В будущем концепция нулевого доверия будет ориентироваться на предоставление доступа на основе контекста, независимо от физического расположения пользователя или устройства, что обеспечит надёжную защиту.

Развитие микросервисной архитектуры и контейнеризации приведёт к дальнейшему развитию микросегментационной архитектуры, которая позволит уменьшить последствия инцидентов и локализовать угрозы.

С увеличением числа распределённых и децентрализованных систем принцип нулевого доверия должен быть адаптирован для работы в условиях гетерогенных и динамических инфраструктур.

Будущие разработки в области нулевого доверия будут направлены на улучшение масштабируемости, простоты внедрения и удобства эксплуатации. Современные решения должны позволять организациям лёгкое развёртывание и адаптацию к новым технологиям и методологиям.

Концепция нулевого доверия продолжает развиваться, становясь неотъемлемой частью современных систем безопасности. В ближайшие годы можно ожидать роста популярности этого подхода в корпоративных и государственных организациях, а также расширения сферы применения в направлении мобильных и периферийных систем, облачной работы и Интернета вещей.

Список литературы

1. Астахова Л. В. Модель нулевого доверия как фактор влияния на информационное поведение сотрудников организации / Л. В. Астахова // Научно-техническая информация. Организация и методика информационной работы. 2022. № 3. С. 13–17.

2. Tang F. Privacy-preserving Authentication Scheme based on Zero Trust Architecture / F. Tang, C. Ma, K. Cheng // Digital Communications and Networks. 2023. URL: sciencedirect.com/science/article/pii/S23528648.

3. Sasada T. Web-biometrics for User Authenticity Verification in Zero Trust Access Control / T. Sasada, Y. Taenaka, Y. Kadobayashi et al. // IEEE 2024. URL: ieeexplore.ieee.org/document/10555260.

4. NIST Guide to a Secure Enterprise Network Landscape 2022. URL: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf.

5. Sallam A. On the Security of SDN: a Completed Secure and Scalable Framework using the Software-defined Perimeter / A. Sallam, A. Refaey, A. Shami // IEEE 2019. URL: ieeexplore.ieee.org/document/8826550.

УДК 004.056.53

ЦИФРОВАЯ АГРОНОМИЯ ПОД УГРОЗОЙ: ИССЛЕДОВАНИЕ КИБЕРУГРОЗ В УМНОМ СЕЛЬСКОМ ХОЗЯЙСТВЕ

К. О. Заложук[1]
Научный руководитель М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Актуальность исследований в области кибербезопасности умного сельского хозяйства обусловлена стремительным внедрением цифровых технологий в агросектор и увеличением числа киберугроз. Умное сельское хозяйство, базирующееся на Интернете вещей (*IoT*), больших данных и искусственном интеллекте, существенно повышает производительность, однако усиливает уязвимости инфраструктуры перед киберпреступлениями.

Нарушение работы систем умного сельского хозяйства может повлечь серьёзные последствия:

1) экономический ущерб – потеря урожая, поломка оборудования, финансовые потери вследствие утечек данных или атак программ-вымогателей;

2) угрозы продовольственной безопасности – сбои в автоматизированных системах могут нарушить цепи поставок и создать дефицит продуктов;

3) экологические последствия – неконтролируемые воздействия на природу из-за неисправностей в системах управления водными ресурсами, удобрениями и пестицидами;

4) потеря доверия к технологиям – массовые кибератаки способны снизить уровень доверия фермеров к цифровым решениям и затормозить процессы цифровизации.

Следовательно, обеспечение кибербезопасности в умном сельском хозяйстве становится ключевым фактором для устойчивого развития аграрной сферы и обеспечения продовольственной безопасности. Разработка и внедрение эффективных мер защиты, а также повышение осведомлённости об актуальных киберугрозах делают эту тематику особенно востребованной в современных условиях.

Работа An SDR-based Cybersecurity Verification Framework for Smart Agricultural Machines [1] авторов Р. Кавильей, Д. Гаггеро, Д. Портомауро, Ф. Патроне и М. Маркезе посвящена проблемам кибербезопасности в контексте умных сельскохозяйственных машин (SAMs). Авторы предлагают фреймворк на базе программно-определяемого радио (SDR) для верификации кибербезопасности SAMs, уделяя особое внимание беспроводным каналам связи.

© Заложук К. О., 2025

С развитием автоматизации и дистанционного управления в сельском хозяйстве возрастает потребность в оценке уязвимостей SAMs. Использование частных протоколов связи усложняет независимую оценку безопасности этих систем.

Авторы подчёркивают, что на данный момент отсутствуют технические стандарты, направленные конкретно на кибербезопасность в среде SAMs, что создаёт пробелы в обеспечении надёжной оценки рисков.

Разработанный авторами фреймворк использует SDR для обнаружения уязвимостей в протоколах управления SAMs. Он включает набор атак различной сложности, позволяющих оценить степень риска.

Авторы акцентируют внимание на необходимости стандартизации и разработки строгих требований для усиления кибербезопасности в сельскохозяйственной сфере. Предлагаемый фреймворк закладывает основу для дальнейшего изучения и совершенствования подходов к защите умных сельскохозяйственных машин.

Статья Cybersecurity for Smart Farming [2] рассматривает значимость кибербезопасности в условиях цифровизации агропромышленного комплекса, уделяя особое внимание социокультурным аспектам. В работе отмечается, что современные технологии, такие как сенсоры, беспилотники и автоматизация, существенно повышают эффективность сельскохозяйственного производства, однако одновременно создают новые киберугрозы.

Кибератаки на цифровые системы в сельском хозяйстве могут привести к снижению продуктивности и нарушению логистических цепей. Поэтому необходимо защищать как операционные (OT), так и информационные (IT) технологии.

Авторы выявили, что различия в культурных и социальных контекстах влияют на восприятие и реализацию кибербезопасности. А проведённое исследование и интервью с разработчиками, фермерами и экспертами по кибербезопасности позволили выявить их подходы к защите данных и потенциальные угрозы.

Авторы подчёркивают необходимость учитывать социокультурные факторы при внедрении цифровых решений в сельское хозяйство для повышения уровня его кибербезопасности. Для дальнейшего развития этого направления рекомендуется проведение дополнительных исследований влияния социокультурной среды на обеспечение информационной безопасности.

Авторы статьи IoT based Animal Trespass Identification and Prevention System for Smart Agriculture [3] предлагают IoT-систему для обнаружения и предотвращения вторжения животных на сельскохозяйственные территории. Данная проблема актуальна для индийских фермеров, чьи поля расположены вблизи лесов и холмов, где частые набеги животных наносят значительный ущерб урожаю.

Проникновение животных на поля представляет собой серьёзную угрозу для фермеров, особенно тех, кто находится в экономически неблагоприятных условиях. Традиционные методы борьбы, такие как фейерверки и электрические заборы, не всегда эффективны и могут причинять вред животным. Разработанная система использует IoT-технологию для создания эффективного и безопасного для животных метода защиты полей. Она включает разнообразные датчики и модули для обнаружения движения животных, их отпугивания и оповещения фермера.

Система состоит из двух модулей: модуль обнаружения проникновения животных и модуль фотографирования поля. Первый включает PIR-датчики для фиксации теплового излучения, ультразвуковые датчики для подтверждения наличия животного и зуммер для его отпугивания. Также используется GSM-модуль для отправки СМС-оповещений фермеру. Второй модуль оснащён камерой ESP32 для передачи фото поля по запросу через «Телеграм».

В статье [4] рассматривается применение технологии LoRa (Long Range) в системах умного сельского хозяйства. Авторы представляют проект, нацеленный на повышение эффективности сельскохозяйственного бизнеса в сельских регионах с помощью LoRa-технологий.

LoRa использует метод модуляции Chirp Spread Spectrum (CSS), позволяющий передавать данные на большие расстояния с минимальным потреблением энергии. Технология находит применение в различных аграрных приложениях, таких как управление поголовьем скота, автоматическое орошение и мониторинг окружающей среды. В частности, авторы отмечают, что во многих сельских районах существуют перспективы для использования LoRa, однако недостаток интернет-соединения и ограниченный доступ к технологиям затрудняют её внедрение.

Авторы делают вывод, что LoRa-технология способна значительно повысить эффективность сельского хозяйства в сельских районах благодаря надёжной связи без необходимости подключения к интернету. В дальнейших исследованиях предполагается интеграция технологии Power-over-Fiber (PoF) для питания удалённых устройств и датчиков, что должно ещё больше усовершенствовать систему.

Исследование [5] посвящено проблемам кибербезопасности в контексте цифровой трансформации сельского хозяйства. Авторы акцентируют внимание на том, что внедрение информационно-коммуникационных технологий (ИКТ) и Интернета вещей (IoT) в точном земледелии (Smart Farming) имеет значительные преимущества, но также порождает новые риски и уязвимости.

Применение дронов, роботов, умных сенсоров и других технологий существенно улучшает управление и качество сельскохозяйственного производства. Эти инновации позволяют фермерам эффективнее мониторить и управлять хозяйством, повышая производительность и конкурентоспособность. Массовое использование технологий делает аграрный сектор подверженным кибератакам. Авторы указывают на рост угроз

кибертерроризма и агротерроризма, способных нанести серьёзный финансовый и человеческий ущерб.

Авторы подчёркивают необходимость дальнейших исследований и разработки комплексных фреймворков для обеспечения кибербезопасности в Smart Farming. Они призывают к активному вовлечению всех заинтересованных сторон в процесс обеспечения безопасности, чтобы минимизировать риски и защитить аграрный сектор от кибератак.

Список литературы

1. Caviglia R. An SDR-based Cybersecurity Verification Framework for Smart Agricultural Machines / R. Caviglia, G. Gaggero, G. Portomauro et al. // IEEE Access. 2023. Vol. 11. Pp. 54 210–54 220. DOI: 10.1109/ACCESS.2023.3282169.

2. Van der Linden D. Cybersecurity for Smart Farming: Socio-cultural Context Matters / D. van der Linden, O. A. Michalec, A. Zamansky // IEEE Technology and Society Magazine. 2020. Vol. 39. No. 4. Pp. 28–35. DOI: 10.1109/MTS.2020.3031844.

3. Usharani S. IoT based Animal Trespass Identification and Prevention System for Smart Agriculture / S. Usharani, R. S. Gayathri, D. S. Kishore et al. // 7th International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai, India, 2023. Pp. 983–990. DOI: 10.1109/ICICCS56967.2023.10142814.

4. Edwin L. LoRa System with IoT Technology for Smart Agriculture System / L. Edwin et al. // IEEE 20th Student Conference on Research and Development (SCOReD). Bangi, Malaysia, 2022. Pp. 39–44. DOI: 10.1109/SCOReD57082.2022.9974084.

5. Nimmala S. A Recent Survey on AI Enabled Practices for Smart Agriculture / S. Nimmala, M. Ramchander, M. Mahendar et al. // International Conference on Intelligent Systems for Cybersecurity (ISCS). Gurugram, India, 2024. Pp. 1–5. DOI: 10.1109/ISCS61804.2024.10581009.

УДК 004.056.5

МЕТОД ТЕСТИРОВАНИЯ УРОВНЯ ЗНАНИЙ ПЕРСОНАЛА В ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ ФИШИНГУ

С. А. Кац, Ю. Е. Чернявская, Д. А. Шпагина[1]
Научный руководитель В. Б. Туговиков[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

Современные информационные системы, несмотря на высокий уровень защищённости, по-прежнему уязвимы перед атаками, ориентированными на

© Кац С. А., Чернявская Ю. Е., Шпагина Д. А., 2025

человеческий фактор. Одним из наиболее распространённых методов социальной инженерии остаётся фишинг – способ получения конфиденциальной информации путём обмана пользователя. Согласно отчёту [1] количество фишинговых атак в 2024 г. выросло на 26 %. Никакие, даже самые современные, средства киберзащиты не помогут, если пользователь откроет письмо, содержащее вредоносную ссылку или файл.

Повышение уровня осведомлённости сотрудников является важным элементом защиты от фишинга. Существует множество обучающих программ, но они не всегда позволяют оценить реальную готовность персонала противостоять атакам. Соответственно, возникает необходимость сопровождать обучение практической проверкой знаний.

Разработанный авторами статьи метод тестирования уровня знаний персонала предназначен для проверки знаний и выявления сотрудников, подверженных риску.

Данный метод включает в себя следующие этапы.

1. Обучение персонала. Перед тестированием все сотрудники проходят обучение противодействию фишингу, где пользователи учатся определять поддельные письма и как правильно на них реагировать.

2. Рассылка на почту псевдофишингового письма. Через две недели после завершения обучения планируется осуществить рассылку с файлом, имитирующим установщик якобы необходимого обновления.

3. Повторное обучение для сотрудников, не прошедших тест.

Текст письма может содержать следующую информацию: «Уважаемые коллеги! В связи с последними изменениями в политике безопасности требуется обязательное обновление корпоративного клиента до версии 3.2.1. Для установки обновления скачайте и запустите прикреплённый файл Client Update 3.2.1.exe. Процедура займёт не более 2 мин. В случае отказа от обновления доступ к корпоративным ресурсам может быть ограничен».

По сценарию тестирования письмо должно содержать признаки фишинговой атаки, на которые тестируемый должен обратить внимание, а именно:

1) использование слов «срочное обновление» в сочетании с угрозой ограничения доступа оказывает давление, чтобы жертва действовала быстро и необдуманно;

2) не указано, какие именно изменения в политике безопасности требуют обновления;

3) корпоративные обновления обычно происходят через официальные каналы (внутренние системы обновлений), а не через имейл-вложения;

4) т. к. адрес отправителя письма может быть поддельным, его всегда нужно проверять.

По предлагаемому авторами сценарию тестирования при запуске этого файла происходит имитация установки приложения на устройство.

После имитации установки скрытно активируется скрипт, основанный на командах *cmd Windows*. Первым шагом скрипт подключает сетевой ресурс и

задаёт путь к текстовому файлу на этом ресурсе. Далее идёт сбор информации с компьютера пользователя. В текстовый файл извлекаются и записываются: дата и время, имя пользователя, *IP*-адрес и версия ОС. В конце работы скрипта происходит отключение сетевого ресурса.

В итоге выполнения тестирования специалисты по информационной безопасности организации получают полную информацию о пользователях, которые не усвоили правила противодействия фишингу и для которых требуются дополнительные мероприятия по повышению осведомлённости.

Таким образом, описанный метод в сочетании с разработанным приложением может стать важным элементом повышения информационной безопасности организации, значительно снижая риски фишинговых атак.

Список литературы

1. Спам и фишинг в 2024 г.: отчёт // Kaspersky. 2024. URL: secure-list.ru/spam-and-phishing-report-2024/111743.

2. Вепрев С. Б. Методы фишинговых атак на электронную почту и способы защиты от них / С. Б. Вепрев, С. А. Нестерович // Вестник РосНОУ. 2021. № 2. С. 91–100.

3. Как провести эффективную проверку на уязвимость к фишинговым атакам // Keeper Security. 2021. URL: keepersecurity.com/blog/ru/2021/02/04/how-to-run-a-phishing-test-in-the-remote-work-environment.

УДК 004.056.55

ОТ ТЕОРИИ К ПРАКТИКЕ: АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ГОМОМОРФНОГО ШИФРОВАНИЯ

И. А. Кузьмин[1]
Научный руководитель М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Гомоморфное шифрование представляет собой метод криптографической обработки данных, позволяющий выполнять математические операции над зашифрованной информацией без её предварительного расшифровывания. Результаты таких вычислений остаются в зашифрованном виде, но после декодирования они совпадают с результатами, которые были бы получены при работе с открытыми (незашифрованными) данными. Этот подход обеспечивает защиту конфиденциальности информации даже при хранении и обработке данных сторонними сервисами.

Целью данного исследования является анализ новых методов гомоморфного шифрования, выявление их ключевых особенностей,

© Кузьмин И. А., 2025

преимуществ и ограничений по сравнению с существующими подходами. Особое внимание будет уделено вопросам эффективности, безопасности и практического применения этих методов в различных областях, таких как облачные вычисления, машинное обучение и защита персональных данных. Кроме того, будут рассмотрены перспективные направления дальнейшего развития технологий гомоморфного шифрования и предложены рекомендации для будущих исследований в этой сфере.

Гомоморфное шифрование – это криптографический метод, позволяющий выполнять операции над зашифрованными данными без использования секретного ключа. Результатом таких вычислений является зашифрованный результат, который после расшифровки соответствует результатам операций, выполненных над исходными данными. Понятие гомоморфизма в криптографии аналогично его определению в алгебре, где функции шифрования и дешифрования выступают как отображения между пространствами открытых текстов и зашифрованных текстов. Это свойство делает гомоморфное шифрование эффективным средством защиты конфиденциальности.

Гомоморфное шифрование включает различные виды шифровальных схем, поддерживающих выполнение разнообразных классов вычислений над зашифрованными данными, включая логические и арифметические операции.

Основные типы гомоморфного шифрования включают:

– частично гомоморфное шифрование (*PHE*), которое поддерживает выполнение одной операции (например, сложение или умножение);

– несколько гомоморфное шифрование (*SHE*), позволяющее выполнять две операции, но ограниченное определённым набором схем;

– полностью гомоморфное шифрование (*FHE*), обеспечивающее возможность выполнения любых операций произвольной сложности, что делает его самым мощным видом гомоморфного шифрования.

Рассмотрим указанные типы гомоморфного шифрования подробнее.

Частично гомоморфные криптосистемы гомоморфны только относительно одной операции – либо сложения, либо умножения. Примеры таких систем включают схему *RSA* (гомоморфную по умножению), схемы Эль-Гамаля и Голдвассера – Микали, а также схемы Пэйе и Бенало, гомоморфные по сложению.

Авторы работы [1] предлагают решение для обеспечения конфиденциальности передачи данных от распределённых сенсоров к агрегатору. Оно основано на протоколах оценки на основе наборов с использованием частично гомоморфного шифрования, которое сохраняет конфиденциальность измерений и устанавливает ограничения для оценок. Работа фокусируется на линейной динамической системе с дискретным временем, где множества представлены зонотопами и ограниченными зонотопами, что позволяет компактно описывать многомерные множества и сохранять их свойства при линейных преобразованиях и сложении

Минковского. Шифруются параметры представления множеств, вводится понятие зашифрованных множеств и пересечений в зашифрованной области, что гарантирует оценку состояния с сохранением конфиденциальности.

Основной проблемой гомоморфного шифрования является риск переполнения после ряда операций в зашифрованном домене. Авторы предлагают решение, включающее многократную передачу зашифрованного набора на узел запроса, который расшифровывает набор, заново шифрует его и возвращает агрегатору. Однако этот подход увеличивает объём вычислений и затраты на коммуникацию, снижая общую производительность системы.

В статье [2] анализируются и сравниваются две гомоморфные схемы – RSA и Paillier – с целью изучения их применимости для обеспечения безопасности в облачных вычислениях. Оцениваются возможности гомоморфного шифрования и вычислений в контексте облачных сред, а также анализируются преимущества и недостатки каждой схемы. Представлены экспериментальные результаты, позволяющие оценить эффективность и безопасность применения RSA и Paillier в облачных вычислениях.

Преимущества RSA:

– широко используемый алгоритм с хорошо изученной математической основой;

– высокая безопасность при использовании длинных ключей;

– поддержка гомоморфных операций над зашифрованными данными.

Преимущества Paillier:

– обеспечивает гомоморфные свойства и возможность выполнения операций над зашифрованными данными;

– высокая безопасность и эффективность в облачных вычислениях.

Недостатки:

– оба алгоритма требуют значительных вычислительных ресурсов для выполнения гомоморфных операций, что может снизить производительность;

– возможны ограничения в функциональности и возможностях гомоморфных операций, что может ограничить применимость схем в некоторых сценариях.

Анализ результатов показывает, что обе схемы эффективны с точки зрения конфиденциальности, но сопровождаются дополнительными затратами на обработку и коммуникацию. RSA требует меньше времени благодаря меньшему количеству операций, тогда как Paillier отличается аддитивными гомоморфными свойствами, что делает его важным дополнением.

Особенность работы заключается в стремлении авторов разработать гибридную систему, сочетающую алгоритмы RSA и Paillier для достижения полного гомоморфного шифрования.

Несколько гомоморфное шифрование (*SHE*) допускает выполнение ограниченного числа операций сложения и умножения над зашифрованными данными до возникновения проблем с переполнением или потерей точности. Известно, что *SHE* требует значительных вычислительных ресурсов, поэтому его использование в реальном времени затруднительно.

В работе [3] предложено четыре схемы гомоморфного шифрования для целочисленных вычислений, ориентированных на безопасные однопартийные вычисления в облачных средах. Основная цель этих схем – вычисление полиномов низкой степени на целых числах или десятичных дробях с фиксированной точкой, которые могут быть приведены к целому виду.

Базовой схемой является *HE*1, предназначенная для гомоморфного вычисления многочленов произвольной степени в одномерном пространстве. На основе *HE*1 разработаны вариации: *HE*1*N* (для входных данных с низкой энтропией), *HE*2 (для вычислений в двумерном пространстве) и *HE*2*N* (для вычислений в двумерном пространстве при входных данных с низкой энтропией).

Экспериментально показано, что скорость выполнения алгоритмов достаточно высока. Сравнение с результатами исследования [4] демонстрирует, что предложенные схемы работают в 1 000 раз быстрее в лучшем случае и в 10 раз быстрее в худшем.

Преимуществами предложенных схем являются возможность вычисления полиномов произвольной степени и обеспечение надёжной защиты для данных с низкой энтропией.

Недостатками являются менее эффективное дешифрование по сравнению с методами, использующими основание 2 вместо большого простого числа, а также необходимость контроля результата вычислений, чтобы он не превышал модуля секретного числа [4].

Полностью гомоморфное шифрование (FHE) представляет собой вершину развития гомоморфного шифрования, поскольку оно поддерживает выполнение произвольных вычислений над зашифрованными данными. Это позволяет создавать программы с любой необходимой функциональностью, работающие с зашифрованными входными данными и возвращающие зашифрованные результаты. Такие программы могут безопасно исполняться на ненадёжных платформах без раскрытия исходных данных и внутреннего состояния. Полностью гомоморфные криптосистемы особенно важны для аутсорсинга частных вычислений – например, в облачных вычислениях, где конфиденциальность данных играет ключевую роль.

В работе [5] авторы предлагают безопасный алгоритм сортировки на уровне слов, основанный на методе полного гомоморфного шифрования. Суть метода заключается в следующем:

1) разработка оптимизированного по глубине алгоритма сортировки, основанного на алгоритме частного сравнения XCMP;

2) решение проблемы однократного применения алгоритма XCMP с помощью метода извлечения постоянных членов, что позволяет выполнять дополнительные гомоморфные умножения, необходимые для сортировки на уровне слов;

3) решение проблемы невозможности проверки на равенство выходного зашифрованного текста алгоритма XCMP с использованием метода, основанного на малой теореме Ферма;

4) реализация метода множественного доступа с одной инструкцией, что снижает размер зашифрованного текста и повышает вычислительную производительность.

Экспериментальные результаты показали, что предложенный алгоритм сортировки на уровне слов более чем в 10 раз эффективнее современных алгоритмов сортировки на уровне битов. Однако для достижения таких результатов потребовалась вычислительная установка с мощным процессором Intel Xeon Gold 6 148 и оперативной памятью объёмом 503 ГБ, что подчёркивает высокие требования к аппаратуре.

В статье [6] авторы предлагают новый метод обеспечения безопасности вычислений в общедоступном облаке, комбинирующий преимущества конфиденциальности полностью гомоморфного шифрования с целостностью доверенных сред выполнения (TEEs). Метод получил название Trusted Fully Homomorphic Encryption (TFHE). Для тестирования алгоритма была создана библиотека TFHE-rs на языке Rust, которую тестировали с использованием анклавов SGX и распределителя dlmalloc от платформы Fortanix Rust EDP. Использование 128-разрядной защиты привело к снижению производительности на 73 %, однако разница во времени выполнения программ с использованием SGX и без него составила всего 3 %.

Авторы работы [8] предложили решение для интеллектуального анализа ассоциативных правил с сохранением конфиденциальности с помощью полностью гомоморфного шифрования с несколькими ключами. Особенностью их работы является поддержка многопользовательского доступа через один сервер. Экспериментальная реализация показала эффективность и выполнимость предложенной схемы, которая превосходит существующие решения по скорости шифрования и передачи данных, экономя около 8,5 % рабочего времени.

В статье [9] авторы рассматривают применение полностью гомоморфного шифрования для создания безопасной и проверяемой системы аутентификации по радужной оболочке глаза. Целью является сохранение конфиденциальности при обучении и классификации моделей ближайшего соседа и многоклассового персептрона. Для этого используется схема Фана – Веркаутерена, обеспечивающая конфиденциальность шаблонов радужной оболочки и агрегированного вектора проверки. Несмотря на положительные результаты, авторы подчёркивают необходимость дальнейшего анализа производительности и масштабируемости системы.

Работа [10] посвящена интеграции метода полного гомоморфного шифрования в архитектуру электронно-вычислительной машины. Авторы изменили принцип работы микропроцессора таким образом, что данные в регистрах, на шинах и в памяти хранятся в зашифрованном виде. Это позволило защитить пользовательские данные, обрабатываемые удалённо или контролируемые ненадёжными операторами. Внедрение такого метода привело к снижению производительности обработки процессора в зашифрованном виде до 60–70 % от производительности незашифрованной обработки.

В заключение отметим, что гомоморфное шифрование представляет собой революционный метод защиты данных, который открывает новые горизонты в области криптографии и обработки информации. Исследование выявило ключевые аспекты различных видов гомоморфного шифрования – от частично гомоморфного до полностью гомоморфного, позволяющего выполнять широкий спектр операций над зашифрованными данными, не прибегая к их расшифровке. Это делает данный подход особенно актуальным для современных приложений в облачных вычислениях, машинном обучении и защите персональных данных.

В ходе анализа были рассмотрены как преимущества, так и ограничения методов гомоморфного шифрования. Несмотря на высокую степень конфиденциальности, сохраняемой при использовании этих технологий, необходимо учитывать проблемы, такие как риск переполнения и возрастающие вычислительные затраты. Предложенные решения, такие как многократная передача зашифрованного набора, представляют собой шаг к снижению этих рисков, однако требуют дальнейшего анализа на предмет оптимизации производительности и уменьшения затрат на ресурсы.

Данное исследование подчёркивает важность продолжения работы в сфере гомоморфного шифрования и инициирует дальнейшие исследования, направленные на улучшение методов шифрования, повышение их устойчивости и эффективности. Перспективные направления также включают интеграцию гомоморфного шифрования в реальных приложениях, что, в свою очередь, может способствовать расширению его применения и внедрению в различные сферы. Таким образом, гомоморфное шифрование не только является важным инструментом в современном мире защиты данных, но и открывает новые возможности для дальнейших исследований и технологических разработок.

Список литературы

1. Alanwar A. Privacy-preserving Set-based Estimation using Partially Homomorphic Encryption / A. Alanwar, V. Gaßmann, X. He et al. // European Journal of Control. 2023. Vol. 71. P. 100 786. DOI: 10.1016/j.ejcon.2023.10086.

2. Munjal K. Analysing RSA and PAILLIER Homomorphic Property for Security in Cloud / K. Munjal, R. Bhatia // Procedia Computer Science. 2022. Vol. 215. Pp. 240–246. DOI: 10.1016/j.procs.2022.12.027.

3. Dyer J. Practical Homomorphic Encryption over the Integers for Secure Computation in the Cloud / J. Dyer, M. Dyer, J. Xu // International Conference on Cryptography and Coding. 2017. Pp. 44–76. DOI: 10.1007/978-19-71045-7.

4. Lauter K. Can Homomorphic Encryption Be Practical? / K. Lauter // 3rd ACM Cloud Computing Security Workshop. Pp. 113–124. DOI: 10.1145/82.

5. Huang H. Secure Word-level Sorting based on Fully Homomorphic Encryption / H. Huang, Y. Wang, L. Wang et al. // Journal of Information Security and Applications. 2022. Vol. 71. P. 103 372. DOI: 10.1016/j.jisa.2022.1372.

6. Brenna L. TFHE-rs: a Library for Safe and Secure Remote Computing using

Fully Homomorphic Encryption and Trusted Execution Environments / L. Brenna, I. S. Singh, H. D. Johansen et al. // Array. 2022. Vol. 13. P. 100 118. DOI: 10.1016/j.array.2021.100118.

7. Drucker N. Achieving Trustworthy Homomorphic Encryption by Combining it with a Trusted Execution Environment / N. Drucker, S. Gueron // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2018. Vol. 9. Pp. 86–99. DOI: 10.22667/JOWUA.2018.03.31.086.

8. Xu K. Multi-key Fully Homomorphic Encryption from NTRU and (R)LWE with Faster Bootstrapping / K. Xu, B. H. M. Tan, L.-P. Wang et al. // Theoretical Computer Science. 2023. Vol. 968. P. 114 026. DOI: 10.1016/j.tcs.2023.114026.

9. Morampudi M. K. Secure and Verifiable Iris Authentication System using Fully Homomorphic Encryption / M. K. Morampudi, M. V. N. K. Prasad, M. Verma et al. // Computers & Electrical Engineering. 2021. Vol. 89. P. 106 924. DOI: 10.1016/j.compeleceng.2020.106924.

10. Breuer P. T. A Fully Encrypted Microprocessor: the Secret Computer is Nearly Here / P. T. Breuer, J. P. Bowen // Procedia Computer Science. 2016. Vol. 83. Pp. 1 282–1 287. DOI: 10.1016/j.procs.2016.04.267.

УДК 004.052.42

ДОВЕРИЕ В ЦИФРОВУЮ ЭПОХУ: БОРЬБА С ФЕЙКОВЫМИ ОТЗЫВАМИ И ПОДДЕЛЬНЫМИ АККАУНТАМИ

А. С. Кунегин[1]
Научный руководитель М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Современные онлайн-платформы, такие как интернет-магазины, социальные сети и сервисы бронирования, во многом зависят от систем рейтингования и пользовательских отзывов. Эти системы играют ключевую роль в формировании доверия к продуктам, услугам и контенту, предоставляя пользователям возможность принимать более обоснованные решения. Однако, наряду с ростом их популярности, увеличивается и количество злоупотреблений, связанных с использованием вредоносных отзывов и фальшивых аккаунтов. Такие действия, как публикация фейковых отзывов для манипуляции рейтингами или создание множества поддельных учётных записей с целью искажения данных, способны подорвать доверие пользователей к платформе и нанести значительный урон её репутации и финансовой стабильности.

© Кунегин А. С., 2025

Обнаружение и предотвращение подобных злоупотреблений представляет собой сложную задачу, требующую применения как традиционных методов анализа данных, так и современных подходов, основанных
на машинном обучении и искусственном интеллекте. Сложности усугубляются разнообразием стратегий, используемых злоумышленниками, а также необходимостью сохранять баланс между эффективностью защиты и удобством использования платформы для добросовестных пользователей.

Рассмотрим различные подходы и методы обнаружения и борьбы с фейковыми отзывами.

В исследовании [1] для противодействия фейковым отзывам предлагается новая модель BMTBA, объединяющая языковую модель BERT, статистические и поведенческие признаки, мультимодальное слияние, а также анализ времени публикации отзывов (Review Weekday).

Авторы указывают, что распределение времени публикации показывает, что настоящие отзывы пишутся людьми в выходные дни, в свободное от работы время, тогда как поддельные отзывы публикуются регулярно. Применение мультимодальной модели на базе нейросетей BERT позволяет интегрировать текстовые признаки и статистические данные, а дифференцированный подход к анализу положительных и отрицательных фейковых отзывов повышает точность классификации.

Анализируя предложенное решение, можно заключить, что мультимодальная модель значительно превосходит базовые модели и предлагает инновационные подходы к решению проблемы. Тем не менее для практической реализации необходимо учитывать вопросы масштабируемости и адаптации к различным языкам и культурным особенностям. Авторы рассматривают возможность применения метода для китайских обзоров. Вместе с тем данное исследование закладывает основы для дальнейшего развития в области анализа онлайн-отзывов. В сравнении с базовыми моделями предложенная в исследовании модель демонстрирует высокую точность (94,68 %).

В статье [2] авторы предлагают подход, основанный на временных характеристиках. Основная идея заключается в анализе временных паттернов публикаций отзывов и выявлении аномалий в их распределении. Для этого используется алгоритм Isolation Forest, который выделяет аномальные отзывы на основе их временных шаблонов.

Эксперимент выявил аномалии, включая всплески отзывов за короткий период. Метод показал высокую точность и скорость, превосходя базовые подходы. Оптимальное временное окно для анализа составило 15–30 дней.

Анализ временных промежутков эффективен для выявления фальшивых отзывов. Дальнейшее развитие метода возможно за счёт интеграции текстовых характеристик, что повысит точность.

Основная задача исследования [3] заключается в повышении точности определения поддельных отзывов с помощью методов обработки текстов и машинного обучения.

Методология включает несколько этапов для выявления фальшивых отзывов. Сначала проводятся подготовка и предварительная обработка данных. Затем выполняются процедуры извлечения слов с использованием двух подходов: сочетания TF-IDF с биграммами и метода хи-квадрат, а также TF-IDF с триграммами и хи-квадрат. После этого производится классификация с помощью алгоритмов машинного обучения, таких как SVM (для задач классификации и регрессии), Random Forest и логистической регрессии.

Наиболее высокие результаты были получены при использовании SVM с триграммами и методом хи-квадрат, где точность составила 92,19 %. Это подтверждает, что включение триграмм и тщательная селекция признаков приводят к существенному увеличению точности.

Преимуществом является комплексный подход, включающий тщательную предобработку текста и использование методов машинного обучения.

В статье [4] авторы предлагают использовать классификатор на основе теории Демпстера – Шейфера для выявления поддельных отзывов. Этот метод позволяет учитывать неопределённость и комбинировать доказательства из различных источников.

Для тестирования метода использовали данные отзывов с платформы Amazon, которые были предварительно размечены как реальные или поддельные. Применялись методы токенизации, удаления стоп-слов и анализа эмоциональной окраски с использованием модели BERT, после чего извлечённые признаки направлялись в классификатор на основе теории Демпстера – Шейфера.

Метод показал высокую точность (88 %) в выявлении поддельных отзывов, что свидетельствует о его преимуществах по сравнению с базовыми алгоритмами. Это подтверждает эффективность подхода, основанного на теории Демпстера – Шейфера для задач классификации текстов.

Основываясь на результатах исследования, можно сделать вывод, что предложенный метод является мощным инструментом, т. к. сочетает современные методы обработки текста на основе нейронной сети (BERT) и мощный инструментарий для обработки неопределённости. Этот подход может быть применён не только для анализа отзывов, но и в других задачах, требующих интеграции данных из различных источников.

В статье [5] авторы создали метод, который объединяет генеративно-состязательные сети (GAN) и модель GPT2. Ключевое достижение заключается в разработке фреймворка на основе GAN для анализа метаданных и поведенческих характеристик. Исследование показало, что добавление поведенческих признаков, таких как оценки отзывов, к текстовым характеристикам значительно повышает точность классификации.

Предложенный метод Score_GPT2GAN продемонстрировал высокую эффективность в обнаружении поддельных отзывов, особенно при ограниченной доступности размеченных данных. Объединение текстовых и поведенческих признаков позволило улучшить качество классификации. Авторы предполагают, что модель может быть адаптирована для многозадачных классификаций или работы с мультилингвистическими данными.

Исследователями в своей работе [6] предлагается новый метод MDU (Metric Learning for Professional Malicious User Detection), предназначенный для выявления профессиональных недобросовестных пользователей (PMUs) в рекомендательных системах. Такие пользователи используют сложные схемы маскирования, такие как рассогласование оценки и содержания отзыва, что затрудняет их обнаружение обычными методами. Метод основан на модификации рекурсивной нейронной сети (HDA-RNN), которая анализирует текстовые данные и преобразует отзывы в оценки эмоционального состояния. Эти оценки затем сопоставляются с рейтингами, и расхождение между ними, называемое sentiment gap, служит индикатором подозрительной активности.

Эксперименты показали, что MDU значительно превосходит существующие подходы, эффективно решает задачу обнаружения фейковых отзывов, несмотря на возможное несоответствие оценки и содержимого отзыва. Метод может быть адаптирован для работы с мультимодальными данными, включая изображения и видео, что расширяет его применение в различных приложениях.

Обнаружение фейковых отзывов и поддельных аккаунтов – ключевая задача цифровой безопасности. Современные методы, включая нейросети и теорию Демпстера – Шейфера, показывают высокую эффективность, но сталкиваются с ограничениями, такими как зависимость от размеченных данных и сложности мультиязычной адаптации. Перспективы связаны с комплексным анализом метаданных, поведенческих паттернов и интеграцией методов для снижения вычислительных затрат. Это необходимо для обеспечения надёжности систем рейтингования.

Список литературы

1. Li X. Fake Review Detection using Deep Neural Networks with Multimodal Feature Fusion Method / X. Li, L. Chen // IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS). Ocean Flower Island, China, 2023. Pp. 2 869–2 872. DOI: 10.1109/ICPADS60453.2023.00411.

2. Liu W. A Method for the Detection of Fake Reviews based on Temporal Features of Reviews and Comments / W. Liu, J. He, S. Han et al. // IEEE Engineering Management Review. 2019. Vol. 47. No. 4. Pp. 67–79. DOI: 10.1109/EMR.2019.2928964.

3. Hadi Z. Detecting Fake Reviews using N-gram Model and Chi-Square / Z. Hadi, A. Sunyoto // 6th International Conference on Information and Communications

Technology (ICOIACT). Yogyakarta, Indonesia, 2023. Pp. 454–458. DOI: 10.1109/ICOIACT59844.2023.10455895.

4. Sree T. R. Fake Review Detection using Evidential Classifier / T. R. Sree, R. Tripathi // 2nd International Conference on Advances in Computational Intelligence and Communication (ICACIC). Puducherry, India, 2023. Pp. 1–5. DOI: 10.1109/ICACIC59454.2023.10435343.

5. Tamimi M. Deceptive Review Detection using GAN Enhanced by GPT Structure and Score of Reviews / M. Tamimi, M. Salehi, S. Najari // 28th International Computer Conference, Computer Society of Iran (CSICC). Tehran, Iran, 2023. Pp. 1–7. DOI: 10.1109/CSICC58665.2023.10105368.

6. Xu Y. Detect Professional Malicious User with Metric Learning in Recommender Systems / Y. Xu, Y. Yang, E. Wang et al. // IEEE Transactions on Knowledge and Data Engineering. 2022. Vol. 34. No. 9. Pp. 4 133–4 146. DOI: 10.1109/TKDE.2020.3040618.

УДК 004.9

МЕТОДЫ РЕАЛИЗАЦИИ MITM-АТАКИ, ПРИМЕРЫ РЕАЛИЗАЦИИ И МЕТОДЫ ЗАЩИТЫ

Е. А. Курбатова, И. В. Василиади[1]
Научный руководитель В. Б. Туговиков[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

С развитием цифровых технологий вопросы информационной безопасности приобретают всё большую актуальность. Одной из наиболее опасных форм кибератак является атака типа «Человек посередине» (Man-in-the-Middle, MITM), при которой злоумышленник незаметно внедряется в коммуникацию между пользователем и сервером, чтобы перехватить, изменить или использовать передаваемую информацию. Особую угрозу такие атаки представляют из-за своей скрытности: обе стороны обычно не подозревают о вмешательстве.

Цель подобных атак – получение доступа к конфиденциальным данным, включая логины, пароли, платёжные реквизиты и другие чувствительные сведения. Поэтому понимание принципов MITM и методов защиты от них крайне важно как для частных пользователей, так и для организаций.

Разберёмся, как работает MITM-атака. MITM-атака обычно реализуется в несколько этапов. На начальном этапе злоумышленник внедряется в канал связи между пользователем и сервером, используя техники, такие как ARP-спуфинг (Address Resolution Protocol), DNS-спуфинг, поддельные Wi-Fi-точки доступа. Далее может применяться метод расшифровки трафика –

© Курбатова Е. А., Василиади И. В., 2025

например, с использованием SSL-стриппинга, при котором HTTPS-соединение заменяется на небезопасный HTTP. На завершающем этапе злоумышленник получает возможность подменять информацию в передаваемом трафике либо сохраняет её для последующего использования.

Среди наиболее распространённых методов MITM-атак можно выделить ARP-спуфинг, при котором в локальной сети подменяются MAC-адреса с целью перехвата трафика. DNS-спуфинг позволяет перенаправить пользователя на поддельный сайт за счёт подмены записей в системе доменных имён. Опасность представляет также SSL-перехват, заключающийся во внедрении фальшивых сертификатов. Кроме того, применяется атака «злой двойник» (Evil Twin), в ходе которой создаётся поддельная Wi-Fi-точка, визуально не отличимая от настоящей, с целью незаметного захвата данных пользователей.

Также расскажем об известных инцидентах.

1. Атака на банк Бангладеш (2016), при которой был похищен 81 млн $ через взлом системы SWIFT.

2. Компанию Lenovo атаковали в отместку за шпионскую программу Superfish (2014–2015), где предустановленное ПО на ноутбуках Lenovo подменяло SSL-сертификаты.

3. Утечка данных Equifax (2017), затронувшая 145 млн пользователей.

4. Случай в Казахстане (2015), где MITM использовалась государственными структурами для мониторинга трафика.

Есть определённые методы защиты – на уровне организации и на уровне пользователя.

Организации должны переходить на современные протоколы, такие как TLS 1.3, использовать системы IDS/IPS (например, Snort) для выявления подозрительной активности, внедрять сертификаты с расширенной проверкой (EV) и проводить регулярное обучение сотрудников в области ИБ.

На уровне пользователя – в целях противодействия MITM-атакам пользователям необходимо использовать HTTPS, обращая внимание на наличие значка замка в адресной строке браузера. Также следует применять VPN-сервисы, обеспечивающие шифрование трафика, и активировать двухфакторную аутентификацию (2FA). Немаловажно регулярно обновлять ПО и избегать ввода конфиденциальных данных в открытых Wi-Fi-сетях.

К числу новых подходов относятся квантовое шифрование, основанное на принципах квантовой физики, и блокчейн-аутентификация, позволяющая исключить посредников при подтверждении личности.

Обучение персонала очень важно, оно должно помогать сотрудникам выявлять потенциальные угрозы: предупреждения браузера о небезопасном соединении, подозрительные Wi-Fi-сети, а также нетипичное поведение приложений. Например, при подключении к Wi-Fi в кафе сотрудник должен сверять название сети и использовать VPN.

Безопасное сетевое поведение. Сотрудников необходимо обучать использовать HTTPS, проверять подлинность сертификатов и избегать работы с конфиденциальной информацией в незашифрованных сетях.

Если, например, сайт банка открылся через HTTP, необходимо воздержаться от ввода данных и уведомить службу безопасности.

Работа с VPN и шифрованием тоже необходимая часть. Важно донести до персонала необходимость использования корпоративного VPN даже при работе из дома, а также объяснить риски отключения шифрования в любой, даже «безопасной» сети.

Наиболее действенными являются практические учения. Вот пример обучения: создаётся поддельная Wi-Fi-точка доступа с названием, похожим на легитимную сеть (например, Guest_Corporate). Сотрудники подключаются к ней, после чего демонстрируются риски перехвата трафика, фишинга и кражи учётных данных. Такие учения повышают осведомлённость и закрепляют навыки безопасной работы.

MITM-атаки остаются серьёзной угрозой для информационной безопасности. Однако сочетание современных технологий шифрования, грамотной сетевой политики и регулярного обучения персонала позволяет значительно снизить риски. Только комплексный подход способен обеспечить устойчивую защиту коммуникаций как на индивидуальном, так и на корпоративном уровне.

Список литературы

1. Что такое атака «человек посередине»? (MITM) // SSL Dragon. URL: ssldragon.com/blog/what-is-a-man-in-the-middle-attack.

2. Man-in-the-Middle: советы по обнаружению // Habr. URL: habr.com/ru/articles/mitm.

3. Атака посредника // Википедия. URL: ru.wikipedia.org/wiki/Атака_посредника.

4. Всё об атаке Man-in-the-Middle // Anti-Malware. URL: anti-malware.ru/mitm-attack.

5. Как защититься от Man-in-the-Middle // Bytwork. URL: bytwork.com/articles/mitm.

6. Что такое Man-in-the-Middle // Kaspersky Daily. URL: kaspersky.ru/blog/what-is-mitm-attack/.

7. Предотвращение Man-in-the-Middle-атак // Morpher. URL: morpher.com/security/mitm.

8. Man in the middle – что это? // MITM Institute. URL: mitm.institute/info.

УДК 004.056.53

ОСОБЕННОСТИ КОМПЬЮТЕРНЫХ АТАК JUICE JACKING И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Т. А. Лакиза, М. А. Жуков, К. А. Устинов[1]
Научный руководитель В. Б. Туговиков[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

В эпоху цифровой трансформации, когда мобильные устройства и персональные компьютеры стали неотъемлемой частью повседневной жизни и профессиональной деятельности, проблема кибербезопасности приобретает особую актуальность. Среди множества современных угроз особое место занимает Juice Jacking – относительно новый, но стремительно развивающийся метод кибератак, который представляет серьёзную опасность как для рядовых пользователей, так и для корпоративных систем.

Juice Jacking – это метод кибератаки, при котором злоумышленники используют публичные USB-порты, чтобы получить доступ к устройству и данным. Под видом обычной зарядки киберпреступники могут получить доступ к данным на устройстве, установить вредоносное ПО или даже скопировать информацию без ведома владельца.

Термин произошёл от слов juice, что в сленговом варианте перевода означает «заряд», и jacking – «кража» [1].

Изначально Juice Jacking ассоциировался преимущественно с атаками на мобильные устройства через публичные USB-порты для зарядки. Однако в последние годы наблюдается тревожная тенденция адаптации этих методов для атак на персональные компьютеры, особенно ноутбуки. Это связано с миниатюризацией схем (настолько, что их можно встроить напрямую в кабель [2]) и с особенностями архитектуры современных вычислительных систем, которые через USB-интерфейсы поддерживают не только передачу данных, но и эмуляцию устройств ввода, выполнение кода и другие потенциально опасные функции.

Актуальность исследования компьютерных аспектов Juice Jacking подтверждается рядом факторов:

1) повсеместное использование USB-интерфейсов в компьютерной технике;
2) рост количества публичных зарядных станций с USB-портами;
3) увеличение сложности и изощрённости атакующих методик;
4) недостаточная осведомлённость пользователей о подобных угрозах.

© Лакиза Т. А., Жуков М. А., Устинов К. А., 2025

Современные атаки Juice Jacking на компьютерные системы отличаются высокой технической сложностью и многообразием векторов атаки.

Наиболее распространёнными являются атаки с использованием эмуляции устройств HID, когда злоумышленники применяют программируемые микроконтроллеры (такие, как Rubber Ducky или BadUSB) для имитации клавиатурного ввода. Такие устройства могут автоматически выполнять заранее запрограммированную серию команд ввода (например, эмуляцией клавиатуры). Примеры: открытие сайтов, установка приложений на IOS или Android или ввод команд в терминал устройств Windows, MAC или Linux. Также возможно логирование нажатий, что может привести к компрометации введённых паролей. Такие атаки может быть очень сложно обнаружить потому, что они не требуют никакого ввода данных или команд от жертвы. Никаких лишних сообщений не появляется потому, что ОС компьютера идентифицирует такие устройства как стандартное периферийное оборудование – например, как мышь, клавиатуру или любое другое HID-устройство.

Особую опасность представляют атаки, эксплуатирующие уязвимости в механизмах автозапуска операционных систем. Несмотря на улучшения в современных ОС, многие системы остаются уязвимыми к выполнению произвольного кода при подключении специально сконфигурированных USB-устройств. Это особенно актуально для корпоративных сред, где может использоваться устаревшее программное обеспечение.

Современные стандарты USB, особенно USB-C с его альтернативными режимами работы, открывают новые возможности для злоумышленников. Атаки могут осуществляться через:

– режимы DisplayPort для перехвата видеосигнала;

– протоколы Thunderbolt для прямого доступа к памяти;

– функции Power Delivery для манипуляций с питанием.

Для защиты от атак такого типа достаточно использовать кабели, предназначенные исключительно для зарядки, – в них присутствуют только линии питания (5V и GND), а контакты передачи данных (Data+ и Data−) физически отсутствуют. Кроме того, существуют простые USB-адаптеры, называемые Data Blocker'ами, которые также блокируют линии передачи данных, полностью исключая возможность обмена информацией по USB-соединению. Необходимо использовать только свои проверенные зарядные устройства и кабели.

Также крайне важно своевременно обновлять прошивку устройств и устанавливать все обновления систем безопасности. В обновлениях часто устраняются уязвимости, которые могут быть использованы для подобных атак [3]. Например, начиная с Android 8, была закрыта уязвимость в компоненте ADB (Android Debug Bridge), позволявшая выполнять произвольные команды на целевом устройстве посредством эмуляции COM-порта через USB [4].

Программные методы защиты должны включать системы мониторинга

USB-активности в реальном времени, способные анализировать поведение подключённых устройств, выявлять аномалии и автоматически блокировать подозрительные устройства. Особое внимание следует уделять политикам централизованного управления USB-доступом в корпоративных средах, включая:

– системы белых списков доверенных устройств;

– детальный аудит всех подключений;

– виртуализацию работы с USB-устройствами.

Организационные меры должны включать регулярное обучение сотрудников, разработку чётких регламентов работы с USB-устройствами и планов реагирования на инциденты. Для критически важных систем рекомендуется полное физическое отключение неиспользуемых USB-портов через BIOS или с помощью аппаратных переключателей.

Для эффективной защиты от атак Juice Jacking необходим комплексный подход, который включает несколько ключевых элементов. Во-первых, это внедрение технических решений, таких как аппаратные USB-фильтры. Во-вторых, разработка продуманных политик безопасности, регламентирующих использование USB-устройств в организации и регулярное обучение персонала.

Особое внимание при организации защиты следует уделять трём важным направлениям. Прежде всего, это корпоративные системы, где последствия успешной атаки могут привести к масштабным утечкам данных и финансовым потерям. Во-вторых, объекты критической инфраструктуры, безопасность которых имеет стратегическое значение. И наконец, персональные устройства сотрудников, работающих с конфиденциальной информацией, поскольку они часто становятся слабым звеном в системе корпоративной безопасности.

Список литературы

1. Почему нельзя использовать публичные USB-зарядки в аэропортах: атаки «juice jacking» и как злоумышленники могут получить доступ к вашим данным // IXBT LIVE. URL: ixbt.com/live/supply/pochemu-nelzya-ispolzovat-publichnye-usb-zaryadki-v-aeroportah-ataki-juice-jacking.html.

2. Что такое juice jacking? // Keeper Security. URL: keepersecurity.com/blog/ru/2023/07/10/what-is-juice-jacking.

3. От 0 % до взлома: Juice Jacking в действии // Securitylab. URL: securitylab.ru/blog/personal/Neurosinaps/353871.php.

4. Exploring USB Connection Vulnerabilities on Android Devices Breaches using the Android Debug Bridge // SciTePress Digital Library. URL: scitepress.org/papers/2017/64759/64759.pdf.

УДК 004.056.55

УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АТАКИ ПО ПОБОЧНЫМ КАНАЛАМ И СТРАТЕГИИ ЗАЩИТЫ В ЦИФРОВУЮ ЭПОХУ

Л. Н. Лежнин[1]
Научный руководитель М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]Сибирский федеральный университет

В цифровую эпоху, когда криптографические методы широко применяются для защиты данных, обеспечение безопасности информационных систем становится приоритетной задачей. Однако существуют уязвимости, которыми могут воспользоваться злоумышленники для несанкционированного доступа к конфиденциальной информации.

Атаки по побочным каналам представляют значительную угрозу как для программного, так и для аппаратного обеспечения. Они осуществляются различными способами, включая анализ временных характеристик, мониторинг энергопотребления, а также исследование электромагнитных излучений и акустических сигналов. Эти атаки нацелены на извлечение секретных ключей, паролей и другой чувствительной информации, что делает их особо опасными для систем, использующих криптографию.

Рассмотрим современные методы атак по побочным каналам, их механизмы и последствия, а также существующие стратегии защиты от них.

В статье [1] авторы A. Albalawi, V. Vassilakis и R. Calinescu исследовали проблему атак по побочным каналам в облачных вычислениях. Они указывают на риск, связанный с совместной эксплуатацией облачных ресурсов несколькими пользователями, одним из которых может оказаться злоумышленник. Совместно используемые виртуализованные системы могут быть подвержены атакам на общий кеш, содержащий недавние данные, что может привести к компрометации ключей шифрования (например, в библиотеках AES и RSA) или утечке конфиденциальных данных исполняемых файлов и приложений.

Для борьбы с этими атаками авторы предлагают следующие **методы**:

1) мониторинг кеш-линий криптографических программных функций для выявления подозрительных активностей, таких как атаки типа FLUSH+RELOAD;

2) гибридный динамический и статический анализ для мониторинга активности виртуальных машин и исключения тех, которые представляют угрозу;

© Лежнин Л. Н., 2025

3) периодические проверки виртуальных машин на наличие вредоносного ПО с использованием комбинации статического анализа и инструмента ClamAV.

Анализ статьи [1] подтверждает наличие уязвимостей в облачных технологиях, позволяющих осуществлять атаки по побочным каналам. Разработанные авторами методы продемонстрировали высокую эффективность в обнаружении таких атак.

В статье [2] авторы H. Jeon, N. Kariman и T. Lehman исследовали атаки по побочным каналам, используя данные профилирования энергопотребления графических процессоров (GPU).

Они обнаружили сильную корреляцию (коэффициент Пирсона 0,973) между энергопотреблением GPU и размером ядер. Как отмечают авторы, в обучении нейронных сетей ключевыми операциями являются векторные и матричные вычисления, поэтому достаточно получить приближённую оценку гиперпараметров нейросети, в отличие от криптографических алгоритмов, где требуется точное знание ключа.

Для защиты от атак по побочным каналам авторы предлагают ослабить связь между потреблением мощности и размером ядра, например, разделив ресурсы между одновременно работающими ядрами. Это усложнит злоумышленнику задачу получения информации о гиперпараметрах нейронных сетей.

Таким образом, нейронные сети тоже подвержены атакам по побочным каналам. Важно продолжать исследовать уязвимости, связанные с GPU, и разрабатывать меры по их устранению.

В исследовании [3] детально рассматриваются атаки на кеш третьего уровня (L3). Авторы начинают с описания трёх видов атак на L3-кеш.

Атака FLUSH+RELOAD. Эта атака нацелена на последний уровень кеша (LLC). Злоумышленник, отслеживая общую линию LLC, может определить, обращается ли жертва к конфиденциальным данным на страницах обмена. Атака состоит из следующих шагов.

1. FLUSH: злоумышленник очищает определённую общую строку кеша с помощью инструкции clflush.

2. IDLE: злоумышленник ожидает заранее установленное время, пока жертва выполняет чувствительные операции.

3. RELOAD: злоумышленник перезагружает строку кеша из общей памяти. Длительность перезагрузки указывает на то, обращалась ли жертва к конфиденциальным данным: длительная загрузка свидетельствует о том, что жертва не обращалась к данным, короткая загрузка – обратное.

Атака FLUSH+FLUSH. Эта атака похожа на FLUSH+RELOAD, но вместо измерения времени загрузки злоумышленник фокусируется на разнице во времени между двумя инструкциями clflush. Поскольку clflush не использует доступ к памяти и работает быстрее, эта атака менее заметна, хотя и менее точна.

Атака PRIME+PROBE. В отличие от предыдущих атак, направленных на общую строку LLC, эта атака ориентирована на набор кеша последнего уровня. Она также состоит из трёх этапов:

1. PRIME: злоумышленник заполняет кеш определёнными данными, чтобы вытеснить данные жертвы.

2. IDLE: злоумышленник ожидает некоторое время, пока жертва выполняет конфиденциальные операции.

3. PROBE: злоумышленник пытается получить доступ к определённым данным из кеша. Если данные жертвы были вытеснены, доступ займёт больше времени, что позволит злоумышленнику сделать выводы о том, какие данные использовались.

Результаты апробации показали, что указанные атаки влияют на такие показатели, как IPC (количество инструкций на цикл), промахи кеша L3, L2 и L1, а также на счётчики спекулятивных и завершённых ветвлений.

Авторы статьи разработали метод обнаружения атак, оптимизируя мониторинг Intel PCM и применяя технику машинного обучения на базе алгоритма классификации SoftMax. Реализованная программа обнаружения успешно идентифицирует и классифицирует атаки через побочные каналы кеша.

Таким образом, для выявления атак FLUSH+FLUSH, FLUSH+ +RELOAD и PRIME+PROBE следует учитывать такие метрики, как IPC, количество промахов кеша L1, L2 и L3, а также счётчики спекулятивных и завершённых ветвлений. Предложенный авторами метод обнаружения атак на основе машинного обучения оказался эффективным способом защиты от указанных атак.

В статье [4] авторы Hodong Kim, Changhee Hahn и Junbeom Hur исследуют атаку на процессорный кеш, а также методы её обнаружения и предотвращения. В центре внимания находится атака PRIME+ABORT, использующая аппаратное обеспечение Intel TSX.

Атака PRIME+ABORT. На этапе PRIME атакующий заполняет набор кеша своими данными. На этапе ABORT жертва вытесняет данные атакующего своими данными, вызывая уведомление атакующего через аппаратный вызов.

Авторы статьи пришли к выводу, что измерение промахов кеша во время атаки PRIME+ABORT неэффективно для её обнаружения. Вместо этого они сосредоточились на трёх событиях, демонстрирующих заметное распределение: RTM RETIRED.START, RTM RETIRED.ABORTED и TX MEM.ABORT.CAPACITY.WRITE.

На основе полученных данных авторы пришли к таким выводам.

1. Значение RTM RETIRED.START больше 3 500 000 указывает на подготовку к атаке.

2. Значения RTM RETIRED.START больше 100 000 и разница между RTM RETIRED.START и RTM RETIRED.ABORTED меньше 4 000 свидетельствуют о проведении атаки.

3. Значение TX MEM.ABORT.CAPACITY.WRITE больше 80 000 и

разница между RTM RETIRED.ABORTED и TX MEM.ABORT.CAPACITY.WRITE меньше 150 000 служат признаками проведения атаки.

Таким образом, некешевые события могут служить индикаторами атак по побочному каналу кеша процессора.

В заключение отметим, что представленные подходы демонстрируют высокую эффективность в выявлении уязвимостей криптографических устройств и других систем, работающих с конфиденциальной информацией. Особое внимание было уделено исследованию механизмов обнаружения таких атак, которые позволяют минимизировать энергопотребление и повысить скорость реакции на угрозы.

Проведённый анализ исследований показывает, что несмотря на существующие защитные меры, атаки по побочным каналам остаются актуальными и требуют дальнейшего изучения. Разработка новых методов противодействия этим атакам должна учитывать не только технические аспекты, но и экономическую целесообразность внедрения защитных мер. Важно отметить, что успешные решения должны обеспечивать баланс между уровнем защищённости и ресурсными затратами на реализацию этих решений.

Таким образом, подчеркнём необходимость продолжения исследований в области атак по побочным каналам и поиска эффективных способов их нейтрализации. Будущие работы могут быть направлены на разработку универсальных методов защиты, применимых к различным типам устройств и систем, а также на создание адаптивных механизмов, способных оперативно реагировать на изменения в условиях эксплуатации и эволюции угроз.

Список литературы

1. Albalawi A. Side-channel Attacks and Countermeasures in Cloud Services and Infrastructures / A. Albalawi, V. Vassilakis, R. Calinescu // IEEE/IFIP Network Operations and Management Symposium (NOMS). Budapest, Hungary, 2022. Pp. 1–4. DOI: 10.1109/NOMS54207.2022.9789783.

2. Jeon H. A New Foe in GPUs: Power Side-channel Attacks on Neural Network / H. Jeon, N. Karimian, T. Lehman // 22nd International Symposium on Quality Electronic Design (ISQED). Santa Clara, USA, 2021. P. 313. DOI: 10.1109/ISQED51717.2021.9424358.

3. Cho J. Real-time Detection on Cache Side Channel Attacks using Performance Counter Monitor / J. Cho, T. Kim, T. Kim et al. // International Conference on Information and Communication Technology Convergence (ICTC). Jeju, South Korea, 2019. Pp. 175–177. DOI: 10.1109/ICTC461.2019.8939797.

4. Kim H. Real-time Detection of Cache Side-channel Attack using Non-cache Hardware Events / H. Kim, C. Hahn, J. Hur // International Conference on Information Networking (ICOIN). Jeju, South Korea, 2021. Pp. 28–31. DOI: 10.1109/ICOIN50884.2021.9333883.

УДК 004.056.53

ОТ РИСКА К ЗАЩИТЕ: ЭФФЕКТИВНОСТЬ ПРИНЦИПА РАЗДЕЛЕНИЯ ПРИВИЛЕГИЙ В ЭРУ ЦИФРОВИЗАЦИИ

Е. А. Лобач[1]
Научный руководитель – М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Принцип разделения привилегий (Separation of Privileges, SoP) представляет собой ключевой элемент обеспечения информационной безопасности. Этот принцип направлен на снижение рисков, связанных с мошенничеством, ошибками и злоупотреблениями, посредством распределения задач и полномочий среди различных пользователей или систем. Основополагающая идея заключается в том, что ни один субъект не должен обладать полным контролем над критическими процессами. Для достижения этой цели задачи делятся на отдельные этапы, выполнение каждого из которых возлагается на разных людей или системы. Примером реализации данного подхода служит финансовая система, где один сотрудник может инициировать платёж, однако его утверждение осуществляется другим сотрудником. Таким образом, SoP не только уменьшает риски, но также способствует повышению прозрачности и надёжности процессов.

Принцип разделения привилегий включает следующие ключевые компоненты, обеспечивающие его эффективность.

1. Разделение. Критические задачи распределяются между различными пользователями, что предотвращает возможные злоупотребления.

2. Многоуровневая проверка. Каждый этап процесса требует утверждения со стороны другого пользователя, создавая систему сдержек и противовесов.

3. Аудит и мониторинг. Регулярные проверки прав доступа и действий пользователей помогают выявить нарушения и предотвратить злоупотребления.

4. Политики и процедуры. Ясно сформулированные политики и процедуры гарантируют соблюдение принципов разделения привилегий.

Применение принципа разделения привилегий варьируется в зависимости от конкретного контекста и характера системы. Так, в финансовой сфере SoP применяется для предотвращения мошенничества, как отмечено в работе [1], где разделение обязанностей между инициацией и утверждением платежей создаёт естественный барьер против злоупотреблений. В облачной среде SoP обеспечивает распределение ответственности между поставщиком услуг и клиентом, где поставщик отвечает за физическую безопасность и инфраструктуру, тогда как клиент управляет доступом и данными, согласно исследованию [2]. В промышленных системах управления

© Лобач Е. А., 2025

(ICS) принцип разделения привилегий используется для защиты критической инфраструктуры, как подчёркнуто в исследовании [3], указывающем на то, что разделение обязанностей между операторами и администраторами сокращает вероятность несанкционированных изменений в системе.

Процесс разработки концепции разделения привилегий начинается с тщательного анализа бизнес-процессов и выявления критически значимых задач, которые требуют распределения обязанностей. Основные этапы проектирования следующие.

1. Идентификация критических процессов: на данном этапе определяются процессы, подверженные риску мошенничества или ошибок. Например, в финансовых системах особое внимание уделяется процедурам инициирования и утверждения платежей.

2. Определение ролей и обязанностей: для каждого идентифицированного процесса создаются различные роли, каждая из которых имеет строго ограниченный набор функций. Например, одна роль может отвечать за запуск транзакций, а другая – за их подтверждение.

3. Создание политик доступа: на основании разработанных ролей формируются политики доступа, определяющие права конкретных пользователей относительно ресурсов системы.

4. Разработка механизмов проверки: чтобы обеспечить эффективную реализацию SoD, внедряются механизмы многоступенчатого подтверждения, гарантирующие выполнение критичных операций разными лицами. Например, система может потребовать, чтобы одну и ту же операцию проверяли разные пользователи.

Практическая реализация SoD зависит от специфики системы и используемых технологий. Среди основных подходов к внедрению выделяются следующие.

1. Ролевой доступ. Разделение привилегий в системах с ролевым управлением осуществляется через распределение ролей и соответствующих им прав доступа.

2. Автоматизация процессов. Для упрощения внедрения SoD применяются автоматизированные решения, такие как системы управления бизнес-процессами (BPM).

3. Интеграция с системами управления доступом (Identity and Access Management, IAM). SoD часто интегрируется с IAM-системами, которые обеспечивают централизованное управление идентификацией и правами доступа пользователей.

Для успешной интеграции SoD в информационную систему необходима координация всех её компонентов. Широко применяемый фреймворк AAA (аутентификация, авторизация, учёт) играет важную роль в реализации SoD.

Аутентификация и авторизация играют ключевую роль в реализации SoD. Подтверждение личности пользователя является начальным этапом обеспечения SoD. Надёжная аутентификация гарантирует, что доступ к системе получают лишь уполномоченные лица. После установления

подлинности пользователя система определяет спектр разрешённых действий. В контексте SoD авторизация позволяет эффективно распределять обязанности между участниками процесса. Эффективное внедрение SoD невозможно без учёта и аудита действий пользователей. Механизмы мониторинга позволяют фиксировать выполненные операции, обеспечивая выявление нарушений и повышая общую защищённость системы.

Несмотря на очевидные преимущества, использование принципа разделения привилегий связано с определёнными трудностями, а именно: ограниченность ресурсов (в малых организациях может отсутствовать достаточное количество сотрудников для полноценного разделения обязанностей); сложности управления (в крупных компаниях с множественными ролями и системами управление SoD может оказаться сложной задачей из-за высоких затрат на мониторинг и аудит); баланс между безопасностью и производительностью (избыточное разделение обязанностей способно замедлить рабочие процессы).

Развитие SoD связано с углублением взаимодействия с принципом минимальных привилегий (Least Privilege Principle, LPP), внедрением автоматизированных инструментов аудита и интеграцией в комплексные системы управления рисками, такие как Governance, Risk management, and Compliance (GRC).

1. Синергия LPP и SoD. Комбинация принципа минимальных привилегий и разделения обязанностей создаёт многослойную защиту, существенно усиливающую кибербезопасность организации. LPP ограничивает доступ пользователей до необходимого минимума, уменьшая вероятность злоупотреблений, в то время как SoD гарантирует участие нескольких лиц в выполнении критически важных процессов. Такое сочетание минимизирует риски как внутренних угроз (например, злоупотребление полномочиями), так и внешних атак, делая систему более устойчивой.

2. Автоматизация процессов аудита. Одним из приоритетных направлений развития SoD является автоматизация аудиторских процедур. Инструменты вроде Creeper [4] позволяют автоматически отслеживать накопление избыточных прав («привилегийный дрейф»). Автоматизированные системы работают быстрее и точнее человеческих аудиторов, что особенно актуально для больших компаний с многочисленными пользователями и сложными системами. Это снижает нагрузку на IT-подразделения и улучшает контроль.

3. Интеграция в GRC-фреймворк. Интеграция SoD в фреймворки управления, риск-менеджмента и соблюдения нормативных требований (GRC) становится значимым шагом в процессе управления рисками и обеспечения соответствия стандартам. GRC помогает систематизировать управление рисками, включая SoD как неотъемлемую составляющую. Такой подход не только препятствует злоупотреблениям, но и обеспечивает прозрачность и отчётность на всех уровнях компании. Это особенно важно для секторов с жёстким регулированием, таких как финансы, здравоохранение и

промышленность.

Таким образом, принцип разделения привилегий представляет собой основополагающий элемент в стратегии обеспечения информационной безопасности современных организаций. В условиях всеобъемлющей цифровизации и усложнения бизнес-процессов принцип SoP становится особенно актуальным, позволяя снизить риски, связанные с мошенничеством, ошибками и злоупотреблениями, путём ясного распределения задач и полномочий среди пользователей и систем.

Объединение принципа разделения привилегий с такими концепциями, как принцип минимальных привилегий и интеграция в системы управления рисками, создаёт дополнительные слои защиты, значительно усиливающие киберзащиту организаций. Несмотря на возможные трудности в реализации SoP, особенно в малых организациях с ограниченными ресурсами, а также в крупных компаниях с множественными ролями, принятые меры по автоматизации процессов и улучшению управления доступом помогают преодолевать эти препятствия.

В заключение следует подчеркнуть, что интеграция принципа разделения привилегий в информационные системы представляет собой стратегически важное направление для повышения уровня кибербезопасности, обеспечения соответствия нормативным требованиям и защиты критически важной информации. Непрерывная работа над усовершенствованием и адаптацией SoP к современным вызовам информационной безопасности станет ключевым фактором устойчивости и успеха организаций в условиях постоянно возрастающих цифровых угроз и вызовов современной эпохи.

Список литературы

1. Gaioto F. An Analysis of Least Privilege Policy and Segregation of Duties for Strengthening Cybersecurity Defense Mechanisms / F. Gaioto // ResearchGate. 2023. URL: researchgate.net/profile/Fiza-Gaioto/publication.pdf. DOI: 10.12136/jhc.2.2.36400.21047.

2. Савельев И. А. Современные подходы к комплексному обеспечению информационной безопасности в облаке / И. А. Савельев, О. Е. Боровская // Правовая информатика. 2023. № 3. С. 89–96.

3. Altaleb H. Enhancing Cybersecurity in Industrial Control Systems through GRC Framework: Principles, Regulations, and Risk Assessment / H. Altaleb, Z. Rajnai // ResearchGate. 2024. URL: researchgate.net/profile/Haya-Altaleb/publication.pdf. DOI: 10.1007/978-3-031-47906-5_20.

4. Brickley J. C. Policy of Least Privilege and Segregation of Duties, their Deployment, Application & Effectiveness / J. C. Brickley, K. Thakur // International Journal of Cyber-Security and Digital Forensics. 2021. Vol. 10. No. 4. Pp. 112–119.

УДК 004.056.55:512.541.54

ГОМОМОРФНОЕ ШИФРОВАНИЕ: РЕШЕНИЕ ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ В ОБЛАЧНЫХ ХРАНИЛИЩАХ

А. Д. Ломова[1]
Научный руководитель – М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Причины популярности облачных хранилищ многочисленные: удобство доступа, экономия на оборудовании, возможность быстрого развёртывания проектов и лёгкость управления данными. Кроме того, облачные хранилища помогают избежать территориальной привязанности и способствуют развитию новых технологий, таких как искусственный интеллект и машинное обучение.

Основная же угроза заключается в безопасности данных. Доверие к провайдерам облачных сервисов ограничено отсутствием полной прозрачности и риском компрометации данных. Даже при наличии шифрования данные подвергаются риску на этапе их обработки в облачной среде. Гомоморфное шифрование решает эту задачу, позволяя производить вычисления над зашифрованными данными без раскрытия их первоначального содержания.

Разработано три варианта гомоморфного шифрования: полное гомоморфное шифрование (*FHE*), частично гомоморфное шифрование (*PHE*) и гибридное шифрование (*SHE*). Полное гомоморфное шифрование поддерживает выполнение всех операций, а частично гомоморфное шифрование и гибридное шифрование поддерживают лишь отдельные операции.

Несмотря на потенциальную выгоду, гомоморфное шифрование сталкивается с рядом проблем. Оно занимает значительное место в памяти, характеризуется ограниченной функциональностью, а также порождает шумовую составляющую (искажающую данные) при выполнении операций, что усложняет его использование. Помимо этого, высокая вычислительная нагрузка и сложность внедрения в существующие приложения затрудняют его массовое применение. Вычислительные ресурсы и ёмкости облачных хранилищ могут помочь сделать гомоморфизм более эффективным инструментом для защиты данных.

В статье [1] рассматривается механизм делегированной проверки подлинности (*DPP*), основанный на гомоморфном шифровании, разработанном

© Ломова А. Д., 2025

Пэйе. Этот механизм включает обработку открытых данных, их шифрование и последующую передачу зашифрованного результата пользователю вместе с открытым ключом. Пользователь может воспользоваться функциями гомоморфного шифрования для проверки достоверности полученного результата. Хотя полное применение гомоморфного шифрования может оказаться избыточным, выборочные его элементы могут существенно повысить уровень конфиденциальности данных, что является важным шагом в направлении укрепления доверия к облачным хранилищам.

В работе [2] применяется уже модифицированный алгоритм гомоморфного шифрования Пэйе, интегрированный в многооблачную архитектуру. Отличительной особенностью модификации является изменённое значение параметра открытого ключа. Согласно результатам исследования, многооблачный подход снижает риски утечек данных и атак со стороны инсайдеров. Дополнительно реализуется механизм разделения файлов на части посредством концепции разделения криптографических баз данных, обеспечивая защиту данных одновременно методами разделения и шифрования.

Статья [3] также предлагает комбинированный подход, объединяющий схему Шамира для разделения секрета методом полиномиальной интерполяции с гомоморфным шифрованием для безопасного вычисления общих данных, формируя метод гомоморфного распределения секрета (*HSS*). Этот позволяет разделить данные на части и хранить их отдельно в одном облаке, исключая возможность облачного провайдера получить доступ к исходным данным. По утверждениям авторов, данная схема характеризуется низкими требованиями к хранилищу и вычислительной нагрузкой, высоким уровнем конфиденциальности, сохраняя при этом приемлемую производительность для приложений реального времени.

Можно разделять пользовательскую информацию на две категории: динамические и статические данные. В работе [4] критически важные данные (динамические) шифруются с использованием расширенного алгоритма Хилла, тогда как оставшиеся (статические) подвергаются гомоморфному шифрованию. Расширенный алгоритм Хилла обрабатывает разнотипные данные с модулем 256, обеспечивая повышенный уровень безопасности по сравнению с классическим вариантом, работающим только с однородными данными по модулю 4. Временная сложность расширенного шифра Хилла возрастает пропорционально размеру данных, однако он демонстрирует улучшенную защищённость.

В следующей работе [5] рассматривается проблема «начальной загрузки», которая из-за затрат на вычисление и пропускной способности памяти ощутимо увеличивает время вычислений на основе FHE. Для решения предлагают FAB-ускоритель на базе FPDA. FAB эффективно использует ограниченные вычислительные ресурсы. Несмотря на то, что ускоритель был разработан для CKKS (схемы FHE Чон – Ким – Ким – Сона (CKKS)), базовые операции сложения, умножения и поворота могут использоваться и для других схем.

Работа посвящена исследованию применения гомоморфного шифрования в облачных вычислениях для производственных нужд. Применение полностью гомоморфного шифрования (FHE), отличающегося большей функциональностью, решает проблему выбора между использованием облачных технологий и обеспечением безопасности, позволяя средним и малым предприятиям внедрять стратегии профилактического обслуживания. Для контрактного производства облачные платформы служат местом обмена данными. Выбор частично гомоморфного шифрования (SHE) позволяет проводить тендеры без предварительного юридического обеспечения, поскольку расчёт предложений по стоимости и срокам осуществляется без разглашения конфиденциальной информации, что особенно актуально в условиях конкуренции.

Несмотря на положительные результаты, отмечается, что текущие алгоритмы гомоморфного шифрования требуют значительных вычислительных ресурсов, поэтому перспективным направлением остаётся разработка специализированных FHE-методов для производственного сектора.

Таким образом, актуальные подходы к внедрению гомоморфного шифрования в облачные хранилища включают следующие решения: деление данных на части, разработка новых аппаратных решений, модификация старых и разработка новых методов шифрования.

Гомоморфное шифрование в облачных хранилищах весьма перспективная область для разработок. Несмотря на значительный прогресс, вычислительная сложность и ограниченная функциональность некоторых существующих реализаций остаются существенными препятствиями для широкого внедрения.

Список литературы

1. Wang J. DPP: Data Privacy-Preserving for Cloud Computing based on Homomorphic Encryption / J. Wang, F. Wu, T. Zhang et al. // IEEE. 2022. DOI: 10.1109/CyberC55534.2022.00016.

2. Kumar R. Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage / R. Kumar, B. Seth, S. Dalal // Recent Advances in Computational Intelligence. 2019. Pp. 77–92. URL: link.springer.com/chapter/10.1007/978-3-030-12500-4_5#author-information.

3. Ali S. Advancing Cloud Security: Unveiling the Protective Potential of Homomorphic Secret Sharing in Secure Cloud Computing / S. Ali, S. A. Wadho, A. Yichiet et al. // Egyptian Informatics Journal. 2024. DOI: 10.1016/j.eij.2024.100519.

4. Das B. K. Security of Cloud Storage based on Extended Hill Cipher and Homomorphic Encryption / B. K. Das, R. Garg // IEEE. 2019. DOI: 10.1109/ICCES45898.2019.9002549.

5. Agrawal R. FAB: an FPGA-based Accelerator for Bootstrappable Fully Homomorphic Encryption / R. Agrawal, L. de Castro, G. Yang et al. // IEEE. 2023. DOI: 10.1109/HPCA56546.2023.10070953.

УДК 004.056.55

УЯЗВИМОСТИ И АТАКИ В СИСТЕМАХ МАШИННОГО ОБУЧЕНИЯ И КОМПЬЮТЕРНОГО ЗРЕНИЯ В ЭПОХУ ЦИФРОВЫХ ДАННЫХ

А. О. Мулонов[1]
Научный руководитель – М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

В эпоху цифровизации объёмы данных, создаваемые ежедневно, растут колоссальными темпами. Искусственный интеллект (ИИ) и машинное обучение (МО) предоставляют инструменты для обработки, анализа и извлечения значимых паттернов из этих данных. Эффективность систем МО обусловлена их способностью значительно быстрее, чем человек, выявлять скрытые закономерности в данных, описывающих различные процессы или явления. Благодаря этой способности системы МО становятся всё более распространёнными в разных сферах человеческой деятельности [1].

В свою очередь, такая область ИИ и компьютерных наук, как компьютерное зрение, представляет собой технологию, позволяющую обрабатывать и извлекать полезную информацию из изображений. Атаки на системы компьютерного зрения, именуемые состязательными (*adversarial*), могут приводить к серьёзным нарушениям безопасности и функциональности этих систем. Суть большинства таких атак заключается в добавлении незначительных возмущений, незаметных для человеческого глаза, к обучающим наборам данных. Это может вызвать неверную классификацию изображений системой, приводя к пометке объекта как принадлежащего к совершенно другому классу или даже к полному его игнорированию. Такие уязвимости подчёркивают необходимость разработки более устойчивых и защищённых алгоритмов, а также методов повышения надёжности систем компьютерного зрения.

Атаки подразделяются на атаки «белого ящика», характеризующиеся полным доступом к информации о модели, включая её структуру, параметры и сведения о входных данных. В противовес атакам «белого ящика», атаки «чёрного ящика» осуществляются без доступа к внутренней структуре модели, что усложняет процесс их проведения.

Атаки с одним пикселем (One-Pixel Attack, OPA) – тип атаки «белого ящика». Предполагается, что входное изображение может быть представлено вектором, в котором каждый скалярный элемент представляет один пиксель [2]. Суть атаки заключается в модификации n пикселей входного изображения. В работе [2] представлено исследование, которое доказывает эффективность

© Мулонов А. О., 2025

однопиксельных атак, а также даны сравнительные характеристики атак с тремя и пятью модифицированными пикселями. Результаты приведены в таблице 1.

Таблица 1

Эффективность атак

Тип атаки	Однопиксельная	Трёхпиксельная	Пятипиксельная
Успешность атаки, %	79,4	79,17	77,09

Таким образом, показано преимущество однопиксельных атак над трёх- и пятипиксельными. Успешность однопиксельной атаки обуславливается тем, что с увеличением числа модифицированных пикселей увеличивается число целевых классов. Атака с одним пикселем является интересным примером того, как минимальные изменения в данных могут приводить к серьёзным последствиям для моделей МО. Этот подход показывает, насколько важно учитывать возможные угрозы при разработке и внедрении систем ИИ, особенно в критически важных областях.

Атаки с нулевым запросом (Zero-Query Attacks, ZQA) представляют собой разновидность атак типа «чёрного ящика». В рамках таких атак злоумышленники могут создавать ложные изображения или видео, способные обманывать системы компьютерного зрения, а также использовать результаты работы одной системы для обхода защиты другой – например, в случае систем распознавания лиц [1].

В работе [3] рассматриваются системы, использующие контекстную информацию изображения для повышения точности задач визуального распознавания. Такие системы применяют детекторы, анализирующие объекты в контексте их окружения. Например, в естественной сцене, содержащей несколько объектов, наличие лодки рядом со знаком «стоп» будет выглядеть аномально, т. к. эти два объекта обычно не встречаются вместе. Контекстно-зависимые детекторы способны выявить такие несоответствия и предотвратить успешность атаки уклонения, направленной на отдельный объект. Однако, авторы статьи [3] предлагают метод, позволяющий обойти проверки на контекстную согласованность у детекторов объектов. В исследовании атаки проводились на модель белого ящика Faster R-CNN и на модели чёрного ящика RetinaNet, Libra R-CNN, FoveaBox. Сравнительный анализ приведён в таблице 2.

Таблица 2

Результаты атак, %

Модель	**ε = 50**	**ε = 40**	**ε = 30**	**ε = 20**	**ε = 10**
Faster R-CNN	92,6	92,0	93,0	88,2	70,6
RetinaNet	51,2	51,8	49,2	44,0	23,2
Libra R-CNN	61,6	55,4	57,2	51,4	27,4
FoveaBox	56,8	54,4	54,0	51,4	28,2

Таким образом, атаки с нулевым запросом представляют собой серьёзную угрозу для систем компьютерного зрения. А эффективность атак зависит от

архитектуры модели и величины вносимых возмущений, что подчёркивает необходимость дальнейших разработок в области защиты и повышения устойчивости систем к подобным угрозам.

Атака методом быстрого градиента (Fast Gradient Sign Method, FGSM) представляет собой технику генерации вредоносных примеров (adversarial examples) для обмана моделей МО, особенно применяемых в области компьютерного зрения.

Метод быстрого градиентного распознавания основан на использовании градиентов нейронной сети для создания примера состязательности. Для входного изображения он вычисляет градиенты потерь по отношению к входному изображению, что позволяет получить матрицу возмущений и шума. Используя эту матрицу, создаётся новый образ противника, который будет неправильно классифицирован моделью [4].

В работе [5] проводились FGSM-атаки на модели Resnet50, VGG16, VGG19. Результаты проведения атак приведены в таблице 3. В ней показаны процентные доли ошибок в выборках, сгенерированных при целевой и нецелевой атаках, выявленных различными классификаторами при разных значениях ε.

Таблица 3

Результаты *FGSM*-атак, %

Модель	**ε = 5**		**ε = 10**		**ε = 20**	
	Целевая атака	Нецелевая атака	Целевая атака	Нецелевая атака	Целевая атака	Нецелевая атака
*ResNet*50	73,61	51,39	78,87	78,87	84,72	100
*VGG*16	23,61	22,22	50,7	59,15	75	84,72
*VGG*19	22,22	25	54,93	60,56	75	90,28

Метод быстрого градиента является важным инструментом для исследования устойчивости моделей МО к атакам. Он помогает понять потенциальные слабые места моделей и стимулирует разработку новых подходов к защите от вредоносных воздействий.

Современные системы защиты демонстрируют высокую эффективность за счёт использования анализа контекстной согласованности [6]. Для этого применяются детекторы, которые анализируют множество объектов на изображении и формируют общий контекст. Если изображение и контекст оказываются согласованными, система функционирует надёжнее. Кроме того, рекомендуется формировать собственные уникальные наборы данных, что снижает риск переноса уязвимостей из уже существующих источников.

Одним из эффективных методов защиты от вредоносных воздействий является использование состязательного обучения (Adversarial Training). Этот подход предусматривает включение состязательных примеров в процесс обучения нейросети, что способствует повышению её устойчивости к атакам [7]. Состязательные примеры генерируются с применением целевой модели, и основная цель состязательной тренировки заключается в обучении

нейросетевой модели корректно классифицировать враждебные изображения, подвергшиеся многократным модификациям.

В заключение отметим, что современная эпоха цифровизации и стремительный рост объёмов данных подчёркивают важность и необходимость разработки надёжных систем МО и компьютерного зрения, способных эффективно обрабатывать информацию и анализировать её в реалистичных условиях. Несмотря на их значительный потенциал, системы МО сталкиваются с серьёзными уязвимостями, которые могут быть использованы злоумышленниками. Основные проблемы, такие как недостаточная репрезентативность обучающих данных, непрозрачность процессов принятия решений, подчёркивают необходимость дальнейших исследований и разработок в области защиты моделей.

Таким образом, в будущем необходимо сосредоточиться на разработке более стабильных и адаптивных алгоритмов, которые будут учитывать указанные уязвимости, а также на создании стандартов и практик, направленных на обеспечение прозрачности и безопасности систем МО и компьютерного зрения. Эти усилия помогут повысить не только функциональность, но и этическую ответственность применения технологий ИИ в различных сферах человеческой деятельности.

Список литературы

1. Котенко И. В. Атаки и методы защиты в системах машинного обучения: анализ современных исследований / И. В. Котенко, И. Б. Саенко, О. С. Лаута и др. // Вопросы кибербезопасности. 2024. № 1. С. 24–37.

2. Su J. One-pixel Attack for Fooling Deep Neural Networks / J. Su, D. V. Vargas, K. Sakurai // IEEE Transactions on Evolutionary Computation. 2019. Vol. 23. Iss. 5. Pp. 828–841.

3. Cai Z. Zero-query Transfer Attacks on Context-aware Object Detectors / Z. Cai, S. Rane, A. E. Brito // IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2022.

4. Jagadeesha N. Facial Privacy Preservation using FGSM and Universal Perturbation Attacks / N. Jagadeesha // International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON). 2022.

5. Xu J. Using FGSM Targeted Attack to Improve the Transferability of Adversarial Example / J. Xu, Z. Cai, W. Shen // IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE). 2019.

6. Li S. Connecting the Dots: Detecting Adversarial Perturbations using Context Inconsistency / S. Li, S. Zhu, S. Paul.

7. Ren K. Adversarial Attacks and Defenses in Deep Learning / K. Ren, T. Zheng, Z. Qin et al. // Engineering. 2020. Vol. 6. Pp. 346–360.

УДК 004.056.5

ИНТЕРНЕТ ВЕЩЕЙ: АКТУАЛЬНЫЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

О. В. Рубцова[1]
Научный руководитель – В. И. Вайнштейн[1]
Кандидат физико-математических наук, заведующий кафедрой информационной безопасности

[1]*Сибирский федеральный университет*

Интернет вещей (*IoT*) представляет собой сеть взаимосвязанных устройств, которые обмениваются данными и взаимодействуют друг с другом через интернет. Несмотря на огромный потенциал *IoT* в различных сферах, таких как умные города, здравоохранение и промышленность, вопросы безопасности остаются одной из главных проблем, с которыми сталкивается данная технология. В настоящей статье рассматриваются основные угрозы безопасности *IoT*, а также предлагаются возможные решения для их преодоления.

Согласно прогнозам, к 2030 г. количество устройств, подключённых к интернету, превысит 30 млрд. Это создаёт не только новые возможности для автоматизации и оптимизации процессов, но и новые вызовы в области кибербезопасности. Уязвимости в *IoT*-устройствах могут привести к утечкам данных, несанкционированному доступу и даже физическим угрозам.

Угрозы безопасности IoT:

1. Уязвимости на уровне устройства. Многие IoT-устройства имеют ограниченные вычислительные ресурсы и не могут поддерживать сложные механизмы защиты. Это делает их уязвимыми для атак, таких как:

– несанкционированный доступ: атакующие могут использовать слабые пароли или известные уязвимости для доступа к устройствам;

– вредоносное программное обеспечение: может быть установлено на устройства, что может привести к компрометации данных.

2. Проблемы с передачей данных. Данные, передаваемые между IoT-устройствами, могут быть перехвачены или изменены во время передачи. Это может произойти из-за:

– отсутствия шифрования: многие устройства не используют шифрование для защиты данных, что делает их уязвимыми для атак «человек посередине»;

– неавторизованного доступа к сети: устройства, подключённые к незащищённым сетям, могут стать мишенью для злоумышленников.

3. Сложности в управлении устройствами. Управление большим количеством IoT-устройств может быть затруднительным, особенно если они находятся в разных местах и имеют разные протоколы связи. Это может

© Рубцова О. В., 2025

привести:

– к отсутствию обновлений безопасности: устаревшие устройства могут не получать обновления, что делает их уязвимыми для известных угроз;

– недостаточной видимости: отсутствие централизованного управления может затруднить обнаружение и реагирование на инциденты безопасности.

Решения для повышения безопасности IoT

1. Укрепление аутентификации. Использование многофакторной аутентификации и сложных паролей может значительно снизить риск несанкционированного доступа к устройствам.

2. Шифрование данных. Шифрование данных как на уровне устройства, так и во время передачи может защитить информацию от перехвата и изменения.

3. Регулярные обновления и патчи. Создание механизма для регулярного обновления программного обеспечения устройств поможет устранить известные уязвимости и улучшить общую безопасность системы.

4. Централизованное управление. Использование платформ для централизованного управления IoT-устройствами позволит улучшить видимость и контроль над безопасностью сети.

5. Образование и осведомлённость пользователей. Обучение пользователей основам безопасности IoT может помочь предотвратить многие угрозы, связанные с человеческим фактором.

Итак, защищённость Интернета вещей является критически важной задачей, требующей комплексного подхода. Учитывая растущее количество подключённых устройств и потенциальные угрозы, необходимо активное сотрудничество между производителями, разработчиками программного обеспечения и пользователями для создания безопасной экосистемы IoT. Внедрение предложенных решений может значительно повысить уровень безопасности и доверия к этой перспективной технологии.

Список литературы

1. Sicari B. Security, Privacy and Trust in Internet of Things: the Road ahead / B. Sicari, A. R. C. M. Miorandi, F. de Pellegrini et al. // Computer Networks. 2015. Vol. 76. Pp. 146–164.

2. Almazroi A. Security Challenges in Internet of Things: a Survey / A. Almazroi, A. Alzahrani, M. Alzahrani // Journal of King Saud University – Computer and Information Sciences. 2021.

3. Ali S. S. M. Internet of Things Security: a Survey / S. S. M. Ali, M. A. M. Ali // IEEE Access. 2020. Vol. 8. Pp. 148 054–148 075.

4. Герасимова А. И. Проектирование системы «Умный дом» / А. И. Герасимова // Проблемы науки. 2015. № 2 (32). URL: cyberleninka.ru.

5. Ли Ю. Архитектура шлюза умного дома на основе блокчейна для предотвращения подделки данных / Ю. Ли, С. Ратор, Д. Парк и др. // Человекоориентированные вычислительные и информационные науки. 2020. Т. 10. С. 1–14.

УДК 004.056.5

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВОПРОСАХ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И РЕВЕРС-ИНЖИНИРИНГА

А. А. Садомский, Д. А. Виншу, А. А. Бармин[1]
Научный руководитель В. Б. Туговиков[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

В современном мире программного обеспечения (ПО) его защита играет одну из ключевых ролей в информационном мире. В связи с этим растущая сложность программных решений и увеличивающийся объём данных требуют новых подходов, где одним из перспективных направлений является использование искусственного интеллекта (ИИ) [2]. Реверс-инжиниринг (РИ) используется как инструмент в защите ПО, и ИИ также открывает для него новые горизонты в автоматизации процессов, позволяя упростить работу. Системы машинного обучения способны адаптироваться к различным архитектурам и языкам программирования, сокращая время, необходимое для РИ. Но не стоит забывать, что РИ могут использовать злоумышленники с целью кражи готовых разработок, нарушения авторского права и т. п. В связи с этим современные методы защиты ПО, также основанные на ИИ, включают в себя современные методы защиты от РИ и иных действий злоумышленников.

Рассмотрим некоторые определения.

Предиктивное моделирование – это метод, который использует исторические данные для прогнозирования будущих результатов.

DNN (Deep Neural Network) – это тип нейронной сети, состоящий из множества слоёв, которые помогают моделям ИИ обрабатывать сложные данные. В отличие от простых нейронных сетей, DNN включает в себя несколько скрытых слоёв между входным и выходным слоями, что позволяет эффективно извлекать и обрабатывать более сложные признаки из данных.

Обфускация – приведение исходного кода или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

Защита информационных систем от атак требует инструментов, способных помогать аналитикам принимать обоснованные решения в режиме реального времени. ИИ успешно применяется для поддержки процесса принятия решений посредством использования таких методов, как

© Садомский А. А., Виншу Д. А., Бармин А. А., 2025

распознавание образов [1], обнаружение аномалий, предиктивная аналитика и обработка естественного языка. Эти ИИ-инструменты способствуют эффективному приоритезированию угроз и их смягчению, тем самым повышая общую устойчивость информационных систем. Кроме того, за счёт автоматизации отдельных этапов ИИ может косвенно поддерживать процессы защиты ПО, выделяя потенциально проблемные области, требующие более глубокого ручного изучения.

Рассмотрим пример применения ИИ в области защиты ПО в статье [5], которая представляет многоуровневую систему для обнаружения вредоносных Android-приложений с использованием глубоких нейронных сетей. Авторы разработали архитектуру, состоящую из трёх компонентов: модуль статического анализа извлекает признаки без запуска приложения, модуль динамического анализа отслеживает поведение во время выполнения, а модуль Refiner объединяет данные с обоих уровней и применяет модель глубокого обучения для финальной классификации.

Система нацелена на преодоление ограничений традиционных методов, особенно в выявлении ранее неизвестного и обфусцированного вредоносного ПО. В ходе экспериментов DeepRefiner показал высокую точность – 98,2 %, значительно превзойдя существующие подходы. Результаты [5] подтверждают эффективность интеграции многоуровневого анализа и нейросетевых моделей для повышения безопасности Android-платформ.

Один из важных аспектов защиты ПО, где ИИ может упростить анализ программного кода – РИ. Согласно принятому определению [2], реверс-инжиниринг – это критически важный набор методов и инструментов для понимания того, что на самом деле представляет собой программное обеспечение. Формально это «процесс анализа предметной системы с целью идентификации компонентов системы и их взаимосвязей, а также создания представлений системы в другой форме». В отличие от традиционного инжиниринга, где разработка идёт от концепции к реализации, РИ движется в обратном направлении: от конечного продукта к его внутреннему устройству.

Основные цели РИ:

– восстановление утерянной документации;

– анализ конкурентных продуктов, создание аналогов;

– поиск уязвимостей и улучшение безопасности;

– обеспечение совместимости.

Основные шаги РИ:

1) декомпозиция;

2) разделение системы на отдельные компоненты;

3) исследование структуры, алгоритмов, используемых библиотек и протоколов;

4) реконструкция;

5) создание модели [4].

Современные подходы к РИ всё чаще включают в себя элементы ИИ с

целью упросить работу специалистам и автоматизировать рутинные процессы декомпиляции и анализа [3].

Для практической демонстрации процесса РИ с использованием ИИ авторами статьи был проведён анализ файла project1.exe, сделанный в рамках учебной деятельности. Согласно предложенному сценарию разработчик этой программы уволился, поэтому РИ нужен для восстановления исходного кода и логики работы приложения. В ходе этой работы было сделано следующее:

1) определена среда разработки – выполнено с использованием ИИ, который по структуре интерфейса и метаданным исполняемого файла определил, что ПО создано в среде Borland C++ с использованием компонентов VCL;

2) декомпиляция и анализ исполняемого кода – выполнено с привлечением средств РИ (DeDe), а также ИИ, генерирующего возможный исходный код на C++ Builder по декомпилированным блокам логики;

3) воссоздание пользовательской документации – с использованием ИИ сгенерировано описание работы программы и её интерфейса.

Использованный в приведённом примере метод менее точный, но он не потребовал от исполнителей какого-либо глубокого понимания в теме РИ. Применённая авторами интеграция ИИ в процесс РИ позволяет существенно упростить задачи, ранее требовавшие часов кропотливого труда и определённых навыков. Особенно актуально это в случае если требуется провести экспресс-анализ ПО, полученного из ненадёжного источника или для восстановления утерянного собственного проекта. Это также важно в случае отсутствия документации или если потребовалось продолжить или возобновить некогда заброшенный, незадокументированный проект. Кроме того, в приведённом учебном задании на основании интерфейса и извлечённой логики ИИ автоматически сгенерировал техническое описание ПО, которое могло бы быть использовано как черновик документации, основа отчёта по аудиту или руководства пользователя.

В заключение стоит отметить, что применение ИИ как в защите ПО, так и в задачах РИ существенно упрощает решение поставленных задач, иногда даже таких, которые ранее требовали высокой квалификации исполнителей. Благодаря доступности и лёгкости в использовании любой заинтересованный пользователь может получить положительный результат.

Список литературы

1. Anderson R. J. Security Engineering: a Guide to Building Dependable Distributed Systems / R. J. Anderson. 2020. 875 p.

2. Eilam E. Reversing: Secrets of Reverse Engineering / E. Eilam. 2005.

3. Stamp M. Malware Analysis using Artificial Intelligence and Deep Learning / M. Stamp, M. Alazab, A. Shalaginov. 2021.

4. Komolafe O. Reverse Engineering: Techniques, Applications, Challenges, Opportunities / O. Komolafe, I. T. Adejugbe, T. I. Olorunsola. 2024.

5. Xu K. DeepRefiner: Multi-layer Android Malware Detection System

Applying Deep Neural Networks Applying Deep Neural Networks / K. Xu, Y. Li, R. H. Deng et al. 2018. DOI: 10.1109/EuroSP.2018.00040.

УДК 004.056.55

ОТ ФЕЙКОВ ДО ФАКТОВ: ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ КОНТЕНТА

Е. Д. Ступницкий[1]
Научный руководитель – М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

За последние десятилетия цифровые технологии прошли значительный путь развития, что привело к стремительному росту создания и распространения цифрового контента, включая изображения, которые стали неотъемлемой частью повседневной жизни. Хотя изображения широко используются в различных областях, таких как социальные сети, профессиональная фотография и реклама, возникли серьёзные вызовы, связанные
с защитой авторских прав и манипулированием контентом. В этом контексте маркирование цифровым водяным знаком стало важным средством защиты интеллектуальной собственности и обеспечения целостности информации.

ЦВЗ представляют собой невидимые метки, встроенные в изображение, содержащие информацию о владельцах авторских прав или подтверждающие подлинность контента. Они служат для защиты авторских прав, а также позволяют отслеживать использование изображений в сети, что особенно важно в условиях распространения фейкового контента и дезинформационных материалов. Они позволяют защищать контент от подделки и обеспечивать целостность информации, а также служат для подтверждения подлинности изображения. Современные методы ЦВЗ должны быть устойчивыми к различным видам атак, включая изменение формата изображения, сжатие и попытки удаления водяных знаков.

Работа отечественных исследователей А. Н. Шниперова, М. С. Сосновского и П. М. Шипулина [1] посвящена разработке метода встраивания цифровых водяных знаков в изображения, основанного на ортогональных моментах Цернике. В своём исследовании авторы заявляют, что предложенный ими метод характеризуется умеренной вычислительной сложностью и устойчивостью к различным видам атак. Чтобы снизить нагрузку на процессор при расчёте моментов Цернике, авторы рекомендуют использовать не всё изображение целиком, а лишь его локальные участки. Эти участки

© Ступницкий Е. Д., 2025

определяются на основе нахождения особых точек, и расчёт ведётся исключительно для окрестностей этих точек.

Предложенный метод имеет ряд преимуществ, таких как пригодность для изображений различных форматов, незначительное воздействие на исходное изображение и устойчивость к широкому спектру атак. Его вычислительная сложность остаётся на приемлемом уровне, что делает его привлекательным для практического применения. Однако авторами отмечается недостаток метода, связанный с невозможностью его использования для изображений, в которых ключевые точки сконцентрированы в одном месте. Тем не менее такая ситуация встречается редко, и авторы считают, что это не является существенной проблемой, поскольку подобных изображений немного.

Альтернативный подход к встраиванию цифровых водяных знаков в изображения, предложенный в работе [2], основан на полярных гармонических преобразованиях (ПГП). По сравнению с методами, использующими моменты Цернике, предложенная техника обладает преимуществами
в вычислительном аспекте и демонстрирует лучшую устойчивость к атакам при тестировании. Авторы изучили различные варианты формирования цифровых водяных знаков на основе ПГП, выделяя различия в выражениях для расчёта радиальной составляющей момента.

В работе авторы подчеркнули, что среди различных полярных преобразований наилучшие результаты были достигнуты при использовании полярных синусоидальных преобразований. Было отмечено, что многократное марочное встраивание на основе максимального совпадения повышает устойчивость метода к атакам, причём рекомендуется использовать водяной знак длиной до 20 Б.

Исследователи А. Г. Зотин и А. В. Проскурин в своей работе [3] утверждают, что методы встраивания и извлечения цифровых водяных знаков, основанные на скремблировании и частотных преобразованиях, обладают высокой устойчивостью к различным видам атак, но требуют значительных вычислительных ресурсов. В мобильных устройствах, где вычислительные мощности ограничены, предлагается использовать методы, направленные на уменьшение вычислительного времени и увеличение скорости операций.

Авторы предложили усовершенствования, которые снижают общие вычислительные затраты и ускоряют процессы подготовки и встраивания цифровых водяных знаков. Эти улучшения включают использование преобразования Арнольда и дискретного вейвлет-преобразования, а также применение методов линейной интерпретации данных как носителей ЦВЗ, использование таблиц преобразований и параллельные вычисления на нескольких потоках. Эти методы позволяют существенно сократить временные и вычислительные издержки, что делает их особенно привлекательными для мобильных устройств.

В статье [4] *H. Agarwal* и *Dr. F. Husain* рассматривают использование ЦВЗ как эффективного средства противодействия цифровому пиратству. В отличие от предыдущих работ, авторы предлагают внедрять ЦВЗ не непосредственно в изображение, а в видеофайл, разбивая его на кадры и применяя специальные методы к каждому кадру отдельно. Затем к каждому фрагменту применяются геометрические методы для создания уникальных маркеров.

В результате проведённого исследования авторы отмечают, что предложенный метод демонстрирует высокую эффективность и устойчивость к различным видам атак.

В статье [5] авторы предлагают алгоритм цифрового водяного знака, основанный на дискретном косинусовом преобразовании. Целью исследования является разработка метода, который обеспечивает незаметное для человеческого глаза встраивание ЦВЗ.

Эксперимент показал, что изображение с внедрённым ЦВЗ, имеющим высокое соотношение «сигнал – шум» (более 36 дБ), сохраняет хорошую степень прозрачности и человек не сможет заметить присутствие водяного знака. Более того, извлечение ЦВЗ из такого изображения оказывается практически невозможно. В исследовании доказано, что разработанный метод обеспечивает незаметность ЦВЗ для наблюдателей, а также высокую степень маскировки, что делает его подходящим для защиты изображений от копирования и модификации.

На основе проведённого обзора резюмируем, что цифровым водяным знаком пользуются разнообразные отрасли, начиная от цифровой фотографии и заканчивая охранением интеллектуальной собственности в мультимедийных приложениях. Объём его использования продолжает расти, что подчёркивает возрастающую потребность в надёжных средствах защиты авторских прав и целостности данных.

Одним из важнейших направлений развития ЦВЗ является улучшение его устойчивости к различным видам атак. Современные методы встраивания ЦВЗ стремятся обеспечить стойкость к атаке на сжатие, изменение размера и удаление самого знака, а разработчики продолжают совершенствовать алгоритмы его встраивания и извлечения, делая их более надёжными и эффективными.

ЦВЗ всё больше внедряется в мультимедиа-приложения, где он используется для защиты аудио-, видео- и графических данных. Эта тенденция ведёт к разработке методов встраивания водяных знаков в различные форматы данных, включая аудиофайлы, видеоматериалы и графическое представление. Такое расширение функционала способствует его применению в широком спектре приложений, увеличивая его ценность для различных отраслей.

Значительный интерес наблюдается в снижении вычислительной сложности ЦВЗ для его применения в мобильных устройствах и системах с ограниченной вычислительной мощностью. Это направление развития

включает оптимизацию методов обработки изображений, сокращение вычислительных затрат на его встраивание и извлечение.

ЦВЗ начинает активно использоваться в различных областях, таких как охрана интеллектуальной собственности, управление правами доступа и защита чувствительных данных.

Отметим, что ЦВЗ также начинает интегрироваться с методами машинного обучения и искусственного интеллекта. Это даёт возможность автоматизировать процессы обработки изображений и повышать точность распознавания подделок и модификаций данных. Интеграция ЦВЗ с ИИ помогает улучшить защиту данных и повысить эффективность обнаружения фейков и попыток модификации изображений.

Маркирование ЦВЗ продолжает оставаться важным инструментом защиты интеллектуальной собственности и обеспечения целостности данных. Современные исследования направлены на улучшение устойчивости ЦВЗ к атакам, его адаптацию к различным форматам данных и снижение вычислительной загрузки. Интеграция методов ЦВЗ с ИИ и другими инновациями позволяет расширить область применения и повысить надёжность и эффективность защиты цифровых активов.

Список литературы

1. Шниперов А. Н. Робастный метод маркирования изображений цифровым водяным знаком, основанный на ортогональных моментах Цернике / А. Н. Шниперов, М. С. Сосновский, П. М. Шипулин // Информационные технологии. 2019. Т. 5. № 7. С. 405–413.

2. Шниперов А. Н. Использование полярных гармонических преобразований при разработке методов маркирования изображений робастным цифровым водяным знаком / А. Н. Шниперов, В. А. Мельников // Безопасность информационных технологий. 2021. Т. 28. № 4. С. 90–103.

3. Зотин А. Г. Способы ускорения подготовки и встраивания цифрового водяного знака с использованием мобильных устройств на основе преобразования Арнольда и вейвлет-преобразования / А. Г. Зотин, А. В. Проскурин // Программные продукты и системы. 2021. № 3. С. 420–432.

4. Agarwal H. Protecting Ownership Rights of Videos against Digital Piracy: an Efficient Digital Watermarking Scheme / H. Agarwal, D. F. Husain // International Journal of Communication Networks and Information Security. 2021. Vol. 13. No. 2.

5. Duang Y. Research on Digital Watermarking Algorithm based on Discrete Cosine Transform / Y. Duang, Y. Wang, C. Cao et al. // 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). 2022.

УДК 004.052.42

ФИШИНГ В ЭПОХУ ЦИФРОВИЗАЦИИ: ЭФФЕКТИВНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ

Р. Ф. Швецов[1]
Научный руководитель – М. В. Сомова[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Фишинг – одна из самых опасных киберугроз, использующая домены и URL для кражи данных через социальную инженерию. Эта тактика остаётся эффективной, а число атак растёт, что подчёркивает важность надёжных методов обнаружения. Фишинговые сайты маскируются под легитимные, усложняя их выявление. Применяются подходы от эвристик до машинного обучения, но решения часто сталкиваются с ложными срабатываниями и слабой адаптацией к новым угрозам.

Е. А. Матюков и А. В. Затонский предложили систему обнаружения фишинговых URL [1]. URL проверяется через DPI по белому списку и восьми эвристикам (код страны, ключевые слова, SSL/TLS, длина URL, символ @, точки, слеши, доступность). Точность – 98,16 %.

В исследовании [2] предложен метод обнаружения фишинговых сайтов, основанный на анализе косвенных признаков с применением многослойной нейронной сети. Авторы акцентируют внимание на актуальной проблеме кражи личной информации в интернете и отмечают ограничения существующих защитных систем, опирающихся преимущественно на чёрные списки сайтов. При отсутствии сайта в таком списке пользователи могут остаться без предупреждения о его потенциально вредоносной природе.

Цель работы заключалась в разработке подхода для идентификации фишинговых сайтов в режиме реального времени, независимого от чёрных списков. Для этого были выделены ключевые критерии, позволяющие опытным пользователям оценить степень подозрительности сайта. Среди рассматриваемых параметров выделяются такие аспекты, как используемый протокол связи (HTTPS), присутствие домена в списке предварительной загрузки HSTS, а также количество и качество гиперссылок на странице.

В статье [3] предложен усовершенствованный инструмент для обнаружения фишинговых атак с использованием методов глубокого обучения. Основной задачей было создание улучшенной системы для выявления фишинга посредством глубокого обучения, а также использование обширного набора данных для обучения и тестирования модели, наряду с интеграцией с чёрными списками и API для оптимизации процесса.

© Швецов Р. Ф., 2025

Для достижения поставленных целей использовались следующие алгоритмы глубокого обучения: нейронная сеть (Neural Network), метод k-ближайших соседей, метод опорных векторов (SVM), случайный лес (Random Forest) и наивный Байесовский классификатор (Naive Bayes Classifier). Результаты исследования показывают, что применение нейронной сети позволило существенно повысить эффективность инструмента при обработке фишинговых данных.

В работе [4] описывается метод обнаружения фишинговых URL с использованием веб-краулинга. Основная цель исследования – разработка эффективного инструмента для выявления фишинговых сайтов, включая те, которые появляются в день атаки (zero-day phishing). Предложенный авторами трёхфазный подход, названный Web Crawler based Phishing Attack Detector (WC-PAD), анализирует веб-трафик, веб-контент и URL-адреса для классификации сайтов на фишинговые и нефишинговые.

При этом ранее описанные подходы имеют существенные недостатки, которые заключаются в необходимости ручного обновления списков и неспособности обнаруживать zero-day атаки. Использование веб-краулеров представляет новый подход, направленный на решение проблемы обнаружения таких атак.

Исследование [5] предлагает альтернативный подход к выявлению фишинга. Работа посвящена разработке метода обнаружения фишинговых сайтов с использованием свёрточной нейронной сети (CNN) и библиотеки Fast.ai для повышения точности распознавания фишинговых URL и сокращения времени обучения модели по сравнению с традиционными методами. Fast.ai позволяет ускорить обучение моделей благодаря использованию графических процессоров (GPU). Предлагаемый метод включает несколько этапов: сбор и предварительную обработку данных, извлечение признаков, уменьшение размерности и обучение модели.

После десяти эпох обучения модель достигла точности 98,84 %. Для подробной оценки модели в исследовании была построена кривая обучения, показавшая, что модель хорошо обучена и не подвержена переобучению.

Зарубежные исследователи [6] предлагают новый метод обнаружения фишинговых сайтов с использованием стекированных ансамблей моделей машинного обучения. Цель исследования заключалась в разработке эффективного и точного способа выявления фишинговых атак, остающихся серьёзной угрозой для пользователей и организаций. Авторы предлагают применять лексические признаки для извлечения характеристик, которые затем классифицируют сайты на фишинговые и легитимные с помощью стекированного классификатора.

Поскольку многие существующие методы машинного обучения требуют значительных вычислительных ресурсов и не всегда универсальны, авторы предлагают использовать стекированные ансамбли моделей для обнаружения фишинга. Метод включает этапы сбора и предобработки

данных, извлечения признаков, снижения размерности и обучения модели. Лексические признаки подразделяются на три категории: признаки, связанные с запутыванием URL; признаки, основанные на сторонних сервисах; и признаки, основанные на гиперссылках.

Предложенный метод демонстрирует высокую точность и скорость обнаружения, что делает его перспективным решением для борьбы с фишинговыми атаками.

В результате проведённого обзора можно сделать вывод, что проблема фишинга остаётся одной из наиболее актуальных и опасных киберугроз. Традиционные подходы, основанные на чёрных списках и эвристиках, всё ещё востребованы, однако они сталкиваются с рядом ограничений, таких как необходимость регулярного обновления и низкая эффективность против новых видов атак.

Современные методы, основанные на машинном обучении и искусственном интеллекте, демонстрируют значительные перспективы в борьбе с фишингом. Они позволяют автоматизировать процессы обнаружения и классификации фишинговых ресурсов, обеспечивая высокую точность и скорость реакции. Использование глубоких нейронных сетей, ансамблевых методов и других инновационных подходов открывает возможности для создания более адаптивных и эффективных систем защиты.

Одним из ключевых направлений развития является интеграция различных методов и технологий, таких как нейронные сети, веб-краулинг и анализ больших данных. Гибридные подходы, комбинирующие разные алгоритмы, позволяют достичь наилучшего результата, повышая точность и снижая количество ложных срабатываний.

Дальнейшее развитие методов обнаружения фишинга должно идти в направлении увеличения скорости и точности, а также улучшения адаптивности к новым видам атак. Важным аспектом является также обеспечение совместимости и интеграции этих методов с существующими системами информационной безопасности, что позволит создать комплексную защиту от фишинговых угроз.

Таким образом, представленные в обзоре исследования свидетельствуют о значительном прогрессе в области борьбы с фишингом, однако дальнейшее развитие и внедрение новых технологий остаются необходимыми для обеспечения безопасности пользователей и организаций в условиях постоянно меняющегося ландшафта киберугроз.

Список литературы

1. Матюков Е. А. Модель обнаружения фишинговых атак на основе гибридного подхода для защиты автоматизированных систем управления производством / Е. А. Матюков, А. В. Затонский // Вестник ЮУрГУ. 2020. № 2. С. 56–66.

2. Мартынюк Р. А. Механизм распознавания фишинговых сайтов по косвенным признакам / Р. А. Мартынюк, И. А. Кононыхин, Ф. В. Ежов и др.

// Молодой учёный. 2020. № 28 (318). С. 19–22.

3. Dawabsheh A. An Enhanced Phishing Detection Tool using Deep Learning from URL / A. Dawabsheh, A. Eleyan // International Conference on Smart Applications, Communications and Networking (SmartNets). 2022.

4. Nathezhtha T. International Carnahan Conference on Security Technology (ICCST) / T. Nathezhtha, D. Sangeetha, V. Vaidehi // Web Crawling based Phishing Attack Detection (WC-PAD).

5. Asani E. O. Detection of Phishing Emails using Support Vector Classifier and Gaussian Latent Variable Model / E. O. Asani, V. O. Adedayo-Ajayi, A. E. Tunbosun et al. // International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG).

6. Murshid M. StackedPhish: a Stacked Ensemble Framework for Identification of Phishing Website / M. Murshid, M. N. Uddin, F. Hossain // 9th International Women in Engineering Conference on Electrical and Computer Engineering (WIECON-ECE).

Прикладная математика, математическое моделирование

УДК 510.644.4

ПРОГНОЗИРОВАНИЕ СТОИМОСТИ АКЦИЙ С ПОМОЩЬЮ ВРЕМЕННЫХ РЯДОВ

Т. Н. Антонова[1]
Научный руководитель А. В. Кошелева[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

В настоящее время фондовый рынок переживает кризис, обусловленный нестабильностью финансовой системы и геополитическими факторами. В этих условиях привлечение инвестиций становится особенно важным, однако инвесторы всё чаще сталкиваются с убытками [1]. Для обеспечения стабильного дохода и своевременного вывода средств необходима грамотно выстроенная инвестиционная стратегия, основанная на тщательном анализе [2], что определяет актуальность данной работы.

Цель исследования – разработка подхода к построению системы поддержки принятия решений на фондовом рынке с использованием методов нечёткой логики. Прогнозирование цен акций позволяет инвесторам оценивать будущие тренды и снижать риски, особенно в условиях рыночной волатильности и множества влияющих факторов [3].

В качестве объекта анализа выбрана компания Apple, обладающая устойчивым финансовым положением, высокой капитализацией и сильным брендом. Например, в 2024 г. её акции выросли на 35 % благодаря внедрению инноваций, включая технологии искусственного интеллекта [4]. Методы нечёткой логики эффективны в прогнозировании акций, поскольку позволяют учитывать размытые и неопределённые данные, обеспечивая более гибкий и адаптивный анализ [5]. Объектом исследования является стоимость акций Apple, а именно цена закрытия за период с 04.01 по 30.06.2021 по неделям. Данные взяты с официального сайта холдинга «Финам». Прогнозируется не сама цена акций на следующей неделе, а изменение их стоимости. Таким образом, из исходных данных получается новый временной ряд T из 25 значений.

Сначала найдём разность между ценой закрытия акций недели и ценой закрытия за предыдущую неделю и составим выборку. После зададим универсальное множество U, которое покрывает все данные в выборке: $U = [–18; 18]$. Далее универсальное множество разделим на девять равных интервалов: $A_1 = [–18; –14]$, $A_2 = [–14; –10]$, $A_3 = [–10; –6]$, $A_4 = [–6; –2]$, $A_5 = [–2; 2]$, $A_6 = [2; 6]$, $A_7 = [6; 10]$, $A_8 = [10; 14]$, $A_9 = [14; 18]$, каждый из которых соответствует определённому лингвистическому терму: очень

© Антонова Т. Н., 2025

сильное падение цены, сильное падение, падение, слабое падение, слабое изменение, слабый рост, рост, сильный рост и очень сильный рост цены закрытия.

После этого сформируем последовательность отношений следования на следующую неделю: $A_i \rightarrow A_j$. Для построения этой последовательности будем попарно сравнивать последовательные фаззифицированные данные. Например, если значение изменения стоимости акций за 5-ю неделю попадает в интервал A_4, а на следующей неделе значение попадает в интервал A_6, то формируем нечёткое отношение $A_4 \rightarrow A_6$. Отношения, полученные таким образом, образуют группы, в которые входят все отношения с одинаковыми левыми частями. Например, $A_1 \rightarrow A_4$, $A_1 \rightarrow A_5$, $A_1 \rightarrow A_6$ образуют группу $A_1 \rightarrow A_4, A_5, A_6$.

Экономический смысл этих групп таков: группы отображают те возможные изменения стоимости акций, которые могут последовать после определённого изменения. Например, группа $A_1 \rightarrow A_4, A_5, A_6$ показывает, что после очень сильного падения возможны слабое падение, слабое изменение или слабый рост цены акций. Из полученных групп сформируем нечёткие отношения R_i по правилу: $R_i = A_i^T \times A_j$, где A_j – терм, следующий за A_i. Например, для группы $A_1 \rightarrow A_4, A_5, A_6$ получается отношение $R_1 = \left(A_1^T \times A_4\right) \cup \left(A_1^T \times A_5\right) \cup \left(A_1^T \times A_6\right)$.

На основе отношений R_i, $i = 1, \ldots, 9$ сформируем матрицу отношений $R_{9\times9}$, в которой каждый элемент r_{ij} отражает нашу экспертную оценку возможного движения тренда акций *Apple* в выбранный период времени с учётом экономического анализа акций данной компании и современного рынка акций в целом.

Получим матрицу со следующими строками:

[0,2; 0,35; 0,5; 0,65; 1; 0,8; 0,5; 0,2; 0], [0,45; 0,5; 0,65; 0,8; 1; 0,6; 0,4; 0,2; 0,1], …,
[0,1; 0,2; 0,4; 0,6; 1; 0,8; 0,65; 0,5; 0,45], [0; 0,2; 0,5; 0,8; 1; 0,65; 0,5; 0,35; 0,2].

Далее произведём фаззификацию исходных данных, т. е. переведём обычные числа (изменение цены акций) в нечёткие числа с помощью функции принадлежности, отражающей нашу оценку степени принадлежности изменения цены каждому из девяти интервалов A_i.

Степень принадлежности μ некоторого значения x_t интервалу A_j зададим по формуле

$$\mu_j\left(x_t\right) = \frac{1}{1 + k\left(x_t - u_j\right)^2},$$

где x_t – фактическое значение временного ряда T в момент времени t; u_j – середина интервала A_j; $k > 0$ – постоянная, задаваемая экспертом (исследователем), и чем k больше, тем оценка экспертом степени принадлежности интервалу меньше. Для нашей задачи мы выбрали $k = 1$.

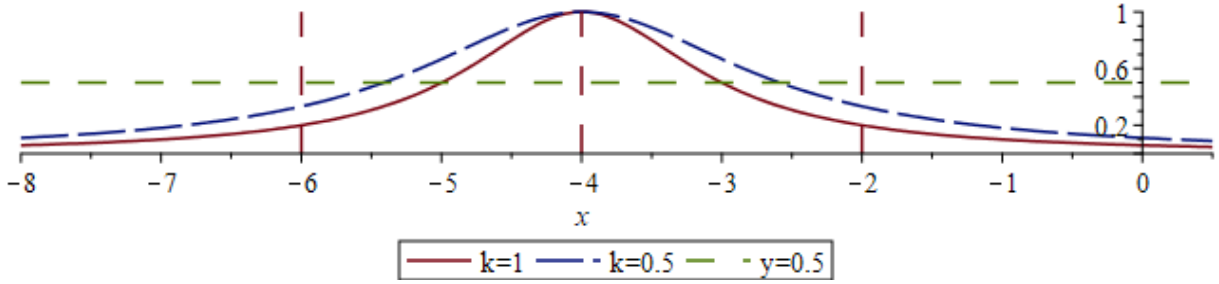


Рисунок 1. Графики функции принадлежности при различных k

Из полученных значений формируем матрицу M, каждая строка которой отражает то, в какой степени соответствующее этой строке значение временного ряда T принадлежит одному из термов A_i, которые расположены в столбцах:

$$M = \begin{pmatrix} \mu_1(x_1) = 0,008 & \cdots & \mu_9(x_1) = 0,0023 \\ \vdots & \ddots & \vdots \\ \mu_1(x_{25}) = 0,0019 & \cdots & \mu_9(x_{25}) = 0,011 \end{pmatrix}.$$

После прогнозное значение изменения цены y_{t+1} находим следующим образом: с помощью max-prod-композиции вычисляем каждое значение матрицы $V = MR$, а затем производим дефаззификацию $x_i = \sum_{j=1}^{9} 0,5 v_{ij} u_j$, где u_j – середина интервала A_j. Находим прогнозные значения стоимости акций: $y_{t+1} = y_t + x_i$, где y_{t+1} – прогнозное значение стоимости акций в момент времени $t + 1$; y_t – реальные данные в момент t; x_t – прогнозные значения изменения стоимости акций.

Построим два графика: реальный и прогнозный.

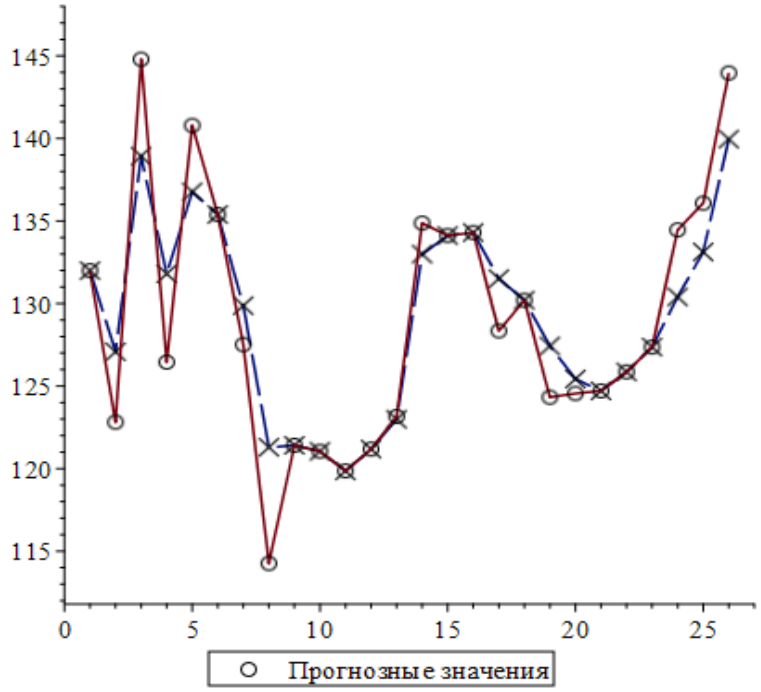


Рисунок 2. Прогнозный и реальный графики тренда акций

На данном этапе считаем результат удовлетворительным. В дальнейшем планируется развивать эту модель, учитывая влияние новостей на тренд и таким образом предсказывая аномалии фондового рынка.

Список литературы

1. Петров М. В. Влияние геополитической напряжённости на международное движение капитала / М. В. Петров // Финансовый журнал. 2024. № 3.

2. Cao G. The Effect of Exit Strategy on Optimal Portfolio Selection with Birandom Returns / G. Cao, D. Shan // Journal of Applied Mathematics. 2013. No. 1.

3. Клебанов Д. А. Прогнозирование цен акций с помощью нейронных сетей: дисс. канд. экон. наук / Д. А. Клебанов. URL: libeldoc.bsuir.by/ bitstream/123456789/52737/1/Klebanov_Prognozirovanie.pdf.

4. Прогноз акций Apple: возвращение на вершину. URL: dzengi.com/ ru/prognoz-akcij-apple-vozvrashchenie-na-vershinu.

5. Конышева Л. К. Основы теории нечётких множеств / Л. К. Конышева, Д. М. Назаров. СПб.: Питер, 2011. – 192 с.

УДК 004.8

РАЗРАБОТКА ДАШБОРДА АКТИВНОСТИ ПРЕПОДАВАТЕЛЯ В ЭЛЕКТРОННОЙ СРЕДЕ

Е. А. Батуро[1]
Научный руководитель Р. В. Есин[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

В условиях активного развития современного образования возрастает потребность в инструментах, позволяющих анализировать и визуализировать данные о деятельности преподавателей в электронной среде [1]. В данной статье рассматривается разработка дашборда для анализа и визуализации метрики зависимости между активностью студентов и преподавателя в ЭОК на основе данных цифрового следа в системе управления обучением.

Для эффективной организации учебного процесса вузы и школы нуждаются в системах управления, которые смогут надёжно и гибко использоваться не только в дистанционном, но и в смешанном обучении. Дистанционным управлением обучения занимаются LMS-платформы. Одной из систем LMS является система LMS Moodle.

Графическое представление информации об активности пользователей в системах управления обучением, таких как LMS Moodle, является критически

© Батуро Е. А., 2025

важным инструментом для анализа и оценки образовательного процесса [2]. Визуализация данных цифрового следа преподавателей в LMS Moodle позволяет наглядно отслеживать их вовлечённость в учебный процесс. В отличие от табличных отчётов, дашборд с графиками не только наглядно отображает периоды сниженной активности, неравномерность нагрузки и корреляцию между действиями преподавателя и студентов, но и работает гораздо быстрее. Табличные данные требуют ручной обработки – фильтрации, сортировки и вычислений, что замедляет анализ.

Целью данной работы является разработка дашборда, который будет осуществлять визуализацию показателей активности преподавателя в ЭОК на основе данных цифрового следа.

Plotly Dash – это фреймворк Python. Он сочетает в себе простоту и универсальность Python с гибкостью и интерактивностью современных веб-технологий, таких как HTML, CSS и JavaScript [3].

С помощью Plotly Dash можно создавать пользовательские панели мониторинга, которые обеспечивают обновления в режиме реального времени, интерактивную визуализацию и бесшовную интеграцию с различными источниками данных.

Эти возможности особенно полезны при работе с цифровым следом пользователей. В статье рассматриваются данные студентов и преподавателей курса СФУ «Анализ временных рядов» за 2023/24 уч. г. Цифровой след содержит 11 172 записи, охватывающие различные виды учебной активности: входы в систему, просмотры материалов, выполнение заданий и другие взаимодействия с образовательной платформой. В анализируемой выборке участвовали 53 студента. Лекционные и практические занятия вёл один преподаватель.

Основными источниками цифрового следа в LMS Moodle являются журнал оценок и журнал событий, содержащий информацию обо всех действиях обучающегося в электронном курсе. Цифровой след формируется автоматически в процессе использования цифровых инструментов.

Каждая запись в логах содержит следующие ключевые атрибуты: «Время», «Полное имя пользователя», «Затронутый пользователь», «Контекст события», «Компонент», «Название события», «Описание», «Источник», «IP-адрес».

Исследования проводились на основе данных системы электронного обучения «еКурсы», реализованной на платформе LMS Moodle.

При анализе цифрового следа в системе LMS Moodle особое значение приобретает исследование взаимосвязи между активностью участников образовательного процесса. Зависимость позволяет выявлять эффективные педагогические практики, такие как своевременная публикация учебных материалов и использование обратной связи. Эффективность этих практик подтверждается тем, что они напрямую влияют на вовлечённость студентов, стимулируя их к более частому взаимодействию с курсом. Для наглядности был разработан дашборд сравнения активности студентов и

преподавателя по неделям. Линейный график сравнивает вовлечённость студентов курса с работой преподавателя.

Рисунок 1. Линейный график зависимости
между активностью студентов и преподавателя в курсе «Анализ временных рядов»

Самое большое количество событий преподаватель проявлял на 11-й неделе, а студенты – на 16-й. На 11-й неделе наблюдается значительное увеличение активности преподавателя, в то время как активность студентов также растёт, но не так резко. Периоды высокой активности преподавателя не всегда совпадают с периодами высокой активности студентов. Для подтверждения статистической значимости выявленной взаимосвязи между активностью преподавателя и студентов была проведена проверка гипотез. Нулевая гипотеза H_0 предполагала отсутствие линейной корреляции, тогда как альтернативная гипотеза H_1 утверждала, что корреляция существует. Для проверки использовался t-критерий для коэффициента корреляции Пирсона. Коэффициент корреляции Пирсона между активностью преподавателя и студентов равен 0,67, что говорит об умеренной прямой линейной зависимости. Рассчитанное значение t-статистики составило $t = 3{,}12$ при числе степеней свободы $df = 16$. Сравнение с критическим значением t-критерия для уровня значимости $\alpha = 0{,}05$ ($t\_crit \approx 2{,}12$) показало, что $|t| > t\_crit$ ($3{,}12 > 2{,}145$), что позволило отвергнуть нулевую гипотезу. Это означает, что коэффициент корреляции 0,67 является статистически значимым и связь между активностью преподавателя и студентов не может быть объяснена случайными колебаниями данных.

Таким образом, результаты анализа выявили умеренную статистически значимую корреляцию между активностью студентов и преподавателя. Это свидетельствует о важности педагогических практик, стимулирующих взаимодействие в цифровой образовательной среде, и позволяет сделать вывод о том, что повышение активности преподавателя способствует росту активности студентов.

В рамках данного проекта было разработано приложение для исследования зависимости между активностью студентов и преподавателя в ЭОК, которое предоставляет возможность сравнивать показатели между

различными преподавателями в различных курсах в электронной среде на основе цифрового следа.

В данной работе была исследована метрика активности преподавателей по данным цифрового следа в системе управления обучением. На основе этой метрики был разработан дашборд, который визуализирует показатели активности преподавателей, позволяя легко отслеживать их вовлечённость и динамику работы. В процессе исследования были выявлены ключевые параметры, такие как частота взаимодействия с курсом, распределение активности по неделям и корреляция между активностью студентов и преподавателя, которые могут использоваться для оценки активности преподавателей и их вовлечённости в учебный процесс.

Список литературы

1. Днепровская Н. В. Понятийные основы концепции смарт-образования / Н. В. Днепровская, Е. А. Янковская, И. В. Шевцова // Открытое образование. 2015. № 6. С. 43–51.

2. Дырдина Е. В. Информационно-коммуникационные технологии в компетентностно-ориентированном образовании: учеб.-метод. пособие / Е. В. Дырдина, В. В. Запорожко, А. В. Кирьякова. Оренбург: Университет, 2012. С. 227.

3. Dabbas E. Interactive Dashboards and Data Apps with Plotly and Dash / E. Dabbas. Birmingham, UK, 2021.

УДК 519.233.5

КОРРЕЛЯЦИОННЫЙ АНАЛИЗ ОЦЕНОК ПО МАТЕМАТИЧЕСКИМ ДИСЦИПЛИНАМ В ВУЗЕ

А. И. Боков[1]
Научный руководитель Т. А. Кустицкая[1]
Кандидат физико-математических наук, доцент
[1]*Сибирский федеральный университет*

Прогнозирование успешности обучения связано со многими факторами, которые требуют отдельного изучения. Данными исследованиями занимается учебная аналитика (learning analytics) – относительно новое междисциплинарное научное направление, находящееся на пересечении педагогики, информатики и психологии [1]. Прогнозирование успешности и поведения студентов в процессе обучения достигается путём создания «модели студента», представляющей собой набор информации о характеристиках студента, таких как текущие знания, результаты по различным дисциплинам и т. д. Студенты различаются значениями характеристик,

© Боков А. И., 2025

и способность методов эффективно оценивать и прогнозировать поведение студента по индивидуальным различиям может поспособствовать улучшению качества обучения студентов [2]. Одним из способов обнаружения связей между различными характеристиками и выявления целесообразности использования различных переменных в задачах прогнозирования является корреляционный анализ.

Корреляционный анализ – это проверка гипотез о связях между переменными с использованием коэффициентов корреляции. Одним из простейших методов корреляционного анализа является проверка гипотезы значимости коэффициентов парной корреляции с помощью *t*-критерия Стьюдента:

$$t = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}};\ H_0 = \{r(X,Y) = 0\};\ H_1 = \{r(X,Y) \neq 0\}, \qquad (1)$$

где $r(X,Y)$ – коэффициент парной корреляции между характеристиками X и Y; n – объём выборки (соответственно, (n – 2) равно числу степеней свободы); H_0 – нулевая гипотеза – коэффициент корреляции равен нулю (незначим); H_1 – альтернативная гипотеза – коэффициент корреляции не равен нулю (значим).

H_0 отвергается в пользу H_1 при получении значения $|t|$, превышающего критическое значение, определяемое по таблице распределения Стьюдента при заданных степенях свободы и уровне значимости α. Принятие H_1 говорит о том, что между переменными X и Y присутствует линейная связь.

Целью данной работы является определение наличия взаимосвязей между результатами по уже пройденным студентами математическим дисциплинам и их успехами по теории вероятностей (4-й семестр обучения), а также по математической статистике (5-й семестр). Выявление данных связей и последующее создание модели предсказания успешности (с помощью методов машинного обучения) может помочь заранее выявить неуспевающих студентов, а также указать на наиболее и наименее важные аспекты образовательной программы с целью корректировки курсов.

Работа в рамках исследования производилась на языке *Python*. Из системы электронных курсов СФУ была выгружена таблица, содержащая данные о студентах Института космических и информационных технологий (ИКИТ) с оценками по различным предметам. Из неё были выбраны записи с оценками по математическим дисциплинам до 4-го семестра включительно, в т. ч. оценки по пересдачам. Отобранные дисциплины: алгебра, аналитическая геометрия, дискретная математика, математическая логика и теория алгоритмов, математический анализ и др. Также были предоставлены таблицы с итоговыми баллами и с результатами входного тестирования по курсам «Теория вероятностей (ПМ)» и «Теория вероятностей и математическая статистика» (для студентов направлений обучения «Прикладная математика» и «Информационная безопасность»). В них содержатся баллы по каждому из пяти вопросов теста, дата прохождения

и затраченное время (отдельно для каждой из двух попыток, которые мог совершить студент). Данные из полученных таблиц были объединены в один датасет по принципу «1 студент = 1 запись» – оценки по различным предметам разделялись по семестрам и сохранялись в отдельные столбцы. Таким образом, получился набор данных более чем на 500 строк (рис. 1).

	КодСтудента	Отдел	Год поступления	Учреждение (организация)	Итоговая оценка за курс (Значение)	ОЦЕНКА: ТВ	ОЦЕНКА: МС	Оценка_Алгебра_Экзамен_1
0	263507	КИ15-01	2015	ИКИТ	31.0	Нет оценки	Отл	Нет оценки
1	263508	ИС18-01Б	2018	ИППС	1.0	Н/я	Нет оценки	Нет оценки
2	263509	КИ15-01	2015	ИКИТ	26.5	Нет оценки	Отл	Нет оценки
3	263761	КИ15-01	2015	ИКИТ	20.0	Нет оценки	Хор	Нет оценки
4	263773	КИ16-18Б	2016	ИКИТ	30.0	Нет оценки	Нет оценки	Нет оценки
...	...	...	...	...	...	...	...	...

509 rows × 68 columns

Рисунок 1. Выдержка из получившейся таблицы данных

Далее качественные переменные переводились в численные. Т. к. кодирование оценки может дать различные результаты при анализе и предсказании, оно производится разными способами: первый – оценки переводятся в шкалу от 0 до 5 (в т. ч. «неявка» = 1, «незачёт» = 2, «зачёт» = 5); второй – разделение по принципу положительная/отрицательная оценка (оценки «5», «4», «3» и «зачёт» переводились в 1, остальное – в 0).

На следующем этапе были вычислены коэффициенты корреляции Пирсона между различными переменными, проверены гипотезы о значимости коэффициентов корреляции согласно (1) (уровень значимости α брался равным 0,05). Также исследовалась мультиколлинеарность с помощью коэффициента инфляции дисперсии (*VIF*-статистика). В итоге получилось, что какие-то коэффициенты корреляции были названы значимыми, а какие-то – нет в зависимости от способа кодирования оценок (например, оценки по алгебре за разные семестры). Однако какие-то коэффициенты значимы всегда (итоговый балл, оценка по математической логике, 5-й вопрос теста и т. д.), а какие-то – никогда не значимы (год поступления, 1-й вопрос теста и т. д.) (рис. 2).

	Переменная	Коэф. корр, кодирование 0-5, ТВ	Значимость, кодирование 0-5, ТВ	Коэф. корр, кодирование 0-5, МС	Значимость, кодирование 0-5, МС	Коэф. корр, кодирование 0-1, ТВ	Значимость, кодирование 0-1, ТВ	Коэф. корр, кодирование 0-1, МС	Значимость, кодирование 0-1, МС
1	Год поступления	0.042711	0.0	-0.015723	0.0	0.042711	0.0	-0.015723	0.0
2	Итоговая оценка за курс (Значение)	0.592211	1.0	0.530033	1.0	0.592211	1.0	0.530033	1.0
5	Оценка_Алгебра_Экзамен_1	0.166081	1.0	0.066041	0.0	0.170242	1.0	0.082011	1.0
8	Оценка_Алгебра_Экзамен_2	0.228908	1.0	0.037500	0.0	0.171050	1.0	0.043088	0.0
11	Оценка_Алгебра_Экзамен_3	0.074110	0.0	0.205175	1.0	0.090644	1.0	0.205200	1.0
23	Оценка_МатЛогика_Экзамен	0.482914	1.0	0.256549	1.0	0.423353	1.0	0.263275	1.0
52	1 попытка: В. 1 /12,5	0.047870	0.0	0.081143	0.0	0.047870	0.0	0.081143	0.0
56	1 попытка: В. 5 /25,0	0.187987	1.0	0.143617	1.0	0.187987	1.0	0.143617	1.0

Рисунок 2. Коэффициенты корреляции некоторых переменных с оценками по теории вероятностей и математической статистике и их значимость

Корреляция может наблюдаться или не наблюдаться в зависимости от способа представления данных (разных способов кодирования). Тем не менее некоторые дисциплины и прочие предикторы могут оказывать существенно большее влияние на исследуемое явление, чем другие. Переменные, для которых выявлена статистически значимая зависимость корреляций с оценками по теории вероятностей и математической статистике, будут далее использованы в качестве предикторов в задаче прогнозирования успешности обучения.

Список литературы

1. Кустицкая Т. А. Развитие учебной аналитики в России / Т. А. Кустицкая, М. В. Носков // Информатизация образования и методика электронного обучения: цифровые технологии в образовании: матер. 5-й междунар. НК. Красноярск, 2021. Ч. 1. С. 273–278.

2. Белоножко П. П. Анализ образовательных данных: направления и перспективы применения / П. П. Белоножко, А. П. Карпенко // Науковедение, 2017. Т. 9. № 4. С. 57.

УДК 550.383.7

РАСЧЁТ МАГНИТНОГО ПОЛЯ ЗЕМЛИ ДЛЯ КРУГОВЫХ ОРБИТ

М. А. Ивлев[1]

Научный руководитель К. А. Кириллов[1, 2]

Доктор физико-математических наук, профессор

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

Магнитное поле Земли (МПЗ) играет ключевую роль в функционировании систем ориентации и стабилизации космических аппаратов (КА). Точные модели магнитного поля позволяют разрабатывать и отлаживать алгоритмы ориентации, а также повышать точность управления движением КА на орбитах различной высоты и наклонения. Актуальность исследования обусловлена необходимостью учёта изменчивости МПЗ, вызванной его вековым ходом и динамическими процессами во внутреннем ядре планеты.

Аналитическое представление МПЗ является наиболее удобным для исследования систем магнитной ориентации. Оно базируется на теории разложения магнитного потенциала Земли в ряд по сферическим гармоникам, что обеспечивает высокую точность моделирования на основе опубликованных международных данных, таких как Международный геомагнитный эталон (International Geomagnetic Reference Field, IGRF).

© Ивлев М. А., 2025

Согласно данной теории, компоненты вектора магнитной индукции, представляющего поле в географической системе координат (ГСК), вычисляются по формулам:

$$Bx_{\Gamma} = \frac{1}{r}\frac{\partial U}{\partial \theta} = \sum_{n=1}^{N}\sum_{m=0}^{n}\left[g_n^m \cos(m\lambda) + h_n^m \sin(m\lambda)\right]\frac{\partial P_n^m(\cos\theta)}{\partial\theta}\left(\frac{R_З}{r}\right)^{n+2} \quad (1)$$

;

$$By_{\Gamma} = \frac{1}{r\sin\theta}\frac{\partial U}{\partial \lambda} = \sum_{n=1}^{N}\sum_{m=0}^{n} m\left[g_n^m \sin(m\lambda) - h_n^m \cos(m\lambda)\right]\frac{P_n^m(\cos\theta)}{\sin\theta}\left(\frac{R_З}{r}\right)^{n+2}; \quad (2)$$

$$Bz_{\Gamma} = \frac{\partial U}{\partial r} = -\sum_{n=1}^{N}\sum_{m=0}^{n}(n+1)\left[g_n^m \cos(m\lambda) + h_n^m \sin(m\lambda)\right]P_n^m(\cos\theta)\left(\frac{R_З}{r}\right)^{n+2}, \quad (3)$$

где $R_З$ = 6 371 км – средний радиус Земли; g_n^m, h_n^m – сферические гармонические коэффициенты (сферические гармоники), соответствуют Международному геомагнитному эталону (*IGRF*); n, m – степень и порядок сферических гармоник соответственно; N – наибольшая степень сферических гармоник; (r, λ, θ) – сферические координаты центра масс КА (r – длина радиус-вектора орбиты; λ – географическая долгота; $\theta = \pi/2 - \varphi$, где φ – географическая широта); $P_n^m(\cos\theta)$ – присоединённые функции Лежандра:

$$P_n^m(\cos\theta) = (2n-1)!!\sqrt{\frac{\varepsilon_m}{(n+m)!(n-m)!}}\sin^m\theta\left[\cos^{n-m}\theta - \right.$$
$$-\frac{(n-m)(n-m-1)}{2(2n-1)}\cos^{n-m-2}\theta +$$
$$\left. +\frac{(n-m)(n-m-1)(n-m-2)(n-m-3)}{2\times 4\times(2n-1)(2n-3)}\cos^{n-m-4}\theta - \ldots\right],$$

где $\varepsilon_m = 2$ для $m \geq 1$ и $\varepsilon_0 = 1$.

Значения сферических координат r, λ, θ вычисляются по формулам:

$$r = h + R_З;\ \varphi = \arcsin\left[\sin i \sin(u_0 + \omega_0 t)\right];$$
$$\lambda = \lambda_0 + \lambda' t + \arccos\left[\cos^{-1}\varphi\cos(u_0 + \omega_0 t)\right]\mathrm{sgn}(\sin\varphi)\,\mathrm{sgn}(\cos i) - \omega_З t,$$

где h – высота орбиты, км; i – наклонение орбиты, рад; λ_0 – начальная долгота восходящего узла орбиты, рад; u_0 – начальное значение аргумента широты, рад; ω_0 – орбитальная скорость; λ' – угловая скорость прецессии орбиты; $\omega_З$ – угловая скорость суточного вращения Земли; t – текущее время, определяет

момент расчёта.

Если учитывать сжатие Земли (эллипсоидальную форму Земного шара), то r нужно вычислить по формуле

$$r = \sqrt{h^2 + 2h\sqrt{A^2\cos^2\varphi + B^2\sin^2\varphi} + \left(A^2\cos^2\varphi + B^2\sin^2\varphi\right)^{-1}\left(A^4\cos^2\varphi + B^4\sin^2\varphi\right)},$$

уточнить значения Bx_Γ и Bz_Γ, найденные по (1) и (3), полагая их равными $Bx_\Gamma\cos(\varphi' - \varphi) + Bz_\Gamma\sin(\varphi' - \varphi)$ и $Bz_\Gamma\cos(\varphi' - \varphi) - Bx_\Gamma\sin(\varphi' - \varphi)$ соответственно, где

$$\varphi' = \operatorname{arctg}\left[\left(A^2 + h\sqrt{A^2\cos^2\varphi + B^2\sin^2\varphi}\right)^{-1}\left(B^2 + h\sqrt{A^2\cos^2\varphi + B^2\sin^2\varphi}\right)\operatorname{tg}\varphi\right];$$

A и B – большая и малая полуоси земного эллипсоида вращения, км; а широту φ уточнить, положив $\varphi = \varphi'$.

Приведённая здесь модель рекомендована Международной ассоциацией геомагнетизма и аэрономии и называется Международным геомагнитным полем (*International Geomagnetic Reference Field*, *IGRF*) [1; 2]. Она широко используется в исследовательских и прикладных задачах, связанных с изучением МПЗ.

Создание расчётной модели МПЗ для круговых орбит производилось в системе *MatLab* (версия *R*2020*b*). Модель содержит максимальную степень сферических гармоник $N = 10$ и рассчитывает изменение компонент вектора магнитной индукции Земли во времени в проекциях на оси географической и орбитальной систем координат.

В ГОСТ 25 645.126-85 [3] приведены результаты расчёта компонент вектора магнитной индукции Земли в ГСК для координат $\varphi = 80{,}6°$ и $\lambda = 58°$ на разных высотах. Значения, указанные в ГОСТ, сравним с результатами, полученными с помощью модели, реализованной в системе *MatLab* версии *R*2020*b*.

Таблица 1

Результаты расчёта компонент вектора магнитной индукции Земли

***h*, км**	**Источник**	***Bx*Г, нТл**	***By*Г, нТл**	***Bz*Г, нТл**
100,0	ГОСТ	4 632,7	2 437,6	53 976,7
	MatLab	4 628,5	2 439,4	53 954,0
3 000,0	ГОСТ	2 140,5	–151,6	18 663,8
	MatLab	2 140,2	–151,6	18 663,0
6 385,0	ГОСТ	948,5	–202,8	7 446,5
	MatLab	948,5	–202,7	7 446,5
12 742,4	ГОСТ	301,4	–94,3	2 203,1
	MatLab	301,4	–94,3	2 203,1
40 000,0	ГОСТ	21,9	–9,5	152,0
	MatLab	21,9	–9,5	152,0

Из приведённой таблицы видно, что результаты расчётов, выполненных с

использованием модели *MatLab*, подтверждают её соответствие данным ГОСТ. Максимальные расхождения находятся в пределах допустимых значений и не превышают 0,1 %, что подтверждает высокую точность расчётной модели для анализа МПЗ.

Список литературы

1. Alken P. International Geomagnetic Reference Field: the 13th Generation / P. Alken, E. Thébault, C. D. Beggan et al. 2021. DOI: 10.1186/s40623-020-01288-x.

2. Гвишиани А. Д. Геомагнетизм: от ядра Земли до Солнца / А. Д. Гвишиани, Р. Ю. Лукьянова, А. А. Соловьев. М.: РАН, 2019. 186 с.

3. Поле геомагнитное. Модель поля внутриземных источников: ГОСТ 25 645.126-85, введ. 01.01.1987 / Госстандарт СССР. М.: Издательство стандартов, 1990. 23 с.

УДК 519.6*537.36

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЭЛЕКТРООСМОСА В ЭЛЕКТРОКИНЕТИЧЕСКОМ НАСОСЕ

А. А. Капитонов[1]

Научный руководитель И. И. Рыжков[1]

Доктор физико-математических наук, профессор

[1]*Институт вычислительного моделирования ФИЦ КНЦ СО РАН*

Электрокинетический насос представляет собой устройство, содержащее многоканальную пористую структуру (мембрану) из диэлектрического материала. К входному и выходному торцам этой структуры примыкают электроды, имеющие отверстия для обеспечения входа и выхода протекающей полярной жидкости. Эти электроды создают электрическое поле, под действием которого происходит электроосмотическое перекачивание жидкости.

Движение жидкости становится возможным благодаря возникновению на границе раздела твёрдой и жидкой фаз т. н. двойного электрического слоя (ДЭС), по природе преимущественно химического происхождения (поверхностная ионизация, адсорбция) [1], причём заряд твёрдой фазы неподвижен. Избыток заряда твёрдой фазы вызывает избыток противоположно заряженных ионов (противоионов) в жидкой фазе, в результате чего она становится подвержена влиянию внешнего электрического поля. Толщина ДЭС определяется длиной Дебая [2], зависящей от концентрации ионов и имеющей характерные размеры порядка единиц нанометров (десятков нанометров для сильно разбавленных растворов).

Классическим уравнением для описания электроосмоса является уравнение Гельмгольца – Смолуховского (1), которое связывает скорость

© Капитонов А. А., 2025

электроосмотического движения с дзета-потенциалом – потенциалом, находящимся на некотором удалении от межфазной поверхности [3]:

$$u_{\text{ЭО,ГС}} = -E_{\text{вн}} \frac{\varepsilon\varepsilon_0\zeta}{\mu}, \quad (1)$$

где $u_{\text{ЭО,ГС}}$ – электроосмотическая компонента скорости, м/с; $E_{\text{вн}}$ – напряжённость внешнего электрического поля, В/м; ζ – дзета-потенциал, В; ε – относительная диэлектрическая проницаемость жидкости; ε_0 – электрическая постоянная, Ф/м; μ – динамическая вязкость жидкости, Па×с.

Одним из ограничений применения уравнения (1) является необходимость значительного превышения радиуса поры над длиной Дебая.

Для получения уравнения электроосмоса в тонких порах, для которых радиус $R_{\text{п}}$ (м) сравним с длиной Дебая λ (м) (3), предлагается использовать модель ДЭС Штерна. Для него известно распределение потенциала внутри поры, экспоненциально убывающего от максимального значения на границе слоя Штерна $\Psi_{\text{Ш}}$ (В). Приближённое выражение для потенциала выглядит как (2), и оно достаточно точно при $|\Psi_{\text{Ш}}| < 2R_{\text{г}}T / zF \approx \approx 0{,}05 / z$ (В):

$$\Psi(r) = \Psi_{\text{Ш}} e^{\frac{r+\delta-R_{\text{п}}}{\lambda}}, \quad r \in [0; R_{\text{п}} - \delta]; \quad (2)$$

$$\lambda = \sqrt{\frac{\varepsilon\varepsilon_0 R_{\text{г}} T}{2F^2 z C_0}}, \quad (3)$$

где r – радиальная координата (0 соответствует центру поры), м; δ – толщина слоя Штерна, м; $R_{\text{г}}$ – универсальная газовая постоянная, Дж/(моль×К); T – температура, К; F – постоянная Фарадея, Кл/моль; $z = z_+ = -z_-$ – валентность ионов электролита; C_0 – объёмная плотность концентрации ионов электролита, моль/м^3.

Используя (2) и теорему Гаусса, можно записать уравнение на баланс сил, действующих на цилиндрический элемент жидкости, где сила электрического взаимодействия с внешним полем и сила, вызванная давлением, будут уравновешены силой трения, в результате чего получится дифференциальное уравнение на скорость. Далее, производя интегрирование, можно перейти к осреднённой по радиусу поры скорости $u_{\text{ср}}$ (м/с), которая запишется как (4):

$$u_{\text{ср}} = \frac{(R_{\text{п}} - \delta)^2}{8\mu} \frac{\Delta P}{L} - \frac{E_{\text{вн}} \Psi_{\text{Ш}} \varepsilon\varepsilon_0}{\mu} K(k_\lambda); \quad (4)$$

$$K(k_\lambda) = \left(3k_\lambda^2 - 3k_\lambda + 1 + e^{-\frac{1}{k_\lambda}} \left(-3k_\lambda^2 + \frac{1}{2} \right) \right); \quad (5)$$

$$k_\lambda = \frac{\lambda}{R_\text{п} - \delta}, \qquad (6)$$

где ΔP – разность давления между левым и правым краями, Па; L – длина поры, м; $K(k_\lambda)$ – поправочный коэффициент; k_λ – степень покрытия поры ДЭС.

Член в (4), связанный с давлением, является следствием уравнения Пуазёйля, а при электроосмотическом члене появляется поправочный коэффициент $K(k_\lambda)$. Можно показать, что для k_λ бесконечно малых $K(k_\lambda) = 1$, а для бесконечно больших – $K(k_\lambda) = 0$, при этом первый случай соответствует очень большим (по сравнению с длиной Дебая) радиусам поры, а электроосмотический член в (4) эквивалентен (1). Второй случай соответствует отсутствию изменения потенциала в поре, когда электроосмос не возникает.

Используя $K(k_\lambda)$, можно исследовать зависимость скорости от концентрации ионов (рис.). Она вполне соответствует известному факту [1], что разбавление электролита приводит к снижению эффекта электроосмоса.

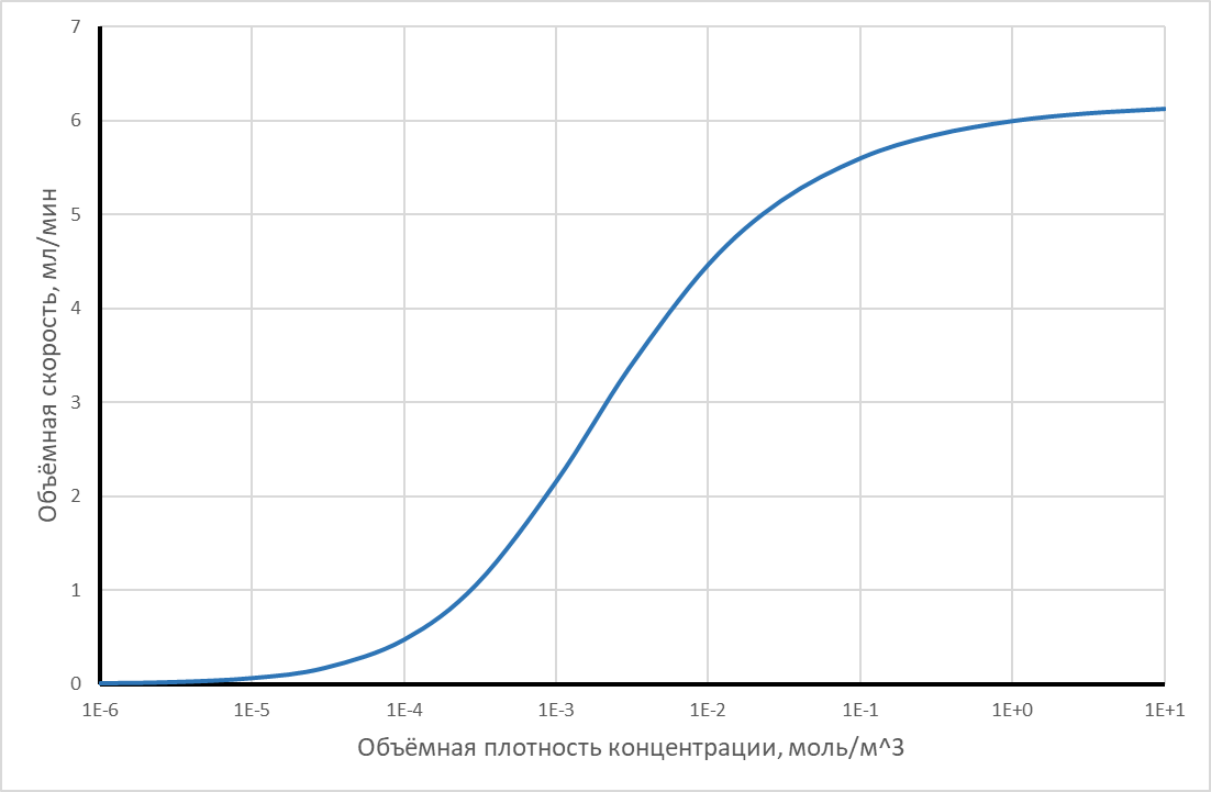


Рисунок 1. Зависимость объёмной скорости от концентрации ионов

Аналогичный график для зависимости от радиуса поры выглядит (качественно) так же. Вместе с тем ожидается, что уменьшение радиуса должно, наоборот, усиливать эффект электроосмоса. Возможное объяснение этого факта заключается в том, что величина $\Psi_\text{Ш}$ является зависимой от радиуса поры (при построении графика она подразумевалась постоянной).

Таким образом, на основе модели ДЭС Штерна было предложено уточнённое уравнение (4)–(6) для электроосмоса.

Список литературы

1. Фридрихсберг Д. А. Курс коллоидной химии: учебник / Д. А. Фридрихсберг. 3-е изд. СПб.: Химия, 1995. 400 с.

2. Schoch R. B. Transport Phenomena in Nanofluidics / R. B. Schoch // Reviews of Modern Physics. 2008. Vol. 80. Pp. 839–883.

3. Брусницына Л. А. Электрокинетические явления / Л. А. Брусницына. 2019. – URL: study.urfu.ru/Aid/Publication/13882/1/Брусницына.pdf.

УДК 004.94

ПРОГНОЗИРОВАНИЕ ДВИЖЕНИЯ КОСМИЧЕСКОГО АППАРАТА МЕТОДОМ ЧИСЛЕННОГО ИНТЕГРИРОВАНИЯ В СРЕДЕ MATLAB

П. Е. Ковалева[1, 2]
Научный руководитель М. И. Медведева[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

[2]*АО «Информационные спутниковые системы» имени академика М. Ф. Решетнёва»*

В условиях сложной динамики космического пространства, где на движение аппарата влияют гравитационные поля небесных тел, сопротивление атмосферы (для низких орбит), солнечное излучение и другие факторы, разработка эффективных методов и инструментов для расчёта траекторий становится критически важной. Цель исследования – разработка эффективного алгоритма и программы расчёта движения и траекторий космического аппарата (КА) для высокоэллиптических и низких круговых орбит.

Актуальность работы обусловлена несколькими факторами: автоматизированные программы позволяют значительно ускорить процесс расчётов и повысить их точность; современные вычислительные мощности и алгоритмы машинного обучения открывают новые возможности для создания более точных и адаптивных систем прогнозирования движения КА. *MatLab* для разработки ПО был выбран по ряду причин: широкий набор встроенных инструментов для математических вычислений, удобство работы с матрицами и векторами, наличие нескольких встроенных методов (*Aerospace Toolbox*, *Simulink*), гибкость и кроссплатформенность, множество инструментов для визуализации данных, что делает процесс расчётов автоматизированным и

© Ковалева П. Е., 2025

воспроизводимым, что важно для задач, требующих многократного моделирования с различными параметрами.

Разработана программа численного интегрирования методом Рунге – Кутта 4-го порядка для проведения вычислений параметров движения КА в гринвичской системе координат. При интегрировании движения КА учитывались: ускорение, обусловленное геопотенциалом; ускорение, вызываемое Луной; ускорение, вызываемое Солнцем; не учитывались: тяга двигателей; ускорение, обусловленное давлением солнечного света; ускорение, обусловленное торможением в атмосфере.

На вход программы подаются: момент даты и времени, начиная с которого происходит интегрирование; необходимое для прогноза число секунд; геоцентрическое положение объекта в инерциальной системе координат; а также скорости объекта в начальный момент времени. Для вычислений внутри всех алгоритмов необходима сквозная нумерация суток, а значит, необходимо выполнить преобразование от календарной даты к модифицированному юлианскому дню.

В пределах Солнечной системы пользуются равномерной шкалой барицентрического динамического времени *TDB*. В этой шкале вычисляются положения Луны, Солнца и параметры прецессии и нутации. Для определения влияния Земли на КА вычисляется геопотенциал. Его расчёт ведётся в земной системе координат, следовательно, выполним преобразования входных координат [1].

Преобразование из небесной (инерциальной) системы координат (ИСК) в земную (гринвичскую) систему координат выполняется по формуле:

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}_{\text{ГВСК}} = R \times N \times P \times \begin{pmatrix} x \\ y \\ z \end{pmatrix}_{\text{ИСК}},$$

где P – матрица прецессии; N – матрица нутации; R – матрица вращения Земли.

Прецессия – явление, при котором ось вращения тела меняет своё направление в пространстве. Нутация – слабое нерегулярное движение вращающегося тела, совершающего прецессию. Причина прецессии и нутации лежит в постоянно изменяющемся гравитационном притяжении Солнца, Луны, а также в малой степени – планет и элементов масс Земли [2].

Рассчитав положения Луны и Солнца, геопотенциал, а также время в необходимой для входа во вложенные функции шкале, можно перейти к интегрированию, которое реализуется классическим одношаговым методом Рунге – Кутта 4-го порядка [3]. Расчёты производятся по следующей формуле:

$$y_{n-1} = y_n + \frac{h}{6} \times \left(k_1 + 2 \times k_2 + 2 \times k_3 + k_4 \right),$$

где $k_1 = f(x_n, y_n);$

$$k_2 = f\left(x_n + \frac{h}{2},\ y_n + \frac{h}{2} \times k_1\right);$$

$$k_3 = f\left(x_n + \frac{h}{2},\ y_n + \frac{h}{2} \times k_2\right);$$

$$k_4 = f(x_n + h,\ y_n + h \times k_3);$$

функция f является суммой ускорений, вызываемых возмущениями, которые описаны выше.

Интегрирование ведётся с постоянным шагом. Время согласно каждому шагу пересчитывается на выполняемом этапе алгоритма.

Результатом проделанной работы является программа, разработанная в среде *MatLab*, позволяющая прогнозировать движение КА на круговой или эллиптической орбите на произвольный интервал времени. Помимо расчётов траекторий движения КА, в программе была реализована функция визуализации полёта КА по орбите, что позволяет увидеть динамически получаемый результат и легко интерпретировать его. Построенные трёхмерные модели орбит КА приведены на рисунках 1 и 2. В первом случае представлен суточный прогноз для круговой орбиты с высотой 1 500 км, наклонением 82,5° и эксцентриситетом 0,001. На рисунке 2 показан суточный прогноз для высокоэллиптической орбиты с эксцентриситетом 0,704, наклонением 63,4°, радиусом апогея 45 275 км и радиусом перигея 7 860 км.

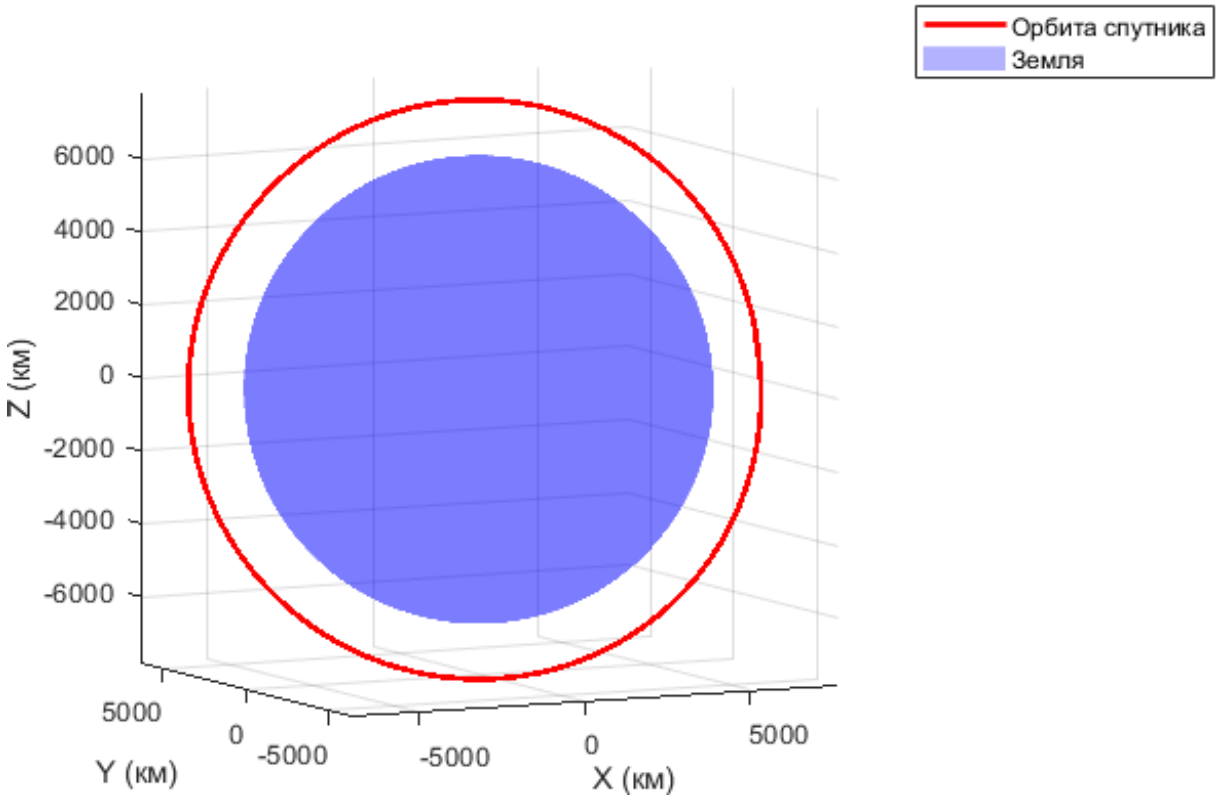


Рисунок 1. Прогноз полёта на круговой орбите

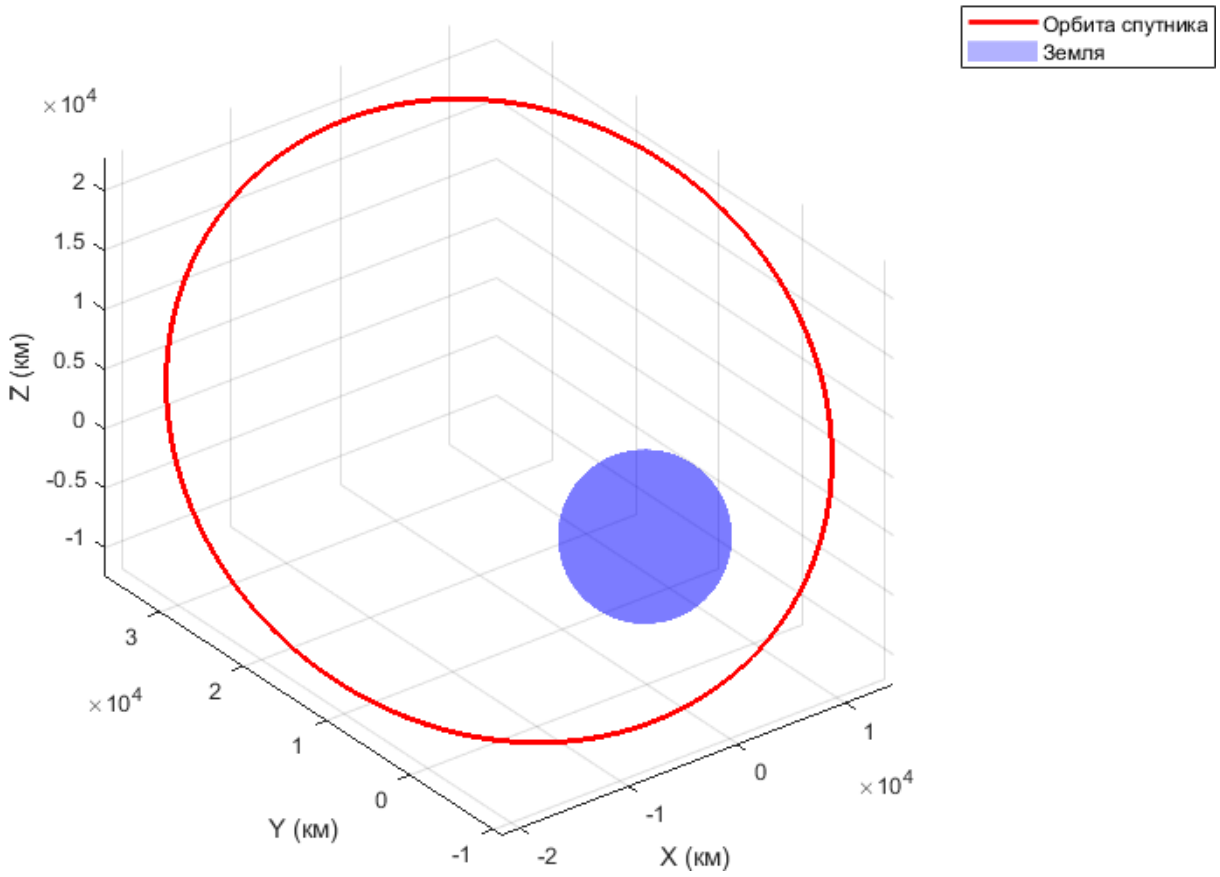


Рисунок 2. Прогноз полёта на высокой эллиптической орбите

Результаты прогнозирования параметров движения КА были сверены с тестовыми примерами, рассчитанными в действующем комплексе для баллистических расчётов, разработанном в АО «Решетнёв». Разница в вычислениях координат КА составила менее 0,001 %. Быстродействие программы зависит от временного периода, на который пользователю требуется прогноз.

Список литературы

1. Бордовицына Т. В. Современные численные методы в задачах небесной механики / Т. В. Бордовицына. М.: Наука, 1984. 136 с.

2. Чеботарев В. Е. Основы проектирования космических аппаратов информационного обеспечения: учеб. пособие / В. Е. Чеботарев, В. Е. Косенко. Красноярск: СибГАУ, 2011. 488 с.

3. Чернявский Г. М. Орбиты спутников связи / Г. М. Чернявский, В. А. Бартенев. М.: Связь, 1978. 240 с.

УДК 519.85

ПРИМЕНЕНИЕ САМОКОНФИГУРИРУЕМОГО ГЕНЕТИЧЕСКОГО ПРОГРАММИРОВАНИЯ ДЛЯ РЕШЕНИЯ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ ПЕРВОГО ПОРЯДКА

М. А. Кошин[1]
Научный руководитель – М. Е. Семенкина[1, 2]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

В настоящее время существуют ситуации, при которых найти аналитически решение дифференциального уравнения не представляется возможным ввиду разных причин. В таких ситуациях уместно использовать численные подходы, особенность которых заключается в нахождении приближённых решений или же различного рода эвристик.

Один из эвристических подходов к решению дифференциальных уравнений – использование эволюционных алгоритмов. Эволюционные алгоритмы – класс стохастических алгоритмов оптимизации, принцип работы которых заключается в моделировании процессов эволюции и естественного отбора [1]. К классу эволюционных алгоритмов относятся генетические алгоритмы, генетическое программирование и дифференциальная эволюция.

Особенностью генетического программирования является подход к представлению решения-кандидата – индивид представляется в виде бинарного дерева, листья которого (терминальное множество) – константы и переменные, остальные узлы (функциональное множество) – операции, проводимые над членами терминального множества [1]. Такой подход позволяет представлять каждое решение в виде функции, программы или прочих подобных представлений в зависимости от того, как поставлена задача и какова конечная цель.

Каждое решение, предложенное в результате работы генетического программирования, как и в прочих эволюционных алгоритмах, оценивается по какому-то критерию – например, в случае задачи регрессии таким критерием может быть среднеквадратичное отклонение между значениями функции-решения и точками, по которым регрессия строится. На рисунке 1 представлено бинарное дерево, взращённое методом генетического программирования.

© Кошин М. А., 2025

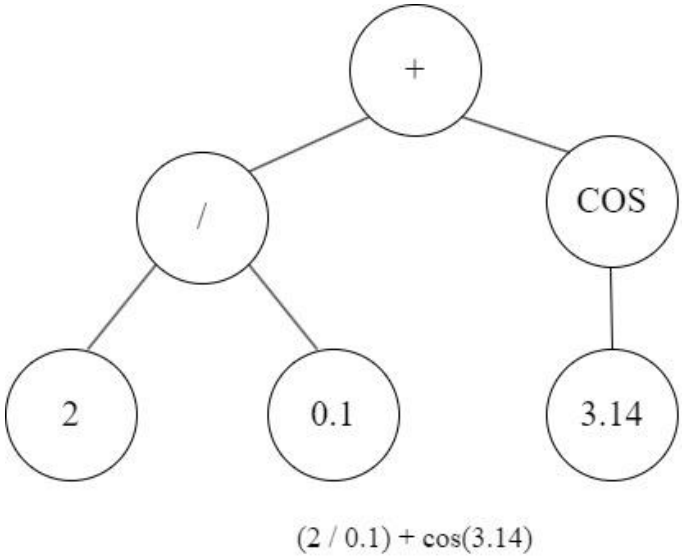


Рисунок 1. Представление индивида в генетическом программировании

В контексте решения дифференциальных уравнений видно, что подобный подход к представлению индивидов позволяет напрямую представить решение дифференциального уравнения – функцию. С одной стороны, дифференциальное уравнение можно представить в виде:

$$y'(x) = f\left(x, y(x)\right).$$

С другой стороны:

$$y' = \frac{y(x+\Delta x) - y(x)}{\Delta x}.$$

Таким образом, каждое решение может оцениваться по следующему критерию (фитнес-функция):

$$Fitness = \left(f\left(x, y(x)\right) - \frac{y(x+\Delta x) - y(x)}{\Delta x} \right)^2 \to \min;$$

$$\frac{1}{1 + Fitness} \to \max.$$

Если задать этот критерий для оценки каждого решения-кандидата, то в результате работы генетического программирования будет находиться множество частных решений. Чтобы решение удовлетворяло заданным начальным условиям, предлагается штрафовать каждое решение по признаку несоответствия начальным условиям.

Предложенный метод можно дополнить различными модификациями: гибридизировать алгоритм с другим эволюционным алгоритмом, реализовать самоадаптацию параметров [2]. В используемом методе генетического

программирования реализована пооператорная самоадаптация и интегрирована модификация дифференциальной эволюции *L-SRTDE* [3].

Тестовые уравнения для проверки работоспособности такого подхода представлены в таблице 1.

Таблица 1

Тестовые дифференциальные уравнения

№	Уравнение
1	$y' = -2 \times y$
2	$y' = -\frac{y \times \ln(y)}{x}$
3	$y' = 2 \times x$

Начальные параметры алгоритма представлены в таблице 2.

Таблица 2

Начальные параметры алгоритма

Параметр	Значение
Число индивидов в поколении	35
Число поколений	25
Глубина дерева	5

Результаты тестирования представлены в таблице 3.

Таблица 3

Результаты тестирования генетического программирования

№ функции	1	2	3
Наименьшее значение фитнес-функции	0,142	0,128	0,023
Наибольшее значение фитнес-функции	0,198	0,211	0,999
Среднее значение фитнес-функции	0,174	0,174	0,843
Тест Шапиро – Уилка	0,96	0,957	0,64

Исходя из полученных результатов, такой подход требует доработки с точки зрения реализации фитнес-функции, а также расширения функционального множества.

Список литературы

1. Koza J. R. Genetic Programming / J. R. Koza. Cambridge, USA: The MIT Press, 1998. 609 p.

2. Семенкина М. Е. Элементы современных методов оптимизации / М. Е. Семенкина. Красноярск: СибГАУ, 2015. 48 с.

3. Stanovov V. Success Rate-based Adaptive Differential Evolution L-SRTDE for CEC 2024 Competition. 1-8 / V. Stanovov, E. Semenkin. 2024.

УДК 004.032.26

НЕЙРОСЕТЕВЫЕ МОДЕЛИ ВРЕМЕННЫХ РЯДОВ ДЛЯ ПРОГНОЗИРОВАНИЯ УРОВНЯ ЗАГРЯЗНЕНИЯ АТМОСФЕРЫ В ГОРОДЕ КРАСНОЯРСКЕ

Н. А. Лев[1]
Научный руководитель Н. Н. Осипов[1]
Доктор физико-математических наук, доцент
Научный руководитель О. С. Володько[1, 2]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Институт вычислительного моделирования ФИЦ КНЦ СО РАН*

Красноярск является одним из нескольких городов России с самым грязным воздухом, концентрация вредных веществ в котором часто превышает допустимые нормы. Возникает необходимость не только в мониторинге, но и в прогнозировании значений концентрации вредных веществ в атмосфере города. В работе представлены результаты прогнозирования величины концентрации твёрдых взвешенных частиц *Particulate Matter* 2.5 (*PM*2.5) в атмосфере Красноярска с помощью моделей рекуррентных нейронных сетей разновидности *Long short-term memory* (*LSTM*), которые являются одними из наиболее эффективных при прогнозировании загрязняющих веществ [1]. Проведено сравнение с ранее построенными моделями временных рядов *ARIMAX*, которые показали лучшее качество прогнозирования по сравнению с другими моделями машинного обучения [2].

Для прогнозирования были взяты данные наземных станций оперативного мониторинга [3] по метеоусловиям (скорость и направление ветра, температура и влажность воздуха, атмосферное давление) и концентрациям твёрдых взвешенных частиц *PM*2.5 в атмосферном воздухе Красноярска за 2019–2024 гг. с промежутком 1 ч.

Модель *LSTM* представляет собой цепочку повторяющихся блоков, каждый из которых состоит из четырёх слоёв, взаимодействующих между собой при помощи следующих механизмов:

– вентиль забывания – определяет, какую долю информации пропускать из внутреннего состояния предыдущего блока;

– вентиль входа – регулирует обновление значений во внутреннем состоянии блока;

– вентиль выхода – контролирует, какая информация передаётся на выход блока;

© Лев Н. А., 2025

– внутреннее состояние – формируется на основе предыдущего внутреннего состояния, выхода предыдущего блока и новой поступающей информации.

Проведено сравнение моделей *LSTM* по периодам усреднения: сутки и часы (табл. 1). Лучшее качество достигается при усреднении до часов.

Таблица 1

Сравнение качества моделей по метрике *MAE*

Временной период	Период усреднения	
	Сутки	Часы
Зима	29,65	10,30
Весна	7,18	5,10
Лето	3,16	2,62
Осень	3,33	3,07

Было проведено сравнение моделей *LSTM* по способу разделения выборки (табл. 2). В одном случае в качестве обучающей выборки использовался срез 1–2 мес. перед периодом прогнозирования. Во втором варианте обучающая выборка разделялась на временные периоды в зависимости от величины концентрации *PM*2.5, приблизительно соответствующие сезонам года [4]. Лучшее качество свойственно сезонной модели.

Таблица 2

Сравнение качества моделей по метрике *MAE*

Временной период	Срез 1–2 мес.	Сезонная модель
Зима	14,04	10,30
Весна	6,81	5,09
Лето	4,01	2,62
Осень	3,46	3,07

Лучшие модели *LSTM* сравнивались с лучшими моделями машинного обучения *ARIMAX*, построенными ранее [2]. Модели *LSTM* демонстрируют существенно лучшее качество на различных временных периодах (табл. 3).

Таблица 3

Сравнение качества моделей *LSTM* и *ARIMAX* по метрике *MAE*

Временной период	*ARIMAX*	*LSTM*
20–22.12.2022	8,34	1,63
20–22.07.2022	2,53	0,35
12–14.08.2022	3,09	1,61
10–12.03.2023	5,43	4,05
10–12.04.2023	3,81	0,72
10–12.05.2023	5,07	0,77
10–12.07.2023	0,29	0,87
23–25.09.2023	4,77	0,84
23–25.10.2023	5,26	0,82
10–12.01.2024	11,83	3,11
10–12.02.2024	13,21	0,93
17–19.03.2024	7,01	0,48

Качественное сравнение прогнозов моделей для одного из тестовых периодов (в данном случае – зимнего) представлено на рисунках 1, 2.

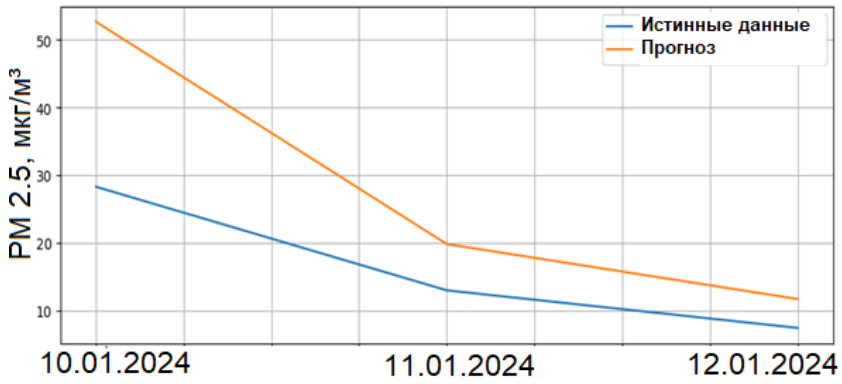


Рисунок 1. Качество прогнозов модели ARIMAX

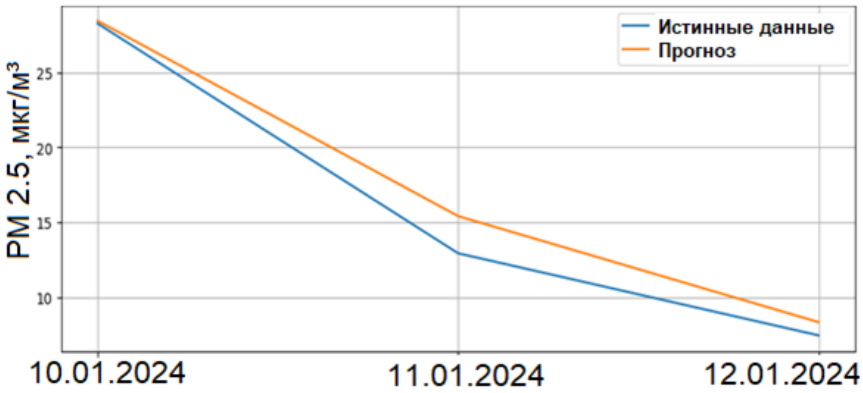


Рисунок 2. Качество прогнозов модели LSTM

Таким образом, сезонные модели класса *LSTM*, обученные на данных за каждый час, справляются с задачей прогнозирования лучше всех ранее исследованных моделей машинного обучения [2] и могут быть использованы для достаточно точного прогноза концентраций *PM*2.5 в атмосфере Красноярска.

Список литературы

1. Das R. High Granular and Short-term Time Series Forecasting of PM2.5 Air Pollutant – a Comparative Review / R. Das, A. I. Middya, S. Roy // Artificial Intelligence Review. 2022. Vol. 55. Pp. 1 253-1 287.

2. Лев Н. А. Прогнозирование величины концентрации загрязняющих веществ в атмосфере г. Красноярска с помощью моделей временных рядов и ансамблевых моделей машинного обучения / Н. А. Лев // Проспект Свободный. 2024. С. 463-466.

3. Геопортал – данные оперативного мониторинга. URL: sensor.krasn.ru/sc.

4. Volodko O. Influences of Meteorological Conditions in PM2.5 Levels in Krasnoyarsk City Atmosphere / O. Volodko, O. Yakubailik, T. Lapo // E3S Web of Conferences. 2023. Vol. 392. P. 02022.

УДК 378, 004.8

ИСПОЛЬЗОВАНИЕ СТУДЕНЧЕСКИХ СТРАТЕГИЙ ОБУЧЕНИЯ В МОДЕЛЯХ ПРОГНОЗИРОВАНИЯ УСПЕШНОСТИ ОБУЧЕНИЯ

П. А. Ошлакова[1]
Научный руководитель Т. А. Кустицкая[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

Развитие цифровых образовательных технологий открыло широкие возможности для анализа поведения студентов на основе данных их цифрового следа [1]. Такие данные позволяют не только выявлять индивидуальные учебные стратегии, но и оценивать их устойчивость во времени, а также использовать эти стратегии как признаки для построения прогностических моделей академической успешности. В настоящем исследовании предпринята попытка соединить два подхода: поведенческую типизацию студентов и машинное предсказание итогов обучения.

Работа основана на данных из LMS Moodle по 13 дисциплинам Сибирского федерального университета, которым обучалось 276 чел. Исследование объединяет методы кластерного анализа и машинного обучения. Показано, что включение студенческих стратегий обучения в прогнозные модели в качестве предикторов улучшает точность прогнозов и повышает информативность полученных результатов.

Анализ цифрового следа студентов включал агрегацию логов взаимодействий с шестью ключевыми компонентами курса (чтение, тесты, тренажёры, задания, клики и форумы) с последующим формированием учебных сессий. Каждая сессия определялась как последовательность действий в электронной среде с интервалом не более 10 мин. Для каждого студента вычислялись характеристики сессий и частота сочетаний компонентов, что позволило сформировать поведенческие профили [2].

С помощью иерархической агломеративной кластеризации были выделены четыре устойчивых кластера студентов, интерпретируемые через призму подходов к обучению по Биггсу [3]:

– кластер 1 – «неактивные» (поверхностный подход);

– кластер 2 – «активизирующиеся к сессии» (стратегический подход с ориентацией на результат);

– кластер 3 – «устающие к сессии» (смешанный или неустойчивый стратегический подход);

– кластер 4 – «стабильно активные» (глубинный подход).

Анализ устойчивости показал, что лишь 25 % студентов сохраняют поведенческую стратегию между семестрами. Особенно неустойчивыми

© Ошлакова П. А., 2025

оказались стратегии поверхностного типа, при этом значительная доля студентов переходила к более активным стратегиям. Это может свидетельствовать об адаптивной природе поведения студентов при изменении условий обучения [4].

Для прогнозных моделей использовались поведенческие данные студентов, сгруппированные по неделям, с бинарной меткой итогового успеха. С целью балансировки классов применялись техники SMOTE и его вариации. Модели обучались с учётом настройки гиперпараметров, отбора признаков и оптимизации порогов классификации.

Обучались и сравнивались разнообразные алгоритмы: логистическая регрессия, деревья решений, случайный лес, нейронные сети, XGBoost и др. На каждом наборе параметров отбирались лучшие модели, которые затем объединялись в ансамбль с «мягким» голосованием, повышающим устойчивость модели к шуму. Анализ динамики метрик по неделям продемонстрировал рост f1-метрики по мере накопления данных, особенно на средних и поздних неделях семестра.

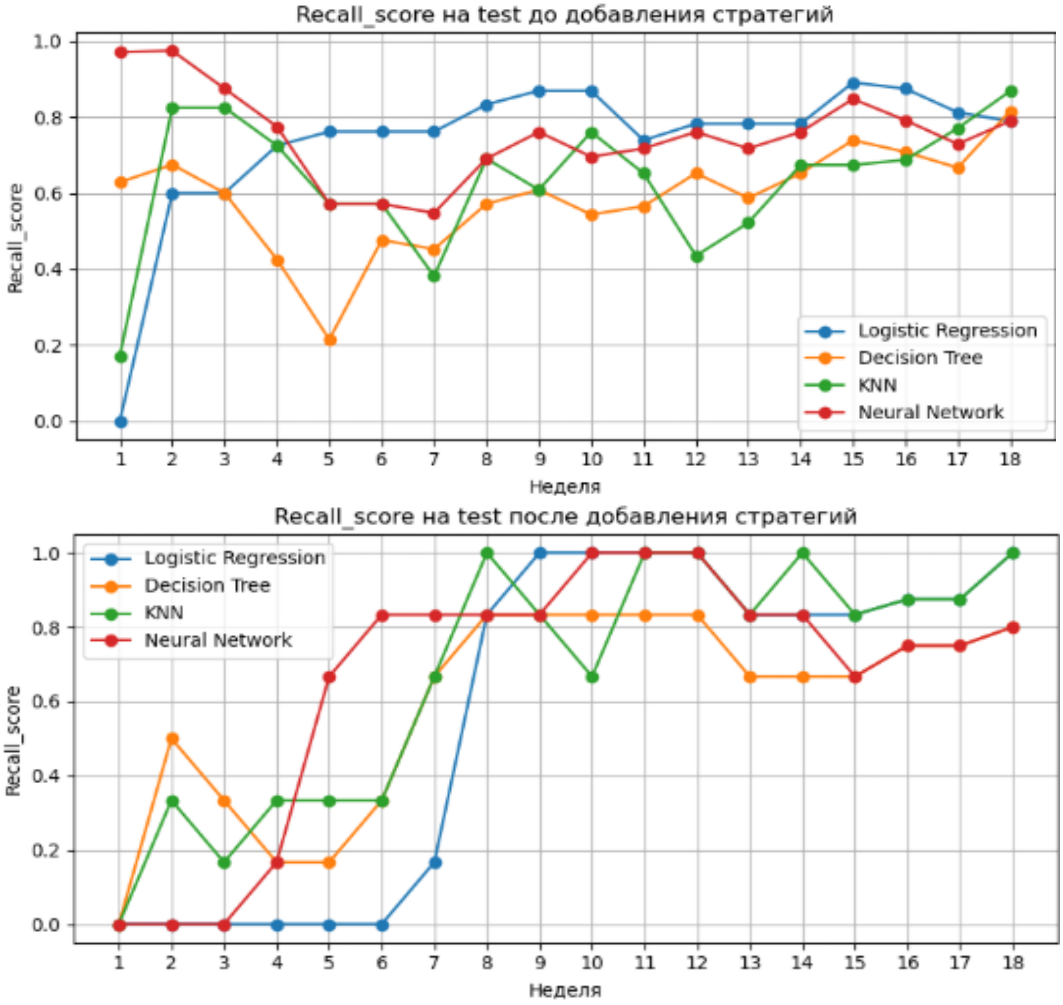


Рисунок 1. Динамики изменения метрики recall моделей
без учёта и с учётом стратегий обучения

Отдельное внимание было уделено оценке вклада стратегий обучения, выделенных на основе данных цифрового следа студентов, в итоговое качество прогностических моделей. Проведённое сравнение с моделями, не содержащими этих признаков, показало улучшение результатов классификации после включения стратегий в качестве предикторов. Особенно выраженное повышение наблюдается по метрике recall, что указывает на более точное выявление студентов, находящихся в зоне академического риска. Это подтверждает, что поведенческие стратегии, помимо своей интерпретируемости в педагогическом контексте, обладают высокой прогностической ценностью и целесообразны для использования в задачах образовательной аналитики.

Объединение анализа стратегий обучения с методами машинного обучения позволяет комплексно подойти к проблеме поддержки академической успешности студентов. Устойчивые стратегии, выявленные на основании поведенческих данных, не только служат индикатором типа учебной мотивации, но и могут быть использованы как информативные признаки в прогностических моделях.

В работе представлена комплексная методология анализа цифрового следа студентов: от типологизации учебных стратегий и оценки их устойчивости до построения эффективных моделей предсказания академической успешности. Показано, что стратегии обучения оказывают положительное влияние на качество обученных моделей.

Разработанный подход может быть использован в системах образовательной аналитики для повышения качества индивидуализации образовательного процесса и своевременного вмешательства в учебные траектории студентов, испытывающих трудности в обучении.

Список литературы

1. Gasevic D. Detecting Learning Strategies with Analytics: Links with Self-reported Measures and Academic Performance / D. Gasevic, J. Jovanovic, A. Pardo et al. // Journal of Learning Analytics. 2017. No. 4 (2). Pp. 113-128.

2. Кустицкая Т. А. Выявление стратегий обучения с помощью цифрового следа в LMS Moodle / Т. А. Кустицкая, П. А. Ошлакова // Преподаватель XXI в. 2024. № 3. Ч. 1. С. 82-98. DOI: 10.31862/2073-9613-2024-3-82-98.

3. Biggs J. B. Student Approaches to Learning and Studying / J. B. Biggs. New York, USA: Hawthorn, 1987.

4. Saqr M. Transferring Effective Learning Strategies across Learning Contexts Matters: a Study in Problem-based Learning / M. Saqr, W. Matcha, N. Ahmad Uzir et al. // Australasian Journal of Educational Technology. 2023. Vol. 39 (3). Pp. 35–57.

УДК 004.032.26

ПРОГНОСТИЧЕСКАЯ МОДЕЛЬ ЗАГРЯЗНЕНИЯ АТМОСФЕРНОГО ВОЗДУХА НА ОСНОВЕ ПОЛНОСВЯЗНОЙ НЕЙРОННОЙ СЕТИ

Д. В. Полянчикова[1]
Научный руководитель В. А. Шершнева[1]
Доктор педагогических наук, профессор
Научный руководитель О. С. Володько[2]
Кандидат физико-математических наук, доцент;

[1]*Сибирский федеральный университет*

[2]*Институт вычислительного моделирования ФИЦ КНЦ СО РАН*

Уровень загрязнения атмосферного воздуха в Красноярске обусловлен многочисленными факторами – пространственной структурой и временной динамикой загрязняющих выбросов, особенностями метеорологических условий, которые на территории города также обладают значительной временной и пространственной изменчивостью. Существует необходимость не только в наблюдении, но и в прогнозировании уровня концентрации вредных веществ в атмосфере города.

Использование главных компонент в качестве входных данных позволяет улучшить экстраполяционную способность моделей и тем самым повысить качество прогноза [1].

Данные метеоусловий и концентрации твёрдых взвешенных частиц *Particulate Matter* 2.5 (*PM*2.5) за 2019–2024 гг. были получены из модели реанализа *National Centers for Environmental Prediction Global Forecast System* (*NCEP GFS*) [2] за каждые 6 ч и наземных станций оперативного мониторинга [3] с промежутком в 1 ч. Полученные данные были разделены на периоды в зависимости от значений концентрации *PM*2.5, приблизительно соответствующие временам года.

В качестве модели прогнозирования использовалась полносвязная нейронная сеть с двумя линейными слоями: первый – с функцией активации *relu*, второй – с функцией активации *tanh*. Нейросеть обучалась 50 эпох (количество проходов по тренировочным данным).

Было получено три конфигурации обучающей выборки:

1) исходные метеорологические данные с наземных станций мониторинга;

2) восемь главных компонент на основе данных *GFS*;

3) топ-5 признаков, вошедших в каждую из восьми главных компонент с максимальными весами на данных *GFS*.

© Полянчикова Д. В., 2025

В таблицах 1, 2 представлено сравнение качества построенных моделей в зависимости от конфигурации обучающей выборки.

Таблица 1

Сравнение качества моделей на тестовой выборке, метрика *MSE*

Конфигурация обучающей выборки	Данные за все годы	Разделение по сезонам
1	195,87	***116,76***
2	***205,03***	265,90
3	177,56	***160,28***

Таблица 2

Сравнение качества моделей на тестовой выборке, метрика *MAE*

Конфигурация обучающей выборки	Данные за все годы	Разделение по сезонам
1	10,31	***7,34***
2	***10,82***	12,34
3	***9,53***	9,83

Лучшее качество показала модель, построенная на данных с наземных станций мониторинга с разделением обучающей выборки по сезонам.

Качественное сравнение прогнозов сезонных моделей при прогнозировании на 3 дня вперёд с 11 по 13 января 2023 г. представлено на рисунках 1–3.

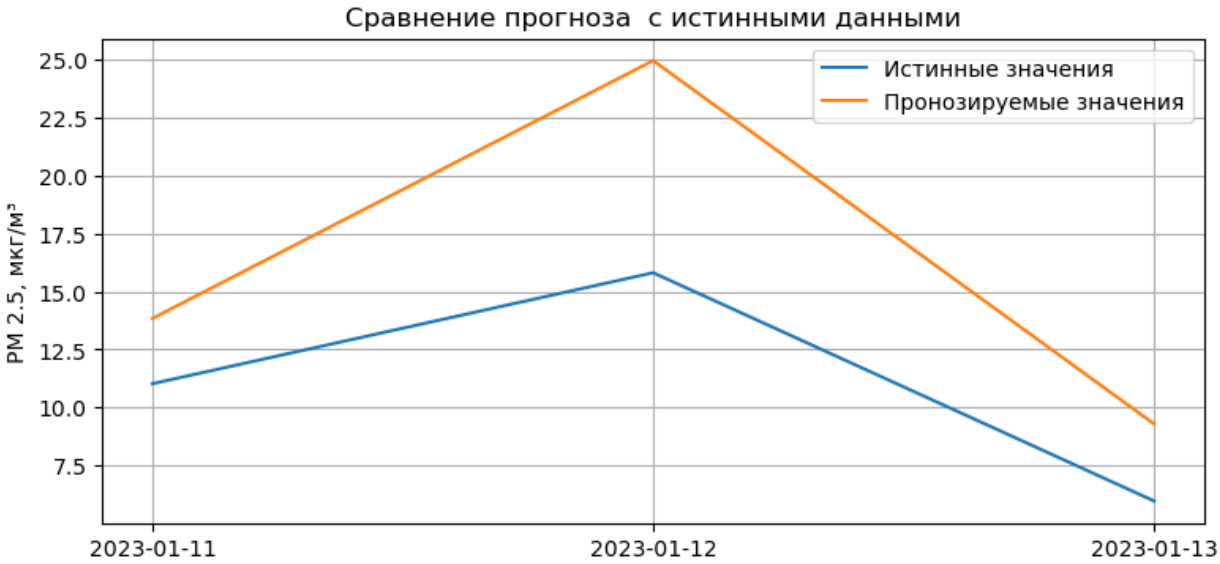


Рисунок 1. Конфигурация выборки 1

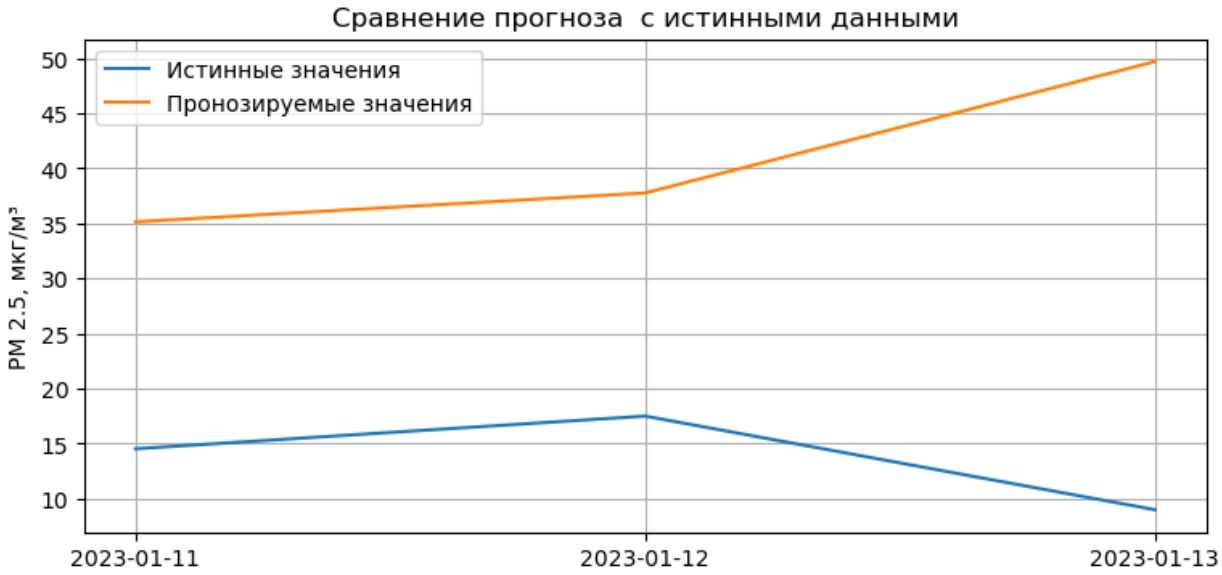


Рисунок 2. Конфигурация выборки 2

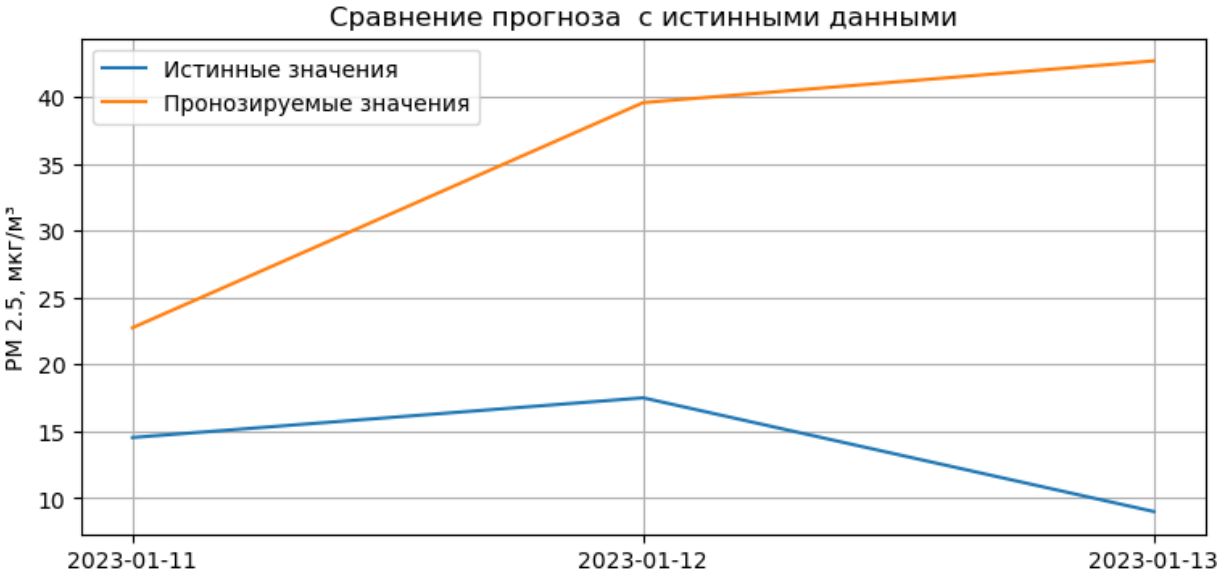


Рисунок 3. Конфигурация выборки 3

Таким образом, модель полносвязной нейронной сети показывает лучшее качество прогнозирования при обучении на данных с наземных станций мониторинга. Разделение выборки по сезонам улучшает качество модели.

Список литературы

1. Abdullah S. Evaluation for Long Term PM10 Concentration Forecasting using Multi Linear Regression (MLR) and Principal Component Regression (PCR) Models / S. Abdullah, M. Ismail, S. Y. Fong et al. // Environment Asia. 2016. – Vol. 9. – Pp. 101–110.

2. The Global Forecast System (GFS). URL: emc.ncep.noaa.gov/emc/pages/numerical_forecast_systems/gfs.php.

3. Геопортал – данные оперативного мониторинга. URL: sensor.krasn.ru/sc.

УДК 539.3+539.4

ТОПОЛОГИЯ ТРАЕКТОРИЙ АРМИРОВАНИЯ ВДОЛЬ ИЗОГОНАЛЬНЫХ ТРАЕКТОРИЙ И УПРАВЛЕНИЕ СВОЙСТВАМИ КОМПОЗИТА

И. Д. Руженцев[1]
Научный руководитель Н. А. Федорова[1]
доктор физико-математических наук, доцент

[1]*Сибирский федеральный университет*

Армирование конструкций с концентраторами напряжений, где возникают большие градиенты полей напряжений, осуществляется высокопрочными волокнами для восприятия этих градиентов. Реальные элементы конструкции подвергаются сложным условиям, которые требуют особого внимания к армированию и распределению напряжений.

Прежде армирование плоских конструкций осуществлялось прямолинейными волокнами, но это эффективно только в некоторых случаях нагружения, когда внутренние силовые линии преимущественно направлены вдоль траекторий армирования. В условиях повышенной нагрузки требуется применение специализированных армированных структур для эффективной работы конструкций.

Актуальность данной темы обусловлена необходимостью повышения прочности и надёжности конструкций, эксплуатируемых в условиях сложных нагружений и наличия концентраторов напряжений, таких как отверстия, вырезы и резкие изменения геометрии. Традиционные методы армирования, основанные на прямолинейной укладке волокон, не всегда обеспечивают оптимальное перераспределение напряжений в зонах с интенсивными градиентами. Применение армирования вдоль изогональных траекторий позволяет значительно повысить эффективность работы композиционного материала. Это особенно важно для современных инженерных задач, где конструкционная эффективность, снижение массы и увеличение срока службы имеют приоритетное значение.

Целью данной работы является поиск конфигураций траекторий армирования волокнистого композита посредством построения изогональных траекторий к данным плоским кривым в декартовой и полярной системах координат.

В работе было разобрано, как строятся изогональные траектории к данному семейству кривых в различных системах координат, рассмотрены примеры построения изогональных траекторий в декартовых и полярных системах координат и построены графически.

© Руженцев И. Д., 2025

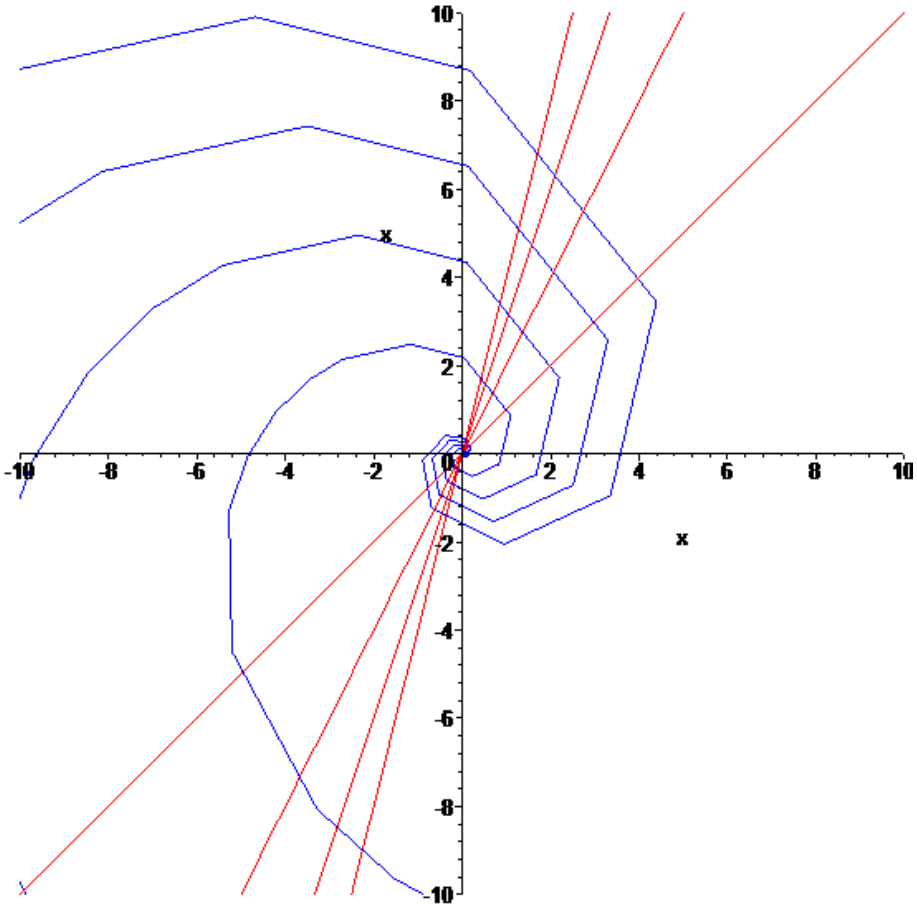


Рисунок 1. График семейства прямых y = ax и изогональных к нему траекторий

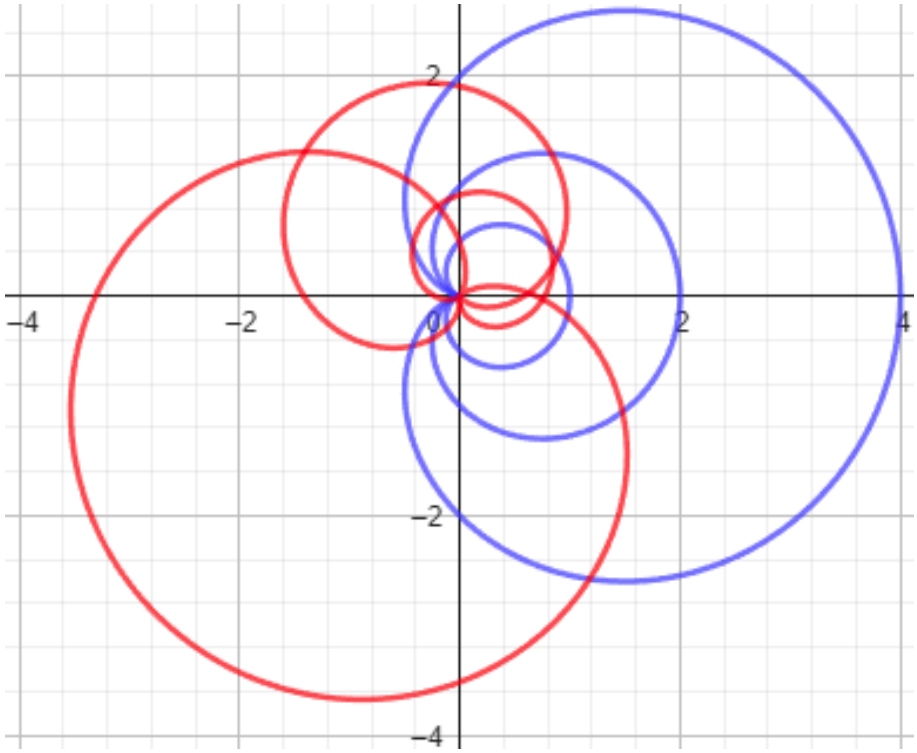


Рисунок 2. График семейства кардиоид ρ = a (1 + cos θ) и изогональные ему траектории

Было рассмотрено влияние поля температур на прочность конструкции по примерам из работы [3].

Список литературы

1. Галанин М. П. Армирование плоских конструкций по изогональным траекториям / М. П. Галанин, Н. А. Федорова // Препринты ИПМ им. М. В. Келдыша. 2017. № 33. 16 с. DOI: 10.20948/prepr-2017-33. – URL: library.keldysh.ru/preprint.asp?id=2017-33.

2. Немировский Ю. В. Исследование рациональных структур криволинейного армирования в полярной системе координат / Ю. В. Немировский, Н. А. Федорова // Вестник СамГТУ. Физ.-мат. Науки, 2013. № 1 (30). С. 233-244. URL: elibrary.ru/item.asp?id=19117446.

3. Немировский Ю. В. Прочность криволинейно армированных пластин в полярной системе координат / Ю. В. Немировский, Н. А. Федорова // Журнал СФУ. Техника и технологии, 2021. № 14 (8). С. 952-964. DOI: 10.17516/1999-494X-0365.

4. Немировский Ю. В. Предельные деформации термоупругих плоских конструкций с криволинейным армированием / Ю. В. Немировский, Н. А. Федорова // Вестник СибГАУ, 2016. Т. 17. № 1. С. 73-78. URL: cyberleninka.ru/article/n/predelnye-deformatsii-termouprugih-ploskih-konst.

УДК 517.54

ВИЗУАЛИЗАЦИЯ ОТОБРАЖЕНИЙ ФУНКЦИЯМИ КОМПЛЕКСНОГО ПЕРЕМЕННОГО

Ж. Э. Сультимов[1]
Научный руководитель Т. О. Кочеткова[1]
Кандидат физико-математических наук, доцент

[1]*Сибирский федеральный университет*

Методы теории функций комплексного переменного находят широкое применение при решении разнообразных прикладных задач [1; 2]. Комплексный анализ применяется в гидродинамике и теории упругости, является одним из основных математических инструментов решения задач в области автоматики и теории электрических цепей. Конформные отображения используются при моделировании композитных материалов, а также помогают упростить задачу изучения плоского векторного поля.

Целью работы является получение графического представления образов линий при отображениях функциями $w = z^2$ и $w = 1/z$. Визуализация реализована на языке программирования *Python* [3].

Рассмотрим отображение с помощью функции $w = z^2$. Выделим действительную и мнимую часть значений функции:

$$w = z^2 = (x + iy)^2 = x^2 - y^2 + i2xy = u + iv. \qquad (1)$$

© Сультимов Ж. Э., 2025

Для нахождения образов вертикальных прямых $x = C$ подставим вместо переменной x соответствующее значение в (1): $u = C^2 - y^2$, $v = 2Cy$. Исключая из полученных равенств переменную y, находим

$$u = C^2 - \frac{v^2}{4C^2}.$$

Получили уравнение парабол, симметричных относительно оси Ou, ветви которых направлены влево, а вершины находятся в точках $(C^2, 0)$. Образом прямой $x = 0$ является луч, совпадающий с отрицательной полуосью действительной оси. Прямые $x = C$ и их образы представлены на рисунке 1.

Найдём образы горизонтальных прямых $y = C$. Подставим вместо y значение C в (1): $u = x^2 - C^2$, $v = 2Cx$, откуда, исключая параметр x, находим

$$u = \frac{v^2}{4C^2} - C^2.$$

Полученное уравнение определяет параболы, симметричные относительно оси Ou, ветви которых направлены вправо, а вершины находятся в точках $(-C^2, 0)$. Образом прямой $y = 0$ является луч, совпадающий с положительной полуосью действительной оси. Прямые $y = C$ и их образы изображены на рисунке 2.

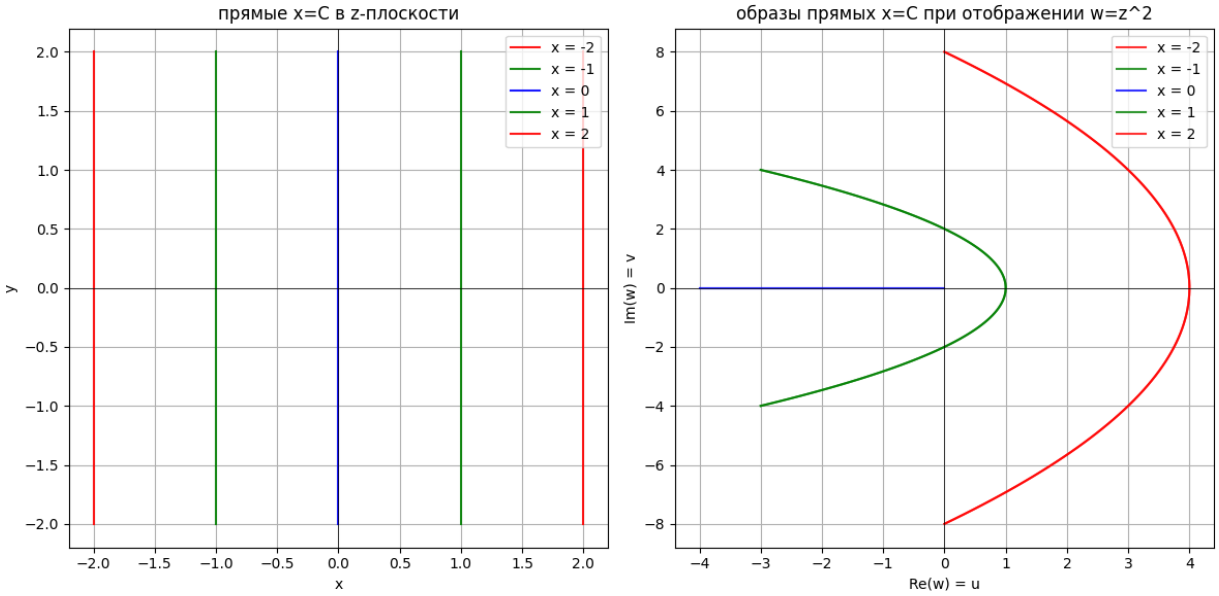


Рисунок 1. Образы прямых x = C при отображении w = z2

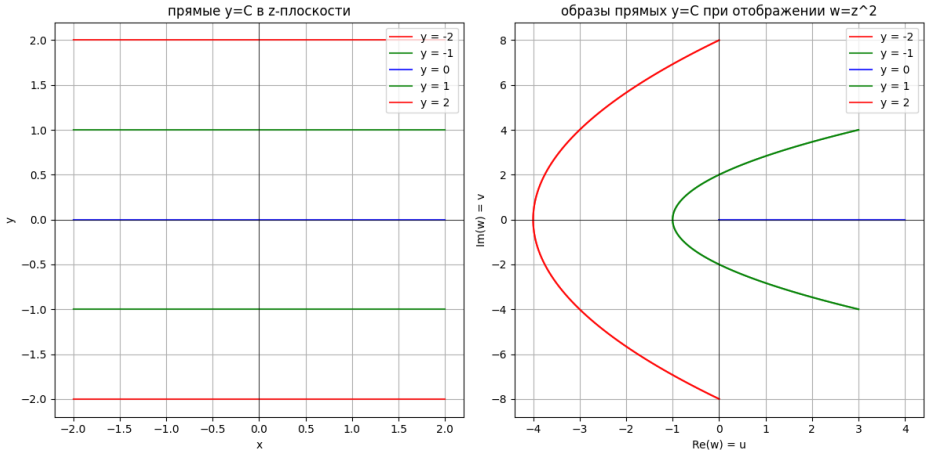


Рисунок 2. Образы прямых y = C при отображении w = z2

Рассмотрим отображение с помощью функции $w = 1/z$. Запишем значения функции в алгебраической форме:

$$\frac{1}{z} = \frac{1}{x+iy} = \frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2} = u + iv. \qquad (2)$$

Для прямых $x = C$ из (2) находим $u = \frac{C}{C^2+y^2}$, $v = -\frac{y}{C^2+y^2}$. Исключая из полученных равенств переменную y, получаем:

$$u^2 + v^2 = \frac{u}{C} \Rightarrow \left(u - \frac{1}{2C}\right)^2 + v^2 = \frac{1}{4C^2}.$$

Последнее уравнение определяет окружности с центром в точках $\left(\frac{1}{2C}, 0\right)$ радиуса $R = \frac{1}{2C}$. Прямая $x = 0$ переходит в мнимую ось $u = 0$. На рисунке 3 изображены прямые $x = C$ и их образы.

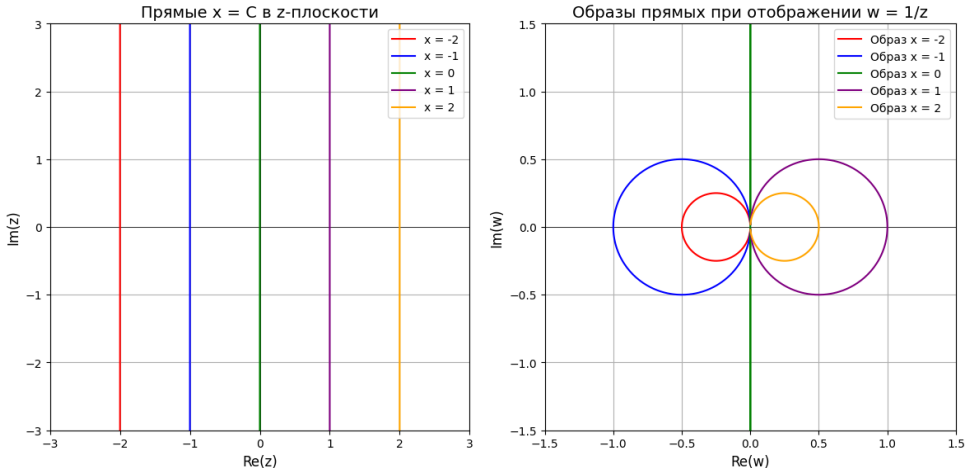


Рисунок 3. Образы прямых x = C при отображении w = 1 / z

Для прямых $y = C$ из (2) имеем $u = \frac{x}{x^2 + C^2}$, $v = -\frac{C}{x^2 + C^2}$, откуда находим:

$$u^2 + v^2 = -\frac{v}{C} \Rightarrow u^2 + \left(v + \frac{1}{2C}\right)^2 = \frac{1}{4C^2}.$$

Получили окружности с центром в точках $\left(0, -\frac{1}{2C}\right)$ радиуса $R = \frac{1}{2C}$. Прямые $y = C$ и их образы изображены на рисунке 4.

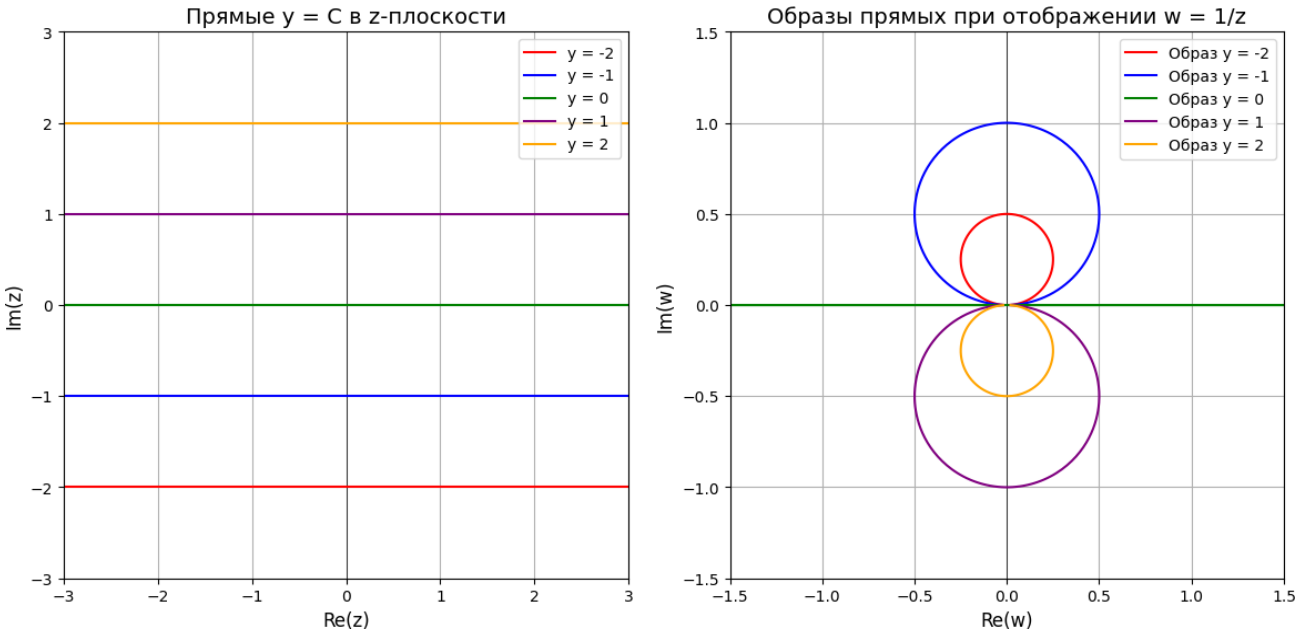


Рисунок 4. Образы прямых y = C при отображении w = 1 / z

Итак, получена визуализация отображения декартовой сетки на плоскости.

Список литературы

1. Сидоров Ю. В. Лекции по теории функций комплексного переменного / Ю. В. Сидоров, М. В. Федорюк, М. И. Шабунин. М.: Наука, 1989. 480 с.

2. Лаврентьев М. А. Методы теории функций комплексного переменного / М. А. Лаврентьев, Б. В. Шабат. М.: Наука, 1987. 688 с.

3. МакКинни У. Python и анализ данных / У. МакКинни. М.: ДМК Пресс, 2023. 536 с.

УДК 681.518.64

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ RAG ДЛЯ СОЗДАНИЯ СИСТЕМЫ АВТОМАТИЧЕСКОГО КОНСУЛЬТИРОВАНИЯ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

В. Д. Хашин[1]
Научный руководитель Л. В. Липинский[1]
Кандидат технических наук, доцент

[1]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

В современном мире большие языковые нейросетевые модели (*LLM*) уже никого не удивляют. Люди постоянно обращаются к ним с разными просьбами, однако большая языковая модель не может дать ответы на вопросы, связанные с узкой сферой деятельности. Одно из их главных ограничений – неспособность отвечать на узкоспециализированные вопросы без доступа к соответствующим данным.

Метод генерации с дополнением запросами (*RAG*) в языковых моделях искусственного интеллекта представляет собой инновационный подход, объединяющий возможности поиска и генерации текста. Этот метод включает в себя использование векторной базы данных для анализа обширных массивов текстовой информации, таких как книги, статьи и веб-сайты, с целью извлечения наиболее релевантных данных для заданного вопроса. Поиск в векторной базе данных осуществляется не по точному текстовому совпадению, а по семантическому сходству, что позволяет находить информацию, соответствующую смыслу запроса [1]. Чтобы данный подход работал эффективно, исходные тексты нужно обработать особым образом.

Процесс работы *RAG* начинается с тщательной подготовки данных. Сначала собирают все необходимые материалы – техническую документацию, научные статьи, внутренние базы данных компании. Эти тексты проходят глубокую очистку: удаляют *HTML*-разметку, стандартные юридические формулировки, рекламные вставки и другие нефункциональные элементы. Особое внимание уделяют нормализации текста – исправлению опечаток, унификации терминологии и форматов данных [2].

Подготовленный текст разбивается на логические фрагменты (чанки) [3]. Это могут быть абзацы, разделы или блоки фиксированного размера. Важно, чтобы каждый чанк сохранял законченный смысл и мог использоваться независимо. Финальный и самый важный этап – векторизация с помощью современных моделей эмбеддингов – такие модели преобразуют текстовые фрагменты в числовые векторы, сохраняя их семантические

© Хашин В. Д., 2025

особенности. Полученные векторы хранят в специализированных базах данных, оптимизированных для быстрого поиска по сходству [3].

Для поиска релевантных чанков в базе знаний используется несколько подходов – как частотных, так и использующих методы векторного сходства и кластеризации [3].

Одним из методов поиска релевантных чанков в контексте запроса является метод поиска ближайших соседей *Hierarchical Navigable Small World* (*HNSW*) [4]. Этот алгоритм представляет эмбеддинговое пространство в виде графа, при поиске старт происходит со случайной вершины в графе верхнего слоя, там мы быстро находим близкие к запросу вершины (кандидаты) и возобновляем поиск с них на предыдущем слое. Метрикой для кластеризации зачастую является косинусоидное подобие векторов [3].

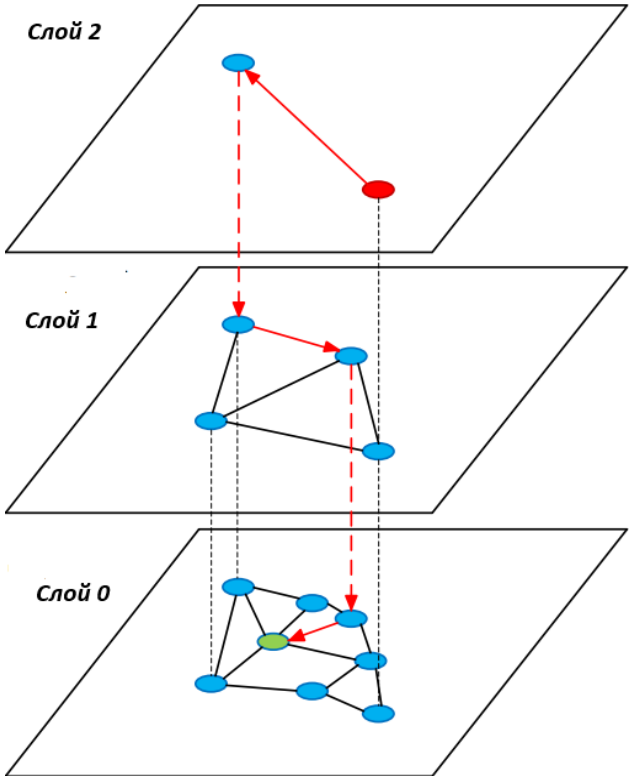


Рисунок 1. Алгоритм HNSW

Вторым подходом является использование алгоритма *BM*25.

*BM*25 – поисковая функция на неупорядоченном множестве термов («мешке слов») и множестве документов, которые она оценивает на основе встречаемости слов запроса в каждом документе, без учёта взаимоотношений между ними. В этом случае нас интересует только размер базы знаний и частота слов в ней [5].

Принцип работы алгоритма: пусть дан запрос Q, содержащий слова q_1, … q_2, тогда функция *BM*25 даёт следующую оценку релевантности документа D по запросу Q:

$$score(D,Q) = \sum_{i=1}^{n} IDF(q_i) \times \frac{f(q_i, D) \times (k+1)}{f(q_i, D) + k \times \left(1 - b + b \times \frac{|D|}{avgdl}\right)},$$

где $f(q_i, D)$ – частота слова q_i в документе D; $|D|$ – количество слов в документе; $avgdl$ – средняя длина документа; k и b – свободные коэффициенты; $IDF(q_i)$ – обратная документная частота [5].

Также можно гибридизировать лексический и семантический поиск релевантных чанков и применить оба алгоритма с назначением весовых коэффициентов.

После нахождения релевантных чанков необходимо подать на вход LLM текст запроса и сами релевантные чанки. После данной процедуры модель сможет дать какой-то осмысленный ответ на вопрос, в случае если релевантные чанки были найдены. Однако, для существенного улучшения работы системы также можно учесть следующие рекомендации.

1. Реранжирование результатов векторного поиска через Cross-encoder-модель. Cross-encoders оценивают семантическую схожесть между двумя текстами напрямую. Это даёт более точную оценку [3].

2. LLM reranking – отправляем в LLM текст и вопрос, спрашиваем: «Этот текст полезен для ответа? Насколько? Определи релевантность от 0 до 1» [3].

3. Добавление системных промптов, правил и ограничений модели, чтобы модель понимала, какую задачу решает, что можно, что нельзя и что от неё хотят.

В заключение можно отметить, что технология RAG представляет собой перспективное решение для создания систем автоматического консультирования на основе больших языковых моделей, позволяя преодолеть их ключевое ограничение – отсутствие доступа к узкоспециализированным знаниям.

Применение методов семантического поиска, включая алгоритмы HNSW и BM25, в сочетании с тщательной предобработкой данных и эффективной векторизацией текстов, обеспечивает релевантность извлекаемой информации. Дополнительное улучшение качества ответов достигается за счёт реранжирования результатов и оптимизации промптов.

Таким образом, RAG открывает новые возможности для разработки интеллектуальных консультационных систем в профессиональных областях, где требуются точные и актуальные знания.

Список литературы

1. Про fine-tuning моделей простыми словами. 2024. URL: habr.com/ru/companies/raft/articles/785616.

2. Проблемы и решения в обучении LLM на низкокачественных данных. 2024. URL: dzen.ru/a/ZuVcLonUu1rZ2qZr?ysclid=m7q4f29n135427560.

3. Как я победил в RAG Challenge: от нуля до SoTA за один конкурс.

2025. – URL: ipcc.ch/pdf/assessment-report/ar4/syr/ar4_syr_ru.pdf.

4. Методы приближённого поиска ближайших соседей. 2017. URL: habr.com/ru/companies/vk/articles/338360.

5. Okapi BM25. 2024. URL: ru.wikipedia.org/wiki/Okapi_BM25.

Прикладная лингвистика

UDC 621.314

STRUCTURAL SOLUTION OF AUTONOMOUS POWER SUPPLY SYSTEMS FOR MICROPOWER POWER SYSTEMS

M. D. Rukosueva, A. D. Lazarev[1]
Research Supervisor E. V. Soboleva[1]
senior lecturer
Research Supervisor Y. V. Krasnobaev[1]
Doctor of technical sciences, professor

[1]*Siberian Federal University*

Nowadays, automatic devices and systems are used in all spheres of human activity. In cases where automatic devices and systems are autonomous, i. e. remote from industrial power grids, such systems are often powered by devices that convert renewable energy such as wind, solar, etc. Such autonomous power supply systems (APS) have been developed and manufactured for over a hundred years and their design issues have largely been resolved. However, the development of technology associated with the miniaturization of electronic devices has led to a significant reduction in the power of many nodes of automatic devices and systems, such as sensors, information processing and control devices, actuators, etc. The power consumption of modern sensors measuring various physical quantities is summarized in the table below.

Table 1

Power consumption of modern sensors

№	Sensor brand	Measured value	Type of output signal	Power consumption, mW
1	ADT7302	Temperature	Analogue	2.1
2	DS18B20	Temperature	Digital	5.5
3	MAX6605	Temperature	Impulse	5.5
4	HTE.TD1	Humidity	Analogue	2.0
5	HIH-6130-021	Humidity	Digital	2.145
6	ДВА-301Д	Vibrations	Analogue	400
7	SW-18015P	Vibrations	Digital	60
8	SX41170	Acceleration	Analogue	120
9	ADXL345	Acceleration	Digital	0.75

From analyzing the data in the table, we can see that the power consumption of modern sensors ranges from 0.75 to 400 mW. Power consumption of low-power photo and web cameras is summarized in the table.

© Rukosueva M. D., Lazarev A. D., 2025

Table 2

Power consumption of low-power photo and web cameras

№	Camera brand	Camera types	Power consumption, mW
1	Raspberry Pi V2	Camera	200
2	Arducam Mini 5MP OV5642	Camera	250
3	Logitech C270	Webcam	250

The circuit design of micropower power supply systems with output power in units of watts has its own peculiarities, shown in [1]. In particular, [1] shows the energetic impracticality of using MPPT-type primary energy source (PES) controllers in micropower systems. In [1], an APS scheme shown in Figure 1 is proposed in which the controller (CT) contains two units, a voltage limiter (VL) and a load switch (LS).

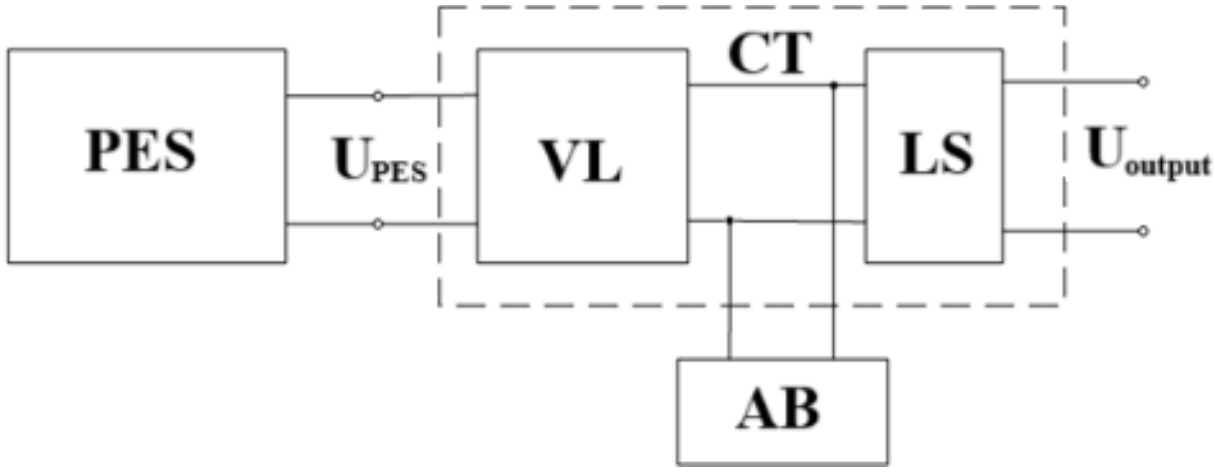


Figure 1. Structural diagram of micro and low power APS

In this scheme, the VL eliminates overcharging of the accumulator battery (AB) by connecting in parallel to it an additional load included in the VL, and the LS eliminates the discharge of the AB below the permissible value by disconnecting the load from the APS when the voltage on the AB reaches the minimum permissible value. In [1], technical solutions of VL and LS are proposed, which have simple circuitry and low intrinsic power consumption.

Solar panels (SP), thermoelectric converters (TEC), wind turbines (WT), etc. are used as PESs in APS. A common property of such PES is the lack of continuous power generation due to the intermittent nature of solar radiation, wind, etc. In this connection, it is reasonable to use several heterogeneous PES as part of the PES, for example, SP and TEC, which will provide the load with energy in the absence of power generation by one of the PES. The developed structural diagram of the APS with three PES is shown in Figure 2. In addition to three PES – PES1, PES2 and PES3 – it includes a diode block (DB), which coordinates the joint operation of heterogeneous PES in the APS.

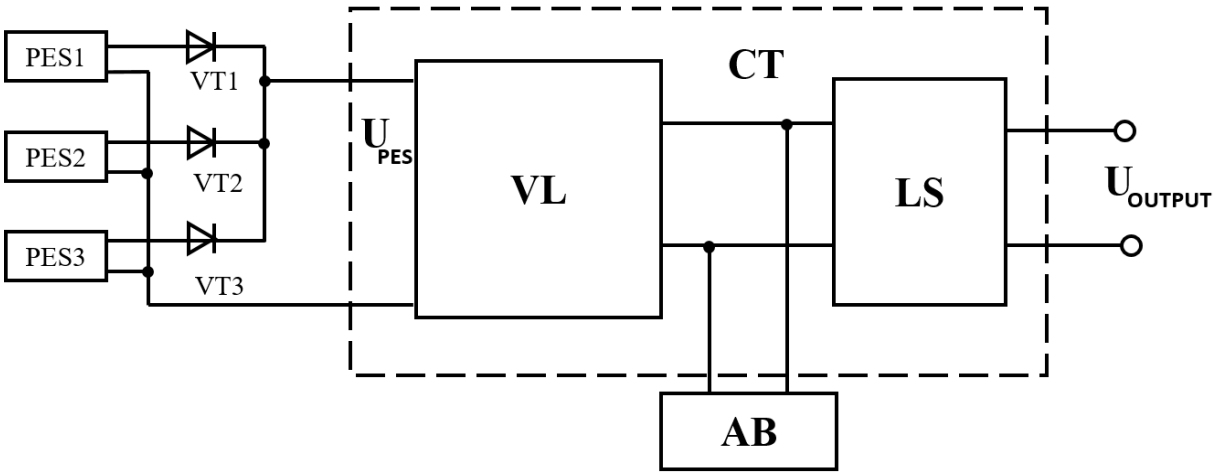


Figure 2. Structural diagram of a micropower APS with three PES

The paper presents the results of studies of joint operation of two heterogeneous PES as part of the APS, made according to the structural scheme shown in Figure 2. The researches carried out with the use of the Multisim program, which allows to simulate on the computer the processes in electronic circuits, have confirmed the operability of the APS in all possible modes.

References

1. Krasnobaev Y. V. Structural and circuit technical solutions for autonomous low-power power supply systems using renewable energy sources / Y. V. Krasnobaev, A. S. Klimov, E. A. Golubev et al. // Engineering Bulletin of Don. 2025. No. 1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9727.

UDC 81'33

THE IMPACT OF TECHNOLOGY ON LEARNING A FOREIGN LANGUAGE

E. A. Bobrov, A. P. Glavinskaya[1]
Research Supervisor A. T. Gordeeva[1]
senior lecturer

[1]Siberian Federal University

Technical English plays a key role in the IT field, as most of the documentation, technical specifications, and professional communication is conducted in English. Effective teaching of this language requires special methodologies that take into account the specifics of the IT industry.

The purpose of our work is to study and compare the methodologies of teaching technical English in the IT field.

© Bobrov E. A., Glavinskaya A. P., 2025

Our work consisted of studying reputable sources, structuring the information received, and comparing methodologies according to basic criteria.

Let's look at the first method of teaching technical English. When teaching a communicative language (CLT), priority is given to interaction in the real world, which makes it especially valuable in the field of information technology. Through modeling scenarios in the workplace, from daily meetings to customer support, this approach helps professionals develop practical communication skills. It promotes collaboration through role-playing, dialogue analysis, and conversational practice, which are crucial for agile teams. However, although CLT promotes rapid language acquisition, it may not take into account technical terminology and requires teachers to have experience in the field of information technology. For example, meetings (sprint planning), discussions of technical requirements, and analyses of real dialogues from the IT environment can be held [1].

The next technique that we will consider is the Integrated Subject Language Learning (CLIL) methodology, which combines language learning with professional information content, allowing students to work with real materials such as technical documentation, source code, and industry standards. By working with authentic resources – from API guides to cloud service guides – students develop both language skills and technical knowledge. This approach is particularly effective for mastering specialized terminology and practical documentation analysis. However, the complexity of IT technologies can become a problem for beginners, and successful implementation requires teachers with extensive experience in IT. The methodology includes reading and commenting on documentation, analyzing source code with explanations in English, studying and analyzing technical standards [2].

Consider a task-based learning method (TBL) that immerses students in real-world IT scenarios, focusing on practical tasks such as writing technical reports, creating setup guides, and participating in open source projects. Modern requirements for an IT specialist include writing code together and tracking problems in English. This methodology bridges the gap between language learning and professional skills. It increases motivation by demonstrating immediate practical value and preparing students to work in a global technological environment. However, its effectiveness depends on well-structured assignments adapted to the level of students' education. The technique may include setting up CI/CD pipelines, writing error messages, discussing issues on GitHub, and pair programming [3].

Let's look at the latest methodology, EdTech, which uses digital tools (online courses, virtual reality simulators, artificial intelligence assistants). All this is done to create a dynamic and personalized learning process for IT professionals. Platforms such as Coursera and Udemy offer specialized language training, while gamified exercises and adaptive technologies make learning technical English more fun. Although this method provides unprecedented accessibility and instant feedback, it cannot fully reproduce real-life human

interaction and can sometimes lead to a superficial understanding of complex topics [4].

For an objective comparison of methodologies, we identified the following key criteria: orientation to the IT context, a practice-oriented approach, flexibility, technology use, and efficiency assessment. We chose these criteria for comparison, because when studying methodologies, these aspects were most often encountered as features of methods.

Table 1

Comparative table of methodologies by criteria

Criteria	CLT	CLIL	TBL	EdTech
Focus on the IT context	Intermediate level spoken English	High level of work with documentation	High level in real-world tasks	Depends on courses' content
Practice-oriented approach	Spoken English	Reading and text analysis	Real projects	Interactive tasks
Flexibility	Low (template dialogues)	Average (depends on materials)	High (depends on the tasks)	Maximum (adaptive methods)
Using technology	Minimum	Average (IT forums, articles)	GitHub, JIRA	AI, VR, and LMS platforms
Effectiveness assessment	Speaking with teacher	Comprehension tests	Real deliverables	Automatic tests

The resulting table allows you to choose the best approach for specific purposes (for example, CLIL for documentation, TBL for project work); combine methods (for example, EdTech + TBL for remote teams).

We believe that combining CLIL (terminology), TBL (practice) and EdTech (flexibility) is the most effective for the IT sector, since by taking the main component from each technique and combining them together, it allows you to meet all the needs of IT specialists when learning a technical language. Such a specialist will know professional terminology, will not have a language barrier and will be well-versed in documents. By combining the methodologies, the specialist will gain all the necessary skills.

References

1. Richards J. C. Communicative Language Teaching Today / J. C. Richards. New York, USA: Cambridge University Press, 2006. URL: professorjackrichards.com/wp-content/uploads/Communicative-Language.pdf.

2. Abubakirova R. CLIL Technology as an Innovative Approach / R. Abubakirova, E. Zhacheva // Deutsche Internationale Zeitschrift für zeitgenössische Wissenschaft. 2021. URL: cyberleninka.ru/article/n/clil-technology-as-an-innovative-approach.

3. Пармели Д. Руководство AMEE № 65 командное обучение (TBL): практическое руководство / Д. Пармели, Л. К. Микаэльсен, С. Кук и др. // Медицинское образование и профессиональное развитие. 2014. URL: cyberleninka.ru/article/n/rukovodstvo-amee-65-komandnoe-obuchenie-tbl.

4. Гудкова С. А. Краудсорсинг как инструмент управления развитием интеллектуальных ресурсов: опыт интеграции EdTech и CLIL в вузе / С. А. Гудкова, М. В. Малащенко, Т. С. Якушева // Вестник ВУиТ. 2022. URL: cyberleninka.ru/article/n/kraudsorsing-kak-instrument-upravleniya-razvitiem-intellektualnyh-resursov-opyt-integratsii-ed-tech-i-clil-v-vuze.

UDC 81'33

THE FUTURE OF CYBERSECURITY JOBS: HOW ENGLISH OPENS GLOBAL OPPORTUNITIES

I. V. Vasiliadi, D. A. Vinchu[1]
Research Supervisor A. T. Gordeeva[1]
senior lecturer

[1]*Institute of Space and Information Technology, Siberian Federal University*

As digital technologies continue to evolve, the importance of cybersecurity has never been greater. Cybercrime is increasing in frequency and complexity, threatening governments, businesses, and individuals worldwide. In response, the global demand for cybersecurity professionals is rapidly rising. Yet, while technical skills are essential, another critical factor is shaping the future of these careers: English proficiency.

English is the global language of the tech industry, cybersecurity included. Whether for education, certification, teamwork, or client communication, English often serves as the default medium. This research paper explores how knowledge of English opens global doors in the cybersecurity job market and includes examples of Russian specialists making a mark internationally.

The cybersecurity industry is growing at an unprecedented rate. According to a report by Cybersecurity Ventures, there will be 3.5 million unfilled cybersecurity jobs globally by 2025 [1]. These roles include penetration testers, security operations center (SOC) analysts, threat intelligence specialists, incident responders, and more. Many of these jobs are international in nature, offering remote or relocation-based employment in companies across the world.

To access global opportunities, professionals must work in English, as most security resources and communities use it. Without English skills, they are often at a disadvantage.

English plays a central role in the cybersecurity field for several reasons.

1. Education and Certification. Most reputable cybersecurity certifications such as CISSP, CEH, and CompTIA Security+ are available only in English [2; 3]. Additionally, most online courses, tutorials, and university programs in cybersecurity are taught in English. Platforms like Coursera, Udemy, and Cybrary offer thousands of hours of training – predominantly in English.

© Vasiliadi I. V., Vinchu D. A., 2025

2. Professional Communication. International companies expect their employees to participate in meetings, write reports, and document incidents in English. In cybersecurity, precision is vital, and miscommunication due to language barriers can lead to severe consequences.

3. Research and Innovation. Most academic research and publications in the field are written in English. Conferences such as Black Hat, DEF CON, and RSA Conference also use English as the official language. Participation in these events gives professionals a chance to network and learn from global experts [4].

4. Open-Source and Community Involvement. Security communities like GitHub, Reddit's r/netsec, and Stack Overflow operate in English. These platforms are crucial for staying updated on new vulnerabilities, tools, and techniques.

Russia has a long-standing reputation for producing highly skilled computer scientists, programmers, and cybersecurity experts. Russian universities such as the Moscow Institute of Physics and Technology (MIPT), ITMO University, and Bauman Moscow State Technical University consistently rank among the top institutions for STEM education.

One of the most prominent figures in the global cybersecurity field is Eugene Kaspersky, the founder of Kaspersky Lab. His company, headquartered in Moscow, is internationally known for its antivirus software and threat research. Kaspersky Lab has offices in more than 30 countries and communicates internally and externally in English [5].

Another example is Dmitry Alperovitch, co-founder of CrowdStrike, a leading American cybersecurity firm. Born in Russia, Alperovitch moved to the U. S. and became one of the top cybersecurity thought leaders globally. His work in digital forensics and nation-state threat analysis has made him a respected figure in the industry [6].

Many Russian cybersecurity professionals work remotely for companies based in the U. S., Europe, and Asia. However, those with strong English skills find it easier to obtain international contracts, collaborate with global teams, and publish their research. Without English, even the most talented specialists can be limited to domestic job markets or low-visibility roles.

Fluency in English gives cybersecurity professionals access to:

– International Employment: professionals can apply for jobs at Google, Microsoft, IBM, and other tech giants;

– Freelance and Remote Work: platforms like Upwork and Toptal require English communication with clients [7].

– Professional Growth: being able to attend international conferences, join global research groups, or take part in competitions such as Capture The Flag (CTF) events helps specialists stay competitive.

Additionally, English enables collaboration in cross-border security investigations, especially those involving cybercrime and malware that span multiple jurisdictions.

Cybersecurity is one of the most promising fields of the 21st century. With threats becoming more complex and frequent, the need for skilled professionals is growing worldwide. However, the global nature of cybersecurity work requires more than just technical expertise. English has become the passport to international opportunities – opening doors to education, certification, employment, and research.

For Russian specialists and others from non-English-speaking countries, investing in English is a powerful strategy. It enables them to participate in the global cybersecurity conversation, access high-paying roles, and contribute to international cyber defense efforts. As cybersecurity continues to expand, those who master both technical skills and English will lead the way into the digital future.

References

1. Cybersecurity Jobs Report: 2023–2025 // Cybersecurity Ventures. 2023. URL: cybersecurityventures.com/jobs.

2. Certified Information Systems Security Professional (CISSP) // ISC2. 2024. URL: isc2.org.

3. Certified Ethical Hacker (CEH) // EC-Council. 2024. URL: eccouncil.org.

4. Global Cybersecurity Events // RSA Conference. 2024. URL: rsaconference.com.

5. Company Overview // Kaspersky. 2024. URL: kaspersky.com/about.

6. Dmitry Alperovitch: CrowdStrike Cofounder // Forbes. 2022. URL: forbes.com.

7. Freelance Cybersecurity Jobs // Upwork. 2024. URL: upwork.com.

УДК 81'33

ОСОБЕННОСТИ ПЕРЕДАЧИ ИМЁН СОБСТВЕННЫХ ПРИ ПЕРЕВОДЕ НАУЧНЫХ ТЕКСТОВ С АНГЛИЙСКОГО ЯЗЫКА НА РУССКИЙ

А. А. Добросердова[1]
Научный руководитель Н. В. Николаева[1]
старший преподаватель

[1]*Сибирский федеральный университет*

Имена собственные (далее – ИС) – неотъемлемая часть любого языка. В научных текстах такая языковая единица встречается довольно часто – например, это имена и фамилии авторов статей и работ, используемых в исследовании. Понимание специфики ИС служит важным условием для грамотного перевода, поскольку эти слова часто несут в себе

© Добросердова А. А., 2025

не только прямое значение, но и культурные, исторические и социальные контексты.

Актуальность обусловлена тем, что ИС встречаются повсеместно, а для полного понимания текста необходимо корректно их передавать, учитывая их тип и происхождение.

Объектом исследования служат ИС, которые употребляются в статье What Do We Think We Think We Are Doing?: Metacognition and Self-regulation in Programming [1]. Предметом – способы и особенности передачи ИС с английского языка на русский.

Цель данной работы заключается в определении и анализе особенности передачи ИС с английского языка на русский.

Имя собственное – это особая категория имён существительных, которая может представлять собой слово, словосочетание или предложение, предназначенная для идентификации уникальных объектов (как одушевлённых, так и неодушевлённых) в языке.

Авторы выделяют различные подходы для передачи ИС. Например, С. И. Влахов говорит о том, что «имя собственное, как правило, при переводе заимствуется, транскрибируется, но, как исключение, может подвергаться переводу…» [2].

В данной работе рассмотрена следующая классификация:

1) транскрипция (метод фонетического подобия);

2) транслитерация (метод графического подобия);

3) транспозиция (принцип этимологического соответствия);

4) калькирование (дословный перевод).

В ходе исследования из статьи были выделены и классифицированы ИС. Общее число найденных ИС в тексте – 111 элементов. Из них к категории антропонимов относится 77. Топонимов обнаружено 11, названий организаций, учреждений и коллективов – 8. Произведения литературы и периодические издания объединены в одну категорию, их число составляет 2 ИС. Названий мероприятий и конференций было найдено 9. Наконец, в категорию названий языков программирования и систем попало 4 ИС.

В контексте данного исследования антропонимы представляют собой имена авторов работ и статей, а также исследователей, научных работников и других значимых личностей. Транскрипция – наиболее популярный способ при переводе имён, т. к. при этом передаётся звучание слова. Также встречаются случаи транслитерации. Примеры транскрипции: James Prather – «Джеймс Пратер»; Paul Denny – «Пол Денни». Транслитерация: Brett A. Becker – «Бретт А. Беккер».

При переводе географических названий используются чаще всего такие способы передачи, как транскрипция и калька. Также необходимо опираться на традиции в переводе, т. к. названия географических объектов важно передавать наиболее понятным способом для конкретной аудитории. Это относится

особенно к названиям стран, штатов и крупных городов, т. к. в русском языке уже есть эквиваленты данных ИС.

Примером традиций в переводе может служить такой случай: New Zealand – «Новая Зеландия». В данном примере была переведена часть New с помощью кальки как «Новая». Вторая часть была изначально транскрибирована, но с течением времени была адаптирована под конкретный язык для соблюдения принципа благозвучия.

При передаче названий организаций, учреждений и коллективов применялись такие способы перевода, как калькирование и транслитерация, иногда в смешанном виде. Как и в случае с географическими названиями, необходимо опираться на традиции в переводе, т. к. большинство известных компаний имеет традиционный перевод, который используется повсеместно и будет понятен при чтении статьи. Например, словосочетание University of Washington было передано как «Вашингтонский университет».

Перевод названий произведений литературы и периодических изданий может включать в себя транслитерацию, транскрипцию и калькирование. Также особенность при передаче таких ИС – использование нарицательного эквивалентного существительного. Т. е. при переводе упоминается не только название, но и то, чем является это ИС (книга, журнал и т. д.). Примером может служить журнал ACM Inroads, в оригинале указания на журнал не было.

При передаче названий мероприятий и конференций используются следующие способы – калькирование и иногда транслитерация или транскрипция. Также есть случаи, когда такие ИС вовсе не переводятся, а остаются на языке оригинала. В качестве особенности данной категории можно выделить то, что при переводе отдельно указывался оригинальный вариант для того, чтобы читателю было проще найти данную конференцию в других источниках.

Названия языков программирования и систем, будучи специфическими терминами, транскрибируются или вовсе не переводятся. Например, название языка Scratch остаётся неизменным, т. к. данный язык не очень популярен и на русском языке может быть не понятен читателям. Язык «Джава» в научной литературе по программированию часто встречается в форме транскрипции, поэтому его уже достаточно уместно переводить таким способом.

Культурные традиции играют важную роль в переводе ИС, такой способ передачи может быть более понятен читателю. С течением времени применялись различные способы перевода, что обусловлено не только лингвистическими факторами, но и социально-культурными. Переводимые ИС видоизменялись, что в конечном счёте приводило к заимствованию данного слова в язык перевода в том или ином виде.

В данной работе традиции в переводе имели место при передаче имён и фамилий, топонимов, а также некоторых названий организаций, в частности названий университетов.

Современные тенденции в данном контексте ориентируются на точность, корректность и адекватность передачи того или иного ИС.

Анализируя данное исследование, одним из примеров современных тенденций можно считать транскрипцию, когда имя передаётся максимально близко к оригинальному звучанию. Такой способ применяется в большинстве случаев при переводе исследуемой статьи.

Также использовалось калькирование для таких ИС, эквиваленты которых в русском языке не были найдены. Например, не было найдено традиционного перевода на русский язык названий мероприятий и конференций, которые не очень популярны в русскоязычном сообществе.

Таким образом, можно сделать вывод о том, что имена собственные играют значительную роль как в языках в общем, так и в контексте перевода. При этом подчёркнута важность культурной традиции в переводе, т. к. от этого напрямую зависит понимание текста читателем.

Список литературы

1. Prather J. What Do We Think We Think We Are Doing?: Metacognition and Self-regulation in Programming / J. Prather, B. A. Becker, M. Craig et al. // Learning Sciences Faculty Publications. DOI: 10.1145/3372782.3406263.

2. Влахов С. И. Непереводимое в переводе / С. И. Влахов. М.: Международные отношения, 1980. 343 с.

3. Виноградов В. С. Введение в переводоведение: общие и лексические вопросы / В. С. Виноградов. М.: ИОСО РАО, 2001. 224 с.

УДК 004.8:316.77

ТЕОРИЯ МЁРТВОГО ИНТЕРНЕТА: КОММУНИКАЦИОННЫЕ РИСКИ АЛГОРИТМИЗАЦИИ «ВКОНТАКТЕ» И «ТЕЛЕГРАМА»

Д. М. Зимин[1]
Научный руководитель А. А. Романовская[1]
старший преподаватель

[1]*Сибирский федеральный университет*

Теория мёртвого интернета (*Dead Internet Theory*), возникшая в начале 2020-х гг., предполагает, что интернет как средство коммуникации постепенно утрачивает свою «живую» сущность из-за доминирования алгоритмически генерируемого контента, ботов и автоматизированных систем [1]. Интернет в этом контексте рассматривается не только как инструмент общения, но и как продукт, подверженный жизненному циклу, на который влияют технологические, социальные и экономические факторы.

© Зимин Д. М., 2025

Цель данной работы – проанализировать влияние алгоритмизации на коммуникативные процессы в русскоязычном сегменте интернета (Рунете), уделяя особое внимание социальным сетям как наиболее эффективным платформам взаимодействия.

Для анализа использовались данные открытых исследований [3; 4], а также результаты мониторинга активности аккаунтов в «Телеграме» за 2022–2024 гг. Применялись методы количественной оценки доли бот-активности, семантического анализа *AI*-генерируемых текстов и анализа динамики ранжирования контента в поисковой системе «Яндекс».

Интернет как средство коммуникации наиболее ярко проявляется в социальных сетях, которые стали ключевым каналом взаимодействия в Рунете. В социальной сети «ВКонтакте» доля аккаунтов, идентифицированных как боты, составляет 18 % (2024 г.), при этом в тематических сообществах (например, «Кино и музыка») боты генерируют до 30 % сообщений (табл.).

Таблица 1

Доля искусственной активности в социальной сети «ВКонтакте» (2023–2024 гг.)

Тематика	2023 г. (%)	2024 г. (%)
Кино и музыка	25	30
Технологии	20	25
Образование	15	18

Отметим, что в «Телеграме» 25 % популярных каналов используют нейросети для генерации текстовых постов. Это снижает долю «органического» контента: вовлечённость аудитории в контент, созданный людьми, упала на 12 % за 2023 г. [3]. Социальные сети, таким образом, демонстрируют наибольшую эффективность в распространении автоматизированного контента, что подтверждает их центральную роль в трансформации интернет-коммуникации.

В «Телеграме» автоматизация контента затрагивает не только информационные каналы, но и творческие проекты, где AI используется для генерации текстов, изображений и даже сценариев. Это явление можно рассматривать как этап жизненного цикла продукта, где ключевым фактором влияния становится технологическая оптимизация.

Анализ 500 сайтов из топ-выдачи «Яндекса» показал, что 35 % текстов написаны с использованием нейросетей (например, YandexGPT). Ключевым фактором ранжирования стала техническая оптимизация, а не уникальность контента [4].

Интернет как средство коммуникации и продукт подвержен жизненному циклу, который включает этапы роста, насыщения и потенциального упадка. Теория мёртвого интернета акцентирует внимание на явлении алгоритмизации, которое можно отследить через рост AI-контента и его влияние на взаимодействие пользователей.

Социальные сети, являясь наиболее эффективным инструментом коммуникации, становятся эпицентром этой трансформации. Критики теории

отмечают адаптацию пользователей, проявляющуюся в иронии и языковых играх как способах сопротивления алгоритмам [1]. Однако централизация власти платформ (например, удаление 60 % материалов в «Яндекс.Дзен», не соответствующих шаблонам [5]) подчёркивает риски утраты «живого» интернета.

Теория мёртвого интернета отражает текущую трансформацию коммуникации в Рунете, где интернет как средство общения и продукт проходит очередной этап своего жизненного цикла. Анализ социальных сетей как сегмента с выраженной алгоритмизацией имеет практическое значение: он позволяет прогнозировать развитие цифрового пространства и разрабатывать меры регулирования. Мы не «похороним» интернет как средство общения, если будем учитывать факторы, влияющие на его эволюцию, и поддерживать баланс между автоматизацией и человекоориентированным контентом. Перспективным направлением остаётся внедрение стандартов маркировки AI-материалов и алгоритмов, сохраняющих «живую» коммуникацию [6].

Список литературы

1. Брайдл Д. Новая тёмная эра: Технологии и конец будущего / Д. Брайдл. М.: Альпина Паблишер, 2018. 320 с.

2. Отчёт о цифровых трендах Рунета // Mediascope. 2024. URL: mediascope.net.

3. Исследование AI-контента в Telegram // Brand Analytics. 2024. URL: brandanalytics.ru.

4. Анализ SEO-оптимизации в Яндексе // Яндекс.Вордстат. 2024. URL: wordstat.yandex.ru.

5. Политика модерации контента // Яндекс.Дзен. 2024. URL: zen.yandex.ru.

6. Рекомендации по этике AI // Аналитический центр при Правительстве РФ. 2024. URL: ac.gov.ru.

УДК 81'33

ЯЗЫКОВАЯ КОНКУРЕНЦИЯ РАЗЛИЧНЫХ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: OPENAI И DEEPSEEK

Е. А. Курбатова, П. В. Толстихин, А. А. Садомский[1]
Научный руководитель Н. Н. Слепченко[1]
старший преподаватель

[1]*Сибирский федеральный университет*

В статье проводится сравнительный анализ языковых моделей искусственного интеллекта OpenAI (ChatGPT) и DeepSeek. Исследуются

© Курбатова Е. А., Толстихин П. В., Садомский А. А., 2025

исторические этапы развития систем, их текущее состояние, качественные характеристики и предпочтения. Также отображены результаты опроса среди студентов о предпочтительных платформах. На основе статистических данных и качественных критериев формулируются прогнозы дальнейшего развития языкового ИИ.

Современные языковые модели ИИ стали неотъемлемой частью цифровой трансформации общества. Среди наиболее перспективных разработок выделяются системы OpenAI и DeepSeek, демонстрирующие различные подходы к обработке естественного языка. Актуальность исследования обусловлена необходимостью понимания конкурентных преимуществ данных платформ для их эффективного использования.

OpenAI основана в 2015 г. В 2018 г. OpenAI выпускает GPT-1; в 2020 г. представляет GPT-3 с 175 млрд параметров; в ноябре 2022 г. – ChatGPT на базе GPT-3.5; в марте 2023 г. – GPT-4, отличающуюся улучшенной логикой. В 2024 г. ChatGPT становится платным, но сохраняет бесплатный доступ.

В июне 2023 г. состоялся первый анонс DeepSeek-V1 (китайская компания). В январе 2024 г. DeepSeek выпускает DeepSeek-V2, в июне 2024 г. – DeepSeek-V3 с улучшенными математическими способностями. Прогноз на 2025 г.: DeepSeek выходит на международный рынок, обеспечивает поддержку русского и английского языков. OpenAI долгое время доминировал, но DeepSeek быстро набирает обороты, особенно в Азии. Для выявления преимуществ данных платформ был проведён сравнительный анализ их текущего состояния.

DeepSeek AI демонстрирует стремительный рост в 2025 г. Всего за полгода ежедневная аудитория платформы увеличилась с 7,5 до 100,8 тыс. пользователей – в 12 раз. Мобильное приложение было скачано более 10 млн раз. Технические характеристики платформы впечатляют: модель обрабатывает до 128 тыс. токенов контекста и генерирует ответы длиной 8 тыс. токенов. При этом стоимость разработки DeepSeek-V3 составила всего 5,5 млн $ – в 18 раз меньше, чем создание GPT-4 от OpenAI. В тестах по программированию DeepSeek-R1 превзошёл аналогичную модель OpenAI в двух из пяти категорий, демонстрируя особые успехи в LiveCodeBench (65,9 против 63,4 %) и SWE Verified (49,2 против 48,9 %).

В таблице представлены качественные критерии нейросетей.

Таблица 1

Качественные критерии нейросетей

Параметр	***ChatGPT* (*GPT*-4)**	***DeepSeek-V*3**
Точность ответов	Высокая (*Stanford HAI*, 2024)	Очень высокая (особенно в *STEM*) (*DeepSeek Research*, 2024)
Креативность	Отличная (*User Reviews*, 2024)	Хорошая, но более техническая (*User Feedback*, 2024)
Контекст	До 128 тыс. (*GPT*-4-*turbo*) (*OpenAI*, 2024)	До 128 тыс. (*DeepSeek Blog*, 2024)
Мультимодальность	Да (текст,	Только текст (на апрель 2025 г.)

	изображения, файлы)	

OpenAI лидирует по охвату и креативности.

DeepSeek сильнее в аналитике, длинных текстах и точности.

Для верификации данных пользователями авторами создан и направлен студентам ИКИТ с разных кафедр опрос в Google Forms из восьми вопросов (URL: docs.google.com/forms/d/e/1FAIpQLSeX4r-V0tSa83D_6ezuL 03T1jrUF-WBI5xHkpGEYkKatW5VRg/viewform).

Проведённый мини-опрос среди пользователей (12 чел.) показал, что ChatGPT пока сохраняет лидерство по частоте использования (58,3 против 41,7 % у DeepSeek), однако разрыв не столь значительный.

В чём ChatGPT опережает? Качество ответов: 41,7 % считают его лучше, тогда как DeepSeek – 25 %. Работа с длинными текстами: 50 % предпочитают ChatGPT против 33,3 % у DeepSeek. Креативность: 41,7 % отдают предпочтение ChatGPT в генерации идей и текстов. Скорость ответов: 50 % отмечают, что ChatGPT быстрее. Образовательные цели: 50 % считают, что выбор зависит от задачи.

Перспективы DeepSeek: несмотря на текущее отставание, 33,3 % респондентов верят, что DeepSeek может стать популярнее через 3-4 года, что говорит о его потенциале. ChatGPT пока доминирует в удобстве, креативности и скорости, но DeepSeek демонстрирует конкурентные возможности, особенно в технических и аналитических сферах.

DeepSeek произвёл фурор, создав ИИ, эффективный, как Google и OpenAI, но требующий меньших ресурсов и меньшего бюджета (менее 10 млн $), чем у конкурентов. Это привело к падению акций Nvidia на 17 %, заставив инвесторов задуматься о спросе на дорогие чипы.

DeepSeek имеет перспективное будущее благодаря низкой стоимости и мощным возможностям. OpenAI, хоть и остаётся гигантом с мощными моделями вроде GPT-4o, сталкивается с конкуренцией более дешёвых альтернатив. OpenAI инвестирует в мультимодальные технологии и укрепляет партнёрства (например, с Microsoft).

Борьба за лидерство в ИИ только начинается, и исход определит, кто будет задавать стандарты в ближайшие годы. Языковые модели OpenAI и DeepSeek представляют два подхода: универсальность vs специализация. Пока ChatGPT популярнее, DeepSeek демонстрирует впечатляющий рост и может стать главным конкурентом в ближайшие годы. Инженеры и учёные могут отдавать предпочтение DeepSeek за его вычислительные возможности, в то время как маркетологи и копирайтеры выбирают ChatGPT за генерацию креативного контента.

Список литературы

1. DeepSeek // Statista & Facts. URL: statista.com/topics/13/deepseek.

2. Анализ трафика, рейтинг, аудитория DeepSeek. URL: similarweb.com/ru/website/deepseek.com/#overview.

3. How Trustworthy are Large Language Models like GPT // Stanford. 2023. URL: hai.stanford.edu/news/how-trustworthy-are-large-language-models.

4. DeepSeek-R1: Технический обзор его архитектуры и инноваций // GeeksforGeeks. URL: geeksforgeeks.org/deepseek-r1-technical-overview.

УДК 81'33

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ НЕЙРОСЕТЕЙ В ИЗУЧЕНИИ ИНОСТРАННЫХ ЯЗЫКОВ

К. А. Кустикова, Д. Э. Дондукова[1]
Научный руководитель А. Т. Гордеева[1]
старший преподаватель

[1]*Сибирский федеральный университет*

В последние годы роль искусственного интеллекта существенно возросла. Он получил широкое применение в разнообразных сферах и областях. Особенно полезным ИИ оказался в обучении. Сейчас его активно применяют в образовании, чтобы сделать процесс обучения более удобным и эффективным.

Целью настоящего исследования является сравнение возможностей современных нейросетей для определения их эффективности в обучении иностранным языкам. Перед авторами поставлены следующие задачи: дать определение ИИ; провести сравнительный анализ производительности, функциональности и удобства использования трёх популярных нейросетей: Qwen, ChatGPT-4 и DeepSeek; оценить их способность выполнять задачи, такие как объяснение грамматических правил, поддержание диалога, перевод текстов, анализ изображений и генерация полезных выражений; выявить сильные и слабые стороны каждой системы; дать рекомендации по выбору наиболее подходящей нейросети для решения конкретных задач пользователя.

Для начала определим, что же такое ИИ? Под ИИ понимается компьютерная программа, способная анализировать данные и делать выводы подобно человеку. При изучении иностранных языков такие программы предлагают ряд значительных преимуществ: неограниченную практику, гибкий график обучения, развитие разговорных навыков, доступную стоимость и оперативную обратную связь. Тем не менее следует отметить и недостатки: отсутствие живого общения и возможные неточности в ответах [1; 2].

Для сравнения нейросетей выбраны три платформы: Qwen, ChatGPT-4 и DeepSeek. Для всех систем использованы одинаковые запросы с целью обеспечения объективности результатов. Критерии включают скорость обработки запросов, качество ответов, возможность загрузки файлов и фото,

© Кустикова К. А., Дондукова Д. Э., 2025

обработку больших объёмов данных, а также удобство интерфейса и доступность.

Qwen. При выполнении первого запроса «Объясни правило Present Perfect Continuous на примере» Qwen потратила 6 с на ответ. Объяснение было чётким, с несколькими примерами, включая корректное использование временных маркеров, таких как for и since. Второй раз мы обратились с просьбой: «Мне бы хотелось попрактиковать устную речь на английском. Предлагаю разыграть сценку в магазине электроники. Ты начинаешь – я продолжаю, обязательно дожидайся моего ответа!», и система ответила за 8 с, предложив хорошее начало диалога. При переводе текста объёмом 700 слов Qwen справилась за 15 с, сохранив все смысловые оттенки. Загрузка фотографии и описание её содержимого заняли 10 с, причём описание было подробным и точным. На запрос «Сгенерируй ряд полезных выражений для деловой переписки» Qwen предоставила список из 20 фраз за 7 с, включая выражения для формального и неформального стилей. Эта нейросеть работает немного медленнее по сравнению с DeepSeek, но сбои случаются очень редко [3].

ChatGPT-4. На первый запрос ChatGPT-4 ответила за 4 с, но примеры оказались менее разнообразными, чем у Qwen. При втором запросе «Мне бы хотелось попрактиковать устную речь на английском. Предлагаю разыграть сценку в магазине электроники. Ты начинаешь – я продолжаю, обязательно дожидайся моего ответа!» система справилась за 5 с, предложив начало диалога: Good afternoon! How can I assist you? Однако после нескольких реплик система иногда теряла контекст или генерировала полный диалог вместо ожидания ответа пользователя. После девятого запроса чат временно блокировался. Также 11.04.2025 ChatGPT-4 обновилась и теперь помнит все переписки так же, как Qwen и DeepSeek, но эта функция пока что доступна только пользователям с платной подпиской. Перевод текста объёмом 700 слов не был выполнен, т. к. система отказалась обрабатывать тексты объёмом более 500 слов без дополнительной подписки. Когда мы пытались загрузить изображения для анализа, выяснилось, что ChatGPT-4 позволяет загрузить только две фотографии за одну сессию. На запрос «Сгенерируйте ряд полезных выражений для деловой переписки» система предоставила список из 15 фраз за 6 с, но некоторые из них повторялись или были недостаточно разнообразными. Основными недостатками ChatGPT-4 являются: блокировка после девяти запросов, ограничение на загрузку файлов, строгий лимит на объём текста, необходимость платной подписки и ограниченный доступ в некоторых регионах [4].

DeepSeek. DeepSeek показала самую высокую скорость обработки запросов среди всех систем. На объяснение правила Present Perfect Continuous она потратила всего 3 с, но примеры оказались менее детальными по сравнению с Qwen. Диалог для тренировки разговорной речи был создан за 4 с, однако иногда возникали повторяющиеся фразы. Перевод текста объёмом 700 слов занял 12 с, но при попытке загрузить текст объёмом более 800 слов произошёл сбой. При анализе изображения DeepSeek выдала

ошибку при первой попытке загрузки. После повторной попытки система смогла описать основные элементы за 5 с, описание оказалось корректным, но менее детальным. Например, она смогла определить основные объекты, но не смогла добавить эмоциональную окраску. На запрос «Сгенерируйте ряд полезных выражений для деловой переписки» DeepSeek ответила за 5 с, предоставив список из 18 фраз, но некоторые из них были слишком общими и не всегда подходили для конкретных ситуаций. Основным недостатком DeepSeek являются сбои при загрузке фото и периодические сбои в работе самой системы, которые могут привести к прерыванию выполнения задачи или некорректным ответам [5].

Несмотря на значительный прогресс в развитии ИИ, ни одна из рассмотренных систем пока не может полностью заменить преподавателя. Однако каждая из них имеет свои преимущества. Qwen идеально подходит для пользователей, которым важна стабильность и отсутствие ограничений. Она успешно справляется с генерацией полезных выражений, поддержанием диалогов и анализом изображений, предоставленных пользователем. ChatGPT-4 лучше использовать для краткосрочных задач, где важны скорость и качество ответов, но её ограничения делают её менее удобной для длительного использования. DeepSeek – лучший выбор для быстрых запросов. Таким образом, выбор нейросети зависит от конкретных потребностей пользователя. Для длительного обучения лучше использовать Qwen, для быстрых запросов – DeepSeek, а для качественных ответов на короткие вопросы – ChatGPT-4. Игнорировать этих помощников не стоит, т. к. они значительно упрощают процесс обучения языкам.

Список литературы

1. Абдуллаев Э. А. Нейросеть: определение, область применения / Э. А. Абдуллаев // Молодой учёный. 2023. № 33 (480). С. 4–5. URL: moluch.ru/archive/480/105477.

2. Богатова С. М. Дидактические возможности нейросетей в обучении иностранным языкам / С. М. Богатова, О. В. Фрезе // Современное педагогическое образование. 2024. № 3.

3. Qwen: нейросеть. URL: chat.qwen.ai.

4. ChatGPT-4: нейросеть. URL: chatgpt.com.

5. DeepSeek: нейросеть. URL: chat.deepseek.com.

УДК 81'33

ЛИНГВИСТИЧЕСКИЙ ДИЗАЙН НАРРАТИВНОГО ТЕКСТА В ВИДЕОИГРАХ

В. И. Лужникова[1]
Научный руководитель Т. Н. Ямских[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Современные видеоигры давно перестали быть исключительно развлечением. Это полноценная форма искусства и интерактивного повествования, где нарратив играет ключевую роль в формировании игрового опыта. Всё чаще разработчики обращаются к продуманному языковому оформлению, понимая, что грамотный лингвистический дизайн усиливает погружение, влияет на эмоциональное восприятие и способствует более тесной связи игрока с персонажами и сюжетом.

Цель настоящего исследования – анализ лингвистического дизайна нарративного текста в видеоиграх как инструмента формирования выразительного и вовлекающего повествования.

Задачи:

1) рассмотреть изученность проблемы;

2) определить, что включает в себя понятие лингвистического дизайна;

3) проанализировать функции нарративного текста в игровых механиках;

4) выявить принципы эффективного лингвистического оформления текста в играх.

На сегодняшний день тема лингвистического дизайна нарративного текста в видеоиграх активно исследуется в разных областях, таких как лингвистика, культурология, медиапсихология и геймдев. Однако, несмотря на существующие работы, данная тема остаётся относительно новой и требует более детального изучения, учитывая последние достижения в области разработки игр и психологии.

Лингвистический дизайн – взаимодействие разноуровневых языковых средств, которые оформляют сайты и страницы в интернете [1]. Лингвистический дизайн формирует взаимодействие пользователя с различными медиаплатформами, в т. ч. с видеоиграми, через нарративный текст.

Нарративный текст – повествование в виде последовательности слов о каком-либо событии, открытии, личностях и т. п. [2]. Он играет большую роль в видеоиграх и выполняет ряд функций:

© Лужникова В. И., 2025

– создание эмоций – формирует эмоциональную связь между игроком и происходящим на экране;

– мотивация – объясняет цели игрока;

– объяснение правил мира игры – показывает рамки, в которых происходит повествование, и создаёт контекст для геймплея;

– объяснение механики и ограничений игрового процесса – даёт правдоподобные причины для ограничений игрового процесса и делает мир игры реалистичнее.

Для создания эффективного лингвистического дизайна нарративного текста в видеоиграх разработчикам необходимо применять несколько принципов:

– точность и ясность выражения мыслей – текст должен быть написан чётко и лаконично, без лишнего словесного мусора;

– грамматическая корректность – необходимо избегать грамматических ошибок;

– аккуратное и эффективное использование специфической терминологии – лучше использовать только ту специальную лексику, которую поймёт игрок из целевой аудитории игры;

– логическая организация текста – материал должен быть структурирован: например, если это диалоги, то должна быть чёткая система, где находится имя говорящего, его текст;

– учёт целевой аудитории – необходимо учитывать её потребности и принятые нормы жанра видеоигры [5].

Итак, лингвистический дизайн нарративного текста в видеоиграх имеет большое значение в формировании игрового опыта пользователя. Он не только выполняет функцию передачи информации, но и активно влияет на эмоциональное восприятие игрового мира и персонажей. Качественно разработанный лингвистический дизайн способствует созданию уникальной атмосферы и поддержанию интереса игрока, а также формирует взаимодействие между текстом и игровыми механиками, что делает сюжет в играх более глубоким и многослойным.

Список литературы

1. Атабекова А. А. Лингвистический дизайн Web-страницы: семиотические аспекты представления информации (на материале русского и английского языков) / А. А. Атабекова // Russian Journal of Linguistics. 2003. URL: cyberleninka.ru/article/n/lingvisticheskiy-dizayn-web-stranitsy .

2. Нарратив // Дзен. URL: dzen.ru/a/XvnGdSxP6WRdHRrR.

3. Зачем нужен нарратив в играх? Как игрок становится частью истории // Дзен. URL: dzen.ru/a/Z4d6N8AzDg_EgMYr.

4. Нарративные роли в игровой индустрии // Нарраторика. URL: narratorika.com/blog/narrativnye-roli-v-igrovoj-industrii.

5. Языковая корректность и структура научной статьи: улучшение в рамках доработки // DissHelp. URL: disshelp.ru/yazykovaya-korrektnost.

УДК 81'33

ВЛИЯНИЕ ТЕХНОЛОГИЙ НА ИЗУЧЕНИЕ ИНОСТРАННОГО ЯЗЫКА

Е. Е. Московских, И. П. Морошкина[1]
Научный руководитель Т. М. Лабушева[1]
старший преподаватель

[1]Сибирский федеральный университет

Влияние технологий на язык и мышление стало активно исследоваться с начала XXI в., когда современные коммуникационные средства начали существенным образом менять наши образцы поведения и способы взаимодействия.

В современных условиях, особенно в сфере технологий, связь между языком и мышлением приобретает особое значение. В последние десятилетия наблюдается значительный рост интереса к созданию систем искусственного интеллекта, которые могут обрабатывать язык.

Вместе с тем рост использования цифровых технологий среди студентов открывает новые горизонты для анализа влияния этих факторов на языковые практики и когнитивные процессы. Студенты, являясь активными пользователями различных информационных технологий, адаптируют свои речевые навыки и подходы к общению в соответствии с новыми условиями.

Целью настоящей работы является исследование того, как современные технологии трансформируют языковые практики и когнитивные процессы у студентов, а также выявление влияния этих изменений на их способы общения и понимания в современном обществе.

С целью анализа влияния технологий на изучение иностранного языка среди студентов разработано специализированное тестирование, в котором приняли участие 47 студентов технических специальностей в возрасте 18–23 лет. Опрос включает вопросы о частоте использования технологий, восприятии изменений в языке и осознании влияния цифровых инструментов на способности к критическому мышлению.

Результаты тестирования, представленные на рисунке, показали, что большинство студентов (51,1 %) регулярно прибегают к использованию приложений для перевода. В то же время мнения о влиянии этих приложений на понимание иностранных языков разделились: 34 % участников полагают, что приложения способствуют улучшению языкового понимания, тогда как столько же (34 %) считают, что они облегчают восприятие, но не способствуют запоминанию новых слов.

© Московских Е. Е., Морошкина И. П., 2025

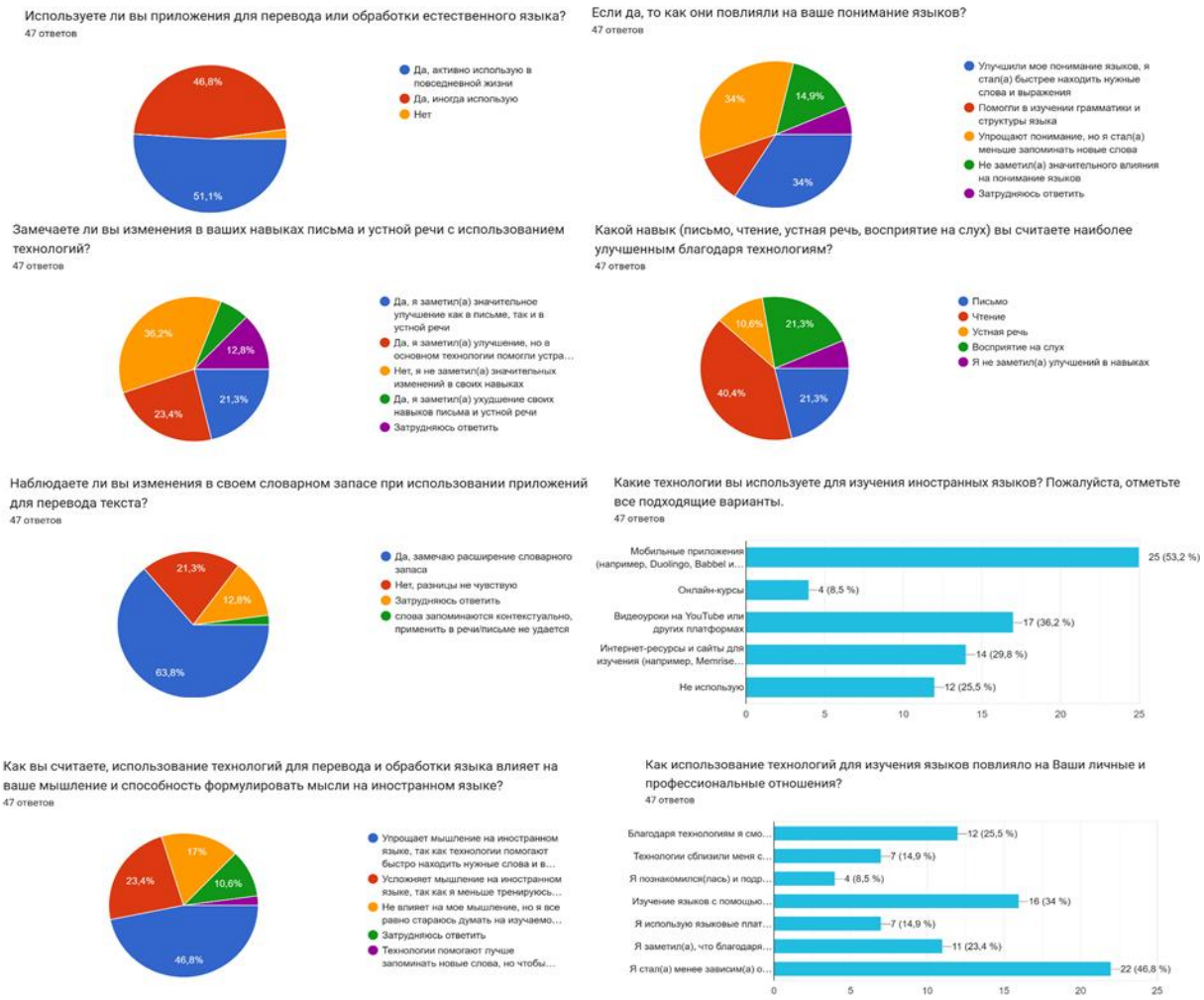


Рисунок 1. Результаты проведения опроса среди студентов в виде диаграмм

Анализ влияния на навыки письма и устной речи показал, что значительная часть обучающихся (36,2 %) не ощутила изменений. Однако 23,4 % отметили, что им удалось преодолеть языковой барьер, в то время как 21,3 % студентов сообщили о значительном прогрессе в обеих областях. Кроме того, 40,4 % респондентов подтвердили улучшение навыков чтения, а по поводу восприятия на слух и письма распределились поровну – по 21,3 %. Всего 10,6 % студентов отметили, что их устная речь также улучшилась благодаря использованию технологий.

Исследование влияния приложений для перевода текста показало положительные результаты: 63,8 % обучающихся отметили увеличение словарного запаса, что указывает на успешную интеграцию цифровых технологий в учебный процесс. Однако 21,3 % студентов не увидели значительных изменений, связанных с использованием переводческих функций, что подчёркивает необходимость дальнейшего анализа их эффективности.

Студенты технических специальностей при освоении новых языковых знаний чаще всего предпочитают мобильные приложения, на которые приходится 53,2 % от общего числа выборов. На втором месте расположились видеоуроки, которые выбрали 36,2 % респондентов. Интернет-ресурсы

занимают 29,8 %, а 25,5 % студентов вообще не используют никаких дополнительных материалов для обучения.

Вопрос о влиянии цифровых технологий на когнитивные процессы при изучении иностранных языков показал следующее распределение мнений:

– 46 % студентов отметили, что технологии упрощают мышление на иностранном языке;

– 23 %, напротив, указали на усложнение мыслительных процессов, объясняя это снижением самостоятельной практики формулирования мыслей;

– 17 % участников исследования сообщили, что технологии не влияют на их мышление, т. к. они сознательно стараются думать на изучаемом языке;

– 10 % респондентов затруднились с ответом, что может указывать на недостаточную рефлексию собственных когнитивных процессов.

Вместе со всем перечисленным исследование выявило многоаспектное влияние цифровых технологий на коммуникативные практики студентов, представленное в таблице.

Таблица 1

Влияние технологий на социально-профессиональные отношения

Эффект	Показатель, %
Повышение уверенности в общении с носителями языка	34
Расширение профессионального кругозора	25
Развитие открытости и коммуникабельности	23
Улучшение рабочих отношений с иностранными коллегами	14
Снижение зависимости от переводчиков	46

Таким образом, проведённое исследование подтвердило значительное влияние цифровых технологий на формирование языковых компетенций студентов. Результаты показывают, что технологии способствуют развитию словарного запаса и письменной речи, однако могут снижать самостоятельность мышления при изучении языка. Наиболее выраженный положительный эффект наблюдается в сфере профессиональной коммуникации. Полученные данные свидетельствуют о необходимости сбалансированного сочетания цифровых инструментов с традиционными методами обучения для достижения оптимальных образовательных результатов.

Список литературы

1. Бондаренко А. О. Психолингвистический взгляд на проблему соотношения языка и мышления / А. О. Бондаренко // Язык. Культура. Коммуникации. 2016. URL: journals.susu.ru/lcc/article/view/374/537.

2. Кабалоева Л. Б. Язык и мышление в свете современных психолингвистических представлений / Л. Б. Кабалоева // Вестник ТГУ им. Г. Р. Державина. Гуманитарные науки. 2009. URL: cyberleninka.ru/article/n/yazyk-i-myshlenie-v-svete-sovremennyh-psiholingvisticheskih.

УДК 81'33

ЭВОЛЮЦИЯ АНГЛИЙСКОГО ЯЗЫКА: КАК ЦИФРОВЫЕ ТЕХНОЛОГИИ МЕНЯЮТ ЯЗЫК

Д. Э. Норбоев, Н. К. Сурин, Е. Е. Красноборов[1]
Научный руководитель Н. В. Николаева[1],
старший преподаватель

[1]Сибирский федеральный университет

Исторически языки менялись медленно, и новые слова входили в обиход десятилетиями. Однако с развитием интернета и цифровых технологий лингвистические трансформации стали происходить значительно быстрее. Исследования показывают, что современный английский язык пополняется новыми словами в 10 раз быстрее, чем в доинтернетную эпоху (Language Monitor, 2023). Это явление обусловлено несколькими ключевыми факторами.

1. Глобальная коммуникация – интернет и социальные сети стирают границы между диалектами, распространяя слова и выражения по всему миру.

2. Мгновенное распространение – короткие сообщения в социальных сетях, таких как Twitter и TikTok, могут быстро стать вирусными и влиять на язык.

3. Технологический фактор – автокоррекция, искусственный интеллект и алгоритмы формируют новые языковые паттерны, создавая инновационные формы общения.

Эти факторы способствуют ускоренной эволюции языка в цифровую эпоху. Рассмотрим их более детально.

Аббревиатуры начали использоваться для экономии времени и пространства. В 1940-х гг., например, аббревиатуры типа ASAP (As Soon As Possible) стали стандартом в военной радиосвязи. В 1980-х гг. с появлением IRC (Internet Relay Chat) аббревиатуры, такие как FYI (For Your Information) и BTW (By The Way), стали широко популярными. В 2000-х с развитием СМС, ограниченных 160 символами, сокращения стали необходимостью. Примеры включают L8R (Later) и GR8 (Great).

В последние годы с развитием социальных сетей и мессенджеров появились новые сокращения, такие как TFW (That Feeling When) и ICYMI (In Case You Missed It), которые часто используются для передачи эмоций или распространения контента в мемах и маркетинге.

Причины популярности: экономия времени и пространства (сокращения позволяют быстро передавать смысл), чувство принадлежности (использование аббревиатур маркирует участников определённых онлайн-сообществ).

© Норбоев Д. Э., Сурин Н. К., Красноборов Е. Е., 2025

Пиктограммы используются для передачи смыслов с древних времён. В 1990-х гг. в Японии были созданы первые эмодзи для мобильных телефонов, что привело к их широкому распространению в интернет-коммуникации. Смайлики, такие как :) и :(, стали популярными символами для выражения эмоций.

Сегодня эмодзи и стикеры – неотъемлемая часть общения в социальных сетях и мессенджерах, таких как WhatsApp, Instagram и Facebook. Эти пиктограммы используются не только для передачи эмоций, но и для создания сложных смысловых конструкций.

Причины популярности эмодзи: универсальность (преодоление языковых барьеров), скорость и эффективность (быстрая передача эмоций и идей), символика и идентичность (обозначение принадлежности к культурным или социальным группам).

Сленг всегда был важной частью разговорной речи, особенно среди молодёжи. В 1950–60-х гг. в США молодёжь активно использовала сленг, который стал частью популярной культуры через музыку и кино. В эпоху интернета сленг приобрёл новые формы благодаря мемам, которые быстро распространяются по сети.

Мемы, которые представляют собой вирусные изображения или фразы, влияют на язык и становятся частью повседневной речи. Такие выражения, как YOLO (You Only Live Once) или FOMO (Fear Of Missing Out), были популяризированы интернет-культурой и теперь используются в различных контекстах – от личного общения до профессиональных сфер.

Причины популярности мемов: креативность и юмор (выражение сарказма и иронии, особенно востребованных среди молодёжи), идентичность и принадлежность (способ выражения групповой идентичности и следования трендам), скорость распространения (лёгкость восприятия и вирусный потенциал, способствующий быстрому проникновению в повседневную коммуникацию).

Цифровые технологии значительно ускорили эволюцию английского языка. Платформы мессенджеров, социальные сети и мемы играют ключевую роль в создании новых языковых форм – от аббревиатур до эмодзи и сленга. Технологии, такие как автоматическая коррекция и искусственный интеллект, также влияют на изменение лексики и грамматики языка.

С развитием новых технологий, таких как искусственный интеллект и машинное обучение, мы можем ожидать, что язык продолжит эволюционировать и изменяться с ещё большей скоростью. Эти изменения влияют не только на лексические практики, но и на способы социального взаимодействия в цифровую эпоху.

Список литературы

1. Baron N. S. Always On: Language in an Online and Mobile World / N. S. Baron. Oxford University Press, 2008.

2. Crystal D. Language and the Internet / D. Crystal. Cambridge University

Press, 2001.

3. Shifman L. Memes in Digital Culture / L. Shifman. MIT Press, 2013.

4. Squires L. Language Change in the Age of Digital Technology: The Influence of Autocorrection on the English Language / L. Squires // Journal of Language Technology and Society. 2015. Vol. 34. No. 1. Pp. 58–73.

5. Walther J. B. The Impact of Emoticons on Message Interpretation in Computer-mediated Communication / J. B. Walther, K. P. D'Addario // Social Science Computer Review. 2001. Vol. 19. No. 3. Pp. 324–340.

6. Засурский И. И. Интернет и языковая динамика / И. И. Засурский. М.: МГУ, 2018.

7. Кронгауз М. А. Русский язык на грани нервного срыва / М. А. Кронгауз. М.: Corpus, 2020.

8. Лутовинова О. В. Лингвистика интернет-коммуникации / О. В. Лутовинова. СПб.: Филологический факультет СПбГУ, 2019.

9. Рахилина Е. В. Когнитивный анализ цифрового дискурса / Е. В. Рахилина. М.: Языки славянской культуры, 2021.

10. Фрумкина Р. М. Язык и цифровая культура / Р. М. Фрумкина. М.: Либроком, 2017.

УДК 004.8:81'33

АНАЛИЗ ЭФФЕКТИВНОСТИ ПОПУЛЯРНЫХ НЕЙРОСЕТЕВЫХ ПРИЛОЖЕНИЙ ДЛЯ ИЗУЧЕНИЯ АНГЛИЙСКОГО ЯЗЫКА С ТОЧКИ ЗРЕНИЯ ИХ АДАПТАЦИИ К IT-СФЕРЕ

А. А. Полягошко, А. О. Озерова[1]
Научный руководитель Н. П. Думлер[1]
Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Современный рынок образовательных технологий предлагает множество приложений для изучения английского языка, однако специализированных решений, основанных на нейросетевых алгоритмах и ориентированных на профессиональные нужды *IT*-специалистов, в настоящее время не существует.

Целью настоящего исследования стало выявление степени эффективности и адаптивности популярных языковых приложений с ИИ-компонентами к задачам *IT*-английского.

Для достижения цели исследования были сформулированы следующие задачи:

1) проанализировать функционал популярных ИИ-приложений для изучения английского языка;

2) оценить их адаптивность к задачам *IT*-специалистов;

© Полягошко А. А., Озерова А. О., 2025

3) провести сравнительное тестирование и выделить наиболее подходящие решения.

Проведён обзор и сравнительный анализ таких платформ, как Claude, DeepSeek, DeepL Write, ELSA Speak, ReadLang и LingQ, с точки зрения их функционала для:

– изучения технической терминологии;

– моделирования профессиональных ситуаций;

– освоения письменной и устной коммуникации в IT-контексте.

В ходе работы протестирована возможность использования указанных инструментов в рамках пробных периодов, проанализированы их возможности настройки в своей области под нужды IT-специалистов, а также удобство интерфейса и глубина проработки профильной лексики.

По результатам исследования установлено, какие приложения максимально приближены к требованиям профессионального языка в сфере информационных технологий и могут быть рекомендованы в качестве эффективных вспомогательных инструментов для его изучения.

Авторами составлена таблица для сравнения оценок адаптивности по ходу проведения соответствующих назначению приложений тестов.

Таблица 1

Оценка эффективности нейросетевых приложений в контексте профессионального английского для *IT*-сферы

Приложение	**Тип теста / функционал**	**Пример задания/ запроса**	**Что понравилось**	**Что не понравилось**	**Оценка адаптивности (1–5)**
1	***2***	***3***	***4***	***5***	***6***
Claude	Объяснение терминологии + + Моделирование диалога + + Перевод	Переведи этот текст из *IT*-документации и сделай краткое резюме. Смоделируй диалог между интервьюером и *frontend*-разработчиком	Объясняет терминологию простым языком, приводит хорошие примеры. Легко моделирует на английском языке диалог собеседования *frontend*-разработчика. Умение переключаться между русским и английским языками в контексте *IT*. Возможность адаптировать уровень сложности языка под потребности пользователя	Иногда может давать слишком общие объяснения для узкоспециализированных технологий. Не всегда точно определяет уровень владения английским пользователя без явного указания. Ограниченная способность оценивать произношение или разговорную речь. Отсутствие возможности предоставлять аудиоматериалы для улучшения восприятия на слух	4

DeepSeek	Перевод технических терминов и фраз + + Генерация примеров кода с комментариями на английском	Перевод. Генерация кода	Чёткие и структурированные объяснения. Гибкость в адаптации уровня сложности. Поддержка технической терминологии – корректно использует термины. Быстрая генерация кода – даёт рабочие примеры с пояснениями	Иногда слишком общие ответы – если запрос расплывчатый, может дать поверхностное объяснение. Ограниченная работа с контекстом – если в диалоге много уточнений, может «забыть» ранние детали. Нет поддержки голоса/аудио – нельзя потренировать произношение. Не всегда идеальный перевод – в редких случаях технические термины переводятся не лучшим образом	3
DeepL Write	Перевод + + Редактирование текста	Технический текст об истории компьютеров; технологии *IPSec VPN*	Корректно обрабатывает технические тексты, улучшает стиль и грамматику. Есть интерактивная функция, которая вместе с вами подбирает идеальный перевод для контекста, задавая вопросы о значении, грамматическом роде, формате чисел, дат, времени и других языковых нюансах. Есть функция глоссария для единообразного перевода терминов	Всего один раз неверно передал аббревиатуру – «ИС» (Информационная система) перевёл буквально как *IC*	5
ELSA Speak	Произношение + + Распознавание английской речи	Тема программирования; настройки сетей	Распознаёт большинство популярных технических слов. Есть отдельный, довольно расширенный урок по лексике из программирования (*Software engineering*). Вовлекает в процесс, с ИИ-помощником можно общаться, как с репетитором	Лексическая база по техническим терминам ограничена. Довольно узкоспециализированные слова не распознаёт. Приложение учит коротким словам и выражениям, большие технические тексты с ним не получится разобрать	3

Окончание табл.

1	*2*	*3*	*4*	*5*	*6*
ReadLang	Чтение с использованием расширения	Чтение информации на английском сайте	Удобно, что переводить можно сразу в тексте по одному или нескольким словам. Возможность выделять для перевода как отдельные слова, так и словосочетания	Расширение работает только в *Google Chrome*. Медленно работает. Не всегда корректно переводит специализированные термины	3
LingQ	Перевод *IT*-документации + + Изучение технических подкастов с транскрипцией	Фрагмент технической статьи с сайта *Medium*. Карточки на базе документации	Возможность импортировать реальную техническую документацию и изучать её в интерактивном формате. Отслеживание прогресса. Возможность создавать собственные коллекции специализированных *IT*-текстов. Удобная синхронизация между устройствами	Отсутствие специализированного контента для программистов, необходимость самостоятельного поиска и импорта. Интерфейс не оптимизирован для работы с техническими текстами (например, с кодом). Ограниченный бесплатный функционал. Ограниченные возможности для практики письменной технической коммуникации. Нет специальных функций для работы с программным кодом (подсветка синтаксиса, форматирование)	2

По итогам сравнения, наиболее функциональными и адаптированными под задачи *IT*-сферы оказались платформы *DeepL Write* и *Claude*. Они смогут хорошо помочь *IT*-специалисту в работе и изучении английского языка для профессиональных целей.

Список литературы

1. The Best AI Platforms for Academic Research and Studying // Educatly. 2025: URL: educatly.com/blog/594/the-best-ai-platforms-for-academic-research-and-studying.

2. Carter E. The Best Free AI Tools to Learn English / E. Carter // Global English Test. 2024. URL: globalenglishtest.com/the-best-free-ai-tools-to-learn-english.

УДК 81'33

ЗАМЕНИТ ЛИ ИИ ПЕРЕВОДЧИКОВ?

М. А. Рыбин, Т. А. Эсавулов, Е. Д. Мурашко[1]
Научный руководитель Н. В. Николаева[1]
старший преподаватель

[1]*Сибирский федеральный университет*

Переводческая отрасль пережила значительные изменения за последние 100 лет благодаря технологическим прорывам и глобализации. «Машинный перевод прошёл путь от простой замены слов до сложных нейросетевых систем», – отмечает Д. Р. Головко [1, с. 24]. Первоначально перевод выполнялся исключительно вручную, с использованием только языковых навыков и когнитивных способностей переводчика. С развитием международной торговли и политики, а также благодаря технологическим новшествам, таким как синхронный перевод и машинный перевод, отрасль преобразилась. Однако, как подчёркивает Н. К. Гарбовский, «язык – это не просто код, а живая система культурных смыслов» [2, с. 4], что требует человеческого подхода.

Исторический контекст. «Синхронный перевод стал революцией XX в.», – пишет Головко [1, с. 25]. Действительно, с развитием международных отношений спрос на переводчиков вырос, что привело к появлению устного перевода, синхронного и последовательного. Появление технологий синхронного перевода в конце XX в. сделало возможным мгновенное переведение речи на несколько языков. В цифровую эпоху технологии, такие как удалённый видеоперевод и онлайн-системы, значительно расширили доступность переводческих услуг. Однако современные исследователи предупреждают: «Технологии ускорили передачу слов, но не всегда смыслов» [3, с. 5].

Текущее состояние ИИ и машинного перевода. «Нейросетевые системы достигли 85 % точности в технических текстах», – констатирует Linguise [4]. Сегодня ИИ играет ключевую роль в процессе перевода. Системы, использующие распознавание речи и машинный перевод, способны обеспечить синхронный перевод в реальном времени. Однако Гарбовский и Костикова уточняют: «ИИ распознаёт слова, но часто “не слышит” интонации и культурных подтекстов» [3, с. 10].

Машинный перевод, в частности нейронный, значительно улучшился благодаря обучению на больших объёмах данных. «Автоматический перевод сокращает время обработки документов на 70 %», – отмечается в исследовании Linguise [4]. Однако, как справедливо замечает Головко,

© Рыбин М. А., Эсавулов Т. А., Мурашко Е. Д., 2025

«эффективность резко падает при работе с художественными текстами» [1, с. 27].

Сильные стороны человека-переводчика. «Человек-переводчик остаётся незаменимым в дипломатии и медицине», – подчёркивают Гарбовский и Костикова [3, с. 15]. Действительно, несмотря на преимущества ИИ, человек-переводчик продолжает обладать уникальными навыками. «Ни один алгоритм не способен полностью имитировать человеческую интуицию», – добавляет Гарбовский [2, с. 4].

Ограничения ИИ-перевода. «При переводе идиом системы ИИ дают сбой в 60 % случаев», – свидетельствуют данные исследования [3, с. 12]. Основным ограничением является неспособность передавать культурные нюансы. «Это цена за отсутствие живого языкового опыта», – комментирует Головко [1, с. 28].

Этические проблемы. «ИИ-переводчики могут невольно тиражировать стереотипы», – предупреждают Гарбовский и Костикова [3, с. 18]. Также существует риск нарушения конфиденциальности. «Без тщательного контроля данные обучения становятся источником предвзятости», – добавляет Linguise [4].

Гибридные модели интерпретации. «Оптимальное решение – симбиоз технологий и человеческого контроля», – предлагают Гарбовский и Костикова [3, с. 20]. Действительно, такие модели позволяют использовать сильные стороны ИИ. «Такие системы уже сокращают ошибки на 40 %», – подтверждает Linguise [4].

Будущее перевода. «Будущее – за разумным сочетанием искусственного интеллекта и человеческого опыта», – заключает Головко [1, с. 29]. В ближайшие 5–10 лет ожидается улучшение пользовательского опыта. Как отмечают Гарбовский и Костикова, «технологии изменят, но не заменят профессию переводчика» [3, с. 21].

Сравнение ИИ и человека-переводчика. Авторами проведено сравнение по разным параметрам ИИ и человека-переводчика и выделены следующие плюсы и минусы (табл.).

Таблица 1

Сравнительная таблица ИИ и человека-переводчика

Пере-водчик	**Плюсы**	**Минусы**
1	***2***	***3***
ИИ	– Быстро переводит большие объёмы текста; – доступен 24/7 – можно пользоваться в любое время; – бесплатно или дёшево (*Google Translate*, *DeepL* и т. д.); – постоянно улучшается благодаря обучению на больших данных.	– Не всегда понимает контекст и смысл сказанного; – может делать глупые ошибки – особенно в сложных или двусмысленных фразах; – не чувствует эмоций, интонации, юмора или культурных особенностей; – не подходит для официальных, художественных или точных переводов без проверки человеком.

Окончание таблицы 1

1	*2*	*3*
Человек	– Понимает контекст, нюансы и эмоции; – может адаптировать перевод к аудитории и культуре; – делает творческий перевод, а не просто дословный; – способен исправить и адаптировать фразы на лету.	– Дорогой (особенно профессионалы); – требует времени – не так быстр, как ИИ; – не всегда доступен (вне рабочего времени, по расписанию и т. д.).

Современные технологии машинного перевода стремительно развиваются, предлагая скорость, доступность и экономичность (24/7, бесплатные сервисы, обработка больших объёмов). Однако ИИ не способен полностью заменить человека – он ошибается в контексте, эмоциях, культурных нюансах и сложных текстах.

Человеческие переводчики остаются незаменимыми там, где нужны точность, адаптация к аудитории и творческий подход, но их услуги дороже и требуют времени.

Оптимальное решение – симбиоз технологий и человеческого контроля: ИИ для рутинных задач и черновых переводов, человек – для финальной шлифовки и сложных кейсов. Будущее отрасли лежит в разумном сочетании этих подходов.

Список литературы

1. Головко Д. Р. Особенности и виды машинного перевода / Д. Р. Головко // Компьютерные и информационные науки. 2020. № 4. С. 24–29.

2. Гарбовский Н. К. Введение / Н. К. Гарбовский // Теория перевода. М.: МГУ, 2007. 4 с.

3. Гарбовский Н. К. Интеллект для перевода: искусный или искусственный? / Н. К. Гарбовский, О. И. Костикова // Теория перевода. 2019. № 4. С. 3–21.

4. Что такое AI-перевод и преимущества перевода веб-сайтов // Linguise. URL: linguise.com/ru/%D0%B1%D0%BB%D0%BE%D0%B3/%D1.

УДК 81'33

ИЗУЧЕНИЕ АНГЛИЙСКОГО ЯЗЫКА ЧЕРЕЗ ПЕСНИ: ПСИХОЛИНГВИСТИЧЕСКИЙ ПОДХОД

А. А. Хлопова[1]
Научный руководитель – Н. В. Николаева[1]
старший преподаватель

[1]*Сибирский федеральный университет*

В данной статье рассматривается эффективность использования песенного материала как инструмента обучения английскому языку. На основе практического опыта демонстрируется, как специально отобранные музыкальные композиции способствуют развитию фонетических навыков, расширению словарного запаса и автоматизации грамматических конструкций у учащихся начального уровня (*A*1–*A*2). Приводятся конкретные методики работы с песенным материалом, анализируются практические результаты их применения и делаются выводы о преимуществах данного подхода.

Традиционные методы изучения английского языка, такие как заучивание правил и механическое повторение, часто не обеспечивают достаточной вовлечённости и мотивации обучающихся [3]. Согласно исследованиям И. В. Смирновой использование песен значительно повышает эффективность освоения языка благодаря комплексному воздействию на когнитивные и эмоциональные процессы [3]. Песни позволяют учить язык в естественном контексте, развивать фонетическое восприятие и расширять словарный запас.

В рамках педагогической практики в музыкальной школе была разработана методика использования современных англоязычных песен для обучения английскому языку учащихся с начальным уровнем владения (*A*1–*A*2). Занятия проводились в группах подростков 14–16 лет.

В процессе обучения применялись специально подобранные композиции, такие как *Sugar* (*Maroon* 5), *I Love You Like A Love Song* (*Selena Gomez*) и *Attention* (*Charlie Puth*). Эти песни были выбраны по критериям, разработанным Л. П. Красиной [1]: простая лексика (уровень *A*1–*A*2), чёткое произношение и наличие базовых грамматических конструкций. Как отмечает Н. А. Петрова, для эффективного обучения необходимо отбирать песни с чёткой артикуляцией и умеренным темпом [2].

Анализ песни Sugar (Maroon 5)

Работа с песней Sugar была сосредоточена на нескольких ключевых лингвистических аспектах.

© Хлопова А. А., 2025

1. Лексические единицы. Особое внимание уделялось словам, связанным с выражением желаний и предпочтений: want, need, sweet, taste. Учащиеся составляли собственные высказывания с этими словами, создавая контекстуальные связи. Например, фраза I want that red velvet стала основой для изучения конструкции «want + указательное местоимение + + существительное» [1]. Слово velvet («бархат») анализировалось с точки зрения его прямого значения и метафорического использования в контексте песни.

2. Грамматические конструкции. В строке it tastes so good исследовалась модель «подлежащее + глагол + наречие + прилагательное» и употребление интенсификатора so перед прилагательным [2]. Учащимся предлагалось создать аналогичные конструкции с другими глаголами чувственного восприятия: smell, look, feel, sound.

3. Фонетические особенности. Отрабатывалось произношение дифтонга [eɪ] в словах taste, baby, day, а также редукция безударных слогов, характерная для естественной английской речи [5]. Учащиеся выделяли ритмические группы в строках песни и имитировали их с сохранением оригинальной интонации.

Анализ песни I Love You Like A Love Song (Selena Gomez)

При работе с композицией акцент делался на следующих аспектах.

1. Сравнительные конструкции. Строка I love you like a love song позволила изучить структуру сравнения с союзом like [3]. Студенты создавали собственные сравнения по модели «глагол + объект + like + существительное с неопределённым артиклем»: I remember you like a dream; I miss you like a lost friend.

2. Эмоционально окрашенная лексика. В тексте песни выделялись слова, выражающие чувства: love, forever, beautiful, melody. Учащиеся составляли словарные карты, группируя лексику по эмоциональному спектру, что соответствует методике, описанной Е. Г. Титовой [4].

3. Повторяющиеся структуры. Анализировались параллельные конструкции в припеве песни, которые способствуют автоматизации речевых моделей. Например, повторение фразы I love you в различных контекстах помогало учащимся усвоить базовую модель выражения чувств в английском языке [1].

Анализ песни Attention (Charlie Puth)

Данная композиция оказалась особенно продуктивной для учебного процесса.

1. Модальные конструкции. В строках You just want attention и You don't want my heart изучались способы выражения желания и отрицания с глаголом want [2]. Особое внимание уделялось наречию just, которое в данном контексте имеет значение «только лишь», что создаёт определённый эмоциональный оттенок высказывания.

2. Выражение предположения. Строка Maybe you just hate the thought of me with someone new использовалась для изучения способов

выражения предположения и неуверенности через маркер maybe [4]. Учащиеся анализировали разницу между конструкциями «maybe + подлежащее + глагол» и «подлежащее + модальный глагол (might/could) + + глагол», составляя собственные высказывания.

3. Абстрактная лексика. Разбирались абстрактные существительные, такие как attention, thought, heart (в переносном значении), и их использование в эмоциональном контексте [5]. Студенты создавали семантические поля для этих слов, добавляя связанные по смыслу глаголы и прилагательные: attention – pay, seek, want, full, undivided.

4. Фразовые глаголы. В песне выделялись фразовые глаголы, такие как run out, figure out, которые характерны для разговорного английского языка [1]. Учащиеся составляли мини-диалоги с использованием этих выражений в различных контекстах.

Таким образом, использование песен в обучении английскому языку является эффективным инструментом для развития навыков восприятия на слух, расширения словарного запаса и преодоления языкового барьера. Выбор композиций с базовой лексикой и чётким произношением позволяет сделать процесс обучения доступным и увлекательным, особенно для начинающих [2].

Детальный анализ лексических единиц, грамматических конструкций и фонетических особенностей в контексте песен создаёт прочные ассоциативные связи и способствует более эффективному усвоению языкового материала. Эмоциональный компонент песен активизирует процессы запоминания и снижает психологические барьеры при использовании иностранного языка [4].

Практическое применение песенных методик подтверждает теоретические положения, изложенные в работах И. В. Смирновой [3] и Н. А. Петровой [2] о том, что музыкальные подходы к обучению способствуют формированию устойчивых языковых навыков и повышению мотивации к изучению иностранного языка. Перспективным направлением дальнейшей работы может стать разработка комплексной методической системы использования современных песен для различных уровней владения языком с учётом принципов коммуникативного подхода и индивидуализации обучения.

Список литературы

1. Красина Л. П. Английский язык через песни / Л. П. Красина // Методика преподавания иностранных языков. 2008. № 3. С. 45–52.

2. Петрова Н. А. Методика обучения английскому языку с помощью музыки / Н. А. Петрова // Иностранные языки в школе. 2015. № 7. С. 32–38.

3. Смирнова И. В. Музыка в обучении иностранным языкам / И. В. Смирнова // Педагогические науки. 2010. № 5. С. 74–81.

4. Титова Е. Г. Психолингвистические аспекты обучения через музыку / Е. Г. Титова // Вопросы психологии и лингвистики. 2012. № 2. С. 118.

5. Шестакова А. М. Современные методы преподавания английского / А. М. Шестакова // Инновации в образовании. 2016. № 4. С. 55–63.

UDC 81'33

LEARNING ENGLISH FOR A CAREER IN IT: ESSENTIAL RESOURCES AND SKILLS

E. V. Khlystova, E. A. Tikhonov[1]
Research Supervisor A. T. Gordeeva[1],
senior lecturer

[1]*Siberian Federal University*

English has become the universal language of the IT industry, playing a key role in international communication, access to knowledge, and career growth. In a globalized world, proficiency in English has become a mandatory skill for programmers, data analysts, system administrators, and other IT professionals. It is not only a tool for communication but also an important instrument for professional development [1].

The purpose of this study is to explore the role of English language proficiency in the professional development of IT specialists and to identify effective tools and strategies for learning English in the context of the technology sector.

The objectives of this study are as follows:

1) to examine the significance of English for career growth in the field of information technology;

2) to identify the key English language skills required by IT professionals;

3) to explore the most relevant educational platforms, tools, and resources for learning English in the IT field;

4) to provide practical recommendations for improving English proficiency among IT learners.

The IT industry is inherently international. Working in distributed teams, participating in online conferences, and interacting with clients and colleagues from other countries require strong English skills. Without them, there are difficulties in understanding tasks and effective communication. Moreover, a significant amount of technical documentation, educational materials, and professional courses are exclusively available in English. Resources such as Stack Overflow, GitHub, Coursera, and others are primary sources of information for specialists. Without knowledge of the language, using these platforms becomes extremely limited [2].

English also opens doors to new career opportunities. Many international companies list it as a mandatory requirement for applicants. Obtaining international certifications, participating in internships, and transitioning to remote work – all of these are related to the need to be proficient in English [4].

For effective language acquisition in the IT field, it is necessary to focus on developing specific skills. One of them is mastering technical vocabulary. Terms

© Хлыстова Е. В., Тихонов Е. А., 2025

such as debug, deploy, API, or cloud computing are commonly used in the professional environment. Mastering them through specialized courses or dictionaries helps professionals adapt quickly to professional communication [5].

An important aspect is reading skills. Technical articles, blogs, forums, and documentation all require the ability to quickly navigate through text and extract useful information. Regularly reading materials in English allows one to not only expand vocabulary but also stay up to date with the latest industry trends.

Writing skills are essential for documenting code, preparing reports, and business correspondence. Accuracy and clarity in writing are especially important when interacting with international teams. Regular practice, the use of templates, and grammar checkers help improve written communication.

Oral communication and listening comprehension play a key role in meetings, presentations, and interviews. Listening to podcasts, participating in webinars, and interacting with native speakers develop these skills. Resources like "Business English Pod", YouTube training channels, and language exchange programs help with more natural language comprehension [6].

To achieve sustainable results, it is important to use a variety of educational resources. Online courses such as English for Career Development on Coursera are focused on developing language skills in the professional field. Courses on Udemy and IEEE Learning Network allow for in-depth study of business English, including specialized vocabulary. Apps like Duolingo and Memrise are suitable for regular vocabulary and grammar practice, while HelloTalk provides the opportunity to communicate with native speakers.

Additionally, it is useful to refer to specialized platforms. Stack Overflow helps learn terminology in the context of real tasks, GitHub helps understand how professionals format documentation and comment on code. FluentU offers vocabulary lists tailored to the needs of IT specialists. Podcasts and videos dedicated to programming and career development help combine learning English with professional growth [3; 7].

To successfully learn English, one must set clear goals: whether it is passing an interview, reading technical documentation, or obtaining a certification. Regular practice, even for 20–30 minutes a day, significantly improves language proficiency. It is important not to fear mistakes – they are part of the learning process. Engaging in communities such as Reddit or professional LinkedIn groups allows you to apply the language in real-life situations and exchange experiences.

Thus, proficiency in English in the IT field is not just an advantage but an essential condition for professional success. The comprehensive development of all language skills, the use of available tools, and involvement in the English-speaking professional environment allow one to reach a new level and feel confident in the international IT community.

References

1. Ebite S. The Importance of English Proficiency in the IT Industry / S. Ebite. 2024. URL: linkedin.com/pulse/importance-english-proficiency-industry-

samuel-ebite-y8kfc.

2. The importance of English in technology careers. 2020. URL: cuti.org.uy/en/blog/la-importancia-del-ingles-en-las-carreras-tecnologicas.

3. The 10 Best Online Courses for Learning English of 2025. 2024. URL: intelligent.com/best-online-courses/learning-english.

4. Brown M. English Is the Language of Tech, and Improving Your Skills is the Best Path to Success / M. Brown. 2022. URL: engineering.com/english-is-the-language-of-tech-and-improving-your-skills-is-the-best-path-to-success.

5. 15 Information Technology Vocabulary Words for English Learners. 2024. URL: fluentu.com/blog/english/information-technology-vocabulary.

6. Gulati B. 12 best English podcasts for every level + 5 tips to learn from them / B. Gulati. 2024. URL: preply.com/en/blog/the-best-podcasts-to-help-you-learn-english.

7. Gerencer T. 10 Best Apps to Learn a New Language / T. Gerencer. 2022. URL: hp.com/gb-en/shop/tech-takes/best-language-learning-apps.

УДК 004.8:316.77

ОЗВУЧИВАНИЕ ТЕКСТА С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Е. Б. Юрова, Р. П. Тетерин[1]
Научный руководитель А. А. Романовская[1]
старший преподаватель

[1]*Сибирский федеральный университет*

В мире информационных технологий искусственный интеллект перестал быть фантастикой и стал неотъемлемой частью нашей повседневной жизни. Одним из его ярких и востребованных направлений является синтез речи – технология, позволяющая ИИ «озвучивать» текст. Голос, созданный с помощью ИИ, способен передавать эмоции, интонации и нюансы, делая общение с машиной не только эффективным, но и увлекательным. Сегодня искусственные голоса звучат с экрана смартфона, помогая ориентироваться в незнакомом городе, или поддерживают беседу с виртуальными ассистентами, такими как *Siri* и Алиса.

В настоящем исследовании рассмотрено, как работает озвучка текстов с помощью современных технологий и как эти технологии развиваются.

Современные системы синтеза речи основаны на нейронных сетях и глубоком обучении, что позволяет добиться невероятной реалистичности. Рассмотрим две наиболее передовые технологии.

1. *WaveNet* от *DeepMind* – это модель, генерирующая звук на уровне отдельных сэмплов. Она может создавать довольно натуралистичную речь,

© Юрова Е. Б., Тетерин Р. П., 2025

учитывать динамику и нюансы интонации. Этот метод способен точно воспроизводить акценты и эмоции, что делает речь живой и естественной.

2. *Tacotron* 2 от *Google* сочетает в себе два этапа: преобразование текста в спектрограмму, а затем использование *WaveNet* для её преобразования в звук. Это даёт речь с идеальной интонацией и эмоциональной окраской, делая её максимально близкой к человеческой.

Такие системы находят применение в самых разных сферах:

– голосовые ассистенты;

– образование – синтез речи используется для озвучивания учебников, курсов и аудиокниг;

– мультимедиа и развлечения – ИИ помогает озвучивать фильмы, игры и мультфильмы, адаптируя речь под действия персонажей и облегчая локализацию контента;

– бизнес и поддержка клиентов – ИИ-голосовые системы автоматизируют работу кол-центров и клиентских сервисов, обеспечивая круглосуточную поддержку.

Для того чтобы показать принцип работы озвучки текста, мы написали программу, которая является очень упрощённой версией ИИ. Программа основана на общедоступных библиотеках, таких как gTTS, playsound и SpeechRecognition:

```
def listen():
    r = sr.Recognizer()
    with sr.Microphone() as source:
        print("Скажите вашу команду: ")
        audio = r.listen(source)
    try:
        our_speech = r.recognize_google(audio, language="ru")
        print("Вы сказали: " + our_speech)
        return our_speech
    except sr.UnknownValueError:
        return "Ошибка"
    except sr.RequestError:
        return "Ошибка"

def this_command(message):
    message = message.lower()
    if "привет" in message:
        say_message("Привет!")
    elif "расскажи о себе" in message:
        say_message("Я голосовой помощник, созданный на основе библиотек для
искусственного интеллекта!")
    elif "пока" in message:
        say_message("До скорой встречи!")
        exit()
    else:
        say_message("Извините, я вас не понимаю!")

def say_message(message):
    voice = gTTS(message, lang="ru")
    file_voice_name = "_audio_" + str(time.time()) + "_" + str(random.randint(0,
100000)) + ".mp3"
    voice.save(file_voice_name)
```

```
    playsound.playsound(file_voice_name)
    print("Голосовой ассистент: " + message)

if __name__ == '__main__':
    say_message("Привет, меня зовут Голос, я ваш голосовой ассистент!")  #
Приветствие при запуске программы
    while True:
        command = listen()
        this_command(command
```

В коде есть три функции: listen, this_command и say_message.

Функция listen отвечает за прослушивание команды пользователя через микрофон. Создаётся объект Recognizer, который используется для распознавания речи. С помощью r.listen(source) программа ждёт, пока пользователь скажет что-то. После этого происходит попытка распознать речь с помощью Google API. Если распознавание успешно, возвращается распознанный текст. Если произошла ошибка, возвращается сообщение об ошибке.

Функция this_command обрабатывает распознанное сообщение.

И, наконец, функция say_message отвечает за преобразование текста в речь и воспроизведение аудио; создаёт объект gTTS, который принимает текст и язык (в данном случае русский); сохраняет аудиофайл и воспроизводит его с помощью playsound.

Конечно, мы не получаем настоящий ИИ, т. к. для этого программа должна уметь саморазвиваться, адаптироваться и выполнять огромное количество команд, а наша ограничена заданным функционалом. Но она является простой моделью ИИ, которая способна эмитировать работу настоящего ИИ и показывает принцип его работы в озвучке текста. А также данная программа показывает, что любой человек абсолютно бесплатно может сам создать программу, которая будет озвучивать текст, и настроить её под свои задачи.

Синтез речи на базе ИИ уже не просто технологическая новинка – это важный инструмент, меняющий наш способ общения с машинами. Сегодня голос ИИ сопровождает нас повсюду: он подсказывает дорогу, озвучивает учебные материалы, отвечает на звонки и даже шутит в видеоиграх. Благодаря достижениям таких систем, как *WaveNet* и *Tacotron*, машина действительно начинает «говорить по-человечески» – с эмоциями, интонацией и выразительностью. Однако за этим прогрессом стоят и вызовы: от этических споров до угроз приватности. Всё это требует осознанного подхода к внедрению и использованию таких технологий.

Список литературы

1. Опанасюк И. В. Синтез речи и его применение в интеллектуальных системах / И. В. Опанасюк. М.: МГУ, 2020.

2. Кудинов Д. А. Искусственный интеллект: технологии и перспективы / Д. А. Кудинов. СПб.: Питер, 2021.

3. Как это работает? Синтез речи. URL: yandex.ru/blog/company/kak-eto-rabotaet-sintez-rechi.

4. SpeechRecognition. URL: pypi.org/project/SpeechRecognition.

5. Как создать голосового помощника на Python. URL: selectel.ru/blog/tutorials/voice-assistant.

6. WaveNet: новая модель для генерации человеческой речи и музыки. URL: habr.com/ru/companies/Voximplant/articles/309648.

УДК 794*008*81.374

ПРОБЛЕМА ДЕФИНИЦИИ ТЕРМИНОВ В ОТЕЧЕСТВЕННОЙ ИГРОВОЙ ИНДУСТРИИ

А. С. Яковлев[1]

Научный руководитель Т. Н. Ямских[1]

Кандидат педагогических наук, доцент

[1]*Сибирский федеральный университет*

Игровая индустрия во всём мире сегодня является не только перспективной сферой развлечений, история которой началась в середине 50-х гг. прошлого века, но и обширной сферой экономики [1, с. 33]. Многообразие направлений игровой индустрии (настольные, азартные, спортивные, видеоигры) обуславливает наличие разобщённости в использовании профессиональной терминологии.

История российской игровой индустрии имеет более позднее начало, одним из её основоположников можно считать А. Л. Пажитнова, создавшего игру «Тетрис» в 1985 г. Однако этот период развития игровой индустрии нельзя назвать периодом активного появления специальной терминологии, поскольку политические события того времени способствовали обособленному развитию сферы и культурный обмен с авангардистом в лице США был затруднён. Вся используемая терминология игровой индустрии 80-х гг. сводилась к применению незначительного числа профессионализмов и сленговых выражений.

Существенные изменения в формировании терминологии отечественной индустрии игр произошли в период «эпохи Горбачёва», когда отечественный рынок заполонили преимущественно западные и японские продукты: видеоигры, оборудование, программное обеспечение и иные материалы, популяризирующие продукты индустрии, – журналы, пособия, плакаты и т. д. С развитием внутреннего рынка начали образовываться и отечественные организации по созданию видеоигрового контента,

© Яковлев А. С., 2025

формируясь благодаря смежным сферам и внешним кругам индустрии (потребительским).

Недостаток отечественных решений, необходимых в производстве видеоигр, привёл разработчиков к единственному выходу – заимствованию. Заимствование решений предполагает их эффективное использование, а значит, создание методик и культуры работы с ними. Так, основываясь на западной экспертизе и создании продуктов, адаптированных к местным реалиям, начала формироваться терминология отечественной игровой индустрии.

Анализ работ исследователей специальной лексики сферы игровой индустрии показал, что наиболее часто выделяют специальные термины, терминоиды и профессионализмы [2, с. 3]. Большую часть профессиональной лексики в игровой индустрии занимают именно термины. В рамках статьи под термином мы будем понимать определение О. Н. Лагута: «термин – в лексической стилистике: слово или словосочетание специального (научного, технического и т. п.) языка, создаваемое (принимаемое, заимствуемое) для точного выражения специальных понятий и обозначения специальных предметов» [3, с. 132].

Профессионализмы и терминоиды менее активно используются специалистами игровой индустрии из-за специфики существенного заимствования слов для профессионального общения. Например, слово «спавн» (от англ. *spawn*), означающее точку появления какой-либо сущности (например, существа или предмета), является заимствованием из западной игровой индустрии, где это слово, в свою очередь, заимствовано из биологии (означает «многочисленный выводок, потомство»).

Большое количество посредников между первоначальной семантикой слова и отечественным разработчиком не даёт ему вариантов для использования, кроме профессиональной среды, переводя его в ряд терминов с однозначной трактовкой. Однако, посредничество, а также частично обособленное развитие организаций по созданию видеоигр и приток специалистов из сторонних индустрий (остающийся основным источником кадров) порождают неоднозначность дефиниций терминов. Один и тот же термин, используемый разработчиком из смежной индустрии (например, киноиндустрии) и разработчиком, на которого повлияли «школы» западной игровой индустрии, может трактоваться по-разному, вызывая временные трудности при взаимодействии, пока одно из толкований не станет ведущим или не будет выбран компромиссный сторонний термин.

Стоит отметить, что наиболее остро проблема дефиниции терминов наблюдается в профессиональных специализациях, возникших исключительно благодаря индустрии и не существующих вне её (например, гейм-дизайн или управление игровыми проектами). Например, одними из самых распространённых терминов с неоднозначным определением в гейм-дизайне являются «иммерсивность», «метагейм», «фан», «кор-геймплей». Одна из причин такой ситуации может заключаться в отсутствии единых «догматов игровой индустрии».

Наиболее часто с проблемой разрозненности трактовок игровой терминологии специалисты сталкиваются на начальном этапе адаптации в новой студии или на новом проекте. Профессиональное общение с коллегами может быть искажено, что приводит к ошибкам или недопониманию при работе.

Анализ практики по нивелированию или предупреждению подобных ситуаций отечественных игровых компаний показал, что наиболее часто используются следующие локальные меры:

– составление терминологии проекта;

– отсылки к известным авторам при общении;

– использование смежных терминов или синонимов;

– обучение сотрудников на одобренных материалах;

– поиск компромиссного (часто обобщающего) значения термина;

– создание новых профессионализмов или заимствование из других индустрий.

Однако, все эти меры не предлагают системного решения проблемы, необходимость в котором не уменьшается, как и количество дефиниций терминов.

Одно из возможных решений проблемы дефиниции терминов в отечественной игровой индустрии мы видим в создании базы знаний о процессах разработки, адаптированной к реалиям российской игровой индустрии с использованием стандартизированной терминологии. Это позволит формировать у новых членов индустрии не только единообразную терминологию и актуальные образы мысли при трудовой деятельности, но и общее понимание профессиональной деятельности. Первые шаги в данном направлении профессиональными сообществами уже сделаны: например, сообщество «Манжеты гейм-дизайнера», позиционирующее себя как объединение профессиональных разработчиков игр, разместило на сайте раздел «Библия ГД», где собраны статьи отечественных разработчиков [4].

Обобщая вышесказанное, можно сделать вывод, что профессиональная лексика игровой индустрии подвижна и подвержена постоянным изменениям, однако, требуется осуществление поиска общего решения проблемы дефиниции терминов для развития отечественной игровой индустрии.

Список литературы

1. Ветушинский А. С. Краткая история игровой индустрии // Видеоигры: введение в исследования / А. С. Ветушинский. Томск: ТПУ, 2018. С. 32–74.

2. Горностаев С. В. Специальная лексика сферы игровой индустрии / С. В. Горностаев // Вестник ННГУ. 2016. № 6. URL: cyberleninka.ru/article/n/spetsialnaya-leksika-sfery-igrovoy-industrii.

3. Лагута (Алешина) О. Н. Стилистика. Культура речи. Теория речевой коммуникации: словарь терминов. Ч. 2 / О. Н. Лагута (Алешина). Новосибирск: НГУ, 2000.

GD CUFFS. URL: gdcuffs.com/gd-bible.

Системный анализ, управление и программная инженерия

УДК 004.45

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ СНИЖЕНИЯ НАГРУЗКИ НА CPU И RAM ПУТЁМ ДЕАКТИВАЦИИ НИЗКОПРИОРИТЕТНЫХ ЗАДАЧ

А. В. Бадьин[1], В. Л. Никандров[1]

Научный руководитель А. В. Хныкин[1]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

Современные персональные компьютеры представляют собой сложные вычислительные системы, которые ежедневно обеспечивают выполнение широкого спектра задач. Однако с увеличением функциональности операционных систем и программного обеспечения всё более актуальной становится проблема нерационального распределения ресурсов. Значительная часть вычислительных мощностей центрального процессора (ЦП) и оперативной памяти (ОЗУ) нередко оказывается занята фоновыми процессами и службами, которые не имеют прямого отношения к текущим задачам пользователя. Эти необязательные процессы, такие как обновления в фоновом режиме, телеметрия или неиспользуемые службы, могут существенно снижать производительность системы, особенно при работе ресурсоёмких приложений. По оценкам различных аналитических исследований, в зависимости от сценария использования от 20 до 50 % мощности ЦП и значительная доля ОЗУ могут быть задействованы для обеспечения работы второстепенных задач, что особенно заметно на устаревших
или слабых устройствах.

Данная проблема приобретает особую значимость в контексте роста популярности многозадачности и необходимости обеспечения высокой скорости работы программного обеспечения. В условиях, когда пользователи стремятся к максимальной эффективности своих систем, возникает потребность в разработке инструментов, способных оптимизировать использование ресурсов за счёт выборочного управления активными процессами и службами. Подобные решения позволяют не только повысить производительность, но и продлить срок службы оборудования за счёт снижения нагрузки на его компоненты.

Целью данной работы стало создание компьютерной программы, которая помогала бы операционной системе *Windows* освобождать ресурсы, занятые низкоприоритетными задачами, тем самым увеличивая её производительность. Мы сосредоточились на изучении влияния отключения второстепенных процессов и служб на загрузку ЦП и потребление ОЗУ

© Бадьин А. В., Никандров В. Л., 2025

в различных условиях эксплуатации – от систем с минимальной фоновой нагрузкой до систем, работающих в режиме интенсивного использования. В ходе экспериментов было установлено, что для ненагруженных систем применение разработанной программы позволяет снизить загрузку ЦП до уровня 5–10 % и уменьшить использование оперативной памяти до 1 ГБ из доступных 8 ГБ. Без применения разработанной программы эти показатели составляют 20–25 % загрузки ЦП и 2,5 ГБ ОЗУ соответственно. Для систем с высокой нагрузкой использование программы обеспечивает ещё более заметный эффект: загрузка ЦП сокращается до 5–15 %, а потребление ОЗУ – до 1–2 ГБ из 8 ГБ, в то время как без программы значения достигают 35–50 % для ЦП и 4–5 ГБ для оперативной памяти.

Объектом исследования в данной работе выступила производительность операционной системы *Windows*, широко используемой на персональных компьютерах по всему миру, а предметом – влияние отключения фоновых процессов и служб на ключевые параметры производительности системы. Разрабатываемая программа была ориентирована на баланс между освобождением ресурсов и сохранением стабильности работы операционной системы. Особое внимание уделялось тому, чтобы критически важные компоненты, такие как процессы управления графическим интерфейсом, базовые службы безопасности и системные утилиты, оставались активными, в то время как ресурсы, занимаемые второстепенными задачами, эффективно перенаправлялись на выполнение приоритетных пользовательских операций. Таким образом, наша работа направлена на повышение общей эффективности работы компьютера, что может быть особенно полезно как для повседневного использования, так и для специализированных задач, требующих максимальной производительности [1].

Приложение было написано с помощью Windows API для программной составляющей и с помощью Qt для интерфейса. Стабильную работу программы обеспечивают функции CreateProcess, TerminateProcess, с помощью которых мы и работаем с процессами системы, запущенными в данный момент [2].

Интерфейс, в свою очередь, был реализован именно на Qt, а не на Windows API для удобства пользователя и понятной структуры. В Windows API ради хотя бы понятного меню нужно: объявить его, вставить элементы в меню, подключить связи, описать его закрытие; в свою очередь, в Qt надо просто перетащить нужный блок на поле и задать ему функционал [3].

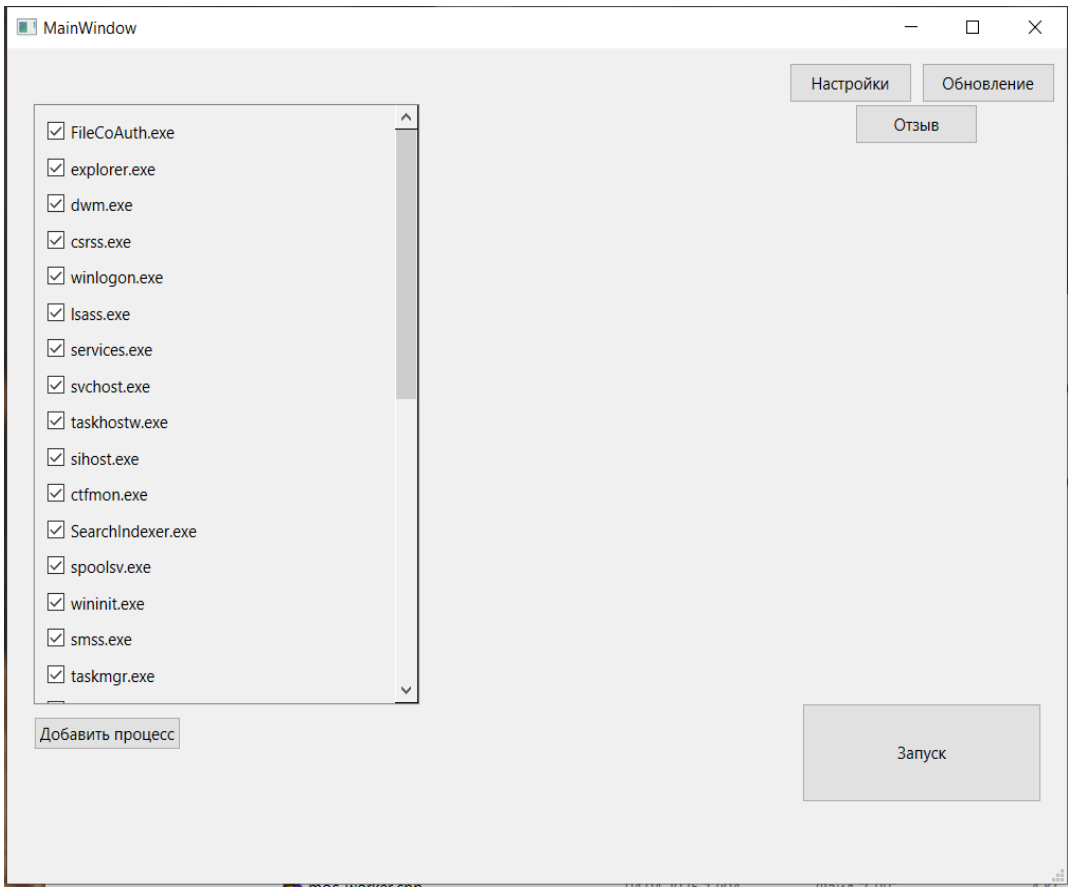


Рисунок 1. Интерфейс программы

Таблица 1

Динамика производительности

Рассматриваемый компонент	**Вне работы программы**		**Во время работы программы**	
	CPU, %	*RAM*, ГБ	*CPU*, %	*RAM*, ГБ
Виртуальная машина	17	2,5	4	1,4
Среднестатистический ПК	36	4	10	2
Сильно загруженная машина	84	8	20	3

По результатам исследования можно сказать, что мы достигли увеличения производительности в несколько раз. Хоть этот показатель и разнится от системы к системе, можно быть уверенными, что как минимум в 2 раза меньше ресурсов будет затрачено на работу системы без дополнительных программ, что напрямую увеличивает производительность ЭВМ.

Список литературы

1. Критически важные системные службы – Win32 apps // Microsoft Learn. URL: learn.microsoft.com/ru-ru/windows/win32/rstmgr/critical-system.

2. Process and Thread Functions – Win32 apps // Microsoft Learn. URL: learn.microsoft.com/en-us/windows/win32/procthread/process-and-thread-f.

3. Взаимодействие процессов (приложений) на WinApi // Хабр. URL: habr.com/ru/articles/149299.

УДК 621.314*004.94

ПРИМЕНЕНИЕ ЦИФРОВОГО ДВОЙНИКА ДЛЯ УПРАВЛЕНИЯ ВЫСОКОЭФФЕКТИВНЫМ ЗАРЯДНЫМ УСТРОЙСТВОМ

Е. А. Голубев[1]
Научный руководитель Ю. В. Краснобаев[1]
Доктор технических наук, профессор

[1]*Сибирский федеральный университет*

Современные системы электропитания космических аппаратов (КА) требуют высокой эффективности, надёжности и минимизации массогабаритных характеристик. Одним из ключевых элементов таких систем является зарядно-разрядное устройство (ЗРУ), обеспечивающее передачу энергии между аккумуляторными батареями (АБ) и нагрузкой. Для повышения КПД и качества управления в таких устройствах перспективным решением является применение цифрового двойника (ЦД), позволяющего оптимизировать алгоритмы переключения силовых ключей и снизить вычислительную нагрузку на управляющий микроконтроллер.

В качестве основы для высокоэффективного ЗРУ рассматривается реверсивный повышающе-понижающий импульсный преобразователь (РИП). Его силовая часть (рис. 1) состоит из четырёх транзисторов (VT_1–VT_4) и дросселя L, что обеспечивает двунаправленную передачу энергии с высоким КПД (до 99 %) благодаря применению стратегии мягкой коммутации. Ключевыми особенностями РИП являются минимальные динамические потери за счёт переключения транзисторов при нулевом напряжении (*ZVS*), астатизм выходного напряжения благодаря синтезированному ШИМ-управлению, возможность работы в режимах заряда и разряда АБ без изменения структуры силовой части [1].

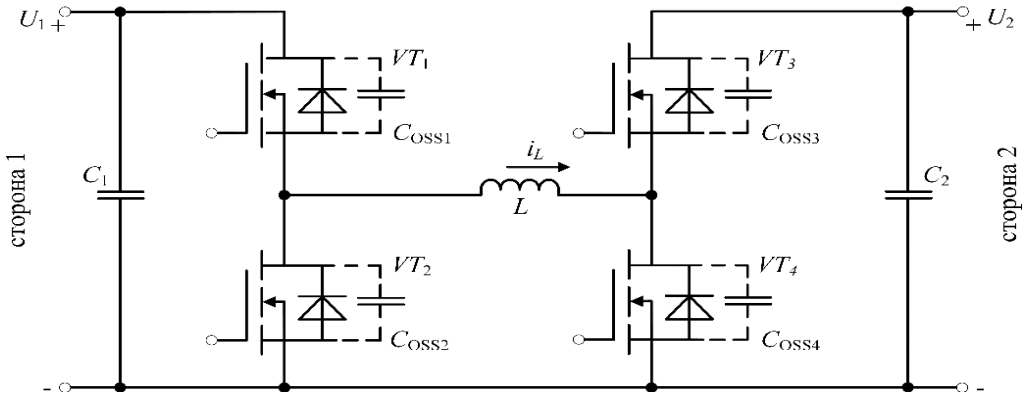


Рисунок 1. Схема силовой цепи реверсивного импульсного преобразователя (РИП)

© Голубев Е. А., 2025

Однако при реализации управления РИП на микроконтроллере возникает проблема: ограниченное быстродействие не позволяет в реальном времени рассчитывать оптимальные моменты переключения транзисторов, что увеличивает длительность переходных процессов. Для решения этой проблемы предложено использование ЦД – системы таблиц, заранее рассчитанных для различных режимов работы преобразователя. На основе уравнений, описывающих ток дросселя (1)–(3), вычисляются моменты переключения транзисторов t_1, t_2, t_3 для разных значений напряжений U_1, U_2, передаваемой мощности P [2].

$$I'_1 = U_{L.1} / L = U_1 / L; \quad (1)$$

$$I'_2 = U_{L.2} = (U_1 - U_2) / L; \quad (2)$$

$$I'_3 = U_{L.3} / L = -U_2 / L. \quad (3)$$

Результаты заносятся в таблицы (рис. 2), где каждому сочетанию параметров соответствуют оптимальные временные параметры управления. В процессе работы микроконтроллер не рассчитывает моменты переключения, а выбирает их из таблиц ЦД, что значительно сокращает время обработки.

№ п/п	U_1, В	t_1, мкс	t_2, мкс	t_3, мкс	$t_{зад.0}$, мкс	$t_{зад.1}$, мкс	$t_{зад.2}$, мкс	$t_{зад.3}$, мкс	Q, мкКл	P, Вт
1	75	1,00	2,40	2,80	0,21	0,18	0,21	0,21	2,63	13,13
2	75	1,11	2,85	3,25	0,21	0,18	0,21	0,21	3,63	18,15
3	75	1,21	3,25	3,65	0,21	0,18	0,21	0,21	4,64	23,19
…	…	…	…	…	…	…	…	…	5,64	28,21
80,75	403,77									
81,78	408,91									
82,82	414,09									
…	…									
173,96	869,82									
174,94	874,70									
175,88	879,39									
176,78	883,89									

№ п/п	U_1, В	t_1, мкс	t_2, мкс	t_3, мкс	$t_{зад.0}$, мкс	$t_{зад.1}$, мкс	$t_{зад.2}$, мкс	$t_{зад.3}$, мкс	Q, мкКл	P, Вт
1	66	1,00	1,76	2,16	0,21	0,18	0,21	0,21	1,26	6,31
2	66	1,20	2,34	2,74	0,21	0,18	0,21	0,21	2,27	11,33
…	…	…	…	…	…	…	…	…	…	16,35
395,22										
400,33										
405,49										
…										
772,43										
775,32										
778,01										
780,50										

№ п/п	U_1, В	t_1, мкс	t_2, мкс	t_3, мкс	$t_{зад.0}$, мкс	$t_{зад.1}$, мкс	$t_{зад.2}$, мкс	$t_{зад.3}$, мкс	Q, мкКл	P, Вт
1	65	1,00	1,71	2,11	0,21	0,18	0,21	0,21	1,16	5,80
2	65	1,21	2,31	2,71	0,21	0,18	0,21	0,21	2,17	10,83
3	65	1,38	2,79	3,19	0,21	0,18	0,21	0,21	3,17	15,86
4	65	1,52	3,21	3,61	0,21	0,18	0,21	0,21	4,17	20,86
…	…	…	…	…	…	…	…	…	…	…
78	65	5,43	14,38	14,78	0,21	0,11	0,15	0,21	78,96	394,79
79	65	5,47	14,47	14,87	0,21	0,11	0,14	0,21	79,98	399,91
80	65	5,50	14,57	14,97	0,21	0,11	0,14	0,21	81,01	405,07
…	…	…	…	…	…	…	…	…	…	…
147	65	8,09	15,25	18,00	0,21	0,09	0,10	0,21	152,35	761,76
148	65	8,14	15,18	18,00	0,21	0,08	0,10	0,21	152,86	764,29
149	65	8,19	15,10	18,00	0,21	0,08	0,10	0,21	153,33	766,63
150	65	8,24	15,02	18,00	0,21	0,08	0,09	0,21	153,75	768,77

Рисунок 2. Набор таблиц ЦД РИП (фрагментарно)

Для проверки работоспособности ЦД была разработана имитационная модель РИП с ЦД в среде динамического моделирования *SimInTech* [2]. Модель включает в себя силовую часть РИП, блок управления РИП, основную и дополнительные нагрузки. Выбор нужной таблицы и строки в ней зависит от величин напряжения на сторонах РИП и величины интеграла сигнала рассогласования выходного напряжения. Моделирование работы производилось при U_1 = 65 В, U_2 = 100 В, L = 20 мкГн, C = 500 мкФ, T = 20 мкс. Временные диаграммы, полученные при ступенчатом изменении тока $I_н$ нагрузки, представлены на рисунке 3.

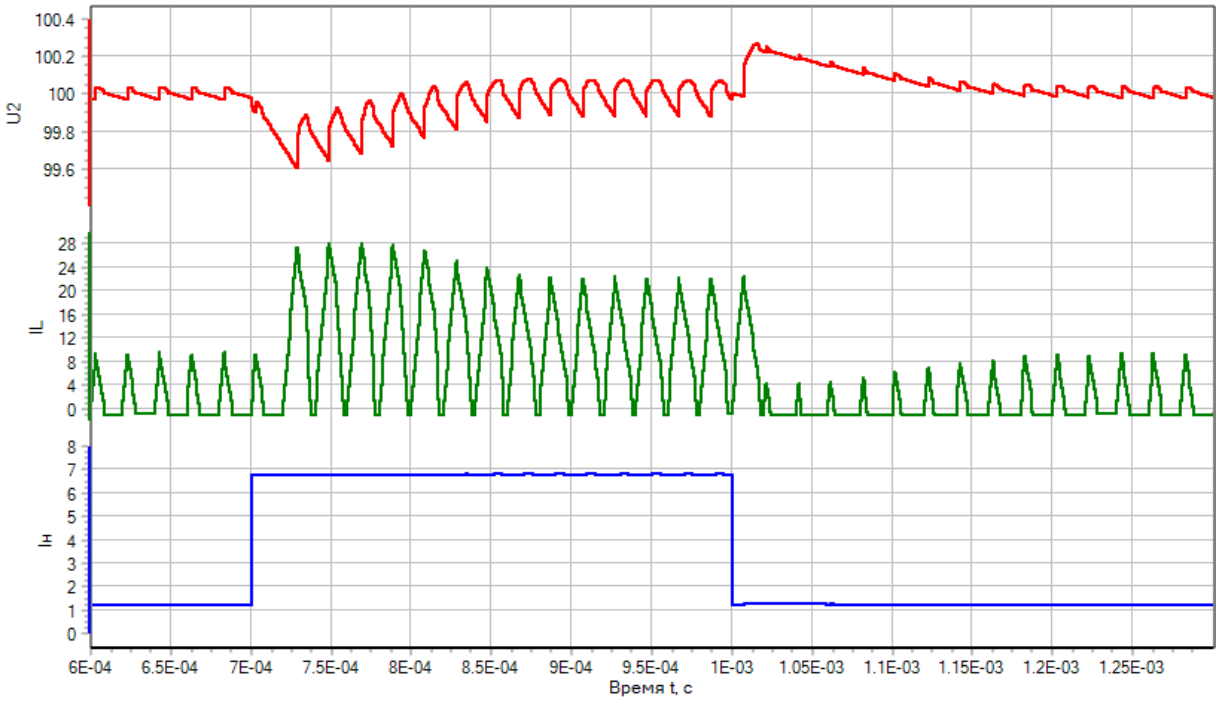


Рисунок 3. Временные диаграммы моделирования процессов в РИП с ЦД

Из данных временных диаграмм можно увидеть, что при увеличении тока нагрузки РИП переход на новую стратегию моделирования осуществляется спустя один период работы преобразователя. Установившийся режим наступает через 4–6 периодов преобразования T, и при этом выходное напряжение U_2 выходит на уровень 100 В – таким образом, статическая ошибка отсутствует.

Исследование выполнено при финансовой поддержке государственного автономного учреждения «Красноярский краевой фонд поддержки научной и научно-технической деятельности» в рамках проекта «Система электропитания на основе генератора электрической энергии, использующего низкопотенциальную тепловую энергию с переменным направлением теплового потока».

Список литературы

1. Краснобаев Ю. В. Применение реверсивного повышающе-понижающего импульсного преобразователя в качестве зарядо-разрядного устройства в автономной системе электропитания / Ю. В. Краснобаев, О. В. Непомнящий, И. Е. Сазонов и др. // Радиотехника, 2023. Т. 87. № 8. С. 155-162. DOI: 10.18127/j00338486-202308-22.

2. Краснобаев Ю. В. Интеллектуальный способ управления высокоэффективным зарядо-разрядным устройством автономного объекта / Ю. В. Краснобаев, И. Е. Сазонов, А. П. Яблонский // Матер. 27-й междунар. НПК. Красноярск: СибГУ им. М. Ф. Решетнёва, 2023. Ч. 2. С. 165-167.

3. Калачев Ю. Н. SimInTech: Преобразователи автономных источников электроэнергии / Ю. Н. Калачев, А. Г. Александров. М.: ДМК Пресс, 2021. 80 с.

УДК 519.87

СТОХАСТИЧЕСКОЕ ОЖИДАЕМОЕ УЛУЧШЕНИЕ ДЛЯ ЭВОЛЮЦИОННОГО АЛГОРИТМА ДОРОГОСТОЯЩЕЙ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ

С. М. Горбунов[1]
Научный руководитель В. В. Становов[1, 2]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

Многокритериальная оптимизация представляет собой важную задачу поиска компромиссных решений при наличии нескольких целевых функций. Эта проблема особенно актуальна в таких областях, как проектирование сложных систем, управление ресурсами и машинное обучение, где оптимизация часто требует дорогостоящих вычислений. В таких сценариях традиционные эволюционные алгоритмы многокритериальной оптимизации сталкиваются с ограничениями из-за высокой стоимости вычисления целевых функций. Для решения этой проблемы разрабатываются методы, сочетающие эволюционные алгоритмы с суррогатными моделями целевых функций, которые позволяют существенно сократить вычислительные затраты за счёт замены ресурсоёмких оценок более простыми аппроксимациями.

В данной работе рассматривается подход *Expensive Multi-/Many-Objective Evolutionary Algorithm* (*EMMOEA*) [1], в котором используется индикатор *IP* для балансировки между разнообразием решений и сходимостью, суррогатные модели Кригинг [2] для оценки индикатора и целевых функций и традиционный подход к оценке точек – *Expected Improvement* (*EI*) [3], применяемый для оценки потенциального улучшения целевой функции в новой точке относительно текущего оптимума. Однако прямое применение *EI* имеет недостатки, включая склонность к попаданию в локальные оптимумы и низкую эффективность в случае многомодальных и сложных ландшафтов целевых функций.

Предлагается критерий *SEI* (*Stochastic Expected Improvement*), разработанный для индикатора *IP* в *EMMOEA*. Суть *SEI* заключается в добавлении стохастической компоненты к *EI* для исследования новых областей. Этот подход позволяет избегать застревания в локальных оптимумах. **Алгоритм** после модификации выглядит следующим образом.

1. Инициализация:
   - создаём начальную равномерно распределённую популяцию P;

© Горбунов С. М., 2025

- генерируем набор равномерно распределённых опорных точек V;
- оцениваем начальные решения, формируя обучающую выборку TS.

2. Основной цикл (пока не исчерпан бюджет оценок целевых функций).

2.1. Построение суррогатных моделей:

- для каждой из M целевых функций строим отдельную суррогатную модель на основе данных из TS.

2.2. Генерация новых решений:

- в цикле от 1 до g_{max}:
  - применяем генетические операторы для создания новых решений потомков $OffDec$;
  - объединяем новую популяцию с текущей: $P = P \cup OffDec$;
  - используем суррогатные модели для предсказания значений целевых функций и их неопределённостей $\sigma(x)$.

2.3. Расчёт показателей качества решений:

- для каждого решения x в популяции P:
  - вычисляем dc как расстояние до идеальной точки Z;
  - вычисляем dd как минимальное расстояние до других решений;
  - рассчитываем индикатор $IP(x) = dc - dd$.

2.4. Построение и использование модели IP:

- строим дополнительную суррогатную модель для значений IP;
- для каждого решения вычисляем:
  - стандартизированное улучшение $\lambda = \dfrac{IP_{\min} - IP_{\text{pred}}(x)}{\sigma(x)}$;
  - $EI = \left(IP_{\min} - IP_{\text{pred}}(x)\right)\Phi(\lambda) + \sigma(x)\varphi(\lambda)$;
  - стохастическую компоненту $S = \text{random}(0, 1) \times EI$;
  - конечный критерий $SEI(x) = EI - S$.

2.5. Отбор и оценка перспективных решений:

- выбираем решение x^* с максимальным значением SEI;
- если решение не дублирует существующие в TS:
  - оцениваем его на реальных целевых функциях;
  - уменьшаем бюджет вычислений на 1;
  - добавляем в обучающую выборку TS.

2.6. Селекция:

- выполняем сортировку решений в TS по Парето-доминированию;
- формируем новую популяцию P из решений первого фронта, ближайших к опорным точкам V.

3. Возврат результата:

- по завершении цикла возвращаем полученную популяцию P.

Сравнение эффективности модифицированного алгоритма *EMMOEA* (*SEI*) и базового варианта *EMMOEA* (*EI*) представлено в таблице на задачах *DTLZ* [4]. Все эксперименты проводились при фиксированном количестве параметров (n = 10) и трёх целевых функциях (M = 3). Для оценки качества решений использовалась метрика *IGD* [5], среднее значение которой приведено по 20

независимым запускам каждого алгоритма. Результаты получены для различных ограничений по числу вычислений целевых функций (300, 400 и 500 оценок). В скобках указано стандартное отклонение.

Таблица 1

Сравнение эффективности алгоритмов *EMMOEA* (*SEI*) и *EMMOEA* (*EI*)

Задача	Оценки	*EMMOEA* (*SEI*)	*EMMOEA* (*EI*)
*DTLZ*1	300	7,0346*e*+1 (1,55*e*+1)	3,5097*e*+1 (1,43*e*+1)
	400	5,1870*e*+1 (1,65*e*+1)	2,3407*e*+1 (1,06*e*+1)
	500	4,3355*e*+1 (1,49*e*+1)	2,2207*e*+1 (7,33*e*+0)
*DTLZ*2	300	5,5210*e*–2 (3,54*e*–3)	6,3157*e*–2 (1,01*e*–2)
	400	4,3411*e*–2 (2,38*e*–3)	4,8017*e*–2 (3,76*e*–3)
	500	3,6087*e*–2 (2,07*e*–3)	3,9820*e*–2 (3,01*e*–3)
*DTLZ*3	300	1,8773*e*+2 (5,10*e*+1)	1,2555*e*+2 (5,56*e*+1)
	400	1,6492*e*+2 (4,95*e*+1)	9,7193*e*+1 (4,63*e*+1)
	500	1,3515*e*+2 (3,61+1)	7,3624*e*+1 (1,96*e*+1)
*DTLZ*4	300	2,4555*e*–1 (7,65*e*–2)	2,6451*e*–1 (8,05*e*–2)
	400	1,7033*e*–1 (7,74*e*–2)	2,1224*e*–1 (8,06*e*–2)
	500	1,2123*e*–1 (8,10*e*–2)	1,6085*e*–1 (7,19*e*–2)
*DTLZ*5	300	1,1750*e*–2 (9,54*e*–4)	1,6377*e*–2 (3,01*e*–3)
	400	8,6492*e*–3 (1,21*e*–3)	1,1529*e*–2 (2,93*e*–3)
	500	6,4766*e*–3 (4,33*e*–4)	8,4045*e*–3 (1,63*e*–3)
*DTLZ*6	300	1,5891*e*+0 (3,06*e*–1)	1,9859*e*+0 (5,32*e*–1)
	400	1,3408*e*+0 (3,65*e*–1)	1,4607*e*+0 (4,89*e*–1)
	500	1,2833*e*+0 (3,26*e*–1)	1,0705*e*+0 (3,87*e*–1)
*DTLZ*7	300	1,9384*e*–1 (2,65*e*–1)	2,0494*e*–1 (2,60*e*–1)
	400	1,1257*e*–1 (1,73*e*–1)	2,2053*e*–1 (2,64*e*–1)
	500	5,3222*e*–2 (4,24*e*–3)	1,5790*e*–1 (2,28*e*–1)

На основе проведённых экспериментов можно сделать вывод о превосходстве модифицированного алгоритма *EMMOEA* с использованием критерия *SEI* над базовым вариантом с традиционным *EI* по метрике *IGD* на большинстве тестовых задач *DTLZ* при различных ограничениях числа вычислений целевых функций. Добавление стохастической компоненты в показатель ожидаемого улучшения позволило существенно повысить качество решений, особенно при ограниченном бюджете вычислений.

Список литературы

1. Qin S. A Performance Indicator-based Infill Criterion for Expensive Multi-/Many-objective Optimization / S. Qin, C. Sun, Q. Liu et al. // IEEE Transactions on Evolutionary Computation. 2023. No. 27 (4). Pp. 1 085-1 099.

2. Chilès J. Fifty Years of Kriging / J. Chilès, N. Desassis. URL: link.springer.com/chapter/10.1007/978-3-319-78999-6_29.

3. Zhan D. Expected Improvement for Expensive Optimization: a Review / D. Zhan, H. Xing // Journal of Global Optimization. 2020. Vol. 78. Pp. 507–544. URL: api.semanticscholar.org/CorpusID:220506265.

4. Deb K. Scalable Test Problems for Evolutionary Multiobjective Optimization / K. Deb, L. Thiele, M. Laumanns et al. // Theoretical Advances and

Applications. 2005. Pp. 105–145.

5. Coello Coello C. A. Solving Multiobjective Optimization Problems using an Artificial Immune System / C. A. Coello Coello, N. C. Cortes // Genetic Programming and Evolvable Machines. 2005. No. 6 (2). Pp. 163–190.

УДК 519.87

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ СИЛЬНОГО ДОМИНИРОВАНИЯ В ЗАДАЧАХ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ ЭВОЛЮЦИОННЫМИ АЛГОРИТМАМИ

В. В. Едреев[1]
Научный руководитель В. В. Становов[1, 2]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

Многокритериальная оптимизация – это одновременная оптимизация двух или более конфликтующих между собой целевых функций в заданной области определения. Задачи однокритериальной оптимизации подразумевают одну целевую функцию и приводят к одному оптимальному решению, однако многие реальные задачи (экономика, инженерия, машинное обучение) не имеют единственного решения, т. к. приходится исследовать несколько конфликтующих целевых функций. Данные критерии могут рассматриваться в совокупности, а выбор осуществляться на основании имеющихся ограничений. Из этого следует, что у задач многокритериальной оптимизации обычно не существует единственного оптимального решения, а есть набор альтернатив.

В общем виде решение задачи многокритериальной оптимизации подразумевает нахождение вектора решений, который будет удовлетворять ограничениям и оптимуму целевой вектор-функции $\vec{f} \in \mathbb{R}^K$. Пусть имеются решения X, каждое из которых является вектором n переменных $\vec{x} = [x_1\, x_2 \ldots x_n] \in \mathbb{R}^n$, и K целевых функций (критериев). Задача многокритериальной оптимизации для вектор-функции $\vec{f} : x \to \mathbb{R}^K$ заключается в нахождении такого $\vec{x}^*$, что:

$$\vec{x}^* = \underset{\vec{x}\in \mathrm{X}}{\arg\,\mathrm{opt}}\, \vec{f}\left(\vec{x}\right) = \underset{\vec{x}\in \mathrm{X}}{\arg\,\mathrm{opt}} \left[f_1\left(\vec{x}\right)\ f_2\left(\vec{x}\right)\ \cdots\ f_K\left(\vec{x}\right)\right]^T.$$

© Едреев В. В., 2025

В рамках исследования был реализован алгоритм многокритериальной оптимизации для формирования фронта оптимальных решений на языке *C++*. В качестве базового метода выступила дифференциальная эволюция (*DE*) с использованием *NSGA*-II [1], который оперирует понятием Парето-доминирования. Говорят, что решение $\vec{x}^p$ доминирует решение $\vec{x}^q$, если:

$$\forall i : f_i\left(\vec{x}^p\right) \geq f_i\left(\vec{x}^q\right) \wedge \exists j : f_i\left(\vec{x}^p\right) > f_i\left(\vec{x}^q\right),\ i = \overrightarrow{1,K}.$$

Т. е. решение $\vec{x}^p$ должно быть не хуже по всем критериям и лучше как минимум по одному. Если нет решений, доминирующих $\vec{x}^p$, то оно называется оптимальным по Парето относительно X. Множество всех недоминируемых точек называют множеством Парето P, а их отображение в критериальном пространстве – фронтом Парето PF.

В работе предлагается и исследуется вариация понятия доминирования из теории игр – сильное доминирование (*strict dominance*) [2], которое можно представить следующим образом:

$$\forall i : f_i\left(\vec{x}^p\right) > f_i\left(\vec{x}^q\right),\ i = \overrightarrow{1,K}.$$

Т. е. решение считается оптимальным, если оно строго лучше другого по совокупности всех критериев.

Для тестирования алгоритма применялись тестовые функции *DTLZ*2 и *DTLZ*7 [3]. Приведём общий вид целевых функций (решаем *K*-критериальные задачи). С деталями можно ознакомиться в оригинальных статьях.

$$DTLZ2:\ f_k\left(\vec{x}\right) = \left(1 + g\left(\vec{x}_{\mathrm{M}}\right)\right) \times \prod_{i=1}^{i=K-k} \cos\left(x_i \frac{\pi}{2}\right) \times$$

$$\times \begin{cases} 1, & k = 1 \\ \sin\left(x_{K-k+1} \times \pi/2\right), & k > 1 \end{cases},\ k = \overrightarrow{1,K};$$

*DTLZ*7:

$$\begin{cases} f_k\left(\vec{x}\right) = x_k,\ k = \overrightarrow{1,(K-1)} \\ f_K\left(\vec{x}\right) = \left(1 + g\left(\vec{x}_{\mathrm{M}}\right)\right) \times \left[K - \sum_{i=1}^{i=K-1} \left(\frac{f_i}{1 + g\left(\vec{x}_{\mathrm{M}}\right)} \left(1 + \sin\left(3\pi f_i\right)\right)\right)\right] \end{cases}.$$

Стоит дополнительно уточнить, что *DTLZ*2 имеет непрерывный фронт, а *DTLZ*7 – с разрывами, что будет показано ниже на рисунке. Для оценки качества аппроксимации использовалась метрика *IGD* [4], отражающая разницу между реальным фронтом Парето PF и его аппроксимацией PF^*:

$$IGD\left(\mathrm{PF}, \mathrm{PF}^*\right) = \frac{1}{\left|\mathrm{PF}\right|} \sum_{\vec{p}\in \mathrm{PF}} \min_{\vec{p}^*\in \mathrm{PF}^*} dis\left(\vec{p}, \vec{p}^*\right).$$

Главный исследуемый показатель – уровень значимости различий метрики *IGD* между сильным доминированием и доминированием по Парето с учётом варьирования количества критериев K и количества поколений, отводимых для поиска решений. Для его оценки применяется непараметрический критерий Манна – Уитни при альтернативной гипотезе, что *IGD* сильного доминирования меньше, чем классического, – фронт аппроксимируется точнее. Для каждого количества критериев осуществляется 100 запусков, в результате которых в конце считывается метрика *IGD* последнего поколения и передаётся на вход тесту.

Характеристики алгоритма для *DTLZ*2: 25 индивидов, размер тестового множества – 250 (истинный PF), размерность векторов-решений $|\vec{x}|$ = 25, селекция на основании *crowding distance* и рангов решений, мутация *DE*/*target-to-best*/1, одноточечное скрещивание.

Характеристики алгоритма для *DTLZ*7: 100 индивидов, размер тестового множества – 500, остальные параметры не меняются.

Результаты приведены на рисунке. Первая строка – график функции *DTLZ*2 (при K = 3) и графики зависимости значения *p-value* от K при разном количестве поколений. Вторая строка – по аналогии для функции *DTLZ*7. Оранжевая черта – *p-value* меньше 0,05 – можно принять гипотезу о том, что *IGD* сильного доминирования меньше при уровне значимости 5 % и ниже.

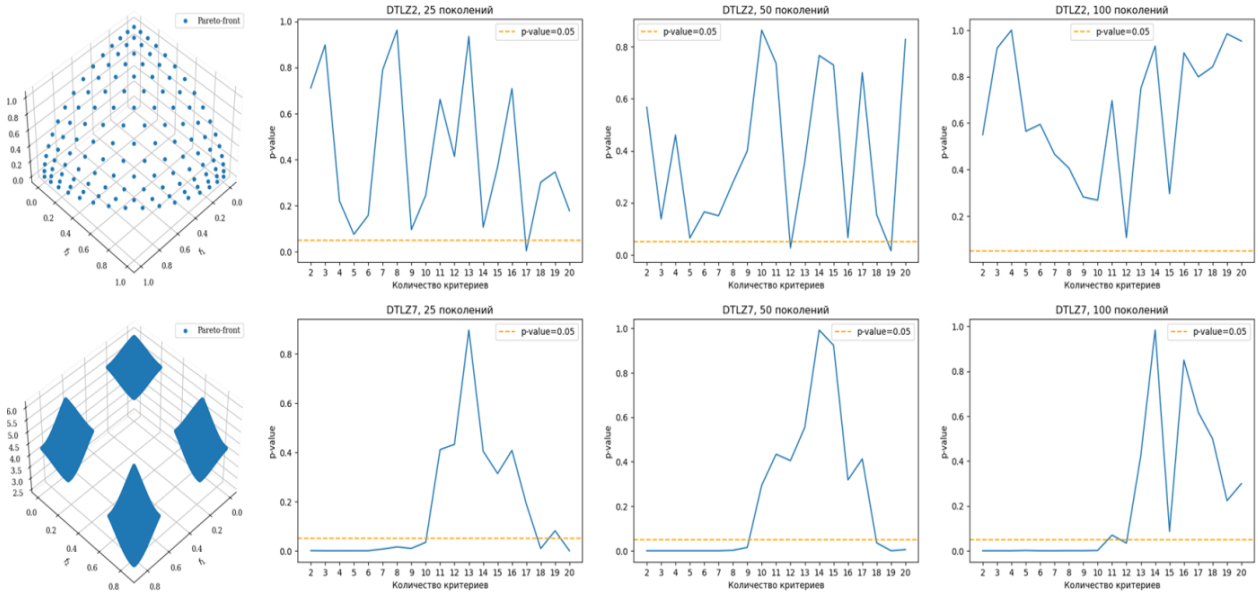


Рисунок 1. Визуализация результатов

Из рисунка можно сделать вывод, что сильное доминирование показало себя лучше при наличии разрывов во фронте Парето (*DTLZ*7) на ряде размерностей (в основном до K = 10, но на 50 поколениях и для 18–20)

при разном количестве поколений алгоритма оптимизации. Таким образом, можно сказать, что использование сильного доминирования в ряде случаев может повысить качество методов многокритериальной оптимизации. В результате можно точнее получать набор оптимальных решений и осуществлять из них выбор.

Работа была поддержана Министерством науки и высшего образования РФ в рамках государственного задания № *FEFE*-2023-0004.

Список литературы

1. Deb K. A Fast Elitist Non-dominated Sorting Genetic Algorithm for Multi-objective Optimization: NSGA-II / K. Deb, A. Pratap, S. Agarwal et al. // Parallel Problem Solving from Nature (PPSN VI): 6th Int. Conf. 2000. Pp. 849-858.

2. Chen Y. C. Iterated Strict Dominance in General Games / Y. C. Chen, N. Van Long, X. Luo // Games and Economic Behavior. 2007. Vol. 61. Iss. 2. Pp. 299-315.

3. Deb K. Scalable Multi-objective Optimization Test Problems / K. Deb, L. Thiele, M. Laumanns et al. // Congress on Evolutionary Computation. 2002. Vol. 1. Pp. 825-830.

4. Sun Y. IGD Indicator-based Evolutionary Algorithm for Many-objective Optimization Problems / Y. Sun, G. G. Yen, Z. Yi // IEEE Transactions on Evolutionary Computation. 2018. Vol. 23. Iss. 2. Pp. 173-187.

УДК 004.031.42

АНАЛИЗ МЕТОДОЛОГИЙ РАЗРАБОТКИ SAAS-ПРИЛОЖЕНИЙ ДЛЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ В МСП

Д. Кантута Зегобия[1]
Научный руководитель В. В. Кукарцев[1]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

Электронная коммерция стремительно развивается, и малые и средние предприятия (МСП) нуждаются в эффективных программных решениях для управления бизнес-процессами. Модель «Программное обеспечение как услуга» (SaaS) характеризуется предложением программных приложений через интернет по схеме подписки. Вместо приобретения бессрочных лицензий и управления локальной инфраструктурой пользователи получают доступ к приложениям из любого места, где есть подключение к интернету [1]. Устраняется необходимость в локальных установках, предлагаются автоматические обновления. Такой подход обладает рядом преимуществ, таких

© Кантута Зегобия Д., 2025

как гибкость, масштабируемость и снижение затрат. Однако существующие методологии разработки приложений не всегда учитывают специфику SaaS для МСП.

В рамках данного исследования проведён анализ методологий разработки SaaS-приложений для электронной коммерции, ориентированных на МСП с акцентом на их особенности и существующие проблемы. Среди множества подходов автор выделяет наиболее распространённые методологии, применяемые при создании SaaS-решений.

1. Extreme Programming (XP) – эта гибкая методология делит процесс разработки программного обеспечения на небольшие части, что снижает затраты на изменение программы на протяжении всего процесса разработки [2]. Подход основан на постоянном совершенствовании, постоянной коммуникации и частой поставке работающего программного обеспечения.

2. SCRUM – это методология управления, позволяющая командам самоорганизовываться и работать над достижением общей цели. Команды SCRUM являются самоуправляемыми и мультифункциональными, состоящими из трёх ролей: скрам-мастера, владельца продукта и команды разработчиков [2]. Такой подход обеспечивает непрерывную поставку ценности, оптимизацию процессов и быструю адаптацию к изменениям.

3. Lean – методология с холистическим подходом, направленная на максимизацию ценности для заказчика и устранение всех видов потерь, таких как время, ресурсы и неэффективные процессы. Она ориентирована на создание высококачественных продуктов с минимальными затратами и оптимизацией всех этапов разработки. Метод подходит для малых, средних и крупных предприятий, не требуя жёсткого следования фиксированному процессу, и позволяет гибко адаптировать подход и время исправлений [2].

4. DevOps – это подход, который объединяет разработку программного обеспечения (разработка) и ИТ-операции (эксплуатация) с целью улучшения взаимодействия между командами, автоматизации процессов и ускорения поставки программного обеспечения с использованием набора лучших практик для разработки [3]. DevOps использует такие инструменты, как Docker, Kubernetes, Jenkins и Git, для упрощения автоматизации, мониторинга и эффективного управления жизненным циклом программного обеспечения.

5. Архитектура микросервисов стала ключевым элементом реализации методологий в SaaS для электронной коммерции. Она позволяет разделить приложение на независимые модули (например, корзина, инвентарь, платежи), обеспечивая масштабируемость для МСП и seamless-интеграцию с практиками DevOps и CI/CD [4]. Например, Shopify использует микросервисы, позволяя МСП настраивать функции без изменения центральной системы.

В таблице представлены ключевые характеристики популярных методологий разработки SaaS-приложений, их преимущества для МСП, а также типовые инструменты и практики, применяемые в рамках каждого подхода. Такая структура позволяет сопоставить сильные стороны методологий и оценить их применимость в условиях МСП.

Таблица 1

Ключевые характеристики и преимущества методологий разработки *SaaS*-приложений для МСП

Методология	Ключевые характеристики	Преимущества для МСП	Инструменты/ практики
XP	Непрерывная поставка, обратная связь, парное программирование	Быстрая адаптация, минимизация ошибок	*TDD*, *CI*, *Unit testing*
SCRUM	Итерации (спринты), роли, ежедневные встречи	Гибкость, высокая вовлечённость заказчика	*Jira*, *Trello*, *Burndown charts*
Lean	Устранение потерь, максимизация ценности	Минимальные ресурсы, высокая эффективность	*Kanban*, 5*S*, *Value Stream Mapping*
DevOps	Интеграция разработки и эксплуатации	Автоматизация, быстрая поставка релизов	*Docker*, *Jenkins*, *GitLab*, *CI*/*CD*
Микро-сервисы	Разделение на независимые сервисы	Масштабируемость, гибкость	*Kubernetes*, *API Gateway*

Несмотря на широкое распространение модели *SaaS* в электронной коммерции, применение существующих методологий обеспечения при создании таких решений для нужд МСП сопряжено с рядом трудностей. Большинство методологий изначально разрабатывались с учётом условий крупных компаний и требуют значительных ресурсов, высокой квалификации персонала и развитой инфраструктуры. Однако МСП часто ограничены в бюджете, не располагают высококвалифицированными техническими специалистами и сталкиваются с трудностями при интеграции новых решений в существующую ИТ-среду.

Для лучшего понимания особенностей применения методологий разработки *SaaS*-приложений в МСП проведено их сравнение по ключевым критериям, включая ресурсоёмкость, квалификацию персонала, гибкость, масштабируемость и интеграционные возможности.

Каждая методология обладает своими сильными и слабыми сторонами в контексте применения на предприятиях с ограниченными ресурсами. Подходы, такие как *XP* и *Lean*, отличаются низкими затратами и простотой внедрения, но уступают в гибкости масштабирования и интеграции. *SCRUM* обеспечивает высокую адаптивность и прозрачность процессов, однако требует организационных усилий. *DevOps* и микросервисная архитектура демонстрируют наибольший потенциал в плане автоматизации, гибкости и масштабируемости, но в то же время предъявляют высокие требования к ресурсам и квалификации команды, что затрудняет их применение в МСП. Эти различия подчёркивают необходимость дальнейших исследований, направленных на адаптацию существующих методологий или разработку гибридных подходов, специально ориентированных на потребности и ограничения МСП в сфере электронной коммерции.

В завершение проведённого анализа можно сделать вывод, что существующие методологии разработки программного обеспечения обладают как сильными сторонами, так и рядом ограничений при их применении

в разработке *SaaS*-приложений для электронной коммерции, ориентированных на МСП. Ни одна из рассмотренных методологий в полной мере не учитывает специфику МСП, связанную с ограниченными ресурсами, необходимостью гибкости, интеграции с уже существующими системами и быстрой адаптацией к изменениям рынка [5].

На основании выявленных особенностей и ограничений существующих подходов автор подчёркивает необходимость разработки адаптированной методологии, способной объединить преимущества различных методов и тем самым компенсировать их недостатки, обеспечивая надёжную, масштабируемую и экономически эффективную разработку *SaaS*-решений в условиях МСП.

Список литературы

1. Armbrust M. A View of Cloud Computing / M. Armbrust, A. Fox, R. Griffith et al. // Communications of the ACM. 2010. Vol. 53. Pp. 50-58. DOI: 10.1145/1721654.1721672.

2. Saeed S. Analysis of Software Development Methodologies / S. Saeed, N. Z. Jhanjhi, M. Naqvi et al. // International Journal of Computing and Digital Systems. 2019. Vol. 8. No. 5. Pp. 446-460.

3. Prosper-Heredia R. DevOps en el Desarrollo SaaS Desde el Punto de Vista de Los Expertos / R. Prosper-Heredia, M. Vargas-Lombardo // RISTI Revista Ibérica de Sistemas e Tecnologias de Informação. 2020. No. E34. Pp. 252-263.

4. Kamisetty A. Microservices vs. Monoliths: Comparative Analysis for Scalable Software Architecture Design / A. Kamisetty, D. Narsina, M. Rodriguez et al. // Engineering International. 2023. Vol. 11. No. 2. Pp. 99-112. – DOI: 10.18034/ei.v11i2.734.

5. Таратухин В. В. Влияние информационно-коммуникационных технологий на управление бизнес-процессами малых и средних предприятий в развивающихся странах / В. В. Таратухин, Е. А. Баженова // Бизнес-информатика, 2012. № 3 (21). URL: cyberleninka.ru/article/n/vliyanie.

УДК 004.021*004.92

ОПТИМИЗАЦИЯ НЕЙРОСЕТЕВЫХ АРХИТЕКТУР ДЛЯ КЛАССИФИКАЦИИ И АНАЛИЗА АКТИВНОСТЕЙ В ВИДЕОПОТОКАХ

В. Н. Мымликов[1], М. М. Фарафонов[1]
Научный руководитель О. А. Антамошкин[1]
Доктор технических наук, заведующий кафедрой программной инженерии
[1]*Сибирский федеральный университет*

Настоящая работа посвящена оптимизации и доработке программного решения для распознавания и классификации действий людей в видеопотоке. Данная система была описана в работах [1; 2], где рассматривались её различные версии. Основными критериями, применяемыми к процессу разработки данной системы, являются скорость обработки кадров, т. к. система должна в идеале работать в реальном времени, а также точность определения действий людей в кадре, что, в свою очередь, необходимо в рамках основного функционала системы. На момент начала процесса оптимизации система уже обеспечивала достаточно высокий уровень точности распознавания действий, однако всё ещё оставалась проблема относительно низкой производительности, при которой обеспечить эффективное распознавание в реальном времени было невозможно. Данный факт частично сглаживался различными ухищрениями и оптимизациями, которые в основном сосредотачивались на пропуске части кадров и выполнении распознавания с некоторой задержкой (например, 1 раз за 3–4 кадра), что, очевидно, требовало некоторых изменений в процессе сбора данных. Однако пути непосредственного увеличения скорости работы системы ещё не были исчерпаны, поэтому настоящее исследование посвящено их изучению.

Корень проблем с производительностью системы распознавания кроется в некоторой тяжеловесности подсистемы распознавания скелетов людей на кадрах видеопоследовательности. В качестве распознавателя поз, начиная с самой первой версии системы, использовалась нейросетевая модель *OpenPose* [3]. Данная модель на основе сравнения качества распознавания в начале разработки была выбрана как самый лучший вариант ввиду точности работы, однако есть в ней и недостатки. Основным среди них является слабая поддержка проекта – последние значимые обновления в репозитории проекта датируются 2020 г., а также данная модель не может быть применена с современными версиями *Python* и его библиотеками. Потому одним из основных направлений оптимизации системы стала замена *OpenPose* на модель *Yolo* 11 [4].

© Мымликов В. Н., Фарафонов М. М., 2025

Одним из направлений улучшения также стала оптимизация скорости работы алгоритма трекирования людей между кадрами. Детальное описание алгоритма было приведено в работе [1]. В обновлённой версии упор был сделан на пересмотр некоторых операций с целью повышения общей производительности. В частности, был переписан механизм построения матрицы оценок кандидатов. Вместо поэлементного вычисления теперь происходит одномоментное вычисление всей строки матрицы разом. Внесённые изменения позволили снизить время работы алгоритма на каждый кадр, особенно при увеличении числа отслеживаемых людей. Замеры времени производились путём многократного выполнения старой и новой версий алгоритма для различного количества людей с последующим усреднением значений. В качестве людей использовались случайно сгенерированные точки скелетов. Число повторений для формирования среднего времени составило 10 000. Графики замеров времени работы показаны на рисунке 1.

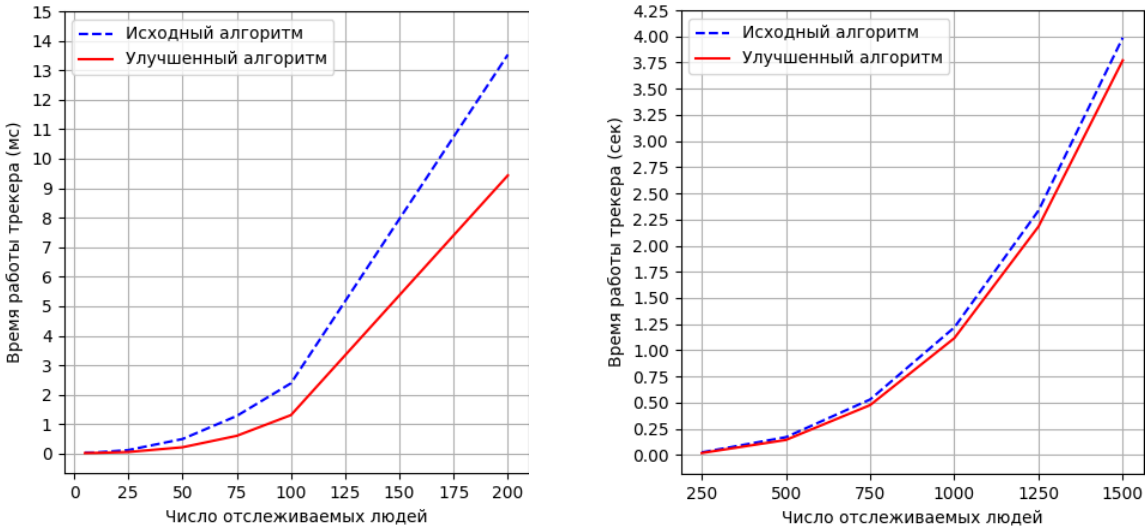


Рисунок 1. Графики усреднённого времени работы трекера на один кадр для разного числа отслеживаемых людей

Вместе с переходом на *Yolo* также была модифицирована модель скелета человека. Теперь у каждого скелета есть одна дополнительная точка, которая содержит информацию о его локальном перемещении в кадре относительно прошлого кадра. Для вычисления перемещения используется та же конечность, что и для трекинга. Это должно помочь учесть динамику действия при классификации типа активности.

После замены *OpenPose* на *Yolo* 11 сразу же встал вопрос поиска оптимальной архитектуры нейронной сети классификатора действий, что необходимо для обеспечения критерия точности работы. Как и в более ранней работе [2], было произведено обучение различных архитектур нейронной сети классификатора и получены данные о лучшей из них. Лучшей архитектурой оказалась обычная *LSTM*-сеть без дропаута и прочих дополнений (рис. 2).

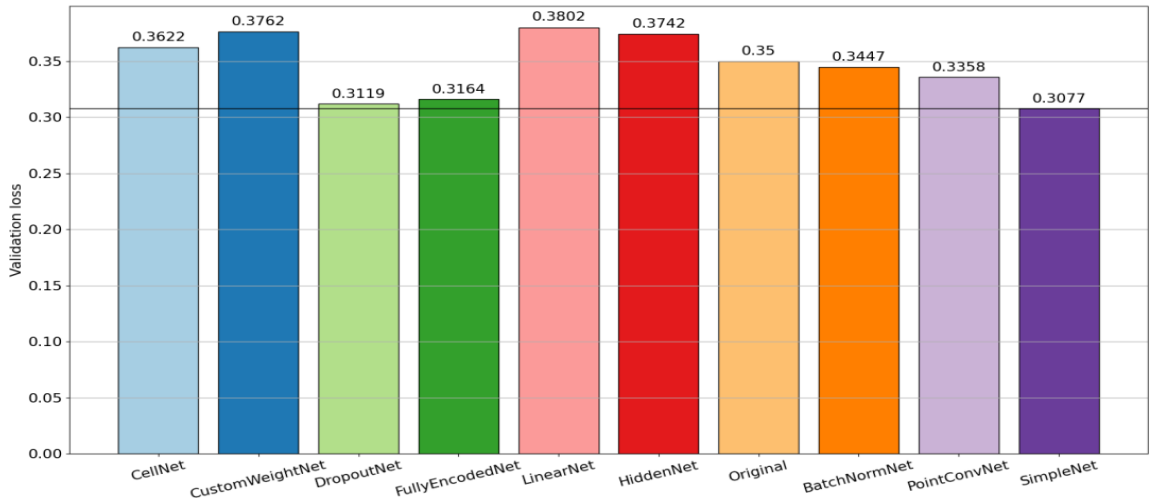


Рисунок 2. Гистограмма валидационных ошибок разных моделей классификатора

Аналогично более раннему исследованию для дальнейшего улучшения результата было произведено обучение с разными пресетами аугментаций данных (рис. 3).

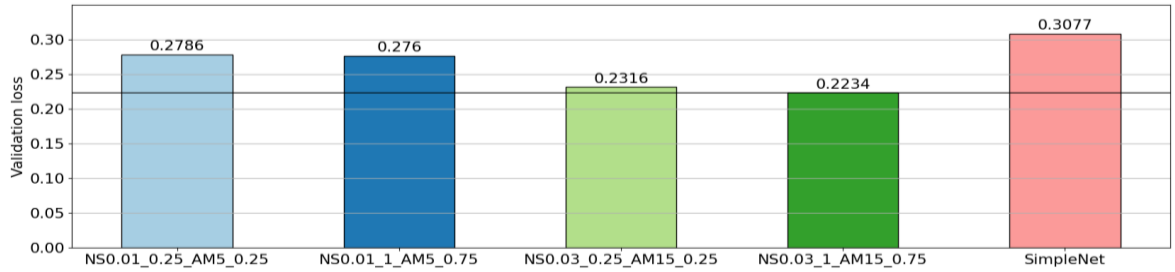


Рисунок 3. Гистограмма валидационных ошибок при использовании разных вариантов аугментации данных для лучшей модели классификатора

Прежняя версия системы работала со средней скоростью 6,7 кадра/с, новая версия имеет скорость 46,8 кадра/с. Таким образом, по итогам работы удалось увеличить скорость вывода в 7 раз, а точность работы фактически осталась без изменений.

Список литературы

1. Мымликов В. Н. Программное средство идентификации скелета человека в видеопотоке / В. Н. Мымликов, М. М. Фарафонов, П. В. Пересунько // Достижения науки и технологий (ДНиТ). 2021. С. 326-333.

2. Farafonov M. Modification of Software Tool for Human Activity Classification / M. Farafonov, E. Peresunko, V. Mymlikov // ITM Web of Conferences. EDP Sciences. 2025. Vol. 72. P. 04005.

3. Cao Z. Openpose: Realtime Multi-person 2D Pose Estimation using Part Affinity Fields / Z. Cao et al. // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019. Vol. 43. No. 1. Pp. 172–186.

4. Khanam R. Yolov11: an Overview of the Key Architectural Enhancements / R. Khanam, M. Hussain // arXiv preprint. 2024. arXiv: 2410.17725.

УДК 004.042

ПРИМЕНЕНИЕ ВЫСОКОСКОРОСТНОЙ ВИДЕОСЪЁМКИ ДЛЯ ВИЗУАЛИЗАЦИИ МИКРОВИБРАЦИЙ КОРПУСА ДВИГАТЕЛЯ

Д. В. Сергеев[1], Д. А. Войцеховский[1]

Научный руководитель А. В. Хныкин[1],
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет,*

В современной промышленности и энергетике электродвигатели являются ключевыми элементами, обеспечивающими работу различных устройств и механизмов. Однако их долговечность и эффективность напрямую зависят от состояния корпуса двигателя, который подвергается динамическим нагрузкам и микровибрациям. Эти микровибрации могут быть вызваны механическими неисправностями, дисбалансом ротора, износом подшипников или другими факторами.

Обнаружение таких микровибраций на ранних стадиях является важной задачей для предотвращения серьёзных поломок и снижения затрат на ремонт. Традиционные методы диагностики (например, использование акселерометров) требуют физического контакта с двигателем и могут быть ограничены в применении. Высокоскоростная видеосъёмка предоставляет альтернативный подход, позволяющий визуализировать микровибрации без необходимости установки дополнительного оборудования.

Анализ микровибраций корпуса электродвигателя с помощью высокоскоростной видеосъёмки выявляет неисправности, визуализирует колебания и оценивает состояние корпуса. Он нужен для мониторинга в реальном времени, контроля качества, прогноза износа и тестирования новых конструкций. Это повышает надёжность и долговечность оборудования.

Целью данного проекта является разработка метода анализа микровибраций корпуса электродвигателя с использованием высокоскоростной видеосъёмки и алгоритмов компьютерного зрения. Конечным результатом является создание программного решения, которое позволяет визуализировать векторы движений точек корпуса двигателя в реальном времени, что упрощает диагностику состояния устройства.

Объектом исследования является корпус электродвигателя, подверженный микровибрациям. Исследование проводится с использованием высокоскоростной видеосъёмки, которая позволяет зафиксировать даже незначительные движения поверхности.

© Сергеев Д. В., Войцеховский Д. А., 2025

Для достижения поставленной цели был разработан программный код, основанный на библиотеках *OpenCV* и *NumPy*. В качестве входных данных используется видеофайл, снятый высокоскоростной камерой.

Приведём основные этапы обработки.

1. Определение области интереса (*ROI*). На первом кадре видео выделяется область, в которой будут отслеживаться точки. Это позволяет сосредоточиться на наиболее значимых участках корпуса двигателя.

2. Отслеживание точек. Используется алгоритм *Shi-Tomasi* [1] для поиска ключевых точек и метод *Lucas-Kanade* [2] для расчёта оптического потока. Эти алгоритмы позволяют определить перемещения точек между последовательными кадрами.

3. Фильтрация точек. Для устранения шума и повышения точности отслеживания применяется фильтрация точек по минимальному расстоянию.

4. Построение графиков векторов движений. Для каждой отслеживаемой точки строятся графики изменения смещений по осям *X* и *Y*. Это позволяет анализировать динамику микровибраций и выявлять аномальные колебания.

5. Визуализация векторов. На каждом кадре видео строятся стрелки, показывающие направление и величину перемещений точек. Это позволяет наглядно представить микровибрации корпуса двигателя.

6. Сохранение результата. Обработанное видео сохраняется в файл, где видны как исходные точки, так и векторы их движений.

В ходе выполнения проекта было создано программное решение, которое успешно обрабатывает видеофайлы и визуализирует микровибрации корпуса электродвигателя.

Основные результаты:

– разработан алгоритм фильтрации точек, который устраняет шум и обеспечивает точное отслеживание ключевых областей;

– построены графики векторов движений, позволяющие анализировать динамику микровибраций и выявлять аномалии;

– реализована визуализация векторов движений с использованием стрелок, что делает анализ данных интуитивно понятным;

– создано выходное видео, демонстрирующее микровибрации корпуса двигателя.

На рисунке 1 из обработанного видео видно корпус электродвигателя с выделенной областью интереса (*ROI*). В углах корпуса отображаются стрелки, указывающие направление и величину микровибраций.

На рисунке 2 представлены изменения смещений точек корпуса двигателя по осям *X* и *Y*. Каждая линия соответствует одной из отслеживаемых точек.

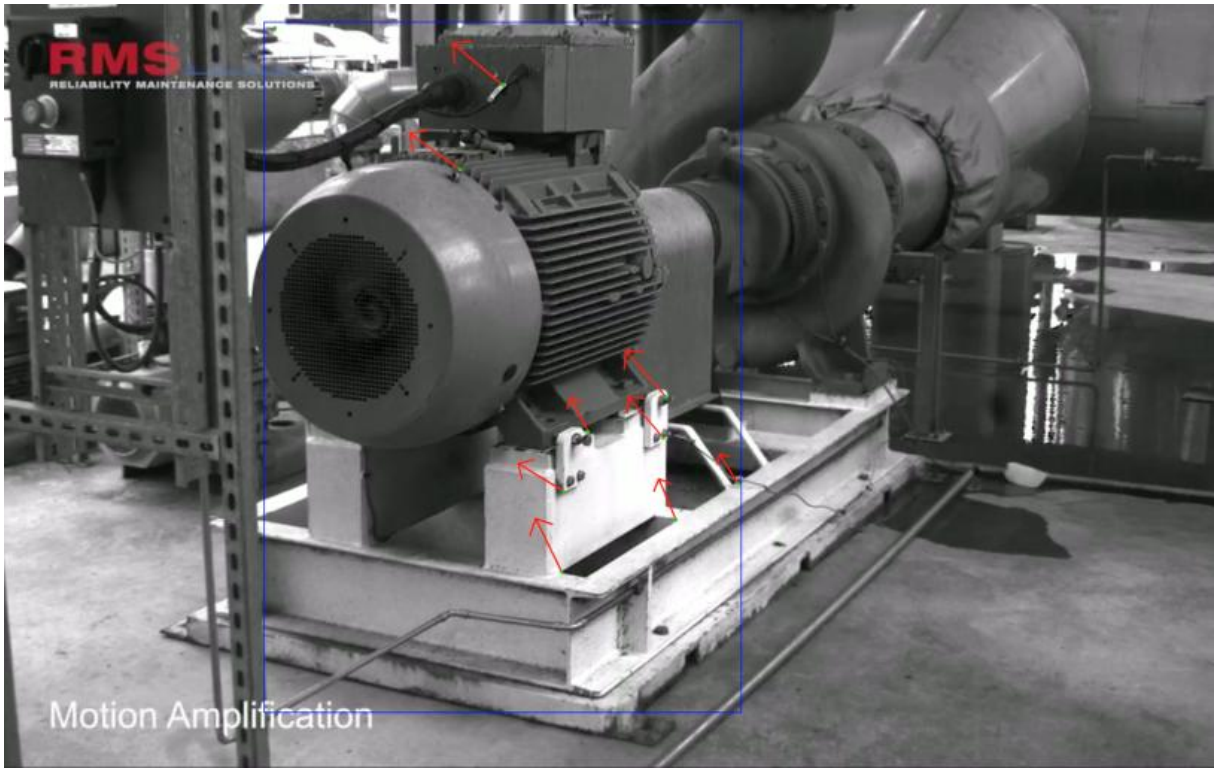


Рисунок 1. Фрагмент выходного видео

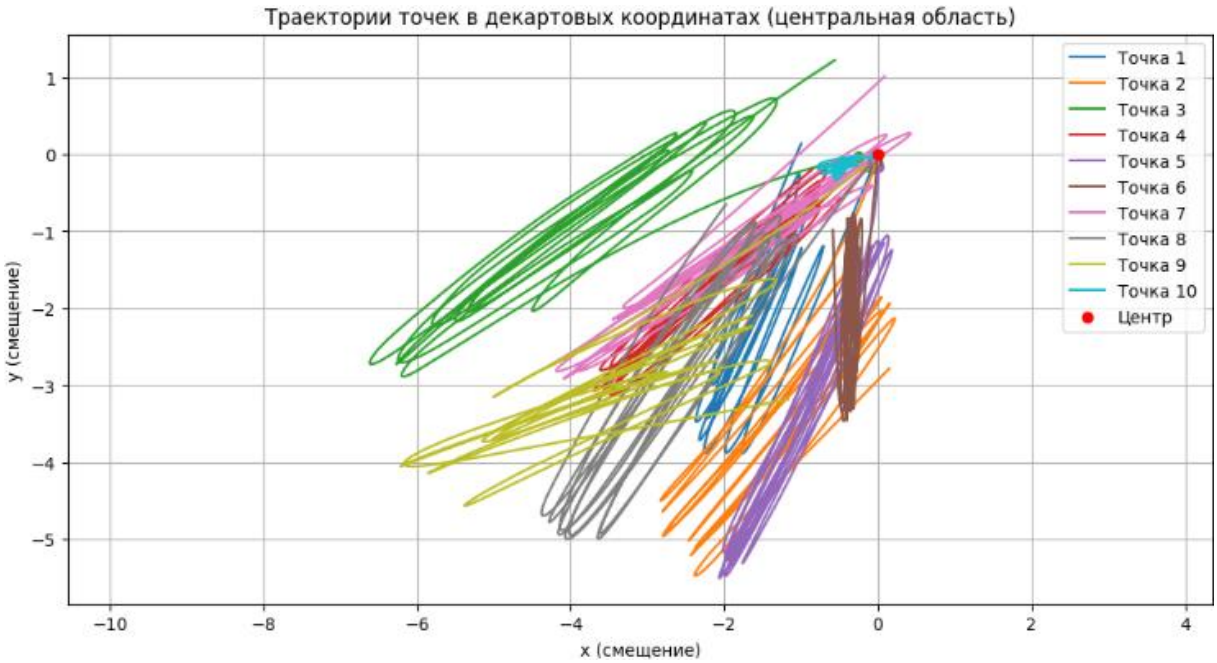


Рисунок 2. Графики векторов отслеживаемых точек

Проект демонстрирует возможность использования высокоскоростной видеосъёмки для анализа микровибраций корпуса электродвигателя. Разработанный метод позволяет визуализировать динамические процессы без необходимости установки дополнительного оборудования. Это открывает новые возможности для диагностики и мониторинга состояния электродвигателей в реальном времени.

Список литературы

1. Python Corner Detection with Shi-Tomasi Corner Detection Method using OpenCV // GeeksforGeeks. 2023. URL: geeksforgeeks.org/python-corner-detection-with-shi-tomasi-corner-detection-method-using-opencv/?ysclid=m98.

2. Python OpenCV: Optical Flow with Lucas-Kanade Method // GeeksforGeeks. 2023. URL: geeksforgeeks.org/python-opencv-optical-flow.

3. Нейросетевая система отслеживания и распознавания объектов в видеопотоке // Современные наукоёмкие технологии. 2018. № 12. URL: s.top-technologies.ru/pdf/2018/12-1/37270.pdf.

УДК 004.852

ИНТЕГРАЛЬНАЯ АППРОКСИМАЦИЯ ФУНКЦИИ ОШИБКИ В ПРОЦЕССЕ ОБУЧЕНИЯ НЕЙРОННЫХ СЕТЕЙ

Р. В. Сысоев[1]

Научный руководитель О. А. Антамошкин[1]

Доктор технических наук, заведующий кафедрой программной инженерии

[1]*Сибирский федеральный университет*

Современные нейронные сети (НС) становятся всё более популярными в различных областях, включая обработку изображений, распознавание речи, машинный перевод и мн. др. Одной из ключевых задач в обучении НС является минимизация функции ошибки, которая измеряет расхождение между предсказанными и истинными значениями. Для эффективного обучения необходимо применять методы оптимизации, которые требуют точного представления функции ошибки [1]. В данном исследовании рассматриваются подходы к интегральной аппроксимации функции ошибки и их влияние на процесс обучения НС.

Функция ошибки (или функция потерь) играет центральную роль в обучении НС. Она позволяет количественно оценить, насколько хорошо модель справляется с поставленной задачей. Наиболее распространёнными функциями ошибки являются среднеквадратичная ошибка (*MSE*) и кросс-энтропия. Для минимизации функции ошибки используются методы градиентного спуска и его модификации, такие как *Adam*, *RMSprop* и др. [2].

Интегральная аппроксимация функции ошибки представляет собой подход, позволяющий сгладить гиперповерхность ошибки, особенно в случаях, когда данные имеют сложную структуру или когда функция ошибки имеет большое число локальных минимумов, что замедляет процессы обучения, использующие алгоритмы, основанные на вычислении градиента функции ошибки.

© Сысоев Р. В., 2025

Метод интегральной аппроксимации основывается на геометрическом смысле определённого интеграла – площадь, объём и гиперобъём функции на заданном (заданных) интервале для функций одной, двух и более двух переменных соответственно. Метод заключается в формировании новой гладкой версии исходной функции и применении к ней уже существующих методов оптимизации.

Пусть мы имеем исходную функцию, имеющую множество экстремумов: $f(x_1, \ldots, x_N)$, где N – число аргументов, тогда гладкая версия функции будет рассчитываться как:

$$f_{smooth}(x_1, ..., x_N) = \int_{(x_1-S)}^{(x_1+S)} \ldots \int_{(x_N-S)}^{(x_N+S)} f(x_1, ..., x_N)\, dx_1 \ldots dx_N, \qquad (1)$$

где S – настраиваемый параметр, имеющий смысл половины ширины аппроксимируемой области с центром, соответствующим точке на исходной поверхности.

В наилучшем случае выбора параметра S исходная функция приводится к форме, имеющей по одному глобальному максимуму и минимуму в точках, соответствующих глобальным максимумам и минимумам исходной функции (при их наличии в исходной функции). Примером такого поведения может служить функция Растригина [3] для трёхмерного пространства:

$$f(x, y) = 20 \times \left(\left(x^2 - 10 \times \cos(2 \times \pi \times x) \right) + \left(y^2 - 10 \times \cos(2 \times \pi \times y) \right) \right). \quad (2)$$

Применяя (1) к (2), получаем обновлённый вид функции:

$$f_{smooth}(x, y) = \int_{(x-S)}^{(x+S)} \int_{(y-S)}^{(y+S)} f(x, y)\, dx dy = 80 \times x^2 + 80 \times y^2 + \frac{160}{3} \qquad (3)$$

при $S = 1$. Как можно увидеть из (3) – сглаженная функция не имеет тригонометрических составляющих. Причина такого преображения заключается в том, что функция косинуса носит монотонный амплитудный характер, где расстояние между двумя соседними максимумами (минимумами) равняется 2π. В функции Растригина аргументами косинуса являются $2\pi x$ и $2\pi y$, что приводит к тому, что расстояние между двумя соседними максимумами (минимумами) становится равным 1. Учитывая, что значение и частота амплитуд косинуса неизменна, среднее значение функции в областях с шириной, большей, чем 1, полностью нивелирует амплитуды косинуса в данном примере. Графики (2) и (3) представлены на рисунке.

В результирующей аппроксимированной функции присутствует только один экстремум, являющийся глобальным минимумом и соответствующий глобальному минимуму исходной функции по значениям аргументов x и y. Значение аппликаты в любой точке аппроксимированной функции будет отличаться от значения аппликаты исходной функции

в той же точке, применение данного метода рассчитано только на нахождение требуемого экстремума.

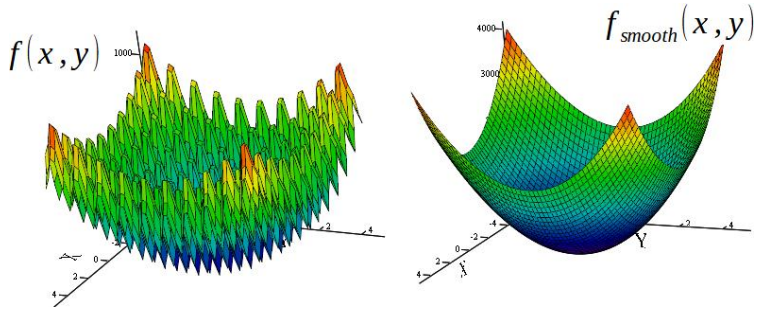


Рисунок 1. Исходная и аппроксимированная функции Растригина

Интегральная аппроксимация функции ошибки представляет собой перспективное направление в обучении НС. Применение интегральных методов позволяет улучшить качество модели, повысить устойчивость к выбросам и ускорить процесс оптимизации. Дальнейшие исследования в этой области могут привести к разработке новых подходов и методов, которые будут способствовать развитию и совершенствованию нейронных сетей.

Список литературы

1. Горбачевская Е. Н. История развития нейронных сетей / Е. Н. Горбачевская, С. С. Краснов // Вестник ВУиТ. 2015. № 1 (23). С. 52–56.

2. Мальцев В. А. Оптимизаторы нейронных сетей / В. А. Мальцев // Научный форум: Инновационная наука: матер. 22-й междунар. НПК. 2019. №. 4. С. 61.

3. Растригин Л. А. Системы экстремального управления / Л. А. Растригин. М.: Наука, 1974.

УДК 621.865.8

СИСТЕМА УПРАВЛЕНИЯ УНИВЕРСАЛЬНЫМ АДАПТИВНЫМ МАНИПУЛЯТОРОМ

Е. Р. Хабибуллин[1], Е. А. Голубев[1], И. Е. Бородин[1]

Научный руководитель Ю. В. Краснобаев[1]
Доктор технических наук, профессор

[1]*Сибирский федеральный университет*

Универсальные адаптивные манипуляторы (АМ) представляют собой многофункциональные устройства, применяемые для решения широкого

© Хабибуллин Е. Р., Голубев Е. А., Бородин И. Е., 2025

спектра технологических задач. Данный спектр можно условно разделить на два класса [1]:

1) перемещение объектов в пространстве;
2) выполнение операций с инструментами.

Одной из задач, решаемых АМ, является задача подготовки комплекта аккумуляторов для их сборки в аккумуляторную батарею (АБ). АБ состоит из последовательно включённых S блоков, каждый из которых образован P параллельно включёнными аккумуляторами. Для сборки АБ необходимо из массива аккумуляторов выбрать аккумуляторы, которые должны быть соединены в блоки. При этом необходимо обеспечить равенство полученной ёмкости каждого из S блоков аккумуляторов заданному значению ёмкости блока $Q_{ср}$ с требуемой точностью и минимизировать разницу между внутренними активными сопротивлениями $R_{вн.а}$ аккумуляторов, входящих в блок.

В современном мире АБ находят широкое применение в различных устройствах, что позволяет считать актуальной задачу разработки и создания АМ для подготовки комплекта аккумуляторов для их сборки в АБ.

Для решения этой задачи необходимо разработать эффективную систему управления (СУ) универсальным АМ.

На рисунке 1 представлены:

– массив аккумуляторов с известными характеристиками, такими как ёмкость Q и внутреннее активное сопротивление $R_{вн.а}$ (склад аккумуляторов);

– кассета для сборки аккумуляторов с аккумуляторами, перемещёнными в неё из массива с известными характеристиками.

Программа для ЭВМ, которая определяет, какие аккумуляторы из массива аккумуляторов с известными характеристиками взять и в какие ячейки кассеты для сборки аккумуляторов поставить, уже разработана авторами доклада при выполнении хозяйственного договора № 20 783 от 15.04.2024 между СФУ и ООО «Модульные системы управления». В результате работы этой программы в массиве аккумуляторов с известными характеристиками определены ячейки, из которых необходимо взять аккумуляторы, а в кассете для сборки аккумуляторов разными цветами назначены ячейки, образующие блоки аккумуляторов с характеристиками, требуемыми для сборки АБ. Ячейки с аккумуляторами, которые необходимо переместить, на рисунке 1 обозначены разными цветами.

Пример отсортированного посредством программы, массива аккумуляторов с выбранными аккумуляторами для сборки АБ
(выбранные аккумуляторы выделены цветом)

№1:1	№1:2	№1:3	№1:4	№1:5	**Б2 №1:6**
Q = 2,1405 Ач	Q = 2,1088 Ач	Q = 2,2374 Ач	Q = 2,2219 Ач	Q = 1,8731 Ач	Q = 1,48 Ач
Rвн.а = 0,0242 Ом	Rвн.а = 0,0192 Ом	Rвн.а = 0,0151 Ом	Rвн.а = 0,0199 Ом	Rвн.а = 0,0222 Ом	Rвн.а = 0,0218 Ом
№2:1	**Б1 №2:2**	**Б1 №2:3**	№2:4	№2:5	**Б2 №2:6**
Q = 1,6389 Ач	Q = 1,3921 Ач	Q = 1,5995 Ач	Q = 1,4634 Ач	Q = 2,2394 Ач	Q = 1,6892 Ач
Rвн.а = 0,023 Ом	Rвн.а = 0,0193 Ом	Rвн.а = 0,0165 Ом	Rвн.а = 0,0225 Ом	Rвн.а = 0,025 Ом	Rвн.а = 0,0206 Ом
Б1 №3:1	**Б2 №3:2**	№3:3	№3:4	№3:5	№3:6
Q = 1,6334 Ач	Q = 1,8489 Ач	Q = 1,6811 Ач	Q = 2,1099 Ач	Q = 1,3366 Ач	Q = 2,2434 Ач
Rвн.а = 0,0152 Ом	Rвн.а = 0,0166 Ом	Rвн.а = 0,0187 Ом	Rвн.а = 0,016 Ом	Rвн.а = 0,017 Ом	Rвн.а = 0,0234 Ом
№4:1	№4:2	**Б1 №4:3**	**Б3 №4:4**	**Б2 №4:5**	№4:6
Q = 1,3057 Ач	Q = 1,3724 Ач	Q = 1,844 Ач	Q = 1,4014 Ач	Q = 1,4862 Ач	Q = 1,4764 Ач
Rвн.а = 0,0245 Ом	Rвн.а = 0,0156 Ом	Rвн.а = 0,0141 Ом	Rвн.а = 0,025 Ом	Rвн.а = 0,0208 Ом	Rвн.а = 0,0146 Ом
№5:1	№5:2	№5:3	**Б3 №5:4**	№5:5	**Б1 №5:6**
Q = 1,985 Ач	Q = 2,0381 Ач	Q = 2,1572 Ач	Q = 1,6734 Ач	Q = 1,8565 Ач	Q = 1,9027 Ач
Rвн.а = 0,0259 Ом	Rвн.а = 0,0224 Ом	Rвн.а = 0,0177 Ом	Rвн.а = 0,0239 Ом	Rвн.а = 0,0202 Ом	Rвн.а = 0,0144 Ом
Б3 №6:1	**Б3 №6:2**	**Б3 №6:3**	№6:4	**Б2 №6:5**	№6:6
Q = 1,2869 Ач	Q = 1,5206 Ач	Q = 1,6756 Ач	Q = 2,1899 Ач	Q = 1,5648 Ач	Q = 2,0328 Ач
Rвн.а = 0,026 Ом	Rвн.а = 0,0254 Ом	Rвн.а = 0,0236 Ом	Rвн.а = 0,022 Ом	Rвн.а = 0,0186 Ом	Rвн.а = 0,0247 Ом
№7:1	№7:2	№7:3	№7:4	№7:5	№7:6
Q = 1,7901 Ач	Q = 1,2542 Ач	Q = 1,6104 Ач	Q = 1,6187 Ач	Q = 1,2913 Ач	Q = 1,9518 Ач
Rвн.а = 0,0193 Ом	Rвн.а = 0,0141 Ом	Rвн.а = 0,0251 Ом	Rвн.а = 0,0237 Ом	Rвн.а = 0,0146 Ом	Rвн.а = 0,0244 Ом

Пример расположения аккумуляторов, перемещённых в кассету для сборки АБ типа 3S5P

Обозначения:
- Q – ёмкость аккумулятора;
- Rвн.а – внутреннее активное сопротивление аккумулятора;
- Qср – суммарная ёмкость блока аккумуляторов.

Блок 1	**№2:2**	**№3:1**	**№2:3**	**№4:3**	**№5:6**
Qср = 8,372	Q = 1,3921 Ач	Q = 1,6334 Ач	Q = 1,5995 Ач	Q = 1,844 Ач	Q = 1,9027 Ач
	Rвн.а = 0,0193 Ом	Rвн.а = 0,0152 Ом	Rвн.а = 0,0165 Ом	Rвн.а = 0,0141 Ом	Rвн.а = 0,0144 Ом
	τ = 0,0269 АчОм	τ = 0,0248 АчОм	τ = 0,0264 АчОм	τ = 0,026 АчОм	τ = 0,0274 АчОм
Блок 2	**№4:5**	**№1:6**	**№6:5**	**№2:6**	**№3:2**
Qср = 8,069	Q = 1,4862 Ач	Q = 1,48 Ач	Q = 1,5648 Ач	Q = 1,6892 Ач	Q = 1,8489 Ач
	Rвн.а = 0,0208 Ом	Rвн.а = 0,0218 Ом	Rвн.а = 0,0186 Ом	Rвн.а = 0,0206 Ом	Rвн.а = 0,0166 Ом
	τ = 0,0309 АчОм	τ = 0,0323 АчОм	τ = 0,0291 АчОм	τ = 0,0348 АчОм	τ = 0,0307 АчОм
Блок 3	**№6:1**	**№4:4**	**№6:2**	**№6:3**	**№5:4**
Qср = 7,568	Q = 1,2869 Ач	Q = 1,4014 Ач	Q = 1,5206 Ач	Q = 1,6756 Ач	Q = 1,6734 Ач
	Rвн.а = 0,026 Ом	Rвн.а = 0,025 Ом	Rвн.а = 0,0254 Ом	Rвн.а = 0,0236 Ом	Rвн.а = 0,0239 Ом
	τ = 0,0335 АчОм	τ = 0,035 АчОм	τ = 0,0386 АчОм	τ = 0,0395 АчОм	τ = 0,04 АчОм

Рисунок 1. Информационное содержание
массива аккумуляторов с известными характеристиками
и кассеты для сборки аккумуляторов с перемещёнными в неё аккумуляторами

Задача АМ – по командам СУ, следуя заданной программе, взять нужные аккумуляторы из массива аккумуляторов с известными характеристиками и переместить в кассету для сборки аккумуляторов. При этом необходимо обеспечить контроль за точностью выполняемых операций.

На рисунке 2 приведена блок-схема алгоритма управления АМ. Ниже поясняются действия, производимые при выполнении ряда блоков алгоритма.

При выполнении действий блока 4 алгоритма по командам СУ, следуя программе, с учётом геометрического расположения ячейки схват манипулятора подводится к нужной ячейке. После чего с использованием технического зрения производится точная доводка схвата манипулятора и контроль соответствия номера ячейки требуемому номеру. Затем схват извлекает аккумулятор из ячейки. От датчика, которым оборудована ячейка, в СУ поступает сигнал об извлечении аккумулятора, и СУ проводит проверку правильности выполненного действия. При выполнении действий блока 11 алгоритма по командам СУ, следуя программе, с учётом геометрического расположения ячейки схват манипулятора подводится к нужной ячейке. После чего с использованием технического зрения производится точная доводка схвата манипулятора и контроль соответствия номера ячейки требуемому номеру. Затем схват размещает аккумулятор в ячейку. От датчика, которым оборудована ячейка, в СУ поступает сигнал о размещении аккумулятора, и СУ проводит проверку правильности выполненного действия.

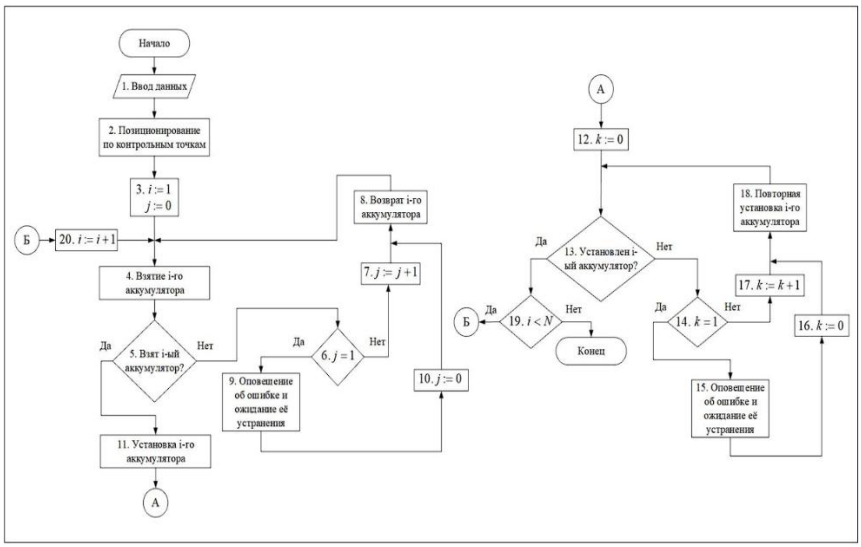


Рисунок 2. Блок-схема алгоритма управления АМ

Таким образом, разрабатываемая система позволяет обеспечить надёжное и стандартизированное формирование комплектов аккумуляторов для последующей сборки АБ.

Исследование выполнено при финансовой поддержке государственного автономного учреждения «Красноярский краевой фонд поддержки научной и научно-технической деятельности» в рамках проекта «Адаптивный робот – комплектовщик аккумуляторов для их соединения в батарею».

Список литературы

1. Зенкевич С. Л. Основы управления манипуляционными роботами: учебник / С. Л. Зенкевич, А. С. Ющенко. 2-е изд. М.: МГТУ им. Баумана, 2004. 480 с. URL: znanium.com/catalog/product/1958415.

УДК 519.87

ГЕНЕРАТИВНЫЙ АЛГОРИТМ ФОРМИРОВАНИЯ ЗВУКОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ GPT-2

М. С. Черкасова[1]
Научный руководитель В. В. Становов[1, 2]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

Музыка – это неотъемлемая часть современной жизни, пронизывающая каждый её момент. Её слышно везде: от уютных кафе до фонового звучания в

© Черкасова М. С., 2025

компьютерных играх. Создание музыки требует значительных усилий и времени, поэтому люди начали искать способы, которые могли бы облегчить этот процесс, среди которых есть генеративные алгоритмы. Развитие генеративных алгоритмов в музыке имеет долгую и увлекательную историю, начиная с ранних экспериментов с алгоритмической композицией и заканчивая современными подходами, использующими нейронные сети и машинное обучение.

Генеративные модели – это тип моделей машинного обучения, которые обучаются на больших наборах информации и способны создавать образцы данных, похожие на те, что были в тренировочном наборе [1]. Генеративные модели находят множество применений в музыкальной индустрии, открывая новые горизонты для композиторов и исполнителей. Одним из наиболее заметных направлений является автоматическое создание музыкальных композиций с помощью таких алгоритмов, как *RNN* (*Recurrent Neural Network* – рекуррентные нейронные сети) [2], и трансформеры, включая GPT (Generative Pre-trained Transformer – генеративный предобученный трансформер) [3]. Модели обучаются на больших наборах данных, содержащих различные музыкальные жанры и стили. Это позволяет им генерировать оригинальные мелодии, гармонии и ритмы, которые могут быть использованы как основа для новых произведений или вдохновение для композиторов. Например, GPT-2 можно адаптировать для генерации музыкальных последовательностей, создавая уникальные цепочки нот.

Для того чтобы нейронная сеть смогла написать музыкальную последовательность, предстоит пройти через несколько этапов:

1) подготовка – сбор данных (датасета), их предобработка, последующая токенизация и разбиение на обучающую и тестовую выборки;

2) настройка модели – анализ архитектуры модели и влияния параметров на её производительность;

3) обучение модели;

4) генерация звуковых последовательностей – генерация новой последовательности инструмента, преобразование токенов в последовательности нот, получение выходных данных.

Первым шагом в подготовке данных является сбор музыкальных последовательностей, которые будут использоваться для обучения модели. Данные могут быть собраны из различных источников – например, из музыкальных баз данных. После сбора данных необходимо провести их предобработку, которая включает в себя следующие шаги: форматирование, очистка, нормализация. Далее токенизация – она преобразует музыкальные последовательности в формат, пригодный для модели, где токены могут представлять такты, динамику или ноты – например, NOTE_ON=60 для ноты до (C4) или NOTE_OFF=60 для её завершения. Зависимость воспроизводимой ноты от токена можно увидеть в таблице ниже.

Таблица 1

Зависимость ноты от токена

Октава	Название октавы	Число ноты											
		C	*C#*	*D*	*D#*	*E*	*F*	*F#*	*G*	*G#*	*A*	*A#*	*B*
–1	–	0	1	2	3	4	5	6	7	8	9	10	11
0	Суб-контроктава	12	13	14	15	16	17	18	19	20	21	22	23
1	Контроктава	24	25	26	27	28	29	30	31	32	33	34	35
2	Большая	36	37	38	39	40	41	42	43	44	45	46	47
3	Малая	48	49	50	51	52	53	54	55	56	57	58	59
4	Первая	60	61	62	63	64	65	66	67	68	69	70	71
5	Вторая	72	73	74	75	76	77	78	79	80	81	82	83
6	Третья	84	85	86	87	88	89	90	91	92	93	94	95
7	Четвёртая	96	97	98	99	100	101	102	103	104	105	106	107
8	Пятая	108	109	110	111	112	113	114	115	116	117	118	119
9	–	120	121	122	123	124	125	126	127	–	–	–	–

Данные делятся на обучающий (80 %) и тестовый (20 %) наборы, обеспечивая данные для обучения модели.

Настройка модели *GPT*-2 включает выбор архитектуры и гиперпараметров, таких как размер эмбеддингов, что влияет на производительность модели или размер дропаута, предотвращающий переобучение. Обучение модели осуществляется через обработку входных данных, обновление весов, оценку производительности и сохранение лучших версий модели.

Генерация звуковых последовательностей начинается с функции, принимающей начальное значение и температуру, что управляет случайностью. Токены преобразуются в формат *NoteSequence*, учитывающий ноты и их параметры. Извлечение информации о сгенерированных произведениях позволяет анализировать инструменты и характеристики. Финальная функция объединяет все шаги, создавая аудиофайлы в формате *MIDI*.

Модель была обучена на 1 816 текстовых файлах (*vocab_size*: 7 699), которые были получены путём токенизации 9 228 *MIDI*-файлов. На момент окончания обучения при размере батча при обучении, равным 8 и при обучении, равным 4, получается значение функции потерь на тесте и на обучении 8,18 и 5,0934 соответственно. Функция потерь для 1 000 эпох представлена на рисунке ниже.

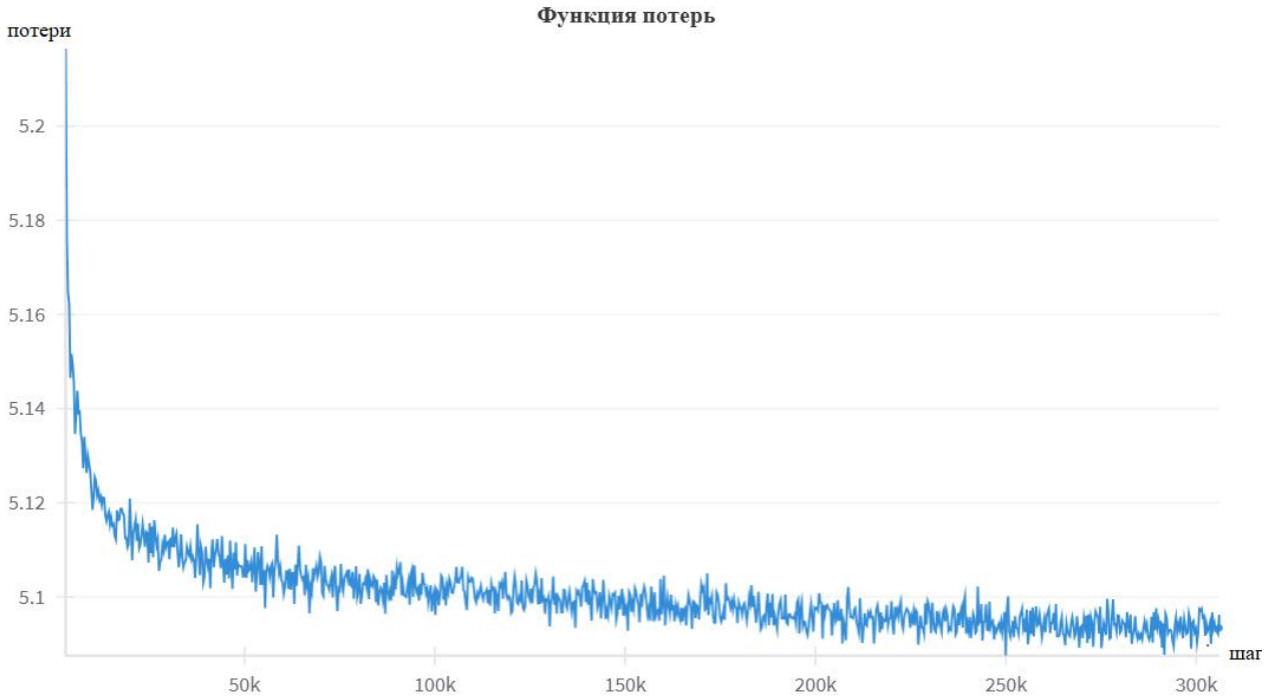


Рисунок 1. Функция потерь

В ходе данной работы было проведено исследование применения нейронных сетей, в частности модели *GPT*-2, для генерации звуковых последовательностей. Архитектура *GPT*-2, основанная на трансформерах, продемонстрировала свою эффективность в генерации текстов и была адаптирована для создания музыкальных последовательностей. Таким образом, результаты исследования подтверждают, что использование нейронных сетей в генерации звуковых последовательностей является перспективным направлением, способным значительно расширить возможности музыкального творчества.

Список литературы

1. Принципы работы генеративных моделей для создания текста и изображений // Хабр. URL: habr.com/ru/companies/fix_price/articles/836.

2. Бендерская Е. Н. Рекуррентная нейронная сеть как динамическая система и подходы к её обучению / Е. Н. Бендерская, К. В. Никитин // КиберЛенинка. 2013. URL: cyberleninka.ru/article/n/rekurrentnaya-neyron.

3. Кумратова А. М. Анализ возможностей нейронной сети на основе языковой модели GPT-3 и способы её применения на производстве / А. М. Кумратова, Н. В. Морозова, А. И. Василенко // КиберЛенинка. 2023. URL: cyberleninka.ru/article/n/analiz-vozmozhnostey-neyronnoy-seti.

УДК 519.87

ВЛИЯНИЕ АРХИТЕКТУРЫ НЕЙРОННОЙ СЕТИ НА ЭВОЛЮЦИОННОЕ ОБУЧЕНИЕ УПРАВЛЕНИЮ АВТОМОБИЛЕМ

Д. С. Шабалин[1]
Научный руководитель В. В. Становов[1, 2]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

В современном мире задачи управления встречаются на каждом шагу. В современных мегаполисах трафик стал неотъемлемой частью города.

Современные задачи управления с развитием технологий становятся комплексными и требующими современных подходов и решений. Современные технологии продвинулись далеко вперёд и позволяют с довольно большой точностью симулировать многие процессы в нашем мире. Благодаря этому мы можем моделировать не только сами миры, но и естественные процессы эволюции в этих мирах. В частности, генетические алгоритмы [1], созданные по подобию естественной эволюции, позволяют нам смоделировать многие процессы адаптации. И задачи управления не являются исключением. Множество работ, основанных на применении генетических алгоритмов, способны успешно решать эти проблемы. Например, существует алгоритм *Paired Open-Ended Trailblazer* (*POET*), в котором эволюционирует не только агент управления, но и окружающая его среда [2]. Кроме того, существует *Multi-Level Evolution* (*MLE*) – процесс создания с нуля готовых роботов, идеально подходящих для управления в необходимой среде [3]. Если требуется подобрать не одно лучшее решение, а получить множество различных решений, пусть и не оптимальных для рассматриваемой задачи, но довольно эффективных и отличных от других решений, на помощь придёт алгоритм *MAP-Elites* [4].

Целью проведённых в данной работе симуляций является получение статистических данных о том, как влияет структура нейронной сети на скорость и качество обучения.

Популяция состоит из 64 индивидуумов, каждый индивидуум представляет собой контроллер для управления автомобилем.

В данной работе симуляция происходит посредством игрового движка Unity. Моделируется трек длиной 243 м. Ширина полосы составляет 3 м. Также моделируется популяция, состоящая из автомобилей. Задача управления

© Шабалин Д. С., 2025

состоит в том, чтобы автомобиль преодолел наибольшее расстояние по данному треку. Время для преодоления ограничено интервалом 25 с.

Для управления автомобилем используется нейронная сеть и получаемые значения датчиков. Каждый автомобиль оснащён тремя датчиками, охватывающими зону сканирования 33,3 м и показывающими в этой зоне расстояние до ближайших объектов. Один датчик направлен вперёд параллельно движению автомобиля, а другие два – слева и справа в 30° от него. На вход нейронной сети поступают значения этих датчиков. Структура скрытых слоёв нейронной сети задаётся пользователем. В результате работы нейронной сети на выходе получаются два значения. Первое отвечает за угол поворота руля автомобиля, а второе – за ускорение автомобиля.

Для того чтобы определить, как структура нейронной сети влияет на обучение, был проведён ряд экспериментов, в которых изменялось количество скрытых слоёв нейронной сети и количество нейронов в каждом скрытом слое.

Было осуществлено девять экспериментов, изменяющих структуру сети. Каждый эксперимент включал в себя эволюцию на протяжении 200 поколений. Для того чтобы уменьшить фактор случайности, каждый эксперимент симулировался три раза.

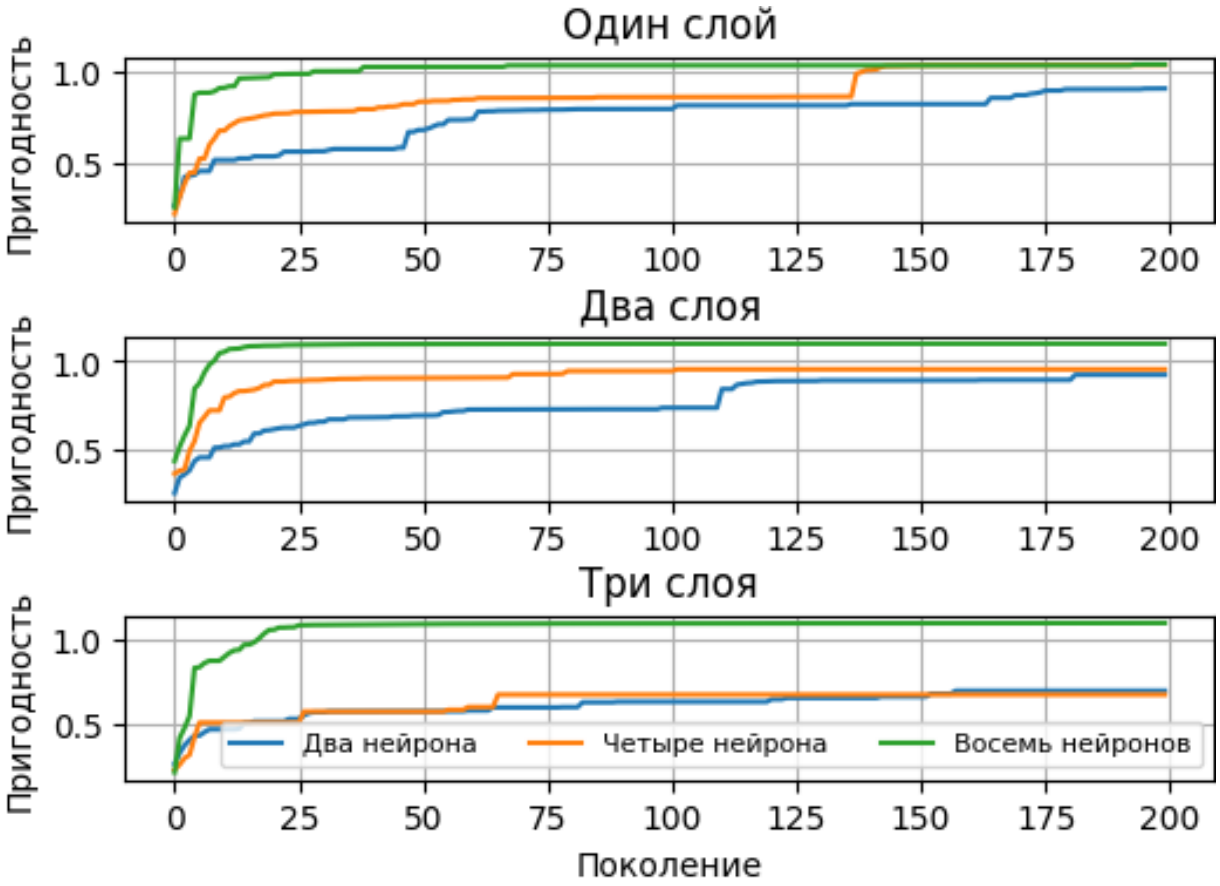


Рисунок 1. Графики пригодности в зависимости от номера поколения

Как можно видеть из приведённого рисунка, использование одного слоя с восемью нейронами позволяет быстро обучить нейронную сеть, однако не позволяет достичь наилучшей пригодности среди проведённых

экспериментов. Использование меньшего количества нейронов замедляет обучение и не всегда позволяет автомобилям доехать до конца трека даже после 200 поколений. При двух и трёх слоях малое количество нейронов слишком замедляет процесс обучения и не позволяет найти решения задачи. Проведённое исследование показало большую значимость выбора архитектуры нейронной сети, поэтому перспективным является автоматический подбор архитектур.

Список литературы

1. Eshelman L. Foundations of Genetic Algorithms 2 / L. Eshelman, J. Schaffer. 1993. Pp. 187–202.

2. Wang R. Paired Open-ended Trailblazer (POET): Endlessly Generating Increasingly Complex and Diverse Learning Environments and their Solutions / R. Wang et al. // ArXiv abs/1901.01753. 2019.

3. Howard D. Evolving Embodied Intelligence from Materials to Machines / D. Howard et al. // Nature Machine Intelligence. 2019. No. 1. Pp. 12–19.

4. Mouret J.-B. Illuminating Search Spaces by Mapping Elites / J.-B. Mouret, J. Clune // ArXiv abs/1504.04909. 2015.

УДК 519.87

СРАВНЕНИЕ СТРАТЕГИЙ МУТАЦИЙ В ДИФФЕРЕНЦИАЛЬНОЙ ЭВОЛЮЦИИ

А. В. Щелконогова[1]
Научный руководитель В. В. Становов [1, 2]
Кандидат технических наук, доцент

[1]*Сибирский федеральный университет*

[2]*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва*

В современном мире необходима оптимизация для повышения эффективности в различных сферах. Она позволяет улучшать процессы, снижать затраты, экономить ресурсы и время, а также повышать качество продукции и услуг. В природе за это отвечает эволюция. Эволюция как процесс позволяет индивидуумам адаптироваться и становиться более приспособленными к различным условиям окружающей среды благодаря механизмам адаптации, естественного отбора и селективного разведения. В эволюционных вычислениях мы пытаемся смоделировать эти принципы, чтобы найти наилучшее решение проблемы. Одним из таких методов вычислений является дифференциальная эволюция.

© Щелконогова А. В., 2025

Дифференциальная эволюция (ДЭ) – это интеллектуальный алгоритм поиска, который многократно улучшает потенциальные решения для оптимизации задач, подобно тому, как происходит эволюция. Райнер Сторн и Кеннет Прайс разработали его в середине 1990-х гг. ДЭ состоит из трёх ключевых компонентов: мутация, скрещивание и селекция, которые в совокупности способствуют её эффективности при решении сложных задач оптимизации [1]. ДЭ является одним из наиболее эффективных методов для решения сложных задач с множеством переменных, она заняла лидирующие позиции на мировых соревнованиях методов оптимизации, таких как *CEC* [2].

ДЭ состоит из трёх основных этапов:

1) мутация – создание пробного вектора на основе разницы между другими векторами популяции;

2) скрещивание – комбинация пробного вектора с целевым вектором;

3) селекция – выбор лучшего вектора для следующего поколения.

В данной работе мы будем сравнивать между собой две стратегии мутации, чтобы определить наиболее эффективную для решения задач *CEC*.

Первый вид мутации (*DE*/*rand*/1) является самым классическим и простым методом, где используются три различных вектора, индексы которых генерируются случайно по равномерному закону, при этом все векторы должны отличаться друг от друга и от целевого вектора [3]:

$$v_j = x_{r_1,\,j} + F\left(x_{r_2,\,j} - x_{r_3,\,j}\right),$$

где x_{r_1}, x_{r_2}, x_{r_3} – случайно выбранные векторы популяции.

F является масштабирующим фактором, в данной работе мы используем адаптивную дифференциальную эволюцию, где начальное значение *F* задаётся 0,5 и изменяется во время работы. Вторая стратегия мутации (*DE*/*target-to-pbest*) представлена формулой:

$$v_j = x_{i,j} + F\left(x_{pb,j} - x_{i,j}\right) + F\left(x_{r_1,\,j} - x_{r_2,\,j}\right),$$

где x_{pb} – один из лучших векторов.

В данной стратегии, помимо прочего, мы находим 10 % лучших векторов и берём случайный из них.

Сравнения проводились на наборе из 12 задач с соревнований *CEC* 2022 [4], результат работы алгоритмов представлен на рисунке.

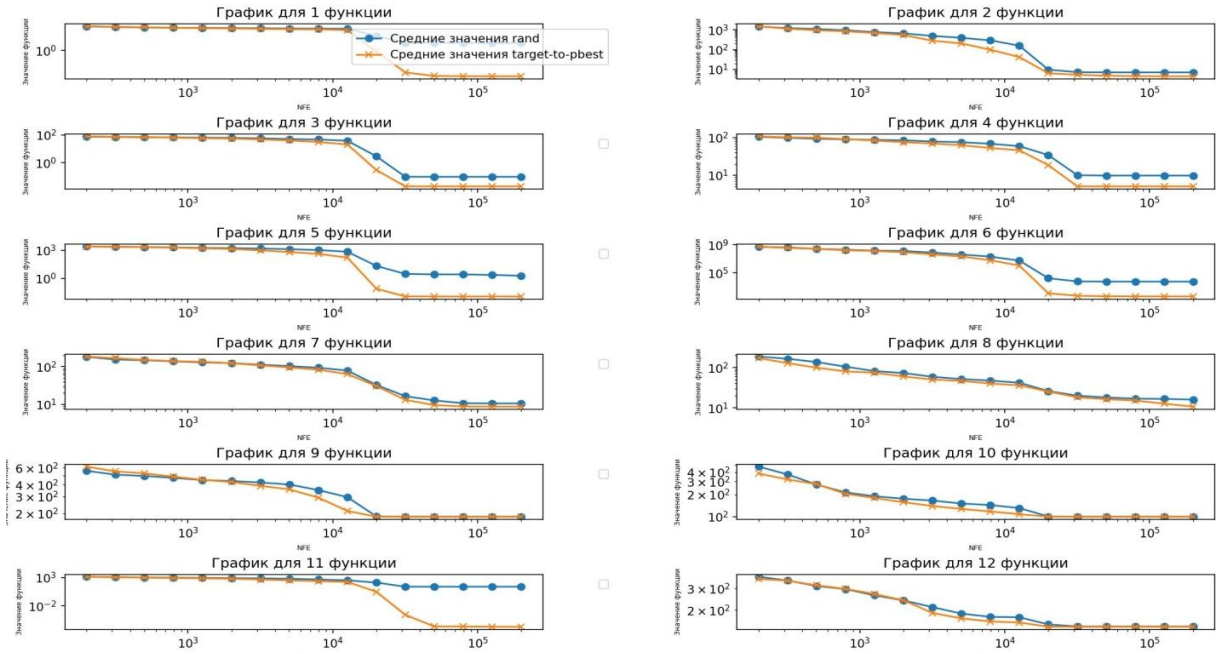


Рисунок 1. Графики сходимости функций

Также в таблице представлены результаты на каждой из 12 функций работы алгоритма для двух стратегий мутаций.

Таким образом, проведённое исследование говорит нам о том, что стратегия мутации *target-to-pbest* имеет лучшую эффективность работы, чем простая стратегия *rand*/1.

Таблица 1

Результаты работы алгоритма

№ функции	***DE*/*rand*/1**	***DE*/*target-to-pbest***
1	2,761*e*+1 ± 7,095*e*+1	1,230*e*–5 ± 4,870*e*–5
2	7,096*e*+1 ± 9,64*e*–1	4,488 ± 0,617
3	9,638*e*–2 ± 2,734*e*–1	1,950*e*–2 ± 2,500*e*–2
4	9,820 ± 3,645	5,074 ± 1,680
5	1,948 ± 2,508	1,190*e*–2 ± 3,100*e*–2
6	5,571*e*+3 ± 4,619*e*+3	4,173*e*+1 ± 5,737*e*+1
7	1,061*e*+1 ± 9,747	8,751 ± 1,010*e*+1
8	1,611*e*+1 ± 7,155	1,079*e*+1 ± 9,534
9	1,856*e*+2 ± 1,543*e*–1	1,855*e*+2 ± 2,870*e*–5
10	1,004*e*+2 ± 1,276*e*–1	1,003*e*+2 ± 5,735*e*–2
11	2,541*e*+1 ± 5,345*e*+1	2,000*e*–6 ± 1,040*e*–5
12	1,468*e*+2 ± 1,119	1,460*e*+2 ± 2,122*e*–1

Стратегия *target-to-pbest* показала значительно лучшие результаты, чем классическая *rand*/1, на большинстве тестовых функций. Она обеспечивает более точные решения (например, ошибка 1,230*e*–5 против 2,761*e*+1 на функции 1) и меньший разброс (σ), что говорит о её устойчивости.

Для некоторых функций (7, 8) разница менее заметна, но *target-to-pbest* всё равно работает не хуже. Итак, *target-to-pbest* – более эффективная стратегия, особенно для сложных задач оптимизации.

Список литературы

1. Sileshi D. Differential Evolution Algorithm / D. Sileshi, M. Krimgen // Baeldung. URL: baeldung.com/cs/differential-evolution-algorithm.

2. Awad N. H. Problem Definitions and Evaluation Criteria for the CEC 2017 Special Session and Competition on Single Objective Bound Constrained Real-parameter Numerical Optimization / N. H. Awad, M. Z. Ali, J. J. Liang et al. // Technical Report. 2016.

3. Становов В. В. Теория эволюционных вычислений: учеб. пособие / В. В. Становов. Красноярск: СФУ, 2024. 259 с.

4. Kumar A. Problem Definitions and Evaluation Criteria for the CEC 2022 Special Session and Competition on Single Objective Bound Constrained Numerical Optimization / A. Kumar, K. V. Price, A. W. Mohamed et al. // Technical Report. 2021.

2025

Федеральное государственное автономное
образовательное учреждение высшего образования
«Сибирский федеральный университет»

Ministry of Science and Higher Education
of Russian Federation
«Siberian Federal University»