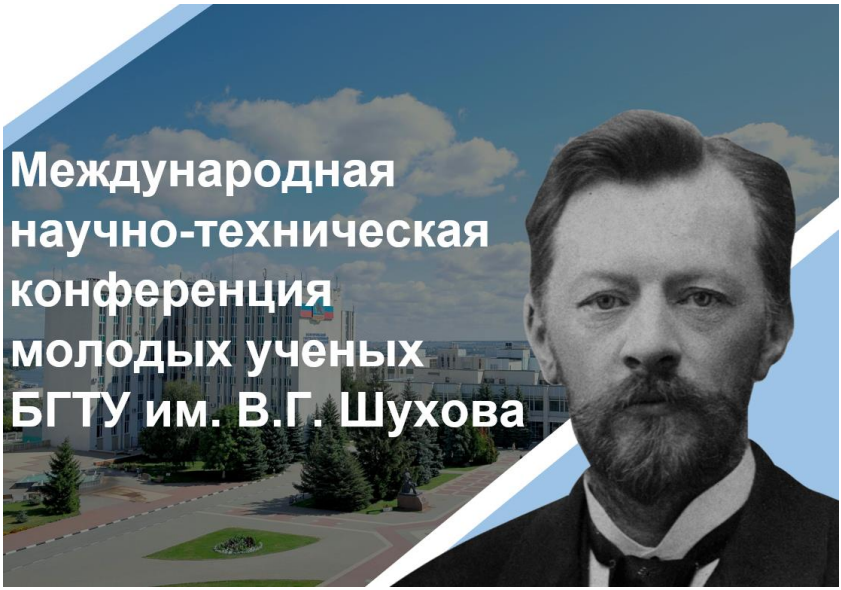
Министерство науки и высшего образования Российской Федерации
Российская академия наук
Российская академия архитектуры и строительных наук
Администрация Белгородской области
ФГБОУ ВО Белгородский государственный технологический университет им. В.Г. Шухова
Международное общественное движение инноваторов «Технопарк БГТУ им. В.Г. Шухова»




**Сборник докладов**

**Часть 13**

# Информационные технологии в управлении, моделировании и в интеллектуальных системах

**Белгород**
**29-30 мая 2025 г.**

УДК 005.745
ББК 72.5+74.48
М 43

М 43 **Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова [Электронный ресурс]**:
Белгород: БГТУ им. В.Г. Шухова, 2025. – Ч. 13. – 528 с.

ISBN 978-5-361-01461-3

В сборнике опубликованы доклады студентов, аспирантов и молодых ученых, представленные по результатам проведения Международной научно-технической конференции молодых ученых БГТУ им. В.Г. Шухова.

Материалы статей могут быть использованы студентами, магистрантами, аспирантами и молодыми учеными, занимающимися вопросами энергоснабжения и управления в производстве строительных материалов, архитектурных конструкций, электротехники, экономики и менеджмента, гуманитарных и социальных исследований, а также в учебном процессе университета.

УДК 005.745
ББК 72.5+74.48

**ISBN 978-5-361-01461-3**

*УДК 004.05*

***Абдусалямова М.В., Якимова А.А., Плеханов Д.В.***
***Научный руководитель: Никонова Е.З., канд. пед. наук, доц.***
*Нижневартовский государственный университет,*
*г. Нижневартовск, Россия*

# ОПТИМИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ ПРОГРАММНЫХ РЕШЕНИЙ

Цифровизация бизнес-процессов стала неотъемлемой частью повышения эффективности компаний. В условиях высокой конкуренции и ужесточения регуляторных требований выбор оптимального программного обеспечения играет ключевую роль в успешном управлении предприятием. С учётом развития цифровых технологий современные компании улучшают своё делопроизводство. Это значительно способствует повышению показателей качества обслуживания клиентов и оптимизации процессов внутри компании[2]. Для реализации большинства задач необходимо иметь профессиональное и зачастую дорогое оборудование, что может стать препятствием для многих малых и средних предприятий.

В рамках бизнес-идей и с учётом большого числа таких компаний необходимо выбрать универсальное решение, которое будет охватывать как автоматизированное рабочее место (АРМ) для персонала, так и соответствующее программное обеспечение (ПО). При этом данное решение должно соответствовать критериям надёжности, качества и приемлемой цены. Важно, чтобы ПО было гибким и модульным, позволяя компаниям адаптировать его под свои специфические нужды и задачи. Оно должно включать инструменты для анализа данных, управления проектами и взаимодействия с клиентами, а также интегрироваться с существующими системами. Однако, как и любые проекты, программное обеспечение должно отличаться по своим задачам и целям[3]. Оно обязано адаптироваться к современным требованиям и ожиданиям пользователей, обеспечивая актуальность и эффективность в быстро меняющемся технологическом мире.

Систематизация данных решений позволяет выработать критерии выбора оптимальных ИТ-инструментов с учетом отраслевой специфики и стратегических задач предприятия.

В данной статье будут рассмотрены основные критерии при выборе ПО для работы с предприятиями и бизнес-проектами и их сравнительный анализ с учётом популярных решений на рынке.

Сравним систему 1С:Предприятие (рис. 1) с ее аналогом СБИС

ЭДО (рис. 2) по нескольким важным показателям для малого бизнеса в сфере розничной торговли: простота операций, удобство и понятность интерфейса для новых пользователей и выгрузка товаров для онлайн реализации. В процессе анализа будет использоваться стандартная версия 8.3 1С:Предприятия для малых предприятий и обычная версия СБИС (система также имеет разные версии, но в меньшем объеме чем 1С).

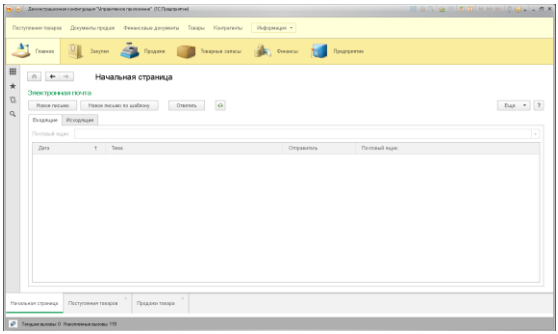



Рис. 1. Интерфейс 1С:Предприятие

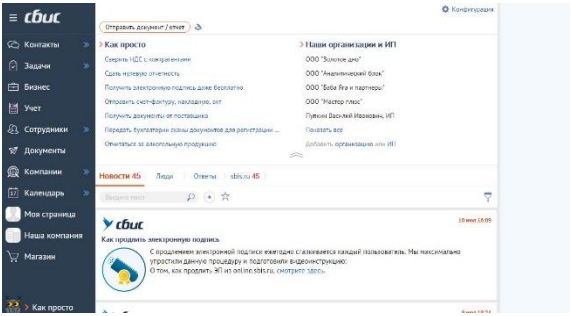



Рис. 2. Интерфейс СБИС

Приведём несколько примеров как одни и те же задачи для малого бизнеса в сфере розничной торговли реализованы в 1С:Предприятие и СБИС:

- **Настройка компании**

В 1С требуется последовательно указать тип организации, систему налогообложения, ввести реквизиты и настроить учетную политику. В то время как СБИС автоматически загружает данные по ИНН из государственных реестров, значительно ускоряя процесс регистрации, без необходимости внесения дополнительных данных.

- **Формирование отчетности**

Система 1С позволяет детально настроить декларацию по НДС через раздел "Регламентированные отчеты", тогда как СБИС предлагает автоматическое заполнение и проверку документа через налоговый календарь или раздел расчета НДС.

- **Работа с отчетностью**

Проверка статусов в 1С осуществляется без электронной подписи, так как данные хранятся локально. В СБИС для доступа к ответам контролирующих органов требуется обязательное использование ЭП, что может создать сложности для предпринимателей без цифровой подписи.

Также было произведено сравнение информационных система по дополнительным критериям. Результаты сравнительного анализа представлены таблице ниже.

Таблица – Результат сравнительного анализа.

| **Критерий** | **1С:Предприятие 8.3** | **СБИС ЭДО** |
|---|---|---|
| Функциональность | Широкий спектр модулей | Ориентирован на отчетность |
| Интерфейс | Сложный, требует обучения | Простой, интуитивно понятный |
| Отчетность | Гибкие возможности, но высокая сложность | Автоматизированные шаблоны, минимум ручных настроек |
| Работа с ЭП | Не требует ЭП для локальной проверки | Обязательное использование электронной подписи |
| Стоимость | Высокая (лицензии, обновлении) | Подписка, доступные тарифы для малого бизнеса |
| Поддержка | Обширная база знаний и обучающие курсы | Упрощенная справочная система |

Таким образом, можно сделать вывод, что система 1С:Предприятие 8.3 в некоторых критериях проигрывает своему аналогу СБИС ЭДО. Но несмотря на удобство СБИС в отдельных аспектах, 1С:Предприятие 8.3 всё равно обладает рядом преимуществ:

Она имеет более **широкий функционал**, который включает в себя

бухгалтерский, налоговый учет, управление финансами и персоналом, что снижает необходимость в дополнительных программах. В то время, как СБИС ЭДО в основном рассчитан на отчетность. Также 1С позволяет адаптировать систему под специфику бизнеса из-за **гибкости настройки**. Дополнительно данная система имеет и**нтеграционные возможности**, она поддерживает подключение к другим сервисам, что важно для комплексной автоматизации.

Исходя из вышесказанного, можно сделать вывод, что выбор программного обеспечения зависит от ИТ-инструментов, соответствующих масштабам предприятия и отраслевым требованиям. Каждое предприятие должно выбрать ПО подходящее для его задач и подходящее под его бюджет.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Кузнецова, И. В. Программные средства для автоматизации бизнеса: Учебное пособие. – М.: Изд-во РУДН, 2020. – 220 с.
2. Иванов, А. П. Эффективное управление бизнес-процессами с помощью программного обеспечения. – СПб.: Питер, 2019. – 300 с.
3. Иванов, А. В. Автоматизация бизнес-процессов: современные тенденции / А. В. Иванов. – М.: Изд-во Альфа-Пресс, 2023. – 215 с.
4. Петрова, Е. Л. ERP-системы: выбор и внедрение / Е. Л. Петрова. – СПб.: Питер, 2022. – 180 с.
5. Федоров, С. О. CRM-системы для бизнеса: Преимущества и недостатки. – М.: Альфа-Пресс, 2021. – 175 с.



***УДК 004***



***Акимова Е.А.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## КИБЕРБЕЗОПАСНОСТЬ В КОСМИЧЕСКИХ ТЕХНОЛОГИЯХ

Давайте поговорим о космосе. Когда-то это слово пахло романтикой, подвигами Гагарина и мечтами о далеких звездах. А что теперь? Теперь космос – это еще и поле битвы, невидимой, но от этого не менее яростной, за нашу с вами цифровую безопасность. Ведь все эти спутники, эти умные железяки, что болтаются у нас над головами, давно уже не просто научные игрушки. Они стали кровью и плотью нашей цивилизации: от навигатора в телефоне и прогноза погоды до

банковских переводов и, чего уж там, обороны целых стран. И вот тут-то на авансцену выходит кибербезопасность, точнее, ее острая, как никогда, необходимость в этой самой космической отрасли.

Будем откровенны: когда полвека назад инженеры корпели над первыми спутниками, о хакерах и кибератаках они если и думали, то где-то в самом конце списка приоритетов. Главное было – запустить, чтоб оно там наверху хоть как-то работало, чтоб сигнал прошел. Безопасность тогда – это больше про защиту от космической радиации или шального метеорита. Но мир перевернулся. Сегодняшний спутник – это, по сути, летающий дата-центр, набитый сложнейшей электроникой и кодом, и он, как любой компьютер здесь, на Земле, чертовски уязвим.

Так откуда ждать беды? Ну, для начала, с Земли. Все эти Центры управления полетами, станции, что ловят и передают сигналы, сети, которые все это хозяйство связывают, – лакомый кусок для киберпреступников. Вломиться в такую систему – это получить ключи от спутника или от данных, которые он шлет. И если раньше это было сюжетом для фантастического боевика, то сегодня – вполне себе рабочая схема. Способы могут быть до банального просты: от фишингового письма, подсунутого сотруднику ЦУПа, до замороченных атак на поставщиков, когда какую-нибудь «закладку» в оборудование вшивают еще на заводе.

А потом – сами спутники. Да, руками до них не дотянешься, гайку не открутишь. Но ведь есть радиоканалы! Именно по ним летят команды, телеметрия, именно по ним текут ценнейшие данные – будь то фотки Земли, метеосводки или сигналы навигаторов. Представьте, что кто-то перехватит управление спутником. Или просто «заглушит» его, как пиратскую радиостанцию. Или подсунет фальшивые данные. Или, чего доброго, отправит команду, которая превратит дорогущую железяку в бесполезный космический мусор. А если кто-то начнет баловаться с сигналами GPS? Хаос на дорогах, в небе, на море – это, поверьте, еще не самое страшное. А если речь зайдет о военных спутниках, то тут последствия могут быть такими, что и представить жутко.

И кто же эти «джентльмены удачи», что могут позариться на космические технологии? Да кто угодно. Тут и государственные спецслужбы, которые ведут свои кибервойны и не брезгуют шпионажем. И обычные бандиты, которые могут попытаться, скажем, «взять в заложники» коммерческий спутник и потребовать выкуп, или стырить ценные коммерческие секреты. И хактивисты, которые хотят громко заявить о какой-то проблеме. Да даже террористы, не дай бог,

могут попытаться использовать космос для своих грязных дел. И не стоит забывать про «вольных стрелков» – талантливых хакеров, которые ломают системы из чистого спортивного интереса или чтобы потешить свое эго.

Самая засада во всей этой истории в том, что многие космические системы – это динозавры, их создавали десятилетия назад, когда о нынешних киберугрозах и не слыхивали. Попробуйте-ка обновить софт на спутнике, который уже лет десять как на орбите крутится. Это вам не винду переустановить – задачка та еще, а порой и вовсе нерешаемая. Плюс к этому, сами спутники часто не могут похвастаться мощными «мозгами» – там каждый ватт энергии на счету, какие уж там навороченные антивирусы или системы обнаружения вторжений. А если добавить сюда длиннющие и запутанные цепочки поставщиков железа и софта – каждый из них может оказаться тем самым слабым звеном, через которое в систему пролезет какая-нибудь гадость.

Так что, все пропало, шеф? Конечно, нет. Инженеры и спецы по кибербезопасности не зря свой хлеб едят. Прежде всего, это подход «безопасность с самого начала» (security by design). То есть, думать о защите нужно не тогда, когда уже все собрано и готово к запуску, а еще на стадии чертежей и первых строчек кода. Шифровать каналы связи – это уже как зубы почистить, само собой. И не абы как, а по-серьезному, чтобы никакая современная отмычка не взяла. Проверять, кто и с какими правами лезет в систему – чтобы команды спутнику отдавал только тот, кому положено, и чтобы сам спутник был уверен, что команда пришла «от своих».

Разрабатываются и особые системы, заточенные под космос, которые будут вынюхивать и блокировать атаки. Много сил вкладывается в то, чтобы сделать системы более живучими – чтобы даже если хакеры куда-то и прорвутся, спутник мог продолжать работать или быстро прийти в себя. И, конечно, без международного сотрудничества тут никуда – нужно договариваться об общих правилах игры, стандартах безопасности, ведь космос-то один на всех, и проблемы одного могут больно ударить по остальным.

Искусственный интеллект с машинным обучением тоже не остаются в стороне – они могут перелопачивать горы данных телеметрии и выискивать всякие подозрительные штуки, которые могут намекать на попытку взлома, причем делают это быстрее и точнее человека. А где-то на горизонте уже маячит квантовая криптография, которая обещает нам чуть ли не стопроцентно защищенные каналы связи, но это, скорее, музыка будущего, хоть и не такого далекого.

Короче говоря, кибербезопасность в космосе – это не просто какая-то модная фишка, а вопрос выживания. Это как ремень безопасности в машине: пока едешь спокойно, о нем и не вспоминаешь, но случись что – он может спасти жизнь. Только в нашем случае – спасти дорогущие аппараты, жизненно важные данные и, возможно, предотвратить крупные неприятности здесь, на Земле. И чем дальше мы будем лезть в космос, чем сильнее наша жизнь будет от него зависеть, тем острее будет стоять этот вопрос. Это игра вдолгую, марафон, а не спринт, и расслабляться тут никак нельзя.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева, Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS.

2. Саенко, С. И. Правовые, организационные и технологические способы обеспечения кибербезопасности на земле и в космосе / С. И. Саенко, В. В. Павлюков // Охрана, безопасность, связь. – 2023. – № 8-1. – С. 100-106. – EDN VXABWI.

3. Желтяков, С. И. Правовые меры защиты информационных систем и данных в космической сфере от кибератак и других угроз / С. И. Желтяков // Актуальные проблемы авиации и космонавтики : Сборник материалов X Международной научно-практической конференции, посвященной 100-летию академика М.Ф. Решетнева и Дню космонавтики. В 3-х томах, Красноярск, 08–12 апреля 2024 года. – Красноярск: Сибирский государственный университет науки и технологий им. акад. М.Ф. Решетнева, 2024. – С. 715-718. – EDN BVHZAA.

4. Шестакова, Е. Н. Правовое регулирование кибербезопасности в космическом пространстве / Е. Н. Шестакова // Международное и национальное право в современных реалиях: задачи и пути их решения : Материалы научной конференции студентов и аспирантов, Москва, 01 июня 2023 года. – Москва: Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации, 2023. – С. 98-104. – EDN SVFAIK.

5. Грудинин, А. М. Информационные технологии и космос / А. М. Грудинин // Экономические и правовые аспекты развития

международной интеграции в современных условиях : материалы Межрегиональной научно-практической конференции студентов, аспирантов и преподавателей, Москва, 19 апреля 2017 года / Московский областной филиал Московского финансово-юридического университета МФЮА. Том 2. – Москва: Московский финансово-юридический университет МФЮА, 2017. – С. 181-183. – EDN ZSPKPV.

***УДК 003.26***

***Акимова Е.А.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И ИХ ВЛИЯНИЕ НА КРИПТОГРАФИЮ

Представьте на секунду: всё, что мы делаем в интернете – от оплаты счетов до секретных переписок – держится на невидимых стражах. Эти стражи – хитроумные шифры, математические головоломки, которые, как мы думали, никому не по зубам. Годами мы доверяли им свои самые сокровенные тайны, полагаясь на то, что даже самые мощные компьютеры будут ковыряться в них целую вечность. Но тут на сцену выходит новый игрок, способный в один миг смести все фигуры с доски – квантовый компьютер. И это не просто "компьютер побыстрее", это совершенно другой способ думать, считать и, увы, взламывать. Он несёт с собой не только фантастические возможности, но и угрозу, от которой у бывалых шифровальщиков волосы встают дыбом.

Так в чём же соль этих квантовых монстров? Если обычный компьютер работает как выключатель – либо "вкл", либо "выкл", ноль или единица, – то квантовый компьютер живёт в мире куда более странном и удивительном. Его "выключатели", кубиты, похожи на волшебные монетки, которые могут одновременно лежать и орлом, и решкой, и ещё кучей состояний между ними. Это называется суперпозиция – такой вот квантовый "и то, и сё одновременно". А если добавить сюда ещё одно квантовое "колдунство" – запутанность, когда два кубита становятся как сиамские близнецы и чувствуют друг друга на любом расстоянии, – то мы получаем машину, способную перебирать варианты с такой скоростью, что наши нынешние суперкомпьютеры покажутся ей древними арифмометрами. По крайней

мере, когда дело доходит до определённых, очень специфических задачек.

И вот тут-то и кроется главная засада для современной криптографии. Самым грозным оружием квантового мира против наших шифров стал алгоритм Шора, придуманный Питером Шором ещё в 1994 году. Эта штука способна с пугающей скоростью разлагать на множители огромные числа – задача, на нерешаемости которой для обычных компьютеров и построена вся система RSA, защищающая львиную долю интернет-соединений. Если классический компьютер будет корпеть над взломом типичного RSA-ключа миллиарды лет, то достаточно мощный квантовый компьютер щёлкнет эту задачку как орешек – за считанные часы, а то и минуты. Такая же печальная участь ждёт и криптографию на эллиптических кривых (ECC), ещё одного кита, на котором держится наша безопасность. Ведь алгоритм Шора так же легко расправляется и с её математической основой. Представьте себе, что все существующие в мире замки вдруг перестали быть преградой. Примерно такие же катастрофические последствия грозят нам, если RSA и ECC падут. Это коснётся всего: защищённых сайтов, цифровых подписей, шифрования почты.

Ну а как насчёт наших старых добрых «симметричных» ребят вроде AES, где один и тот же ключик и запирает, и отпирает? Тут, казалось бы, можно выдохнуть – они не строятся на фокусах с разложением чисел. Но не тут-то было! Для них у квантовых умников тоже припасён «сюрприз» – алгоритм Гровера. Он, конечно, не ломает шифр в открытую, но здорово помогает подобрать ключ методом «тыка», только гораздо быстрее. Чтобы было понятнее: если раньше для взлома ключа надо было перепробовать, ну, скажем, триллион вариантов, то Гровер поможет найти нужный, перебрав всего лишь миллион. Звучит круто для взломщика, правда? А для нас это значит, что для былой надёжности ключи придётся делать в два раза длиннее. Тот же 128-битный AES, который сегодня считается почти неприступной крепостью, перед квантовой атакой станет хлипким, как 64-битный заборчик для обычного взлома. А это уже, знаете ли, дыра в броне, а не надёжная защита. Так что, хотя симметричные шифры и не сдадутся без боя, их броню придётся серьёзно наращивать.

Естественно, криптографы всего мира не стали сидеть сложа руки и ждать, пока эта «квантовая буря» снесёт всё к чертям собачьим. Так и зародилось целое движение – постквантовая криптография. Говоря по-человечески, это попытка придумать шифры, которым квантовые супермозги будут не по зубам. Учёные мужи (и дамы!) сейчас, как заправские инженеры, возводят новые математические «крепости»,

которые, по их расчётам, должны устоять даже под самым яростным квантовым штурмом. И кандидатов в эти «новобранцы» уже хватает, каждый со своей изюминкой:

Например, шифры на решётках. Это как если бы вам предложили найти иголку в невероятно запутанном, многомерном стоге сена – или, если хотите, выбраться из хитроумного лабиринта, где каждый поворот сложнее предыдущего. Задачка та ещё, зато считается очень перспективным направлением – и надёжно, и работает довольно резво.

Есть ещё криптография на кодах. Тут идея в том, чтобы так запутать сообщение с помощью специальных кодов (похожих на те, что исправляют ошибки при передаче данных), что расшифровать его без ключа становится практически нереально. Старый добрый алгоритм Мак-Элиса из этой оперы держится аж с 1978 года, и хоть бы хны!

Не забываем про шифры на хеш-функциях. Эти ребята строят цифровые подписи, полагаясь целиком и полностью на надёжность хешей – таких уникальных «отпечатков пальцев» для любых данных. Подписи получаются железобетонные, но иногда ключи или сами подписи выходят громоздкими, или же их можно использовать только один раз.

Многомерная криптография – звучит уже устрашающе, правда? Тут вся соль в решении таких зубодробительных систем уравнений с кучей неизвестных, что даже у математиков голова кругом идёт.

И, наконец, экзотика – шифры на изогениях. Это довольно свежее направление, где используются очень абстрактные математические «тропинки» между эллиптическими кривыми. Зато ключи у них получаются на удивление компактными, почти как у классики.

Американский Национальный институт стандартов и технологий (NIST) уже не первый год проводит настоящий кастинг этих постквантовых алгоритмов, отбирая самых-самых со всего света. И скоро мы увидим первых "выпускников" – официальные стандарты новой, квантово-стойкой криптографии.

Переодеться всем миром в новые "квантово-стойкие одежды" – задачка, мягко говоря, не из лёгких. Это затронет всё, от наших телефонов до государственных систем. И одна из самых коварных проблем – это так называемая тактика "собери сейчас, расшифруй потом". Представьте: злоумышленники уже сегодня, как запасливые цифровые пираты, могут собирать зашифрованные данные, которые кажутся им ценными, и просто ждать, когда появятся достаточно мощные квантовые компьютеры, чтобы вскрыть их. Это особенно опасно для информации, которая должна оставаться секретной долгие

годы – государственные тайны, истории болезней, коммерческие секреты.

Поэтому тянуть с переходом на постквантовую защиту нельзя. Скорее всего, сначала мы будем использовать "гибриды" – старые добрые шифры вместе с новыми, постквантовыми, чтобы подстраховаться со всех сторон. Компаниям и организациям придётся научиться "криптографической гибкости" – умению быстро и безболезненно менять шифры, как только появляются новые, более надёжные, или если в старых находят дыры.

Забавно, что сама квантовая физика, которая создаёт нам проблемы, может подкинуть и решение. Есть такая штука, как квантовое распределение ключей (QKD). Используя фундаментальные законы квантового мира (например, тот факт, что нельзя измерить что-то, не изменив это), можно создавать абсолютно защищённые каналы для передачи секретных ключей. Любая попытка подслушать тут же будет замечена. Правда, и у QKD есть свои "но": оно пока не решает проблему, как убедиться, что ты передаёшь ключ именно тому, кому нужно, да и на большие расстояния без специальных "перевалочных пунктов" сигнал не передать. Но как дополнительный слой защиты для особо важных данных – очень даже перспективно.

Итак, что мы имеем в сухом остатке? Квантовые компьютеры – это не просто "ещё одна железка", а настоящий тектонический сдвиг, который ставит перед всем цифровым миром задачу выживания. Пусть машины, способные взломать нынешние шифры, – это ещё дело завтрашнего дня, но это "завтра" приближается с каждым днём всё быстрее. Делать вид, что ничего не происходит, – значит играть с огнём. Разработка, проверка и внедрение постквантовой защиты – это уже не вопрос "а вдруг?", а вопрос "когда?", и это "когда" уже стучится в дверь. Это будет непросто, но это цена, которую мы должны заплатить за безопасность нашего цифрового будущего в мире, где квантовые технологии станут такой же обыденностью, как сегодня смартфоны.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева, Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS.

2. Тачмурадов, М. Будущее Квантовых Вычислений: Трансформация Вычислительных Парадигм / М. Тачмурадов, Ш. Дурдыев, М. Ниязгельдиев // Открытия, прорывы и перспективы в науке : Сборник материалов XII-ой международной очно-заочной научно-практической конференции, Москва, 09 октября 2024 года. – Москва: Научно-издательский центр "Издание", 2024. – С. 83-86. – EDN MRCRTE.

3. Наташкин, Д. А. Перспективы квантовых вычислений в информационных технологиях / Д. А. Наташкин // Векторы развития современной науки : Сборник статей II Международной научно-практической конференции, Петрозаводск, 27 декабря 2023 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2023. – С. 55-62. – EDN LFKPYU.

4. Криптография будущего - это квантовая криптография // Фотоника. – 2020. – Т. 14, № 5. – С. 412-413. – EDN NKUVGF.

5. Лаптева, Е. А. Криптография. История криптографии / Е. А. Лаптева // Конкурентоспособность территорий : материалы XXVI Всероссийского экономического форума молодых ученых и студентов, Екатеринбург, 26–29 апреля 2023 года / Уральский государственный экономический университет. Том Часть 2. – Екатеринбург: Уральский государственный экономический университет, 2023. – С. 12-14. – EDN ZPIOER.

***УДК 004.8***

***Акимова Е.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИИ-МОШЕННИЧЕСТВО: КАК НЕЙРОСЕТИ УПРОЩАЮТ ВЗЛОМ ЧЕЛОВЕЧЕСКОГО ДОВЕРИЯ

Мы живем в такое время, когда цифровой мир, где информация летит со скоростью света, стал ареной для тревожной метаморфозы старых как мир мошеннических схем. Искусственный интеллект, особенно его «мозг» – нейросети, подливает масла в огонь этих перемен, давая нечистым на руку дельцам такие инструменты для игры на человеческом доверии, о которых раньше и мечтать не могли. Если когда-то, чтобы состряпать убедительную фальшивку, нужно было приложить немало сил и обладать особыми талантами, то сегодня

нейросетевые алгоритмы позволяют поставить обман на поток, сделать его куда более изощренным, таким, что и не сразу раскусишь.

То, как современные языковые модели, вроде нашумевших GPT и их собратьев, научились писать тексты, которые не отличишь от написанных человеком, — это просто какой-то Клондайк для тех, кто хочет создавать убедительные фишинговые письма, личные сообщения в мессенджерах, да что там – целые правдоподобные истории для социальной инженерии. Раньше-то мошенникам приходилось попотеть, чтобы составить грамотное и психологически верное письмецо, часто они делали ляпы, которые их и выдавали, особенно если пытались работать не на своем родном языке. А теперь? Нейросеть в мгновение ока наклепает контента на любом языке, идеально подогнанного под нужную аудиторию, учтет и культурные тонкости, и манеру общения. Эти системы способны перелопатить гигантские объемы данных из открытых источников, тех же соцсетей, чтобы составить такие подробные досье на потенциальных жертв, что мошенники могут обращаться к ним с предложениями или угрозами, которые выглядят до жути адресными и личными.

А уж технология синтеза и клонирования голоса – это вообще что-то из ряда вон выходящее по своей коварности. Хватает буквально пары секунд аудиозаписи голоса человека, чтобы нейросеть воссоздала его с пугающей точностью, сохранив и интонации, и тембр. Это распахивает двери для нового поколения вишинга – голосового фишинга, когда мошенники могут звонить от имени ваших родных, коллег или представителей каких-нибудь служб, используя синтезированный голос. Представьте: звонок, а на том конце провода – «ваш ребенок» с мольбой срочно перевести деньги из-за какой-то выдуманной беды, или «начальник» с грозным требованием немедленно оплатить невесть какой счет. Эмоциональный удар в таких случаях такой силы, что времени на трезвую оценку ситуации почти не остается.

Рука об руку с этим идет и развитие дипфейков – синтетических картинок и видео, где лицо одного человека приделывают к телу другого или вообще создают полностью вымышленный, но до ужаса реалистичный видеоряд. Если раньше качественный видеомонтаж был уделом профи, то сейчас появляются все более «народные» инструменты, позволяющие генерировать дипфейки почти на коленке. Это прямой путь к шантажу, к попыткам очернить человека, к мошенническим схемам, где жертва якобы получает видеосообщение от человека, которому доверяет, с просьбой о помощи или компрометирующее видео с собственным участием. Убедительность

таких материалов способна сломить даже самых прожженных скептиков.

Весь фокус ИИ-мошенничества не только в технологических наворотах, но и в том, как тонко оно играет на струнах человеческой души. Нейросети позволяют автоматизировать и масштабировать атаки, которые бьют по нашим когнитивным слабостям: мы склонны искать подтверждение своей точке зрения, поддаемся «эффекту ореола», боимся упустить выгоду. Массовая рассылка писем, которые выглядят так, будто написаны лично вам, имитируя стиль общения конкретного человека или организации, многократно увеличивает шансы на успех. Эффект срочности, авторитета, «все так делают» – все эти крючки становятся доступнее благодаря способности ИИ создавать иллюзию подлинности и персонализации в невиданных ранее масштабах. Мошенники могут даже задействовать ИИ для анализа реакции жертвы в режиме реального времени и тут же менять свою тактику, превращая обман в живой, подстраивающийся процесс.

И вот тут-то последствия такого «апгрейда» мошенничества выходят далеко за рамки дыры в чьем-то кошельке. Происходит то, что можно назвать эрозией базового человеческого доверия – того самого фундамента, на котором держатся наши социальные и экономические связи. Когда уже не понимаешь, где правда, а где искусно слепленная подделка, люди начинают смотреть волком на любую информацию, приходящую по цифровым каналам. Это мешает нормальному общению, подрывает веру в институты и даже в отношения между людьми, ведь каждый может стать объектом или, хуже того, орудием манипуляции. Складывается какая-то дикая ситуация: технологии, придуманные, чтобы объединять людей и упрощать обмен информацией, становятся инструментом разобщения и тотального недоверия.

Что делать со всей этой напастью? Нужен комплексный подход, тут одним махом не решишь. Разработка хитрых алгоритмов, которые будут вычислять ИИ-сгенерированный контент, создание цифровых «водяных знаков» и систем, подтверждающих подлинность, – это все важные технические задачки. Но не менее важно и другое – повышать цифровую грамотность людей, учить их критически мыслить и постоянно быть в курсе новых уловок мошенников. Важно прививать культуру «цифровой гигиены»: проверять информацию по нескольким источникам, с опаской относиться к неожиданным просьбам и сообщениям, даже если они вроде как от знакомых.

Получается, что нейросети – штука с огромным потенциалом для добра – в руках нечистоплотных дельцов превращаются в реально

опасное оружие для взлома человеческого доверия. То, что создавать высококачественные подделки и персонализированные атаки стало в разы проще, требует от общества и от каждого из нас повышенной бдительности и готовности приспосабливаться к новой реальности, где подлинность – понятие все более туманное. Борьба с ИИ-мошенничеством – это не просто гонка технологий, это, если хотите, борьба за то, чтобы оставаться людьми в этом все более цифровом мире.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство: Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.
2. Галимова, А. А. Виды мошенничества с применением искусственного интеллекта / А. А. Галимова // Формирование финансовой культуры в образовательных организациях: интеграция финансовой и цифровой грамотности: Материалы XI Всероссийской научно-практической конференции. В 2-х томах, Институт развития образования Республики Башкортостан, 28 ноября 2024 года. – Уфа: Институт развития образования Республики Башкортостан, 2024. – С. 40-42. – EDN AUBAPT.
3. Краснова, Е. Д. Нейросеть как источник современного мошенничества / Е. Д. Краснова, С. П. Лозовская // Безопасность личности, общества и государства: теоретико-правовые аспекты : Сборник научных статей XVII международной научной конференции обучающихся образовательных организаций высшего образования, проводимой в рамках IV Санкт-Петербургского международного молодежного научного форума "Северная Пальмира: территория возможностей", Санкт-Петербург, 30 мая 2024 года. – Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2024. – С. 1626-1633. – EDN KDNHAZ.
4. Коломыцева, Е. П. Информационные технологии и экология / Е. П. Коломыцева, А. В. Портнова. // XII Международный молодежный форум "Образование. Наука. Производство". - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2020. - С. 1969-1972.

5. Гекк, Б. В. Борьба с киберпреступностью в РФ: анализ явления и законодательные меры противодействия / Б. В. Гекк // Молодой ученый. – 2024. – № 8(507). – С. 149-151. – EDN LPHOLD.

***УДК 004***

***Акимова Е.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## АНОНИМНОСТЬ В DARKNET: МИФЫ И РЕАЛЬНОСТЬ

Даркнет… Одно только слово, а в голове сразу рисуются картинки какого-то цифрового подполья, этакого Дикого Запада интернета, где, как нам кажется, можно творить что угодно, ведь ты полностью анонимен, как невидимка. Продавцы всякой дряни, хитрые хакеры, неугодные властям диссиденты – все они, по слухам, прячутся там, укрывшись за непроницаемой завесой технологий. Но насколько это правда? Так ли крепка эта броня анонимности, о которой слагают легенды, и где заканчиваются факты, уступая место досужим вымыслам?

Давайте сразу начистоту: идея, что Даркнет – это какая-то неприступная цифровая цитадель, где каждый твой шаг надежно скрыт от чужих глаз, – это, мягко говоря, большое преувеличение. Спору нет, штуки вроде Tor (тот самый «луковый маршрутизатор»), I2P или Freenet действительно дают куда больше приватности, чем наш обычный, повседневный интернет. Сама идея, например, в Tor, построена хитро – на «луковой маршрутизации». Представьте себе кочан капусты: ваши данные, прежде чем долететь до цели, прыгают по цепочке случайных серверов, и каждый раз «оборачиваются» новым слоем шифрования, как капустный лист. Каждый узел в этой эстафете видит только соседа слева и соседа справа, но не всю трассу целиком. И уж точно не знает, кто вы и куда конкретно ваш запрос в итоге прилетит. Вроде бы, железобетонно, да?

Но, как обычно, вся соль в нюансах. Во-первых, самая большая дыра в любой системе анонимности – это, как ни банально, сам человек. Простая неосторожность, незнание технических тонкостей или обычная человеческая рассеянность могут пустить коту под хвост все эти навороченные шифры. Ну, например, ляпнуть один и тот же никнейм в Даркнете и в обычном интернете, залогиниться в свою реальную почту

или соцсеть через Tor, или даже просто болтать о вещах, которые могут на вас указать. Если в браузере Tor (который по умолчанию это дело блокирует из-за безопасности) включить JavaScript, то через какую-нибудь дыру в нем может «утечь» ваш настоящий IP-адрес. Скачали или загрузили файлик, а в нем – сюрприз! – метаданные: какая камера сделала фотку, кто автор документа Word. Классика жанра саморазоблачения. Народ часто думает, что анонимность – это как антивирус: поставил и забыл. А на самом деле это целая наука, комплекс мер предосторожности, то, что спецы называют операционной безопасностью (OPSEC).

Во-вторых, и сама сеть – не стальной сейф. Хотя вскрыть шифрование Tor «в лоб» – задачка из разряда почти невыполнимых, есть обходные пути. Например, так называемая атака по времени, или корреляционная. Если кто-то контролирует достаточно много точек, где ваш трафик входит в сеть Tor и где он из нее выходит в обычный интернет, то, сопоставляя время и объемы данных, можно с некоторой вероятностью связать вас с вашей активностью. Да, это требует колоссальных ресурсов, но для серьезных ребят из спецслужб или крупных хакерских банд это уже не выглядит такой уж фантастикой. Уже были прецеденты, когда исследователи показывали, как можно вычислять пользователей Tor, находя лазейки в самом браузере или подсовывая свои, «зараженные» узлы.

А самое слабое звено в этой цепи – это выходные узлы Tor. Почему? Да потому что именно через них ваш трафик вываливается в «чистый» интернет, и там он уже не прикрыт шифрованием самого Tor (хотя, если сайт работает по HTTPS, то соединение все равно будет защищено). Так вот, кто контролирует такой выходной узел, тот может, как рыбак сетью, вылавливать незашифрованные данные: логины, пароли, переписку. Вот почему пользоваться HTTPS, когда вы в Даркнете, особенно если лезете на обычные сайты, – это просто жизненно необходимо.

Понятное дело, и правоохранители не дремлют. Они вовсю разрабатывают и используют свои фишки для борьбы с преступностью в Даркнете: внедряют агентов, вербуют информаторов, ломают серверы с нелегальщиной (вспомните громкие истории с Silk Road или AlphaBay), или ищут дыры в программах, которыми пользуются сами преступники. Иной раз людей ловят не потому, что взломали сам Tor, а потому что они сами наделали глупостей или попались в хитроумные сети оперативных разработок.

И да, не стоит питать иллюзий: огромная часть того, что плавает в Даркнете, – это не какие-то там тайные сокровища или эксклюзив, а

банальный развод, фейки и ловушки. Их расставляют либо мошенники, либо те же самые органы, чтобы подловить слишком любопытных или неосторожных.

Но знаете, было бы большой ошибкой видеть в Даркнете одно только зло и считать его прибежищем исключительно для отморозков. Для кучи людей, которые живут там, где за неосторожное слово можно сесть или где интернет под тотальным контролем, Даркнет – это чуть ли не единственный глоток свежего воздуха. Шанс получить доступ к независимой информации, свободно высказаться или безопасно связаться с внешним миром. Журналисты, правозащитники, всякие активисты – они могут использовать эти инструменты анонимности, чтобы защитить свою работу и тех, кто им помогает. И тут уже анонимность Даркнета – это не плащ-невидимка для бандита, а скорее щит для свободы слова и прав человека.

Так что, как видите, с этой самой анонимностью в Даркнете все куда запутаннее и интереснее, чем кажется на первый взгляд. Это вам не волшебная палочка, которая делает невидимым, а довольно сложный инструмент. И то, насколько он будет эффективен, зависит от того, насколько хорошо ты сам в нем разбираешься, насколько ты дисциплинирован, и как быстро меняется вся эта кухня угроз и методов защиты. Стопроцентной анонимности, скорее всего, не бывает нигде, и Даркнет тут не исключение. Это вечная игра в кошки-мышки: одни придумывают, как спрятаться, другие – как их найти. И вот понимать этот тонкий баланс между сказками и реальностью – чертовски важно для любого, кто решит нырнуть в эти мутные, но порой и необходимые, глубины интернета.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева, Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS.

2. Свищев, А. В. Darknet: полезный инструмент или источник угрозы / А. В. Свищев, А. С. Лаухина // Colloquium-Journal. – 2020. – № 10-2(62). – С. 66-69. – DOI 10.24411/2520-6990-2020-11702. – EDN BKULZO.

3. Симаков, А. А. Анонимность в глобальных сетях / А. А. Симаков // Научный вестник Омской академии МВД России. – 2017. – № 2(65). – С. 62-65. – EDN YZIEQR. 4. Криптография будущего - это квантовая криптография // Фотоника. – 2020. – Т. 14, № 5. – С. 412-413. – EDN NKUVGF.

4. Караулова, О. А. Тёмная сторона анонимности - Даркнет / О. А. Караулова, Н. В. Киреева // Этнополитический и религиозный экстремизм в России: социально-культурные истоки, угрозы распространения в информационной среде, методы противодействия : Сборник материалов Всероссийской молодежной научной школы-конференции, Уфа, 04–05 декабря 2020 года. – Уфа: ООО "Издательство "Диалог", 2020. – С. 32-37. – EDN APKKYE.

5. Попов, А. Д. Основы функционирования Даркнет / А. Д. Попов // Охрана, безопасность, связь. – 2023. – № 8-3. – С. 57-61. – EDN UJJIYG.

6. Сетько, А. А. Darknet - одна из сторон интернета / А. А. Сетько, Ю. Н. Швец // Наука - образованию, производству, экономике : материалы XXII (69) Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов: в 2 томах, Витебск, 09–10 февраля 2017 года. Том 2. – Витебск: Витебский государственный университет им. П.М. Машерова, 2017. – С. 78-80. – EDN YNPMFZ.

***УДК 004.8***

***Акимова Е.А.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## УЯЗВИМОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ В КИБЕРБЕЗОПАСНОСТИ

Искусственный интеллект сегодня – это уже не фантастика, а наш повседневный помощник, от врачебного кабинета до беспилотного такси. Но у этой медали есть и оборотная сторона: новые технологии породили и новые, изощрённые угрозы. Среди них особенно коварны так называемые adversarial-атаки – хитрые трюки, которыми злоумышленники умудряются обмануть даже самые навороченные алгоритмы.

Эта проблема стала по-настоящему горячей в последние пять лет. Именно тогда исследователи начали находить просто поразительные

способы водить нейросети за нос. Классика жанра: берём фото панды, добавляем капельку хитрого «шума» – глазу он почти не виден, – а нейросеть уже с полной уверенностью заявляет: «Это гиббон!». Легко представить, чем могут обернуться такие «фокусы» в системах безопасности аэропортов или когда банк пытается опознать вас по лицу.

**Так как же злоумышленникам удаётся обвести ИИ вокруг пальца?**

Если упрощать, то атаки можно разделить по тому, когда именно они наносятся.

Есть, например, «отравляющие» атаки, которые происходят ещё на этапе «воспитания» модели. Представьте, что вы тайком подсовываете нейросети-«студенту» учебники с поддельными фактами. Незаметно для «преподавателя» (разработчика), модель впитывает искажённые знания, и её «мировоззрение» смещается. В итоге она будет принимать неверные решения, даже не подозревая об этом.

Но гораздо чаще встречаются атаки уже на готовую, обученную модель. Здесь фантазия злоумышленников не знает границ. Например, хитрый узор на очках – и система распознавания лиц принимает вас за другого человека. А есть и «универсальные отмычки» – специальные изображения или сигналы, которые способны обмануть сразу несколько разных моделей.

Особняком стоят атаки, цель которых – не просто обмануть, а «вскрыть» саму модель. Подобно шпиону, злоумышленник задаёт системе каверзные вопросы, анализирует ответы и постепенно «вычисляет» её архитектуру, а то и конфиденциальные данные, на которых её учили. Для компаний, чьи ИИ-модели – это интеллектуальная собственность и коммерческая тайна, такие утечки сродни катастрофе.

**Можно ли вообще защититься от этой напасти?**

Задача, прямо скажем, не из лёгких, но инженеры и учёные не сидят сложа руки.

«Прививка от обмана» (Adversarial Training): Модель, как новобранца, на этапе обучения «натаскивают» на типичные трюки мошенников. Столкнувшись с ослабленной угрозой, она учится ей противостоять. Правда, это как гонка вооружений: метод требует уйму ресурсов и не спасёт от совершенно новых, ещё не известных атак.

«Детекторы лжи» для ИИ (Обнаружение аномалий): Специальные алгоритмы выискивают в поступающих данных странности и аномалии, которые могут указывать на попытку обмана. Они как бы стоят на входе, пропуская к основной модели только «чистые» данные.

Математическое «доказательство» надёжности (Формальная верификация): Учёные пытаются математически доказать, что при определённых условиях модель будет вести себя предсказуемо, как её ни пытайся обмануть. Пока это работает в основном для простых моделей, но это важный шаг к созданию систем, которым можно доверять.

«Запутывание следов» (Обфускация): Сложнее всего защищаться, когда хакер знает модель «как облупленную» (white-box атаки). Тут на помощь приходят методы «запутывания следов». Можно, например, слегка «зашумлять» ответы системы или время от времени менять её настройки. Атакующему становится гораздо труднее понять, как именно работает ИИ, и подобрать к нему «ключик».

ИИ с «иммунитетом» (Самоадаптирующиеся системы): Мечта разработчиков – создать ИИ, способный сам адаптироваться к новым угрозам, учиться на атаках и постоянно усиливать свою защиту. Это как если бы ваш антивирус сам писал обновления против только что появившихся вирусов. Звучит здорово, но пока это скорее из области научной фантастики – технических и теоретических препятствий масса.

**А как же этика?**

Борьба с обманом ИИ – это не только гонка технологий, но и серьёзная этическая головоломка. Создавая всё более «подозрительные» и защищённые системы, мы рискуем перегнуть палку. Где та грань, за которой необходимая осторожность превращается в паранойю, отсекающую добросовестных пользователей? Представьте, что система в больнице или суде ошибочно примет честный запрос за атаку – цена такой ошибки может быть человеческая судьба.

Разработчики мечутся между желанием сделать ИИ неуязвимым и необходимостью сохранить его полезность и доступность. Это уже не просто инженерная задача, а вопрос, требующий участия юристов, социологов и философов. Возможно, будущее за ИИ, который не просто слепо блокирует «подозрительное», а пытается понять контекст и намерения человека – как опытный охранник, отличающий туриста от грабителя.

**Что день грядущий нам готовит?**

Уязвимость ИИ к обману – это бомба замедленного действия под нашим всё более цифровым обществом. Ведь мы доверяем алгоритмам всё больше: от постановки диагнозов до управления городским трафиком. И если их можно так легко обмануть, это уже вопрос не технологий, а нашей с вами безопасности.

Скорее всего, панацеи не будет. Будущее – за многослойной обороной, где разные методы защиты дополняют друг друга, как в средневековом замке с его рвами, стенами и башнями. Но и расслабляться не стоит: это вечная игра в «кошки-мышки», где хакеры и защитники постоянно меняются ролями, изобретая всё новые уловки и контрмеры.

В сухом остатке, adversarial-атаки – это не просто техническая загвоздка, а лакмусовая бумажка, показывающая фундаментальные слабости нынешнего поколения ИИ. Они заставляют нас задуматься: а что вообще такое «интеллект», если его так легко провести? Чтобы построить действительно умные и надёжные системы будущего, понадобятся усилия не только программистов и математиков, но и специалистов по кибербезопасности, психологов, лингвистов и даже философов. Это вызов, который мы должны принять все вместе.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство: Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Норкина, А. Н. Искусственный интеллект (ИИ) и кибербезопасность / А. Н. Норкина, С. С. Носова // Финансовая безопасность - новые горизонты : Материалы X Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 19–20 ноября 2024 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2024. – С. 436-441. – EDN UJHIMH.

3. Уязвимости ИИ: угрозы и атаки на процесс сериализации моделей и их вычислительные графы / Н. М. Григорьева, Д. Н. Лисов, Ф. Д. Епишев [и др.] // The 2024 Symposium on Cybersecurity of the Digital Economy - CDE'24 : Сборник трудов VIII международной научно-технической конференции, Казань, 23–25 сентября 2024 года. – Санкт-Петербург: ООО Издательский Дом "Афина", 2024. – С. 127-132. – EDN PFEQIW.

4. Коломыцева, Е. П. Информационные технологии и экология / Е. П. Коломыцева, А. В. Портнова. // XII Международный молодежный форум "Образование. Наука. Производство". - Белгород: Белгородский

государственный технологический университет им. В.Г. Шухова, 2020. - С. 1969-1972.

5. Синякин, И. Н. Как можно обмануть генеративный искусственный интеллект и какие уязвимости существуют / И. Н. Синякин, В. Е. Реебер // Технические науки: проблемы и решения: сборник статей по материалам XCI международной научно-практической конференции, Москва, 17 декабря 2024 года. – Москва: Общество с ограниченной ответственностью "Интернаука", 2024. – С. 28-33. – EDN BWKDUK.

***УДК 004***

***Акуппа Ю.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МЕДИЦИНЕ

За прошедшие десять лет блокчейн эволюционировал из малоизвестной идеи в популярную технологию, активно используемую в разных областях, в том числе в здравоохранении. Его децентрализованность и распределённость, невозможность внесения изменений в записи и поддержка смарт-контрактов открывают новые перспективы для улучшения сервисов и повышения их надежности.

В медицинской отрасли блокчейн применяется для управления электронными медицинскими записями, обеспечения безопасного обмена информацией, контроля поставок медикаментов, медицинского страхования и удаленного наблюдения за пациентами. Его внедрение способствует уменьшению расходов на обработку данных, росту прозрачности и защите личной информации. Помимо этого, криптовалютные решения на основе блокчейна способны упрощать проведение платежей в медучреждениях.

Блокчейн - это общий цифровой реестр, состоящий из последовательных «блоков», которые формируют непрерывную «цепь». У каждого пользователя системы хранится копия этого реестра, и все вместе они подтверждают каждое изменение, что исключает необходимость в посредниках. Данные могут включать информацию о транзакциях, соглашениях, цифровых активах, идентификационных данных и любых других цифровых записях.

Использование криптографических методов обеспечивает

неизменность данных и защиту от фальсификации. Механизмы открытого/закрытого ключа, хеширование и цифровая подпись гарантируют высокий уровень безопасности и позволяют участникам сети взаимодействовать, не опасаясь мошенничества.

Одним из первых практических применений блокчейна оказалась криптовалюта, наиболее известным представителем которой является Биткойн. Со временем возникли и другие платформы, например, Ethereum и IPFS, предлагающие расширенные возможности.

В блокчейне Биткоина применяется криптография на эллиптических кривых. Структура блока содержит хэш предыдущего блока, хэш всех транзакций, отметку времени, параметры для майнинга и перечень транзакций.

Транзакции в блокчейне состоят из входов и выходов: входы указывают на источники средств, а выходы — на адреса получателей. Для их обработки применяется специальный язык программирования, а также механизмы консенсуса, гарантирующие единогласное подтверждение каждой новой записи всеми участниками сети.

Блокчейн прочно закрепился в медицине, предлагая решения для хранения и управления медицинской информацией, улучшения прозрачности поставок лекарств и оптимизации страховых процессов. Благодаря технологии распределенного реестра медицинские записи становятся более защищенными, неизменяемыми и удобными для обмена между различными медицинскими организациями.

Применение блокчейна позволяет создать надежную систему хранения медицинских карт пациентов. Такая система обеспечивает мгновенный доступ к данным для врачей, минимизирует вероятность ошибок и повышает безопасность информации. Записи невозможно подделать или потерять, так как все изменения фиксируются в реестре и доступны только с разрешения пациента.

Современные медицинские устройства постоянно собирают данные о здоровье пациентов. Блокчейн позволяет надежно регистрировать и отслеживать эти данные, предотвращая подделку или несанкционированные изменения. В результате улучшается контроль за состоянием пациентов, а также повышается эффективность диагностики и лечения.

Фальсификация лекарственных средств – серьезная проблема. Блокчейн помогает отслеживать путь каждого препарата от производителя до конечного потребителя. Записывая информацию о каждой стадии поставки в блокчейн, можно гарантировать подлинность препарата, сократить потери и предотвратить незаконное распространение контрафактных лекарств.

Страховые компании могут использовать блокчейн для автоматизации процессов, связанных с обработкой заявок. Смарт-контракты позволяют мгновенно проверять условия страхового полиса и подтверждать выплаты без привлечения посредников. Это снижает вероятность мошенничества и ускоряет предоставление страховых услуг.

Блокчейн всё чаще используется в системах удалённого наблюдения за пациентами. За счёт интеграции с носимыми гаджетами и датчиками, мед. информация фиксируется в реестре и видна врачам в реальном времени. Это помогает следить за состоянием пациентов с затяжными болезнями, предупреждать ухудшения и вовремя менять терапию.

Блокчейн гарантирует высокий уровень безопасности медицинских данных. Шифрование и система прав доступа дают пациентам возможность управлять доступом к своей информации. Медучреждения могут ограничивать или открывать доступ к данным, исходя из статуса запроса, что усиливает конфиденциальность.

Технология блокчейн способствует укреплению доверия между пациентами, врачами и фармацевтическими компаниями. Алгоритмы консенсуса делают невозможным подделку данных, а все изменения записываются в реестр и доступны для проверки в любое время.

В России уже стартовало внедрение блокчейн-технологий в медицинские проекты. В ряде регионов разворачиваются системы контроля за оборотом лекарств, основанные на распределенном реестре. Это дает возможность отслеживать расход дорогостоящих медикаментов и исключать их нерациональное использование.

С развитием цифровизации блокчейн приобретает всё большее значение в здравоохранении. Он позволяет построить безопасную среду для обмена медицинской информацией, уменьшить вероятность мошенничества и улучшить работу медицинских организаций. В будущем прогнозируется расширение использования данной технологии, в том числе её интеграция с искусственным интеллектом для анализа медицинских данных и создания индивидуальных подходов к лечению.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Жданова С.И., Иванов И.В. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра // В сб.: Материалы конференций ГНИИ "НАЦРАЗВИТИЕ". Июнь 2017: Сборник избранных статей. - СПб.: ГНИИ

"НАЦРАЗВИТИЕ", 2017 с. 116-119.

2. Сергей Павлов. Bitcoin in a nutshell - Blockchain. URL: https://habr.com (Дата обращения: 15.05.2018).

3. Куракова, Н.Г. Технологии блокчейн в здравоохранении: позиции России на глобальном публикационном ландшафте / Н.Г. Куракова, О.В. Черченко, Л.А. Цветкова // Врач и информационные технологии. – 2021. – № 1. – С. 25-39.

4. Блокчейн в медицине и фармацевтике: полный обзор возможностей [Электронный ресурс]. − Режим доступа: https://vc.ru − Дата доступа: 10.04.2023.

5. Вишняков, В.А. Технология блокчейн в образовании и ИТ-медицине: модели, алгоритмы, программные средства. Монография. / В.А. Вишняков, Д.А. Качан. – Минск: РИВШ, 2023. – 184 с

***УДК 004***

***Акуппа Ю.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕМ С ИСПОЛЬЗОВАНИЕМ ДАТЧИКОВ

В современных крупных городах усиливаются проблемы, обусловленные интенсивным движением транспорта: пробки становятся все более частыми, растет число дорожно-транспортных происшествий, ухудшается состояние окружающей среды. Одним из главных способов преодоления этих трудностей является внедрение автоматизированных комплексов регулирования дорожного трафика, основанных на технологиях "Интернета вещей" (IoT).Эти технологии позволяют создавать "умные" транспортные сети, оптимизирующие передвижение транспорта, повышающие уровень безопасности на дорогах и уменьшающие отрицательное воздействие на экологию. IoT-системы могут анализировать ситуацию на дорогах в режиме реального времени, настраивать работу светофоров, изменять маршруты общественного транспорта и другие показатели, что позволяет сократить пробки и снизить выбросы загрязняющих веществ.

В интеллектуальных транспортных системах ключевую роль играют IoT-устройства, такие как сенсоры обнаружения, видеокамеры, радары и лидары. Эти устройства, использующие оптические, инфракрасные и радиоволновые технологии, способны с высокой

точностью регистрировать объекты в пределах своей зоны действия. Например, датчики присутствия, работающие на основе линз Френеля, реагируют на изменения температуры окружающей среды при появлении человека или машины. При обнаружении объекта информация передается в централизованную систему управления, где она анализируется для принятия оперативных решений.

Интеллектуальное регулирование светофорных объектов выступает одним из ключевых направлений автоматизации транспортного потока. В противовес традиционным схемам, функционирующим на основе заданных временных циклов, IoT-технологии предоставляют возможность интеграции гибких алгоритмов, анализирующих текущие условия на дороге. Допустим, при приближении пешехода к пешеходному переходу, сенсор инициирует отправку сигнала на светофор, который активирует зеленый свет в течение 5 секунд. Подобные меры приобретают особую значимость в районах с интенсивным пешеходным движением, таких как учебные заведения, рекреационные зоны и жилые массивы. Это способствует не только повышению уровня безопасности для пешеходов, но и уменьшает риск дорожно-транспортных происшествий, вызванных отвлечением внимания водителей.

При создании автоматизированных комплексов регулирования трафика на дорогах критически важно придерживаться установленных правил и норм. К примеру, порядок смены сигналов светофора должен быть строго регламентирован: красный → красный с жёлтым → зелёный → жёлтый → красный. Длительность одновременного включения красного и жёлтого сигналов не должна быть больше 2 секунд, а жёлтого – не более 3 секунд. Соблюдение подобных стандартов является гарантом безопасности для всех участников движения, включая водителей и пешеходов, поскольку существенно снижает вероятность ДТП.

В современных системах управления транспортом радарные сенсоры играют ключевую роль. Они применяются для вычисления скорости приближения и дистанции до различных объектов, включая транспортные средства, людей и другие преграды. Принцип действия радарного датчика заключается в излучении электромагнитных волн и фиксации их отражений от объектов, что позволяет определить их положение в пространстве и скорость движения. На основании полученной информации система может оповестить водителя о возможной угрозе столкновения или даже автоматически активировать элементы управления автомобилем, например, систему торможения или рулевое управление. Радарные сенсоры функционируют в диапазоне

радиочастот сверхвысокой частоты (20–100 ГГц), что гарантирует высокую точность измерений. Для улучшения устойчивости к помехам и предотвращения ошибочных срабатываний используются методы цифровой обработки сигналов и повышение частоты излучения.

Применение технологий интернета вещей в сфере организации дорожного движения открывает широкие возможности. Прежде всего, они значительно улучшают дорожную безопасность. К примеру, дистанция, необходимая для полной остановки машины, едущей со скоростью 30 км/ч, варьируется от 5 метров на сухом покрытии до 18 метров на заснеженной дороге. Размещение сенсоров и предупреждающих сигналов дает возможность водителям вовремя реагировать на перемены условий движения. Кроме того, IoT-устройства вносят вклад в повышение энергоэффективности. К примеру, датчики способны автоматически менять интенсивность света уличных фонарей, учитывая уровень естественного освещения и наличие людей или транспорта. Это позволяет существенно снизить потребление энергии, что не только экономит средства, но и снижает выбросы углекислого газа, поддерживая экологичное развитие городов. Также IoT-комплексы создают большие массивы информации, пригодные для анализа и совершенствования городской инфраструктуры. Например, изучение информации о потоке машин помогает определять наиболее перегруженные участки и разрабатывать меры по уменьшению заторов. Это помогает городским службам принимать взвешенные решения при планировании дорог, строительстве новых переходов и оптимизации существующих маршрутов.

Использование технологий IoT в регулировании дорожного движения продемонстрировало заметный прогресс в различных мегаполисах. В частности, в Сингапуре интеллектуальная система транспортировки (ИТС), функционирующая на базе IoT, смогла уменьшить пробки на дорогах на 20-30%. Система задействует совокупность сенсоров, камер и радаров для отслеживания трафика в текущем времени, что дает возможность гибко настраивать светофоры и улучшать перемещение транспорта. В результате, средняя продолжительность поездок для водителей сократилась на 15%. В столице Нидерландов, Амстердаме, концепция " Smart Mobility" реализуется посредством применения IoT-решений для оптимизации транспортного потока. Собранные с дорожных сенсоров данные анализируются системой, которая в автоматическом режиме адаптирует алгоритмы светофоров. Благодаря этому удалось на четверть уменьшить пробки в часы наибольшей загруженности. В дополнение к

этому, развертывание "умных" парковочных систем, функционирующих на базе IoT, дало возможность на 30% сократить время, затрачиваемое на поиск места для парковки.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мухачева Э.А., Верхотуров М.А., Мартынов В.В. Модели и методы расчёта раскроя упаковки геометрических объектов / Э.А. Мухачева, М.А. Верхотуров, В.В. Мартынов // УГАТУ. — 1998. — 216 с.

2. Стоян Ю.Г., Яковлев С.В. Математические модели и оптимизационные методы геометрического проектирования / Ю.Г. Стоян, С.В. Яковлев // Наукова думка. — 1986. — 268 с.

3. Стативко Р.У., Коломыцева Е.П. Алгоритм поддержки принятия решения по расстановке датчиков движения в помещении / Р.У. Стативко, Е.П. Коломыцева // Название журнала. — 2021. — Т. 10, № 2 (54). — С. 101–104.

4. Ким П.А. Снижение риска наезда на пешеходов в условиях ограниченной видимости на нерегулируемых пешеходных переходах // Вестн. Иркутского гос. техн. ун-та, № 6(89): Иркутск: Изд-во ИрГТУ, 2014. –С. 147 – 154.

5. Волков, В.С. Расчет вероятностных оценок опасности конфликтных точек на дорожных пересечениях // "Мир транспорта и технологических машин"2016. №4(55), С. 105-110.

***УДК 004***

***Акуппа Ю.А.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ПЛАТФОРМЕ ARDUINO ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современную эпоху цифровизации защита информационных активов становится крайне значимой. Криптографическая защита данных уже не просто сложный технический процесс, а жизненно необходимый инструмент, гарантирующий нашу безопасность и конфиденциальность. Когда мы осуществляем покупки в интернете, общаемся через мессенджеры или храним файлы в облаке, наши данные

защищаются с помощью криптографических алгоритмов. Для специалистов в области кибербезопасности шифрование является не только профессиональной обязанностью, но и постоянной задачей, требующей глубоких знаний и креативного подхода для формирования эффективных систем защиты.

Часто программы шифрования работают только на определённых операционных системах и устройствах, что создает уязвимость: даже самое надежное шифрование теряет свою эффективность, если на устройстве уже установлено вредоносное ПО, предшествующее шифрованию. В такой ситуации злоумышленник может обойти все меры защиты и получить доступ к информации в незащищенном виде. Чтобы предотвратить это, необходимо разрабатывать стратегии, снижающие риск утечки данных на этапе их обработки. Одним из решений может стать применение изолированных сред или специализированного оборудования для обеспечения защиты.

Использование специализированных микроконтроллеров для шифрования информации представляет собой перспективный подход к повышению уровня безопасности. В отличие от обычных вычислительных систем, такие устройства обладают улучшенной защитой от несанкционированного доступа и имеют низкое энергопотребление.

Тем не менее, внедрение данного подхода сопряжено с рядом сложностей. Помимо временных затрат на разработку, требуются финансовые средства для приобретения микроконтроллеров и сопутствующих компонентов, таких как модули для ввода текста, отображения данных и обмена информацией между устройствами.

В качестве практического решения можно рассмотреть использование микроконтроллеров Arduino, которые стали популярными в электронике благодаря своей доступности и универсальности. Они позволяют реализовывать различные алгоритмы шифрования, обеспечивая высокий уровень безопасности и автономности. Этот подход открывает новые возможности для создания компактных и энергоэффективных решений в области защиты информации.

Arduino является востребованной платформой для разработки прототипов и создания электронных устройств, активно применяемой в автоматизации, робототехнике и управлении технологическими процессами. Она предлагает простые инструменты для реализации разнообразных проектов, включая системы защиты данных

Для шифрования данных на микроконтроллерах Arduino можно применять библиотеку AESLib, которая реализует симметричный

алгоритм AES (Advanced Encryption Standard). Эта библиотека позволяет защищать информацию как для хранения на устройстве, так и для передачи через Интернет с использованием дополнительных коммуникационных модулей.

Кроме того, существует библиотека ArduinoDES, которая реализует алгоритм DES (Data Encryption Standard). Тем не менее, DES считается менее безопасным по сравнению с AES, так как AES является его усовершенствованной версией и предлагает более высокий уровень защиты.

Интересным примером применения AESLib является проект Cipherbox, разработанный пользователем Habr Дмитрием Брайтом.


Рис. 1. Супершифратор Cyberbox

Cipherbox представляет собой устройство, предназначенное для кодирования, хранения и декодирования текстовых данных. В рамках проекта реализована система учетных записей с функциями авторизации и регистрации пользователей, что позволяет контролировать доступ к зашифрованной информации. В дополнение к AES, Cipherbox использует и другие алгоритмы шифрования, такие как Blowfish и Serpent, что увеличивает гибкость и надежность системы.

Центральным элементом системы является микроконтроллер ESP32, который отвечает за криптографическую безопасность и взаимодействие с базой данных SQLite. Управление клавиатурой и считывателем RFID-меток осуществляется с помощью Arduino Uno. ESP8266 используется в качестве приемника для расшифрованных данных.

Наиболее надежной комбинацией, устойчивой к квантовым атакам, является Blowfish + AES + Serpent + AES. В качестве альтернативы, без использования Blowfish, можно применить AES +

Serpent + AES. Комбинация Serpent + AES обеспечивает приемлемый уровень защиты, хотя и уступает по надежности предыдущим вариантам. Blowfish + Serpent представляет собой средний уровень безопасности, а Serpent обеспечивает минимально допустимый уровень защиты. AES является самой простой реализацией, которая потенциально может быть уязвима для взлома.

Система поддерживает многопользовательский режим, а аутентификация пользователей осуществляется с помощью RFID-карт. Также предусмотрена возможность масштабирования для создания безопасных сервисов.

Cipherbox демонстрирует эффективное использование микроконтроллеров Arduino и ESP для разработки компактных и мощных систем шифрования.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Habr [русскоязычный веб-сайт в формате системы тематических коллективных блогов с элементами новостного сайта]. URL: https://habr.com.

2. Ткаченко, С.А. Применение платформы Arduino для реализации автоматического освещения комнаты / С.А. Ткаченко, Е.П. Коломыцева // Название журнала. — 2018. — С. 4052-4056.

3. Беркана А. Стоит ли выходить на российский рынок умных домов? URL: https://rb.ru (дата обращения: 03.05.2018).

4. Гороховатенко Е.С., Блажкова Е.Н. Разработка цифровой метеостанции на базе Arduino с измерением геомагнитного поля // Вестник молодёжной науки России. – Калининград, 2021. – № 1. – С. 3.

5. Столяренко А.С. Цифровая метеостанция на основе микроконтроллера arduino // Техническое творчество молодежи. – Москва, 2018. – №4. – С. 34-37.

*УДК 004*

***Акуппа Ю.А.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ: АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ДАННЫХ

Трудно представить себе современное общество без компьютерных технологий, которые кардинально изменили все аспекты нашей жизни. От простейших задач до управления сложными предприятиями – сегодня большинство дел выполняется с применением вычислительных систем, и, как правило, люди полностью полагаются на результаты автоматизированных расчетов. Этот технологический скачок привел к масштабной информатизации, сформировав совершенно новую цифровую действительность.

Банковские карты, e-mail, онлайн-платежи и Интернет прочно обосновались в нашей жизни. Однако вместе с развитием компьютерных технологий увеличиваются и угрозы, связанные с защитой информации. Компьютеры хранят ценные данные: личную информацию, коммерческую тайну, финансовые операции, научные разработки и так далее. Утечка или несанкционированный доступ к этой информации способны привести к серьезным последствиям – от финансовых потерь до ущерба репутации и нарушения авторских прав.

Несанкционированный доступ к информации, как правило, осуществляется через взлом систем защиты. Все кибератаки условно делятся на два основных вида: активные и пассивные.

Самыми опасными кибератаками считаются активные, при которых злоумышленник не просто следит за системой, но и активно в нее внедряется. Такие атаки могут быть разными, и каждая из них наносит существенный вред информационной инфраструктуре. Самым распространённым видом активных атак являются атаки типа "отказ в обслуживании" (DoS), когда злоумышленник перегружает систему запросами, блокируя доступ к ней для легальных пользователей. Более сложным типом являются распределённые атаки (DDoS), когда атака проводится одновременно с многих компьютеров, что существенно усложняет защиту. Наибольшую угрозу несут атаки, нацеленные на изменение данных. В таких случаях злоумышленник получает доступ к изменению содержимого баз данных, подмене файлов конфигурации

или искажению передаваемой информации. Подобные действия способны стать причиной неверных решений, убытков или сбоев в технологических процессах. Отдельную проблему представляют атаки с применением вредоносного софта, в особенности программ-вымогателей, что кодируют данные и требуют выкуп за их восстановление. Современные атаки злоумышленников становятся все более хитрыми: они используют уязвимости в цепочках поставок, недоработки архитектуры систем или приемы социальной инженерии для получения доступа. Особенностью таких атак является оставление следов в системе, что теоретически упрощает их обнаружение. Однако современные злоумышленники применяют методы сокрытия, что существенно затрудняет своевременное выявление угрозы. Последствия успешных атак могут быть крайне серьезными: от краткосрочного сбоя в работе систем до полной потери данных и многомиллионных финансовых потерь, а в случае критической инфраструктуры – даже угрозы жизни и здоровью.

Пассивные кибератаки особенно опасны своей скрытностью: в отличие от активных, они не оставляют явных следов и могут долго оставаться незамеченными. Суть таких атак – в тайном наблюдении и перехвате информации, без внесения изменений в данные или воздействий на систему. Наиболее часто встречающиеся типы пассивных атак – перехват сетевого трафика (сниффинг), анализ электромагнитного излучения, прослушивание каналов связи и прочие способы неинвазивного сбора данных. Особую угрозу представляет перехват учетных данных - паролей, сессионных токенов, биометрических данных, что позволяет злоумышленникам получить полный доступ к системе, выдавая себя за легального пользователя. Трудность выявления подобных атак заключается в том, что они не мешают штатной работе системы и не приводят к появлению подозрительных признаков. Тем не менее, современные средства защиты, такие как сквозное шифрование данных с применением надежных криптографических алгоритмов (AES-256, RSA-4096), динамическая смена ключей, применение защищенных VPN-туннелей и технологий сокрытия трафика (например, Tor), позволяют успешно бороться с пассивным перехватом информации. Немаловажным аспектом защиты является и физическая безопасность - экранирование кабелей, защита от утечек через побочные каналы, контроль доступа к сетевому оборудованию. В отличие от активных атак, которые можно выявить по аномальному поведению системы, пассивные атаки требуют специальных инструментов мониторинга сетевой активности и анализа трафика для обнаружения отклонений. Современные системы защиты

данных всё чаще ориентируются на профилактику: систематическое обновление криптографических стандартов, использование квантово-устойчивых алгоритмов шифрования, строгий контроль доступа к конфиденциальной информации, что значительно усложняет злоумышленникам проведение успешных пассивных атак.

Защита данных строится на трех ключевых принципах: конфиденциальность (доступ к сведениям разрешен только авторизованным лицам), целостность (информация защищена от несанкционированного изменения или удаления) и доступность (система должна предоставлять непрерывный доступ к данным для легальных пользователей).

В компьютерных системах возможны такие виды атак:

1.Прерывание (атака на доступность) — блокировка доступа к информации, удаление данных, отказ в обслуживании.

2.Перехват (атака на конфиденциальность) — несанкционированное получение информации.

3.Модификация (атака на целостность) — внесение изменений в данные злоумышленниками.

4.Фальсификация (атака на аутентичность) — добавление поддельных записей или транзакций.

Наиболее уязвимы системы с удалённым доступом, так как они подвергаются атакам извне. Сложная маршрутизация трафика и множество узлов увеличивают вероятность несанкционированного проникновения.

Для управления доступом применяются:

1.Логин и пароль —простой, но небезопасный способ.

2.Криптографические ключи (смарт-карты, токены, RFID-метки) — более надежный вариант.

3.Биометрическая идентификация – наиболее надежный метод, базирующийся на неповторимых физиологических или поведенческих особенностях (отпечатки пальцев, распознавание голоса и т.д.).

Развитие биометрии обусловлено ростом вычислительной мощи и улучшением алгоритмов обработки. Но для ее внедрения необходимы высокоточные датчики и производительные системы анализа.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алгулиев Р.М., Рагимов Э.Р. Об одном методе оценки информационной безопасности корпоративных сетей в стадии их проектирования // Информационные технологии. 2005. № 7. С. 35–39; Швырев Б.А. Перспективы применения системы электронного

мониторинга в отношении осужденных, отбывающих наказания в колониях-поселениях // Ведомости уголовно-исполнительной системы. 2011. № 11. С. 26–27.

2. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. СПб., 2001; Pfleeger C.P. Security in Computing, Prentice Hall. Upper Saddle River. NY., 1997.

3. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке Си. М., 2005. С. 610; Pfleeger C.P. Security in Computing, Prentice Hall. Upper Saddle River.

4. Мао В. Современная криптография. Теория и практика. Вильямс, 2005. С. 768; Швырев Б.А. Перспективы применения системы биометрической идентификации при исполнении наказаний в виде лишения свободы // Ведомости уголовно-исполнительной системы. 2011. № 9 (112). С. 10–13.

5. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. СПб., 2001; IEEE Computer. 2010. Vol. 43.

6. Жданова С.И., Иванов И.В. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра // В сб.: Материалы конференций ГНИИ "НАЦРАЗВИТИЕ". Июнь 2017: Сборник избранных статей. - СПб.: ГНИИ "НАЦРАЗВИТИЕ", 2017 с. 116-119.

***УДК 004***

***Акуппа Ю.А., Чикин Н.А.***
***Научный руководитель: Алексеевский С.В., асс.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ОПТИМИЗАЦИЯ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ С ПОМОЩЬЮ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ

Применение нейронных сетей для улучшения генетических алгоритмов открывает новые перспективы для ускорения и усовершенствования эволюционных вычислений. Одним из главных достоинств такого подхода является возможность замены трудозатратных вычислений fitness-функции предсказаниями нейросетевой модели. В традиционных ГА оценка каждой особи может требовать значительных вычислительных мощностей, особенно если для этого необходимо проводить сложное моделирование или настоящие эксперименты.

Нейросеть, обученная на предыдущих данных, способна аппроксимировать показатели приспособленности, существенно сокращая время работы алгоритма. К примеру, в задачах оптимизации инженерных конструкций, где каждая оценка требует запуска ресурсоемких CFD- или FEA-симуляций, surrogate-модель на основе нейросети может давать приближенные оценки в тысячи раз быстрее, направляя эволюционный процесс в перспективные области поискового пространства.

Ещё одним немаловажным аспектом считается применение нейросетей для формирования начальной популяции. Вместо случайной инициализации, которая может оказаться неэффективной в сложных пространствах решений, генеративные модели вроде GAN или VAE способны создавать особи, уже обладающие определённым потенциалом. Это особенно полезно в задачах, где хорошие решения сконцентрированы в узких областях поискового пространства. Например, при проектировании молекул с заданными свойствами или создании архитектур нейронных сетей генеративная модель может предлагать заранее работоспособные варианты, сокращая время на "разогрев" генетического алгоритма.

Нейросети способны улучшить функционирование генетических операторов, делая их более адаптированными. В привычных ГА параметры мутации и кроссинговера обычно фиксированы или изменяются по простым эвристическим методам. Однако нейросетевая модель, обученная на информации о том, какие изменения приводят к улучшению fitness, может динамически подбирать оптимальные параметры операторов для каждого конкретного индивида или этапа эволюции. Более того, методы глубокого обучения с подкреплением позволяют создать систему, которая будет самостоятельно учиться выбирать лучшие стратегии скрещивания и мутации в процессе работы алгоритма.

Еще одно многообещающее направление - применение нейросетей для умной селекции в генетических алгоритмах. В отличие от стандартных методов вроде турнирного отбора или рулетки, которые базируются только на текущих значениях fitness-функции, нейросетевые модели могут производить многомерный анализ особей, учитывая не только их прямую приспособленность, но и скрытые эволюционные потенциалы.

Современные архитектуры нейронных сетей, особенно трансформеры и графовые нейросети, могут выявлять сложные шаблоны во внутренней структуре решений, которые неочевидны при поверхностном анализе. Например, в задачах оптимизации

молекулярных структур нейросеть может оценивать не только текущую активность соединения, но и его "эволюционную пластичность" - возможность порождать улучшенные версии после генетических операций. Это достигается через обучение модели на исторических данных о том, какие структурные особенности в прошлом приводили к появлению многообещающих потомков.

Практические воплощения подобных гибридных подходов уже показывают впечатляющие итоги. В задачах автоматического машинного обучения сочетание генетических алгоритмов с нейронными сетями позволяет результативно подбирать архитектуры глубоких сетей и их гиперпараметры. В робототехнике нейроэволюционные методы успешно используются для co-optimization морфологии и управляющих алгоритмов. А в фармацевтике и материаловедении surrogate-модели ускоряют поиск молекул с желаемыми характеристиками в разы по сравнению с традиционными ГА.

Перспективы последующего прогресса этой области обусловлены интеграцией более запутанных нейросетевых архитектур, включая трансформеры нового поколения и нейросети с вниманием к топологии данных (topology-aware neural networks), которые особенно эффективны при работе со сложными структурированными решениями. Возможность обработки разнородных данных - от табличных параметров до графовых представлений и временных рядов - открывает путь к созданию универсальных оптимизационных систем, способных работать в мультимодальных пространствах поиска.

Комбинация нейрооптимизированных ГА с иными передовыми метаэвристическими методами - такими как роевой интеллект, имитация отжига или алгоритмы колонии муравьёв - может привести к возникновению гибридных систем нового поколения. Эти системы смогут сочетать достоинства различных подходов: глобальный поиск ГА, локальную оптимизацию методов градиентного спуска и коллективный интеллект роевых алгоритмов.

Особенно перспективным выглядит направление нейро-эволюционного метаобучения, где сама структура гибридного алгоритма оптимизируется в процессе решения серии родственных задач. Это может привести к созданию самообучающихся оптимизационных систем, способных адаптироваться к специфике конкретной проблемы без ручной настройки.

Дополнительный потенциал кроется в интеграции квантовых вычислений, которые могут ускорить как работу нейросетевых моделей, так и выполнение генетических операторов, открывая путь к

решению задач беспрецедентной сложности. Развитие этого направления потребует тесного взаимодействия специалистов по машинному обучению, эволюционным алгоритмам и квантовым вычислениям.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Степовой А.А., Рубанов В.Г. Повышение живучести мобильного робота с использованием аппарата нейронных сетей. Математические методы в технике и технологиях: сб. тр. междунар. науч. конф.: в 12 т.; под общ. ред. А.А. Большакова. СПб.: Изд-во Политехн. ун-та. 2019;3:26-29.

2. Башмаков А. И., Башмаков И. А. Интеллектуальные информационные системы : учеб. пособие. М. : Изд-во МГТУ им. М. Э. Баумана, 2005. 304 с.

3. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / пер. с польск. И. Д. Рудинского. М. : Горячая линия – Телеком, 2006. 384 с.

4. Цой Ю. Р., Спицын В. Г. Эволюционный подход к настройке и обучению искусственных нейронных сетей // Электронный журнал «Нейроинформатика». 2006. Т. 1. № 1. С. 34–61.

5. Эволюционные методы моделирования и оптимизации сложных систем : конспект лекций / Е. С. Семенкин, М. Н. Жукова, В. Г. Жуков и др. Красноярск : Изд-во СФУ 2007.

***УДК 004***

***Акуппа Ю.А., Чикин Н.А.***
***Научный руководитель: Алексеевский С.В., асс.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КИБЕРБЕЗОПАСНОСТЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ СИСТЕМАМИ

Переход к цифровому формату в промышленности, часто называемый Индустрией 4.0, произвел революцию в методах организации технологических операций. Сегодняшние автоматизированные системы управления технологическими процессами (АСУ ТП) представляют собой комплексные киберфизические структуры представленная на рисунке 1, объединяющие производственное оборудование, инструменты

автоматизации и корпоративные ИТ-системы.


Рис. 1 Киберфизические структуры АСУ ТП

Тем не менее, подобная интеграция формирует новые направления киберугроз, способных вызвать не только денежные убытки, но и промышленные аварии. Согласно анализу IBM Security, в 2022 году 35% всех кибернетических атак были нацелены на промышленные объекты, а средний ущерб от одного случая достигал 4,5 миллиона долларов.

Управление производственными процессами существенно отличается от стандартных информационных технологий, требуя специализированных подходов к защите. Во-первых, их длительный период эксплуатации (от 15 до 30 лет) обуславливает использование устаревшего программного обеспечения. Во-вторых, промышленные протоколы, такие как Modbus TCP, PROFINET и DNP3, изначально не проектировались с учетом требований безопасности. В-третьих, необходимость бесперебойной работы часто препятствует своевременной установке обновлений, направленных на повышение защищенности. Кроме того, в промышленных системах часто используются специализированные операционные системы (например, VxWorks и QNX) и устройства с ограниченной вычислительной мощностью.

Современные кибернетические риски для автоматизированных систем управления технологическими процессами (АСУ ТП) можно классифицировать по нескольким направлениям представленная диаграмма на рисунке 2, демонстрирует процентное соотношение каждой категории. К первой категории относятся целенаправленные атаки, такие как Stuxnet, Havex или Triton, которые специально разрабатываются для дестабилизации промышленных процессов.

Вторая категория включает в себя атаки программ-вымогателей, на которые, согласно данным отчетов Dragos, в 2021 году приходилось 27% всех зарегистрированных инцидентов. Третья категория – это внутренние угрозы, связанные с действиями персонала.

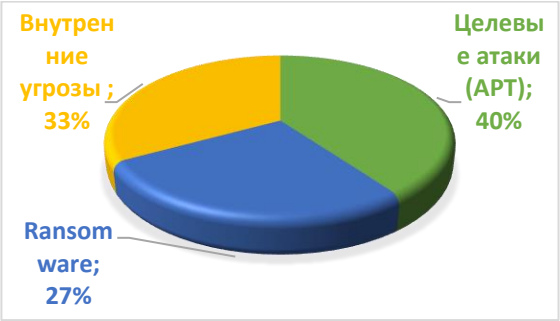



Рис. 2 Диаграмма киберугроз для АСУ ТП

Наибольшую угрозу несут атаки, направленные на аппаратную часть, способные вызвать физические разрушения имущества. В качестве примера можно привести инцидент на металлургическом предприятии в Германии в 2014 году, когда в результате кибернападения была серьезно повреждена доменная печь.

**Стратегии и технические средства обеспечения безопасности:**

В современных реалиях, защита производственных комплексов строится на многослойном принципе. Контроль физического доступа и системы видеонаблюдения формируют первый рубеж обороны. На уровне сети, критически важным является разделение на сегменты, реализованное с помощью специализированных межсетевых экранов промышленного класса (например, Siemens SCALANCE). Защита конечных устройств обеспечивается специализированным антивирусным ПО, представлены на рисунке 3. (Kaspersky Industrial CyberSecurity, CyberBit SCADA Shield).

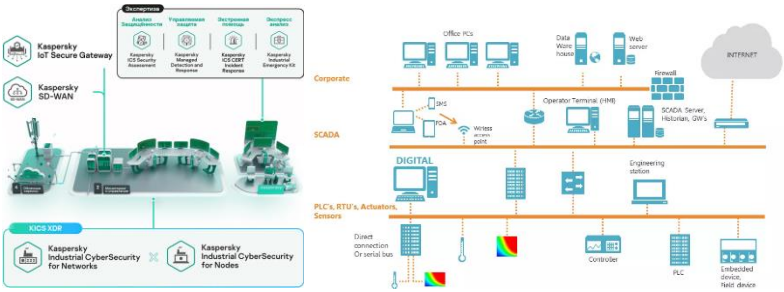



Рис. 3 Структуры безопасности компаний, предоставляемых услуги безопасности промышленным организациям

Особое внимание уделяется системам мониторинга (Nozomi Networks, Claroty), которые анализируют трафик промышленных протоколов. Создание центров управления безопасностью (SOC) для промышленных объектов также является ключевым элементом.

**Правовая основа и регламенты:**

Ключевые международные стандарты, регулирующие кибербезопасность промышленных систем:

- Серия IEC 62443 – основной международный стандарт.
- NIST SP 800-82 Rev.2 – рекомендации по обеспечению безопасности ICS.
- ISO/IEC 27001 – требования к системам управления информационной безопасностью.
- ГОСТ Р 57580-2017 – национальный стандарт Российской Федерации. В европейском регионе действует Директива NIS2, в Соединенных Штатах – стандарт NERC CIP. В России в 2021 году был принят закон "О безопасности критической информационной инфраструктуры", вводящий дополнительные требования к промышленным системам.

Анализ произошедших инцидентов помогает выявить слабые места в защите. Инцидент с вирусом Triton в 2017 году выявил уязвимости в системах безопасности (SIS). Атака на Colonial Pipeline в 2021 году продемонстрировала необходимость защиты цепей поставок. Изучение подобных атак позволяет совершенствовать методы защиты.

Для защиты промышленных сетей от киберугроз необходима всесторонняя стратегия, включающая технические решения, организационные процедуры и соблюдение нормативных требований. Крайне важны непрерывное повышение квалификации сотрудников и распространение сведений о новых опасностях. В перспективе кибербезопасность в промышленности будет опираться на передовые

методы прогнозирования и автоматизированные системы реагирования на инциденты.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Козлова Д.Р., Козлова Н.Ш. Информационная безопасность в виртуальной среде // Наука и творчество: вклад молодежи: материалы Всерос. молодеж. науч.-практ. конф. студентов, аспирантов и молодых ученых. Махачкала, 2020. С. 48–50.

2. Арсентьев М.В. К вопросу о понятии «Информационной безопасности» // Информационное общество. 1997. № 4. С. 48–50.

3. Герасимов В.В., Минина Л.С., Васильева А.В. Информационные технологии производственных систем: учеб. пособие. Новосибирск: НГАСУ, 2019. 74 с.

4. Ищейнов В.Я. Информационная безопасность и защита информации: учеб. пособие. Москва: Директ-Медиа, 2020. 271 с.

5. Статьев В.Ю., Тиньков В.А. Информационная безопасность распределенных информационных систем // Информационное общество. 1997. № 1. С. 68–71.

6. Ковалев Д.В. Информационная безопасность: учеб. пособие. Ростов-на-Дону: ЮФУ, 2016. 74 с.

7. Жданова С.И., Иванов И.В. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра // В сб.: Материалы конференций ГНИИ "НАЦРАЗВИТИЕ". Июнь 2017: Сборник избранных статей. - СПб.: ГНИИ "НАЦРАЗВИТИЕ", 2017 с. 116-119.

***УДК 004.02***

***Амиров М.С.***
***Научный руководитель: Барков И.А., канд. техн. наук, доц.***
*Казанский национальный исследовательский технический университет им. А.Н. Туполева, г. Казань, Россия*

## АНАЛИЗ ИСХОДНОГО КОДА ПРИ ТРАНСЛЯЦИИ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ

Язык программирования - формальная знаковая система, предназначенная для записи компьютерных программ. Язык программирования определяет набор лексических, синтаксических и семантических правил, задающих внешний вид программы и действия, которые осуществит исполнитель (компьютер) под ее управлением.

Все языки программирования относятся к классу формальных языков и становятся доступными для использования лишь после создания трансляторов этих языков. С темой построения трансляторов самым тесным образом связана тема формальных грамматик и автоматов, которая является теоретической и, одновременно, практической базой конструирования трансляторов.

В самом общем виде реализуемые транслятором функции заключаются в проверке исполнения перечисленных в приведенном определении языка программирования правил в исходной программе, а также в обеспечении эквивалентных действий в исполняемой компьютером программе.

Основой для анализа исходного кода служат формальные грамматики. Грамматика, как наука, является разделом языкознания, который изучает грамматический строй языка, а также закономерности построения осмысленных речевых или текстовых отрезков на этом языке.

Грамматично построенные предложения являются связными, т. е. лишенными разрывов в цепочке синтаксических отношений. Отношения являются бинарными. Важная особенность синтаксических зависимостей заключается в том, что они далеко не всегда связывают слова, находящиеся рядом в цепочке слов. В этих случаях часто говорят о контекстном анализе текста.

В системе трансляторов грамматика это набор правил, с помощью которых, можно построить корректные выражения. Грамматика состоит из:

1) Терминала – конкретные символы или слова, которые встречаются в реальных выражениях (обозначается строчными буквами);

2) Нетерминала – абстрактные понятия, которые раскрываются в правилах (обозначается заглавными буквами);

Правил – инструкции, по которым нетерминал преобразуются в другие символы или слова. Каждое правило показывает, как абстрактные символы (слева) раскрываются в конкретные конструкции (справа).

Проблемой задачи анализа является огромное количество альтернативных вариантов, возникающих в ходе разбора, связанных как с неоднозначностью правил разбора, так и многозначностью самих входных данных.

При автоматизированном построении синтаксических анализаторов выполняется анализ исходной грамматики языка. Для этой цели часто используют три функции: *FIRST, FOLLOW, EFF,*

которые обеспечивают процесс создания таблиц синтаксического анализа. Данные функции позволяют построить предсказывающий анализатор, который работает без возвратов и переборов.

$FIRST_k(\alpha)$ – это множество k последовательных терминалов, которые могут появляться в начале строк, выводимых из цепочки символов α.

С помощью функции $FIRST_k(\alpha)$ вида $V^* \rightarrow T^*$, можно определить в заданной грамматике множество последовательностей длиной k символов, с которых может начинаться терминальная цепочка x, выводимая из сентенциальной формы α. Для цепочки α в алфавите V и цепочки x в алфавите T действуют правила:

1. если $\alpha \Rightarrow^* x$ и $|x| \leq k$, т.е. $x = yz$, $y \in T^k$, $z \in T^*$ значение функции $FIRST_k(\alpha)$ равно y;
2. если $\alpha \Rightarrow^* x$ и $|x| > k$, и значение функции $FIRST_k(\alpha)$ равно x;

Функция $FOLLOW_k(A)$ для нетерминала A это множество k терминалов, которые могут располагаться непосредственно справа от A в некоторой сентенциальной форме. Чтобы вычислить $FOLLOW_1(A)$ для всех нетерминалов A грамматики, применяются следующие правила до тех пор, пока ни к одному множеству FOLLOW нельзя будет добавить ни одного символа:

1. В FOLLOW(S) помещается $, где S – начальный символ грамматики, а $ - правый ограничитель входного потока символов.

2. Если имеется грамматическое правило $A \rightarrow \alpha B \beta$, то все элементы множества FIRST(β), кроме ε, помещаются в множество FOLLOW(B).

Если имеется правило $A \rightarrow \alpha B$ или $A \rightarrow \alpha B \beta$, где FIRST(β) содержит ε, то все элементы из множества FOLLOW(A) помещаются в множество FOLLOW(B).

EFF(α) — это расширение FIRST(α), которое учитывает влияние ε-правил на выбор следующего символа.

Отличие от FIRST

FIRST(α) показывает только первые терминалы в α.

EFF(α) дополнительно учитывает терминалы из FOLLOW, если α может быть пустым.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Барков, И.А. Основы трансляции языков программирования / И.А. Барков // 2024

2. Барков, И.А. Теория формальных грамматик и автоматов / Учебно-методическое пособие по выполнению курсовой работы // 2020

3. Мясников, Е.В. Основы трансляции языков программирования / Е.В. Мясников // 2015

***УДК 004.02***

***Амиров М.С.***
***Научный руководитель: Барков И.А., канд. техн. наук, доц.***
*Казанский национальный исследовательский технический университет им. А.Н. Туполева, г. Казань, Россия*

## СТРАТЕГИИ СИНТАКСИЧЕСКОГО РАЗБОРА ДЛЯ ФОРМАЛЬНЫХ ГРАММАТИК

Синтаксический разбор представляет собой процесс определения синтаксической структуры предложения в соответствии с грамматикой. Синтаксическая структура представляется в виде дерева разбора. Синтаксический анализ основан на части грамматики, которая имеет дело с единицами, более протяженными, чем слово, — словосочетаниями и предложениями. При синтаксическом анализе, предложение разделяют на составляющие, и определяют отношения между ними. В результате синтаксического анализа линейная последовательность слов преобразуется в набор синтаксических отношений.

В программировании синтаксический анализ нужен для выявления синтаксических ошибок, сделанных программистом. А также для предотвращения компиляции некорректно написанного исходного кода.

Стратегии синтаксического разбора — это методы, используемые для анализа структуры текста согласно заданным правилам грамматики. Их основная задача — преобразовать последовательность символов или токенов в структурированное представление (например, абстрактное синтаксическое дерево), которое отражает иерархию и смысл исходных данных.

Стратегии синтаксического разбора делятся на нисходящие (top-down) и восходящие (bottom-up), каждая из которых имеет свои преимущества.

Нисходящий синтаксический анализ начинается со стартового символа грамматики, после чего последовательно применяются правила для построения дерева разбора. Цель – сопоставить входные токены с ожидаемыми структурами. Каждое правило грамматики раскрывается в последовательность терминалов и нетерминалов. На каждом шаге

анализатор решает какое правило применить, основываясь на принципы выбранного алгоритма. Основные алгоритмы нисходящего анализа:

Рекурсивный спуск – каждое правило грамматики реализуется как функция;

LL-анализаторы – используют таблицу предсказаний для выбора правил на основе текущего токена и предпросмотра следующих символов.

Особенности нисходящих анализаторов:

Требуют устранения левой рекурсии (например, $A \rightarrow Aa \mid b$ нужно переписать как $A \rightarrow bA'$, $A' \rightarrow aA' \mid \varepsilon$);

Не поддерживают неоднозначности.

Восходящий синтаксический анализ начинается с терминальных символов и движется к стартовому символу грамматики. Основная задача – найти “основы” (подстроки, которые можно свернуть в нетерминалы). Основные алгоритмы восходящего анализа – это LR-анализаторы.

LR-анализаторы – используют конечный автомат и стек для отслеживания состояний. Решения принимаются на основе таблиц действий.

Особенности восходящих анализаторов:

Используют алгоритмы сдвига-свертки;

Поддерживают левую рекурсию и более сложные грамматики.

Сравнив восходящий и нисходящий анализ, можно сделать вывод, что нисходящий проще для ручного разбора, и подходит для простых грамматик. Восходящий анализ сложнее, требует таблиц состояний, подходит для сложных формальных языков.

Для решения задачи автоматического синтаксического разбора в системе транслятора некоторого предложения, зачастую, используют один из двух методов: LL(k)-разбор и LR(k)-разбор. Второй метод входит в группу, включающую также SLR(k)-разбор и LALR(k)-разбор. Обычно вторую группу обобщенно называют LR(k)-разбор.

LL-разбор, заключается в восстановлении левостороннего вывода предложения в процессе редукции предложения. В левостороннем выводе подстановке всегда подлежит самый левый нетерминальный символ текущей сентенциальной формы.

В обозначении LL метода первый символ обозначает левосторонний вывод, а второй - чтение исходного текста слева направо.

Грамматика принадлежит классу $LL_k$, если:

1) Для любых двух правил $A \rightarrow \alpha \mid \beta$ выполняется $FIRST_k(\alpha) \cap FIRST_k(\beta) = \emptyset$

2) Если $\varepsilon \in FIRST_k(\alpha)$, то $FIRST_k(\beta) \cap FOLLOW_k(A) = \emptyset$.

Алгоритм LL(k)-анализатора обычно реализуется с помощью автомата с магазинной памятью. Автомат формализует процесс разбора, делая его пригодным для программной реализации, а также позволяет избежать рекурсии. Так же автомат таблицы гарантирует O(1) сложность принятия решений. Стэк магазинного автомата позволяет эффективно управлять вложенными конструкциями (скобками).

В исходном состоянии автомата содержимое стека имеет вид ⊢S, где S – начальный символ грамматики. При каждом перемещении, выполняемым автоматом, из стека извлекается один символ. Если извлекаемый символ оказывается нетерминальным, то ему в соответствии ставится правило, правая часть которого заносится в стек. Правило выбирается в соответствии со значениями функции $FIRST_k$. Если же извлеченный из стека символ оказывается терминальным, то он используется в качестве входного символа и, следовательно, определяет следующее перемещение автомата: если входной символ совпадает с верхним символом магазина, то входной символ допускается автоматом и читающая головка сдвигается на одну позицию вправо. При этом верхний символ магазина удаляется.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Барков, И.А. Основы трансляции языков программирования / И.А. Барков // 2024

2. Барков, И.А. Теория формальных грамматик и автоматов / Учебно-методическое пособие по выполнению курсовой работы // 2020

3. Мясников, Е.В. Основы трансляции языков программирования / Е.В. Мясников // 2015

***УДК 004.8:69***

***Анджич Дж.***
***Научный руководитель: Стативко Р.У., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНЖЕНЕРИИ И АРХИТЕКТУРЕ: ОТ ГЕНЕРАТИВНОГО ДИЗАЙНА К АВТОНОМНОМУ ПРОЕКТИРОВАНИЮ

Искусственный интеллект радикально меняет подходы к инженерному и архитектурному проектированию. Вместо

традиционного процесса, где специалист вручную прорабатывает каждую деталь, новая парадигма основывается на сотрудничестве человека и машины: **проектировщик задаёт цели и ограничения, а AI генерирует множество решений**, зачастую таких, которые невозможно было бы предсказать или разработать вручную.

В дальнейшем тексте приведем примеры платформ которые используют искусственный интеллект для работы с инженерными и архитектурными проектами. Данные решения являются новшеством на рынке, но уже доказывают, что искусственный интеллект вносит большой вклад в индустрию

. **Autodesk Fusion 360 Generative Design** — платформа, где ИИ предлагает десятки или сотни вариантов конструкции на основе заданных критериев (например, прочность, масса, стоимость).

**Dreamcatcher Project** — экспериментальная система от Autodesk, способная генерировать архитектурные формы с учётом функциональных и эстетических параметров.

Один из ярких примеров — сотрудничество компании Airbus с Autodesk. Airbus стремился снизить массу своих самолётов, чтобы уменьшить расход топлива и выбросы углекислого газа. Одной из задач стало проектирование облегчённой перегородки кабины. С помощью генеративного дизайна в Fusion 360 была создана конструкция, масса которой оказалась на 45% меньше, чем у оригинала, при сохранении всех прочностных характеристик. Получившаяся форма была органической, напоминающей структуру костей или кораллов — решение, которое вряд ли могло быть предложено человеком без помощи ИИ.

Другой пример — проект General Motors, в котором инженеры оптимизировали кронштейн сидения автомобиля. Вместо восьми компонентов, составляющих исходную деталь, генеративный дизайн предложил одну цельную форму. Итог: на 40% меньше веса и на 20% выше прочность. Такая конструкция могла быть реализована только с помощью 3D-печати, что также открыло возможности для дальнейшей оптимизации производства.

Компания Under Armour применяла генеративный дизайн для разработки подошвы спортивной обуви. Цель состояла в создании лёгкой и эргономичной структуры, адаптированной под анатомию стопы и различные сценарии движения. В результате получилась сложная решётчатая форма, обеспечивающая хорошую амортизацию и лёгкость, которую затем производили методом 3D-печати из TPU-пластика. Проект Dreamcatcher от Autodesk представляет собой более экспериментальную систему генеративного проектирования,

ориентированную на архитектуру и промышленный дизайн. В отличие от Fusion 360, где акцент сделан на технические характеристики и инженерные параметры, Dreamcatcher учитывает также эстетические качества формы. Архитектор задаёт параметры — например, освещение, вентиляция, акустика, нагрузка, допустимые материалы — а система предлагает формы, которые отвечают этим требованиям. Dreamcatcher применялся при создании временных архитектурных павильонов и выставочных инсталляций. Такие конструкции не только визуально эффектны, но и функциональны: они учитывают прохождение света, потоки воздуха и движение людей внутри и снаружи. Формы, полученные с помощью системы, органичны и сложны, напоминают природные структуры — и реализуются с использованием CNC-станков, роботизированной кладки или 3D-печати.

Одним из значимых примеров является исследовательский проект Autodesk Research совместно с Gramazio Kohler Research из ETH Zurich. В этом проекте фасад здания проектировался с учётом множества параметров: светопропускание, вентиляция, акустика, устойчивость, количество материала. Dreamcatcher сгенерировал форму, которую затем реализовали с помощью промышленных роботов, укладывающих кирпичи по заданной траектории. Итог — фасад, который выглядит уникально и в то же время идеально соответствует техническому заданию. Также система применялась при проектировании мебели — например, стульев, оптимизированных под форму тела человека. Учитывались точки давления, положения тела в покое и в движении, а итоговая форма получалась максимально эргономичной и при этом эстетически выразительной. Такие конструкции чаще всего производятся с помощью 3D-печати или цифровой обработки дерева и пластика.

В заключение, чтобы внедрение искусственного интеллекта в инженерные и архитектурные процессы было эффективным, необходимо подготовить сотрудников к использованию новых инструментов. Обучение должно быть поэтапным, с учётом уровня подготовки персонала и специфики задач компании. Вот пошаговый план обучения:

Первым шагом должно стать ознакомление с основами генеративного проектирования и ИИ в инженерии. На этом этапе важно сформировать общее представление о том, как работают такие системы, какие задачи они решают, и в чём их отличие от традиционных CAD-инструментов. Это может быть достигнуто через вводные лекции, презентации, просмотр кейсов и демонстраций. На втором этапе

следует организовать практические курсы или тренинги, где сотрудники смогут работать с платформами вроде Autodesk Fusion 360 или Dreamcatcher. Обучение должно быть адаптировано под конкретные роли: инженеры будут изучать, как формировать техническое задание для ИИ, а дизайнеры — как анализировать предложенные формы и адаптировать их к визуальным требованиям. Хорошим решением станет сотрудничество с Autodesk или сертифицированными учебными центрами, предлагающими курсы по генеративному проектированию. Следующим этапом необходимо интегрировать ИИ-инструменты в текущие рабочие процессы. Это требует наставничества: опытные специалисты (возможно, прошедшие углублённое обучение) помогают коллегам применять новые инструменты на реальных проектах. Важно сформировать внутреннюю культуру экспериментов, где пробовать новое — это часть повседневной практики, а не исключение. Наконец, необходимо обеспечить постоянную поддержку и развитие навыков. ИИ-инструменты быстро развиваются, и сотрудники должны иметь доступ к обновлённым материалам, сообществам, семинарам, а также возможности обмениваться опытом внутри компании.

Преимущества использования ИИ в инженерии и архитектуре очевидны. Во-первых, это ускорение проектирования: ИИ генерирует десятки вариантов за минуты, что позволяет быстрее переходить к стадии тестирования и производства. Во-вторых, это оптимизация конструкции — по весу, прочности, стоимости и материалам. В-третьих, ИИ расширяет границы креативности, предлагая формы, которые человек бы не смог придумать, а значит, рождаются инновационные продукты и архитектурные решения. Также важное преимущество — возможность персонализированного проектирования, особенно в промышленном дизайне, мебели, медицинских изделиях.

Однако есть и недостатки. Один из главных — зависимость от технологии: при отсутствии должной подготовки сотрудники могут потерять навык ручного проектирования и критического анализа форм. Также важно учитывать, что ИИ не всегда предлагает решение, готовое к немедленному производству — иногда формы требуют доработки, адаптации или вовсе оказываются непригодными из-за технологических ограничений. Кроме того, барьер входа для некоторых специалистов может быть высоким: необходимость изучения новых интерфейсов, понимания принципов параметризации, работы с облачными системами. В целом, успешное внедрение ИИ требует не только новых инструментов, но и изменения подхода к проектированию, культуры внутри команды и постоянного развития

компетенций. Только тогда ИИ станет не заменой человеку, а его полноценным партнёром в создании высокотехнологичных и эстетически выразительных решений.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Autodesk Inc. Generative Design with Fusion 360 [Электронный ресурс]. – Режим доступа: https://www.autodesk.com (Дата обращения 5.5.25)

2. Autodesk Research. Project Dreamcatcher: Generative Design System [Электронный ресурс]. – Режим доступа: https://www.autodeskresearch.com (Дата обращения 5.5.25)

3. Airbus and Autodesk. Lighter Partitions through Generative Design [Электронный ресурс]. – Режим доступа: https://www.autodesk.com (Дата обращения 5.5.25)

4. General Motors and Autodesk. Reducing Weight with Generative Design [Электронный ресурс]. – Режим доступа: https://www.autodesk.com (Дата обращения 5.5.25)

5. Under Armour. Footwear Innovation with Generative Design [Электронный ресурс]. – Режим доступа: https://www.autodesk.com (Дата обращения 5.5.25)

6. ETH Zurich – Gramazio Kohler Research. Robotically Fabricated Brick Wall [Электронный ресурс]. – Режим доступа: https://gramaziokohler.arch (Дата обращения 5.5.25)

7. Autodesk University. Generative Design: Changing the Way We Think About Design [Электронный ресурс]. – Режим доступа: https://www.autodesk.com

***УДК 004.75***

***Булгаков В.Д., Воскобойников И.С.***
***Научный руководитель: Гвоздевский И.Н., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## МЕТОДЫ ШИФРОВАНИЯ И ЗАЩИТЫ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ В ДЕЦЕНТРАЛИЗОВАННЫХ БЛОКЧЕЙН-ХРАНИЛИЩАХ

Современные информационные системы сталкиваются с резким ростом объемов неструктурированных данных, таких как текстовые документы, расшифровки голосовых сообщений и разговоров, лог-

файлы. Это порождает необходимость поиска надежных и эффективных способов защиты и хранения данных. Централизованные системы хранения подвержены рискам единой точки отказа, взломов и утечки данных[1].

Альтернативой становится применение децентрализованных решений на базе технологии блокчейн. Подобный подход к хранению данных обеспечивает высокую степень защиты, прозрачность операций и отказоустойчивость. Цель данной статьи – изучить и проанализировать методы шифрования и защиты неструктурированных данных в децентрализованных блокчейн-хранилищах, выявить ограничения и предложить перспективные направления развития.

Неструктурированные данные – это информация, не имеющая четкой структурной организации, например, тексты, изображения, аудио и видео. Защита таких данных требует подходов, учитывающих их разнообразие, большой объем и сложность индексации.

Для защиты данных в блокчейне применяются:

- Симметричное шифрование (AES, ChaCha20). Обеспечивает высокую скорость обработки, но требует надежной передачи ключа.
- Асимметричное шифрование (RSA, ECC). Обеспечивает безопасную передачу ключей, но требует больше вычислительных ресурсов.
- Гибридное шифрование. Подход комбинирует преимущества обоих методов, например, AES для данных и RSA для обмена ключами.

Наиболее известные системы – IPFS, Filecoin, Storj и Sia. В этих системах данные распределяются между множеством узлов сети, а безопасность обеспечивается криптографическими методами[2].

IPFS – это протокол распределённого хранения, который адресует контент по его криптографическому хэшу.

Принцип работы IPFS:

1. Файл разбивается на блоки.
2. Каждый блок хэшируется (обычно используется метод SHA-256).
3. Создаётся Content Identifier (CID) — уникальный адрес по хэшу содержимого.
4. CID хранится в блокчейне и используется для получения файла из сети[3].

Хэширование в IPFS используется для идентификации, а не шифрования. Схематично принцип работы IPFS отражен на рисунке 1.

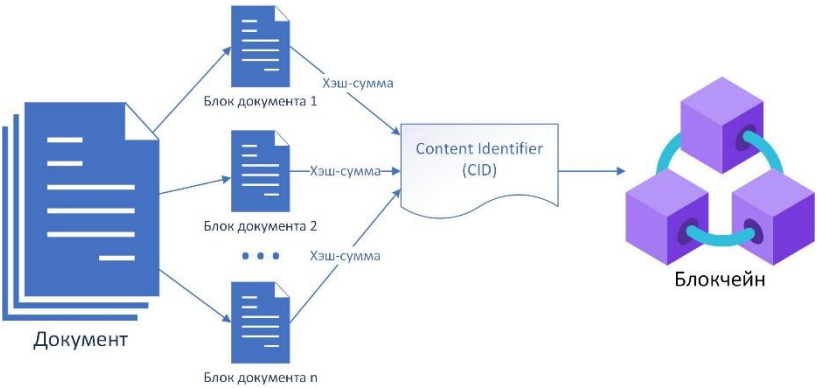



Рис. 1 – схема работы IPFS.

Протокол Filecoin берет за основу IPFS, но добавляет шифрование данных перед их публикацией в распределенном реестре.

Принцип работы:

1. Файл симметрично шифруется на стороне клиента (AES).
2. Файл делится на блоки.
3. Блоки распределяются по узлам в сети
4. Майнеры, для получения вознаграждения, доказывают (с помощью Proof-of-Replication и Proof-of-Spacetime), что они действительно хранят данные[4].

Нововведением относительно IPFS является симметричное шифрование документов до загрузки, где только владелец ключа может расшифровать данные. Хранители данных (узлы сети) не знают содержимого, они видят только зашифрованный набор байт. Схема работы изображена на рисунке 2.

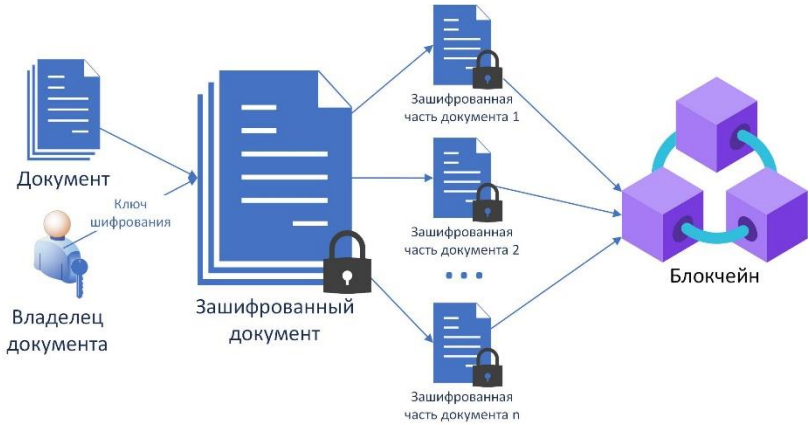



Рис. 2 – схема работы Filecoin.

Storj – децентрализованная облачная платформа хранения данных, аналогичная Filecoin, но более продвинутая в плане распределения частей хранимых файлов. В случае Storj используется следующий алгоритм работы:

1. Данные симметрично шифруются на стороне клиента (AES-GCM).
2. Файл разбивается на 80 и более шардов, применяя Reed-Solomon кодирование. Восстановить файл в таком случае можно по 29 из 80 фрагментов.
3. Шарды распределяются по узлам в сети.

Особенностью также является то, что метаданные файлов также шифруются и хранятся распределенно.

Sia также является децентрализованным облачным провайдером, ориентированным на безопасное зашифрованное хранение, также, как FileCoin и Storj, но с собственными архитектурными особенностями.

Принцип работы:

1. Данные симметрично шифруются на стороне клиента (AES-256).
2. Файл разбивается на 30 частей. Восстановить файл можно по любым 10 фрагментам (принцип кодирования Reed-Solomon, как у Storj).
3. Клиенты и хосты (узлы сети) подписывают смарт-контракты, которые содержат условия хранения данных и оплаты.
4. Узлы, хранящие данные, периодически предоставляют криптографическое доказательство хранения данных (консенсус-механизм Proof-of-Storage).

Ниже, в таблице 1 представлена сравнительная характеристика вышеописанных систем хранения данных.

Таблица 1 – Сравнительная таблица систем хранения.

| Характеристика | IPFS | Filecoin | Storj | Sia |
|---|---|---|---|---|
| Тип сети | Контент-адресуемая P2P-сеть | Блокчейн с экономикой хранения | Децентрализованное облако | Децентрализованное облако |
| Адресация | Хэш (CID) | Хэш через IPFS | Уникальные ID шардов | Уникальные ID шардов с контрактами |
| Шифрование | Отсутствует | AES-256 | AES-256-GCM | AES-256 |
| Фрагментация | Блочная | Блочная | Шардируемая | Шардируемая |
| Восстановление данных | Отсутствует | Отсутствует | Требуется 29 из 80 шардов | Требуется 10 из 30 шардов |
| Доказательство хранения | Отсутствует | Proof-of-Replication | Проверки доступности | Proof-of-Storage |
| Основной фокус | Публичный доступ, публикация | Оплачиваемое долговременное хранение | Защищённое распределённое хранилище | Защищённое хранилище со смарт-контрактами |

По итогам сравнительного анализа систем IPFS, Filecoin, Storj и Sia, можно сделать вывод о целесообразности применения каждой отдельной технологии в конкретной ситуации, в зависимости от экономических требований, требований к адресации и шифрованию.

Использование IPFS будет уместно для открытых публикаций и контент-адресации, когда не требуется шифрование и достаточно репликации обычными узлами сети.

Выбор Filecoin будет оправдан для проверяемого долговременного хранения. Клиентское симметричное шифрование и смарт-контракты с Proof-of-Replication обеспечат гарантии сохранности.

Протокол Storj идеален для коммерческих облачных решений. AES-GCM шифрование, в совокупности с Reed-Solomon шардированием и S3-совместимым API дают высокую отказоустойчивость и простоту интеграции с уже существующими системами хранения.

Sia рекомендуется разработчикам, нуждающимся в гибких условиях хранения и максимальной приватности: симметричное

шифрование, смарт-контракты и схема фрагментации 30/10 оптимизируют цену и надёжность.

Использование криптографических методов защиты неструктурированных данных в децентрализованных блокчейн-хранилищах является перспективным направлением, обеспечивающим высокую безопасность, прозрачность и устойчивость к взломам. Однако для массового внедрения требуется решение существующих проблем, таких как управление ключами, вычислительная сложность и масштабируемость систем. Дальнейшие исследования должны быть направлены на оптимизацию существующих алгоритмов, разработку новых криптографических схем и повышение производительности децентрализованных хранилищ[5].

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Буквина, Е. А. Разработка методов обеспечения информационной безопасности децентрализованных баз данных / Е. А. Буквина, Е. В. Зверева, Е. В. Фалеева, Р. А. Ешенко // Известия Петербургского университета путей сообщения. – 2021. – № 2.

2. Muradov, C. D. Case studies of IPFS-based file-sharing systems / C. D. Muradov // Вестник науки и творчества. – 2023. – № 3. – С. 58-60.

3. Намиот, Д. Е. Архитектурные модели Web3 / Д. Е. Намиот, В. П. Куприяновский // International Journal of Open Information Technologies. – 2024. – № 2.

4. Эйнман, А. Д. Аутентификация пользователей и управление данными с помощью блокчейн-системы / А. Д. Эйнман, И. А. Нагорный // Экономика и качество систем связи. – 2023. – № 1. – С. 78-84.

5. Гвоздевский И.Н. Интеграция технологии блокчейна в инновационном предпринимательстве / Гвоздевский И.Н., Кадацкая Д.В., Лаврова Ю.С. // Modern Economy Success. – 2024. – № 4. – С. 292-299.

*УДК 004.912*

***Воскобойников И.С., Булгаков В.Д.***
***Научный руководитель: Гвоздевский И.Н., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ОБЗОР И СРАВНЕНИЕ МЕТОДОВ ОБРАБОТКИ НЕСТРУКТУРИРОВАННЫХ ТЕКСТОВЫХ ДАННЫХ

В современных информационных системах более 80% данных неструктурированы, а текст является их преобладающей формой [1]. Такие данные включают в себя все — от твитов и писем до научных публикаций и медицинских заключений. В отличие от структурированных данных, текстовая информация не имеет фиксированной схемы и отличается высокой языковой изменчивостью, что затрудняет ее автоматическую обработку.

Цель обработки естественного языка (НЛП) — сделать эти данные машиночитаемыми, что позволяет решать задачи анализа настроения, классификации документов, определения по смыслу и т. д. Однако разнообразие доступных подходов от простых правил до моделей трансформеров требует систематизации и обоснованного выбора методов. В статье мы рассмотрим основные методы обработки неструктурированных текстовых данных, разделив их на три этапа (Рис. 1): предварительная подготовка, преобразование в векторы и классификация.

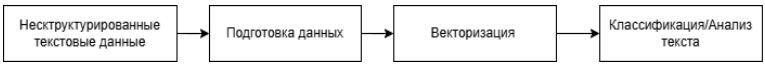



Рис. 1 – Этапы обработки не структурированных текстовых данных.

Текстовые данные сильно различаются по форме и сложности:

- пользовательский контент: неформальный, с ошибками (социальные сети, форумы);
- формальные документы: длинные, предметно-ориентированные (юридические тексты, научные статьи);
- полуструктурированные тексты: встроены в другие форматы (HTML, электронные письма).
- диалоговые данные: чаты, расшифровки разговоров, требуют понимания контекста.

На этапе предобработки выполняются токенизация, приведение к регистру, удаление стоп-слов, лемматизация. Для более сложных

задач — разметка частей речи и извлечение именованных сущностей (НЭР).

Методы векторизации:

- TF-IDF: разреженные и интерпретируемые сведения;
- Word2vec/GloVe: плотные эмбеддинги, отражающие семантику.
- BERT / Sentence-BERT: контекстно-зависимые векторные представления с использованием трансформеров.

BERT использует маскирование слов и двунаправленное внимание, что позволяет моделям учитывать контекст [2]. Sentence-BERT используется для получения векторов предложений [3].

Классификация текста сопоставляет входные данные с предопределенными категориями. Методы делятся на три большие группы:

- правила и словари — простые, но ограниченно масштабируемые;
- классические модели — наивный байес, SVM, логистическая регрессия. Эффективны при наличии качественных признаков (например, TF-IDF).
- глубокое обучение: CNN — выявляют локальные закономерности. LSTM/GRU — работают постоянно. Трансформаторы (BERT, GPT) — лидеры по точности в большинстве НЛП-задач.

Для борьбы с высокой размерностью применяются методы уменьшения размерности:

- PCA/SVD (LSA) — линейные методы для основных признаков;
- t-SNE/UMAP — нелинейные методы визуализации;
- автокодировщики — нейросетевые модели для компактных представлений.

Эти методы часто используются после векторизации для кластеризации и визуального анализа.

Роль блокчейна в обработке неструктурированных текстов.С недавнего времени блокчейн всё активнее интегрируется в задачи обработки неструктурированных данных, в том числе текстов. Его применение позволяет решить ключевые проблемы, связанные с доверием, подлинностью и отслеживаемостью текстовых данных.

Хеши документов или текстов могут храниться в блокчейне, обеспечивая доказательство подлинности и возможности аудита при анализе юридических и медицинских текстов.

При использовании систем NLP на распределённых платформах блокчейн может выступать как инфраструктура согласования между независимыми агентами, обрабатывающими тексты (например, в новостных агрегаторах).

Проекты, такие как Ocean Protocol, позволяют токенизировать доступ к наборам текстов (научные публикации, документы), предоставляя участникам вознаграждение за предоставление данных, что особенно актуально для обучения NLP-моделей.

С помощью блокчейн-смарт-контрактов можно реализовать безопасный доступ к чувствительным текстовым данным, например, пациентским записям, без утраты контроля со стороны владельцев.

Таким образом, блокчейн-технологии не заменяют методы NLP, а усиливают их, предоставляя надежную инфраструктуру для хранения, обмена и верификации текстовых данных.

Сравнительный анализ методов обработки неструктурированных текстовых данных позволяет систематизировать существующие подходы и сопоставить их по ключевым критериям, отражающим их практическую применимость. В условиях большого разнообразия задач (от фильтрации спама до тематического моделирования) и ограничений (вычислительные ресурсы, потребность в интерпретируемости, ограниченный объём обучающих данных) важно выбирать методы осознанно, с учётом их сильных и слабых сторон.

В таблице ниже представлены наиболее популярные методы, классифицированные по четырём параметрам:

- точность — способность модели корректно выполнять предсказание;
- интерпретируемость — насколько легко понять, как и почему модель приняла то или иное решение;
- масштабируемость — способность работать с увеличением объема данных;
- Стоимость ресурсов — оценка потребности в вычислениях (обучение, инференс).
-

Таблица – Сравнительный анализ методов

| Метод | Точность | Интерпритируемость | Масшатбируемость | Стоимость ресурсов |
|---|---|---|---|---|
| Naive Bayes | Средняя | Высокая | Высокая | Низкая |

| | | | | |
|---|---|---|---|---|
| SVM + TF-IDF | Высокая | Средняя | Средняя | Низкая |
| BERT | Очень высокая | Низкая | Низкая | Высокая |
| Sentence-BERT | Высокая | Средняя | Высокая | Средняя |
| Random Forest | Средняя | Средняя | Средняя | Средняя |
| LDA (Topic Model) | Средняя | Средняя | Высокая | Низкая |
| NLP + Blockchain | Зависит от NLP | Высокая | Средняя | Высокая |

Результаты показывают: точность трансформеров (BERT) значительно выше, однако классические модели более интерпретируемы и пригодны для использования в ограниченных количествах ресурсов.

Обработка неструктурированных текстов — ключевая задача в комплексном анализе данных. В статье мы рассмотрели методы векторизации, классификации и уменьшения размерности. Выяснили, что выбор метода должен учитывать специфику задачи, имеющиеся ресурсы и требования к интерпретируемости.

Трансформеры демонстрируют рекордную точность, но требуют значительных ресурсов. Классические модели остаются актуальными для задач в первое время и в условиях ограниченных ресурсов.

Блокчейн открывает новые горизонты для обработки текстов, особенно в контексте достоверности, децентрализации и контроля доступа. Его синергия с NLP — перспективное направление развития, особенно в системах с повышенными требованиями к надёжности.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Gandomi A., Haider M. Beyond the hype: Big data concepts, methods, and analytics // International Journal of Information Management. – 2015. – Vol. 35, No. 2. – P. 137–144.

2. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding // Proceedings of NAACL-HLT 2019. – 2019. – P. 4171–4186.

3. Reimers N., Gurevych I. Sentence-BERT: Sentence embeddings using Siamese BERT-networks // Proceedings of EMNLP-IJCNLP 2019. – 2019. – P. 3982–3992.

4. Фирова, Д. В. Обзор методов и средств извлечения числовых данных из неструктурированный документов на естественном языке / Д. В. Фирова, М. Ю. Барышникова // Матрица научного познания. – 2022. – № 2-1. – С. 56-71.

5. Михнев, И. П. Цифровые технологии Big Data в современном высшем образовании: технологии поиска и обработки неструктурированной информации / И. П. Михнев // Преподавание информационных технологий в российской Федерации : Материалы Семнадцатой открытой Всероссийской конференции, Новосибирск, 16–17 мая 2019 года / Ответственный редактор А. В. Альминдеров. – Новосибирск: Новосибирский национальный исследовательский государственный университет, 2019. – С. 326-329.

6. Zhang Y. et al. Blockchain-Based Secure Data Storage and Sharing for Industrial IoT with Deep Learning // IEEE Transactions on Industrial Informatics. – 2020.

***УДК 004.912***

***Воскобойников И.С.***
***Научный руководитель: Гвоздевский И.Н., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ЭПИСТЕМОЛОГИЯ И ФИЛОСОФИЯ НАУКИ В КОНТЕКСТЕ ОБРАБОТКИ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ

Современная наука и технологии переживают фазу интенсивной трансформации, вызванной экспоненциальным ростом объемов данных. Особенно остро стоит задача обработки неструктурированных данных — текстов, изображений, аудио и видео. Эти данные составляют более 80% всей информации в цифровом мире [1]. На этом фоне появляется необходимость не только в эффективных вычислительных методах, но и в философском осмыслении природы данных, знаний и моделей.

Эта статья рассматривает методы обработки неструктурированных данных сквозь призму эпистемологии — теории познания, а также философии науки, с акцентом на технологические аспекты: алгоритмы, архитектуры, модели и инструменты.

С позиций эпистемологии данные не являются знанием сами по себе — они становятся знанием только после интерпретации, классификации и включения в когнитивную систему [2]. Модели машинного обучения и искусственного интеллекта выступают здесь как инструменты «эпистемического посредничества» [3].

Каждая модель — это форма приближения к реальности, имеющая онтологические ограничения. Например, использование нейросетей предполагает, что в данных существуют латентные представления, которые можно извлечь с помощью оптимизации [4].

Технологические методы обработки.

1. Обработка естественного языка (NLP)

Основные методы:

- tokenization, POS-tagging, Named Entity Recognition (NER);
- векторизация: Word2Vec, BERT;
- тематическое моделирование (LDA, NMF);
- классификация текстов и анализ тональности.

Применение этих моделей связано с необходимостью интерпретации текстов как когнитивных структур [5].

2. Обработка изображений

Ключевые подходы:

- CNNs — для классификации и выделения признаков;
- faster R-CNN, YOLO — для объектного детектирования;
- u-Net, DeepLab — сегментация изображений;
- GANs — генерация и восстановление визуального контента.

Эти методы находят применение в медицине, автономных системах и системах видеонаблюдения [6].

3. Обработка аудио и видео

Используемые подходы:

- преобразование звука в спектрограммы;
- RNN и LSTM для анализа временных последовательностей;
- совмещение аудио и видео каналов в мульти-модальных моделях [7].

Модели данных и философия репрезентации. Нейросети, особенно трансформеры, представляют имплицитные формы репрезентации знания — они извлекают паттерны, но не объясняют их [8]. Это порождает «проблему чёрного ящика» — один из центральных эпистемологических вызовов ИИ [9].

Архитектуры обработки: централизованные и децентрализованные.

Рассмотрим три архитектурных направления:

- hadoop/Spark — распределённая обработка Big Data;
- apache Kafka — стриминг неструктурированных данных;
- IPFS/Filecoin — хранение в децентрализованных P2P-сетях.

Переход к децентрализованным архитектурам требует переосмысления понятий доверия, валидности и авторства данных.

Эпистемологические риски

Проблема объяснимости. Алгоритмы вроде GPT и BERT имеют миллиарды параметров, но не объясняют, почему они выдают тот или иной результат. Это нарушает критерий верифицируемости научного знания.

Ограниченная обобщаемость. Модели часто переобучаются и не справляются с данными вне обучающей выборки. Это нарушает критерии универсальности и фальсифицируемости гипотез.

Смещённые данные. Если обучающая выборка предвзята, то предвзятыми становятся и выводы.

Этические и социальные последствия

Технические системы требуют этических регламентов:

- информированное согласие пользователей;
- защита приватности и данных;
- прозрачность принятия решений.

Современные ИИ-системы способны воспроизводить социальные стереотипы — особенно в чувствительных сферах (кредитование, здравоохранение, правосудие).

Современные методы обработки неструктурированных данных — это не просто инструменты, но и формы научного мышления. Их применение требует учёта философских ограничений, таких как:

- ограниченность познания и принцип фальсификации;
- историчность и смена парадигм;
- этика интерпретации и доверие к алгоритмам.

Только междисциплинарный подход, соединяющий инженерную практику, философию и когнитивные науки, может обеспечить устойчивое и ответственное развитие технологий обработки данных.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гандемы, А., Хайдер, М. Большие данные: революция в аналитике и принятии решений // International Journal of Information Management. – 2015. – Т. 35. – № 2. – С. 137–144.

2. Стёпин, В. С. Теоретическое знание / В. С. Стёпин. – М.: Прогресс-Традиция, 2000. – 400 с.

3. Кун, Т. Структура научных революций / Т. Кун. – М.: АСТ, 2021. – 352 с.

4. Поппер, К. Логика и рост научного знания / К. Поппер. – М.: Рефл-бук, 2002. – 606 с.

5. Петров, П. Эпистемология и её вызовы / П. Петров. – СПб: Изд-во СПбГУ, 2012. – 298 с.

6. Иванов, И. Современные методы компьютерного зрения / И. Иванов. – М.: Наука, 2016. – 290 с.

7. Сидоров, С. Интеллектуальный анализ информации / С. Сидоров. – М.: Прогресс, 2017. – 310 с.

8. Иванов, И. Когнитивные механизмы обработки информации / И. Иванов. – М.: Наука, 2015. – 270 с.

9. Фейерабенд, П. Против метода / П. Фейерабенд. – М.: Мысль, 1975. – 432 с.

10. Михнев, И. П. Цифровые технологии Big Data в современном высшем образовании: технологии поиска и обработки неструктурированной информации / И. П. Михнев // Преподавание информационных технологий в российской Федерации : Материалы Семнадцатой открытой Всероссийской конференции, Новосибирск, 16–17 мая 2019 года / Ответственный редактор А. В. Альминдеров. – Новосибирск: Новосибирский национальный исследовательский государственный университет, 2019. – С. 326-329.

***УДК 004.85***

***Гарайшин Р.Р., Бабенков Ю.М., Елютин И.П.***
***Научный руководитель: Жораев Т.Ю., канд. техн. наук, доц.***
*Национальный исследовательский университет*
*г. Зеленоград, Россия*

## ОБУЧЕНИЕ НЕЙРОСЕТИ DARKNET ДЛЯ РАСПОЗНОВАНИЯ ОБЪЕКТОВ

В современном мире на производствах и в автоматических системах управления популярность набирает распознавание объектов с помощью машинного зрения. Для этого создаются специальные нейронные сети, которые на основе обучения выдают данные о распознанном объекте. Такие нейронные сети можно обучать как просто на фотографиях объектов, так и на формах объекта, что даёт свободу выбора инженерам для решения производственных задач.

Для того чтобы обучить нейросеть, необходимо собрать

множество фотографий интересующего объекта, сделанных в разных условиях, и на каждой фотографии отметить этот объект. Далее остаётся лишь запустить обучение и после оценить качество работы нейросети. В случае неудовлетворения результатом можно либо заменить нейронную сеть, либо улучшить датасет фотографии, разнообразив его.

В начале было определено, что для выделения объектов захвата будет использоваться нейросеть. Для проекта была выбрана нейросеть Darknet, основанная на YOLO-tiny V3 [1].

Для обучения нейросети, сначала необходимо создать датасет фотографий, где объекты вручную будут размечены (рис.1). Важно, чтобы фотографии, используемые для обучения, были сделаны на той же камере, которая будет использоваться для распознавания объектов [2].

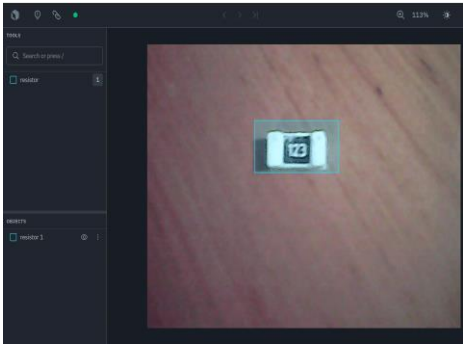


Рис. 1 Процесс разметки объекта обучения на фотографии

После разметки датасета необходимо приступить к обучению нейросети. В процессе обучения, как видно на рисунке 2, точность распознавания со временем увеличивается, и получается нейросеть, которая обучилась распознавать белый кусок пластика с черным квадратом посередине.

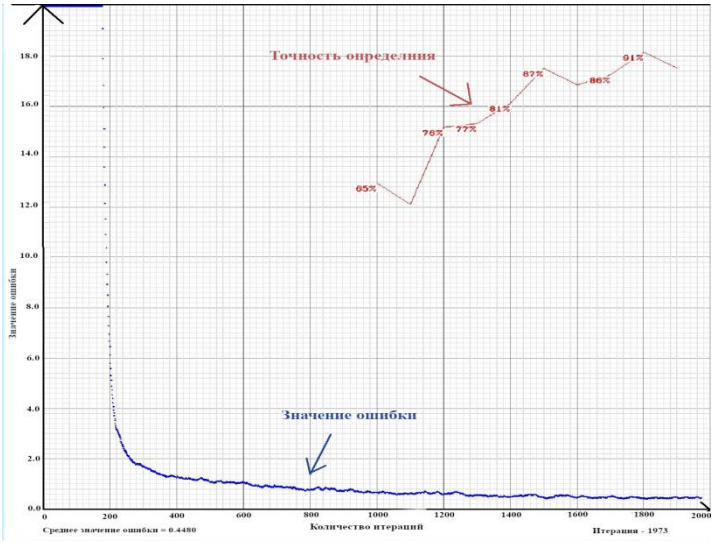
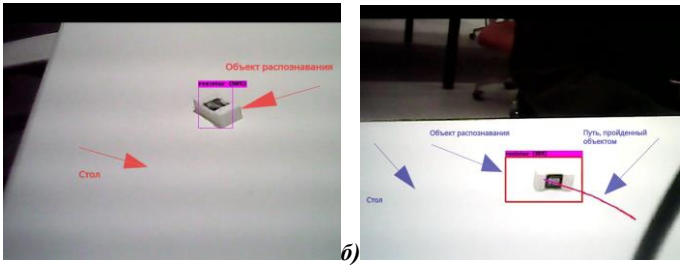



Рис. 2 Графическая иллюстрация обучения нейросети

Запускаем Darknet в режиме распознавания, где в качестве источника изображения указываем видеокамеру. Процесс работы программы представлен на рис.3




*а)* *б)*

Рис. 3 Иллюстрации обнаружения объекта распознавания:
а - обнаружение объекта и визуализация рамки над объектом с использованием нейросети Darknet; б - обнаружение объекта, визуализация рамки над объектом, а также пройденного пути с ипользованием нейросети Darknet и алгоритма KCF.

Действительно, был определён объект в кадре, даже находящийся на фоне такого же цвета, но этого недостаточно. Нейросеть неидеальна, поэтому необходимо прибегнуть к библиотеке OpenCV. С помощью нее можно использовать алгоритмы распознавания, несвязанные с

искусственным интеллектом. Когда нейросеть теряет объект из виду, алгоритм продолжает отслеживание, пока нейросеть не возобновит работу [3]. В данном случае был выбран алгоритм KCF - Kernelized Correlation Filters. Таким образом, получается два независимых метода отслеживания объекта в пространстве. В отличие от нейросети, алгоритм KCF не знает изначально, что ему нужно отслеживать. Для этого нужно написать функцию, которая инициализирует интересующий объект. Сначала объект должен быть найден с помощью нейросети, затем задается прямоугольник, где находится интересующий объект. Теперь алгоритм будет знать, где находится нужный объект и что ему отслеживать. И во время движения объекта, он будет строить путь, пройденный объектом (рис. 3б).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Скляр, А.Я. Детекция жестов с помощью YOLO / А.Я. Скляр, А.А. Высоцкая, А.А. Горячев // Столыпинский вестник. – 2022. – №9. – с. 4926-4936.

2. Лоу Гуанпин. Улучшение алгоритма YOLO-v3 для распознавания небольших объектов // StudNet. – 2021. – №6. – с. 372-385.

3. Телепнев С.А. Разработка комплексного алгоритма обнаружения и сопровождения объектов в видеоряде с использованием глубоких нейронных сетей: 15.03.06. – СПб., 2019. – 81 с.

***УДК 004.8***

***Гоенко И.О.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## РАЗВИТИЕ И ФУНКЦИОНАЛ ИГРОВОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Погружение в виртуальные миры современных видеоигр нередко заслоняет от конечного пользователя грандиозный объем инженерной и творческой работы, вложенной в их создание [1]. Центральным, хотя и не всегда явным, компонентом, обеспечивающим динамику и интерактивность этих цифровых пространств, является игровой искусственный интеллект (ИИ). Важно оговориться: речь идет не о гипотетическом сверхразуме, а о совокупности специализированных

алгоритмов и программных решений, предназначенных для имитации осмысленной деятельности неигровых персонажей (NPC) и управления многообразными аспектами игровой механики.

Игровой ИИ, по существу, функционирует как своего рода управляющая система для компьютерных оппонентов, союзников и даже отдельных интерактивных элементов окружения. Его ключевая задача – формирование у игрока устойчивого восприятия взаимодействия с квази-разумными агентами, способными адекватно реагировать на его действия, осуществлять тактическое планирование и следовать заданным, пусть и программно детерминированным, целям. Наглядными примерами служат патрульные юниты, активирующие сигнал тревоги при фиксации нарушителя; противники, реализующие тактику флангового маневра; или сложные симуляции экосистем, функционирующих по собственным внутренним законам.

Функциональное назначение игрового ИИ многогранно:

1) Создание игрового вызова (Challenge): ИИ-управляемые оппоненты должны демонстрировать тактическую компетентность, достаточную для представления реальной угрозы и мотивации игрока к поиску эффективных стратегий противодействия.

2) Обеспечение правдоподобия (Believability): Поведение NPC должно коррелировать с логикой игрового мира, усиливая эффект погружения (иммерсивности).

3) Поддержка игрока (Support): Контролируемые ИИ союзники могут выполнять вспомогательные роли: оказание медицинской помощи, предоставление тактических рекомендаций, огневая поддержка.

4) Динамическое управление игровым миром: Отдельные ИИ-системы способны в реальном времени изменять окружение, генерировать процедурные события или адаптировать сложность игрового процесса.

Следует подчеркнуть, что разработчики игрового ИИ не всегда стремятся к реализации «идеальной» рациональности. Приоритетом остается создание убедительного и увлекательного игрового опыта. В некоторых случаях предсказуемое, пусть и не оптимальное с точки зрения «интеллекта», поведение ИИ предпочтительнее сверхсложных, но непрозрачных для игрока алгоритмов.

Разработка игрового ИИ представляет собой комплексный поиск баланса между сложностью поведенческих моделей, требованиями к вычислительной производительности и необходимой степенью предсказуемости для пользователя. В арсенале специалистов имеется ряд апробированных методик:

- Конечные автоматы (Finite State Machines, FSM): Одна из ранних и по-прежнему востребованных техник. NPC оперирует набором дискретных состояний (например, «патрулирование», «атака», «отступление»). Переходы между состояниями инициируются выполнением заданных условий (обнаружение цели, получение повреждений). FSM относительно просты в реализации и отладке, но при ограниченном числе состояний могут приводить к стереотипному поведению [3].
- Деревья поведения (Behavior Trees, BT): более гибкая и масштабируемая альтернатива FSM. Дерево поведения представляет собой иерархическую структуру задач. ИИ последовательно обходит узлы дерева, выбирая актуальную ветвь поведения в зависимости от текущей игровой ситуации. BT позволяют конструировать более комплексное и адаптивное поведение [3].
- Алгоритмы поиска пути (Pathfinding): Фундаментальный компонент для любого ИИ, отвечающего за навигацию в игровом пространстве. Алгоритмы типа A* (A-звезда) позволяют NPC вычислять оптимальные или правдоподобные маршруты, обходя препятствия. Качественная система поиска пути критична для предотвращения застревания юнитов и обеспечения адекватного перемещения.
- Сценарные последовательности (Scripting): предварительно запрограммированные сценарии действий или реакций на определенные триггеры. Часто используются для постановочных сцен или специфического поведения ключевых противников (боссов). Скрипты предоставляют разработчикам полный контроль над поведением, но снижают его адаптивность.

Наряду с этими базовыми техниками, в современных проектах применяются и более продвинутые подходы:

- Системы планирования (Planning): Архитектуры, где ИИ определяет высокоуровневую задачу (например, «нейтрализовать игрока») и далее декомпозирует ее в последовательность тактических шагов для достижения (найти оружие -> определить позицию игрока -> занять выгодную точку -> атаковать). Это способствует формированию более «осмысленного» поведения.
- Нечеткая логика (Fuzzy Logic): Позволяет ИИ принимать решения в условиях неполной или неоднозначной информации, оперируя степенями уверенности, а не бинарными категориями. Например, NPC может находиться в состоянии «умеренной встревоженности», что модулирует его последующие действия.
- Системы восприятия (Sensing Systems): Для адекватной

реакции ИИ необходимы виртуальные «органы чувств» (зрение, слух). ИИ «обнаруживает» игрока в секторе обзора или «регистрирует» звуки на определенном расстоянии, что определяет объем доступной ему информации.

- Коллективный ИИ (Squad AI / Flocking): Обеспечивает координацию действий группы NPC. Противники могут действовать согласованно (подавление, обход с фланга), а союзники – обеспечивать взаимное прикрытие. Алгоритмы типа «флокинг» моделируют стайное поведение для групп.
- «Режиссерский» ИИ (AI Director): Система, подобная реализованной в Left 4 Dead. Вместо прямого управления каждым отдельным противником, данная система выполняет роль «дирижера» игрового процесса: регулирует частоту и места появления врагов, распределение ресурсов, интенсивность атак в зависимости от успехов игроков, поддерживая динамическое напряжение и реиграбельность.

Ключевая задача при разработке игрового ИИ – создание убедительной иллюзии разумности. Зачастую ИИ не столько «мыслит» в антропоморфном смысле, сколько искусно симулирует целенаправленное поведение, опираясь на набор эвристик и заранее заготовленных поведенческих шаблонов. Игрок взаимодействует не с программным кодом, а с его внешним проявлением. Если противник эффективно использует укрытия и ведет точный огонь, у пользователя формируется впечатление столкновения с тактически грамотным оппонентом, даже если в основе такого поведения лежит относительно несложный алгоритм.

Дискуссионным аспектом в игровом сообществе остается практика использования ИИ «нечестных» преимуществ, или «читинга» (cheating). Под этим понимается:

- Информационная асимметрия: ИИ обладает знанием о местоположении игрока без прямой сенсорной информации (например, «видит» сквозь препятствия).
- Манипулирование параметрами: ИИ-управляемые объекты могут получать искусственные бонусы (ускорение, повышенное здоровье/урон) для поддержания сложности.

Хотя подобные ухищрения могут быть оправданы необходимостью обеспечить должный уровень вызова при ограниченных ресурсах на разработку более сложных поведенческих моделей, их чрезмерная очевидность подрывает иммерсивность и вызывает фрустрацию. Идеальный ИИ должен достигать превосходства за счет продуманных тактических решений, а не скрытых преференций. Разработчики стремятся к созданию «честного» ИИ, оперирующего в

рамках тех же правил, что и игрок, однако это остается сложной и ресурсоемкой задачей.

Область игрового ИИ находится в процессе непрерывной эволюции. Если ранее вершиной считался противник, способный к элементарному преследованию и атаке, то современные ожидания пользователей значительно возросли.

Игровой искусственный интеллект – это нечто большее, чем просто набор строк кода; это синергия инженерной мысли и творческого замысла, направленная на «одушевление» виртуальных миров. От базовых алгоритмов патрулирования до комплексных тактических схем и адаптивных систем управления – ИИ прошел значительный эволюционный путь и продолжает свое развитие, обещая еще более захватывающие, правдоподобные и непредсказуемые игровые сценарии. Именно благодаря постоянному совершенствованию ИИ-технологий мы получаем возможность испытывать азарт в противостоянии с изощренными противниками, рассчитывать на поддержку виртуальных союзников и глубже погружаться в реальность происходящего на экране. И хотя до появления полноценного «Скайнета» в играх еще предстоит долгий путь, невидимые архитекторы наших цифровых приключений становятся все более искусными.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кузнецова, Е. Н. Применение нейросетей для создания интерактивного видео контента / Кузнецова, Е. Н. // Инновации и технологии. — 2023. — С. 34-42.

2. Рязанов, Ю. Д. Построение рекурсивных распознавателей формальных языков на основе синтаксических диаграмм с многовходовыми компонентами / Рязанов, Ю. Д. // Актуальные задачи математического моделирования и информационных технологий. Материалы Международной научно-практической конференции. — 2017. — С. 85-88.

3. Анохин, А. О. Разработка поведенческих моделей интеллектуальных агентов на базе деревьев поведения и конечных автоматов / Анохин, А. О. // Наука и бизнес: пути развития. — 2021. — № № 12 (126). — С. 10-13.

4. Стальная, В. А. Индустрия развлечений: понятие и основные категории. / Практический маркетинг — 2008. — №9. — URL: https://www.cfin.ru (Дата обращения 15.05.2025)

5. Пивнев, Д. И. Бизнес модель «free-to-play», как современный

инструмент генерации прибыли в мобильном сегменте игровой индустрии / NovaInfo.Ru. — 2015. — №30-1. — URL: https://novainfo.ru (Дата обращения 15.05.2025)

***УДК 004.021***

***Гоенко И.О.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## МЕТОДЫ УПРАВЛЕНИЯ ИГРОВЫМИ ОБЪЕКТАМИ В КОМПЬЮТЕРНЫХ ИГРАХ

Компьютерные игры стали значимым элементом социальной сферы, оказывающим непосредственно влияние на жизнь человека, затрагивая его социальную жизнь и навыки. Вокруг компьютерных игр формируются целые культурные группы, связанные между собой интересом к играм и развитию игровой индустрии. Люди, играющие в компьютерные игры, называют себя «Геймерами». Сообщество геймеров в основном состоит из молодежной группы общества 15-30 лет, но четкие границы выделить сложно ведь геймером может стать любой человек в независимо от его возраста и навыков из-за огромного разнообразия игр и игровых жанров. Во многих странах проводятся официальные мероприятия для геймеров посвященные компьютерным играм, где люди делятся своими впечатлениями и пережитым игровым опытом, одеваются в костюмы игровых персонажей, копируя их внешность и поведение, и обсуждают выход новых игровых новинок в индустрии компьютерных игр. Популярность компьютерных игр можно связать с тем, что в отличии от кино или литературы, где человек может лишь наблюдать за развитием сюжета, игры предоставляют возможность принять непосредственное участие в событиях, происходящих в игре или даже создать собственную историю, ограниченную лишь воображение человека и технической составляющей игры [1]. Возможность взаимодействия с игровым миром компьютерной игры и возникновение событий, не связанных с действиями игрока на прямую, делают его «живым». Но для того, чтобы игрок мог управлять и взаимодействовать с игровыми объектами в игре, разработчику необходимо заложить в игровую логику такую возможность и проработать поведение игровых объектов в своей компьютерной игре. Для управления поведением игровых объектов в

компьютерных играх были рассмотрены 3 метода: скриптовое управление, машины состояний, поведенческие деревья.

Рассмотрим подробнее каждый из них.

**Скриптовое управление**

Центральным элементом рассматриваемого метода является конструирование автоматизированной управляющей системы, чье функционирование детерминируется исполнением скриптовых сценариев. Под скриптом в данном контексте понимается упорядоченная совокупность команд, выраженных на формальном языке программирования и предназначенных для реализации конкретно очерченной задачи. Отличительной чертой таких программных единиц является отсутствие выраженного пользовательского интерфейса; они представляют собой фрагменты кода, активация которых происходит через командную строку или иной программный вызов, после чего они автономно выполняют заложенную последовательность действий и самостоятельно завершают свою работу.

Сфера применения подобных программных решений преимущественно охватывает задачи автоматизации повторяющихся, циклических операций. Так, в индустрии разработки компьютерных игр специалисты часто прибегают к скриптам для описания алгоритмов поведения виртуальных персонажей, управления внутриигровой логикой и создания пользовательских расширений или модификаций. Внедрение данного подхода способствует не только существенной автоматизации рутинных процессов, но и обеспечивает более высокую степень предсказуемости и детерминированности системного поведения. Одним из ключевых достоинств скриптового подхода выступает его модульность, позволяющая рассматривать отдельные скрипты в качестве автономных функциональных блоков, не нуждающихся в глубокой системной интеграции. Присущие данному методу гибкость и универсальность гарантируют его применимость в контексте широкого спектра интерпретируемых языков программирования. Более того, заложенный функционал открывает возможности для имплементации разнообразных специфических поведенческих моделей и сложных логических сценариев.

Применение скриптового подхода также сопряжено с определенными вызовами и ограничениями. Во-первых, потенциальное наличие уязвимостей в коде скриптов создает риски несанкционированного доступа к конфиденциальной информации или компрометации целостности системы. Во-вторых, интенсивное исполнение скриптов, особенно при решении ресурсоемких задач, способно повлечь за собой снижение общей производительности

вычислительной среды. Наконец, процессы отладки и тестирования скриптовых решений могут представлять значительную сложность, в особенности для объемных кодовых баз или при реализации комплексных алгоритмов, что требует от разработчиков повышенного внимания и соответствующей квалификации.

**Машины состояний**

В процессе проектирования программного обеспечения, особенно в такой динамичной сфере, как разработка компьютерных игр, часто возникает задача описания множества дискретных состояний объектов и переходов между ними. Классические подходы к реализации подобной логики нередко приводят к избыточной сложности кода из-за необходимости многочисленных проверок текущего состояния объекта и условий его изменения. Это негативно сказывается на читаемости и поддерживаемости кода, затрудняя коллективную разработку и отладку.

Одним из решений данной проблемы выступает машина состояний (Finite State Machine, FSM) — формальная модель, описывающая поведение системы через конечное множество дискретных состояний и переходов между ними. В игровой индустрии FSM активно применяется для управления поведением персонажей, объектов окружения и других элементов игрового мира. Преимуществом этого подхода является предсказуемость и структурированность логики, что значительно упрощает разработку и повышает устойчивость программного кода к ошибкам [3].

Машина состояний состоит из:

1) Состояний: различные состояния, в которых может находиться объект.
2) Переходов: условия, при которых объект переходит из одного состояния в другое.
3) Действий: логика, выполняемая при входе в состояние, выходе из состояния и во время нахождения в состоянии

Например, объект типа "дверь" может иметь следующие состояния: «закрыта», «открывается», «открыта», «закрывается». В зависимости от действий пользователя или других игровых условий, объект последовательно переходит между этими состояниями. Такой подход обеспечивает высокий уровень интерактивности и предсказуемости поведения игровых элементов.

Тем не менее, по мере увеличения числа состояний и переходов между ними, FSM теряет свою масштабируемость. Управление сложной логикой начинает представлять значительные трудности, особенно при внесении изменений или расширении функциональности.

**Поведенческие деревья**

Для решения проблемы машины состояний в разработке игр всё чаще используется дерево поведения (Behavior Tree, BT). Это структура, представляющая собой ориентированный ациклический граф, узлы которого описывают возможные действия или поведения объекта. В отличие от машины состояний, где логика переходов жёстко привязана к каждому состоянию, в BT логика отделена от конкретных состояний и реализуется на уровне структуры дерева. Это обеспечивает более гибкое управление и облегчает модификацию поведения даже в процессе выполнения программы.

Узлы BT называют задачами или поведениями. Каждая задача может иметь четыре состояния:

- «Успех», если задача выполнена успешно;
- «Неудача», если условие не выполнено или задача, по какой-то причине, невыполнима;
- «В работе», если задача запущена в работу и ожидает завершения
- «Ошибка», если в программе возникает неизвестная ошибка.

Процесс исполнения дерева начинается с корневого узла и реализуется посредством обхода в глубину слева направо. Различают несколько типов узлов: действия, последовательности, селекторы, условия, инверторы и параллельные конструкции. Возможность декомпозиции дерева на поддеревья делает поведенческую модель особенно удобной для разработки, отладки и повторного использования кода.

Среди преимуществ деревьев поведения можно выделить формализованность, модульность и масштабируемость. Однако, их слабой стороной является ограниченность в области реализации сложной логики принятия решений. Деревья поведения не предоставляют встроенных механизмов для динамической оценки контекста, что ограничивает их применение в задачах, требующих интеллектуального анализа ситуации [3].

Проанализировав существующие методы управления игровыми объектами в компьютерных играх, удалось выделить их достоинства и недостатки. Можно сказать, что универсального метода не существует. Каждый из этих метод может использоваться для решения конкретных задач, с которыми один из методов будет справлять лучше всего. Разработчику не составит труда использовать комбинированный подход, в зависимости от сложности поведения каждого создаваемого игрового объекта и от результата которого он хочет добиться.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стальная, В. А. Индустрия развлечений: понятие и основные категории. / Практический маркетинг ― 2008. ― №9. ― URL: https://www.cfin.ru (Дата обращения 15.05.2025)

2. Пивнев, Д. И. Бизнес модель «free-to-play», как современный инструмент генерации прибыли в мобильном сегменте игровой индустрии / NovaInfo.Ru. ― 2015. ― №30-1. ― URL: https://novainfo.ru (Дата обращения 15.05.2025)

3. Анохин, А. О. Разработка поведенческих моделей интеллектуальных агентов на базе деревьев поведения и конечных автоматов / Наука и бизнес: пути развития. ― 2021. ― № 12 (126). ― 10-13.

4. Рязанов, Ю. Д., Построение рекурсивных распознавателей формальных языков на основе синтаксических диаграмм с многовходовыми компонентами / Актуальные задачи математического моделирования и информационных технологий. Материалы Международной научно-практической конференции. — 2017. — С. 85-88.

5. Рузанов, П. А. Защита данных в наиболее популярных системах управления контентом с открытым кодом / П. А. Рузанов, М. С. Чисталев // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей LX Международной научно-практической конференции, Пенза, 15 октября 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 14-17. – EDN NNNAVZ.



***УДК 004.891.3***



***Гончаренко Е.Д.***
***Научный руководитель: Коршак К.С. ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ, МОДЕЛИРОВАНИИ И ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ: КАК ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ МЕНЯЮТ КОРПОРАТИВНУЮ КУЛЬТУРУ

С каждым днём сфера информационных технологий развивается всё стремительнее. Еще недавно мы восхищались первыми примитивными чат-ботами, а сегодня уже никого не удивишь очередной нейросетью, за

секунды генерирующей музыку на любой вкус. Конечно, на этом революционном фоне, чтобы компании оставаться на плаву, ей необходимо внедрять цифровые технологии и следовать новым трендам в информационной сфере. Данный процесс перевода сфер жизни общества и экономики в цифровой мир называется цифровизацией.

Неудивительно, но цифровая трансформация не всегда проходит гладко. Компании переходят на новые современные технологии, приспосабливаются, следят за миром IT. Но почему одни компании после внедрения автоматизированных систем (SAP) получают значительный прирост к эффективности, а другие — массовые увольнения?

Цифровизация – это не только про технологии, но и про самих людей. Как бы информационная сфера ни развивалась, на сегодняшний день полноценной замены человеческой рабочей силы нет. Это говорит о том, что до сих пор именно сотрудники приносят компаниям основную прибыль и определяют их рыночный успех.

Как пример можно привести работоспособность таких организаций во время прошедшей пандемии. До этого люди выстраивали социальные связи у кофемашин: там рождались идеи, передавались сплетни, обсуждались недавние события, – происходило живое общение. С переходом работников на удалённый режим данный «культурный код» перенёсся в «Zoom». Цифровизация не просто перенесла офис в онлайн формат — она переписала негласные законы корпоративной культуры [1].

На фоне различных очевидных плюсов в виде возможности работать из любого удобного места, не соблюдать офисный дресс-код и тратить время на дорогу, присутствуют и значительные минусы. Руководителям стало труднее контролировать работу подчинённых. Некоторые сотрудники чувствуют себя изолированными, теряют связь с коллективом. Особенно страдает командный дух - сложнее поддерживать корпоративную культуру, когда люди редко видят друг друга.

Современные технологии позволяют принимать решения на основе конкретных данных, а не интуиции [2]. Например, CRM-системы показывают, с какими клиентами нужно связаться в первую очередь, а системы аналитики помогают определить, какие проекты приносят больше прибыли.

Такой подход помогает избежать субъективных ошибок. Когда есть чёткие цифры, проще убедить коллег в правильности своего решения. Однако есть и обратная сторона - сотрудники могут перестать предлагать нестандартные идеи, если их нельзя сразу подтвердить

статистикой.

Цифровые технологии позволяют по-новому организовывать рабочие процессы. Теперь легко создавать временные проектные команды из сотрудников разных отделов. Работа становится более гибкой - можно подстраивать график под свои потребности.

Но такие изменения требуют пересмотра многих привычных правил. Должностные инструкции часто устаревают, когда появляются новые способы работы [3]. Нужно обучать сотрудников работать в цифровой среде, помогать им осваивать новые навыки.

Цифровая трансформация - это не просто установка новых программ. Она меняет саму суть работы компании: как люди общаются, как принимаются решения, как организован рабочий процесс.

Самая важная задача для руководителей - не просто внедрить технологии, а помочь сотрудникам адаптироваться к изменениям. Нужно находить разумный баланс между цифровыми инструментами и человеческим фактором, сохраняя при этом эффективность работы. Несоблюдение этого баланса грозит катастрофическими последствиями для всей компании: резким падением мотивации сотрудников, потерей ценных кадров и в конечном итоге - снижением конкурентоспособности бизнеса.

Когда технологии ставятся выше людей, возникает несколько серьёзных проблем:

- Сотрудники чувствуют себя "винтиками в системе", что убивает их вовлечённость
- Творческие работники уходят в компании с более гибким подходом
- В коллективе нарастает сопротивление любым изменениям
- Клиенты замечают формализацию отношений и тоже начинают уходить

Яркий пример - когда компании внедряют системы тотального контроля за удалёнными сотрудниками, такие как трекеры активности, постоянные скриншоты экрана и другие. В краткосрочной перспективе это может дать иллюзию порядка, но очень скоро:

- Лучшие специалисты уходят туда, где им доверяют
- Оставшиеся сотрудники тратят силы на "обход" системы контроля вместо работы
- В коллективе формируется «токсичная» атмосфера подозрительности

Поэтому мудрые руководители понимают: цифровизация должна не заменять человеческий фактор, а усиливать его. Технологии - это инструмент, а люди - главный актив компании.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стативко Р. У., Пентюк С. И., Тетюхин А. О. Подходы к разработке модуля генераторов тестовых заданий и модуля адаптивного тестирования для поддержки учебного процесса в режиме онлайн // Информатизация образования и науки. 2021, № 4. С. 178-185
2. Стативко Р. У., Коломыцева Е. П. Разработка алгоритмов определения необходимости использования типовых моделей датчиков // Известия Юго-Западного государственного университета. 2018, № 6. С. 118-126
3. Стативко Р. У., Коломыцева Е.П. Алгоритм поддержки принятия решения по расстановке датчиков движения в помещении // XXI век: итоги прошлого и проблемы настоящего плюс. 2021, № 2 С. 101-104



***УДК 004.82:519.6***



***Гуленко Д.Г.***
***Научный руководитель: Коломыцева Е.П., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им В.Г. Шухова, г. Белгород, Россия*


## ДИСКРЕТНАЯ МАТЕМАТИКА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ЗАДАЧИ И ОБЛАСТИ ПРИМЕНЕНИЯ

Дискретная математика как область математики, которая занимается изучением дискретных объектов, таких как графы, символы и числа, находит применение в инновационных технологиях таких как большие данные (Big Data), искусственный интеллект (Artificial Intelligence), нейронные сети (Neural networks), машинное обучение (Machine learning), используемые в цифровую эпоху в различных экономических и социальных сферах, в повседневной жизни и в работе.

С.В. Маленков подчёркивает, что дискретная математика (ДМ) является фундаментом для дальнейшего развития подходов к анализу дискретных структур и решения задач [2].

В этой связи, использование искусственного интеллекта (AI), обладающего педагогическим потенциалом может открыть новые возможности в изучении ДМ, автоматического распознавания графовых структур, в распознавании образов, что выводит обучение ДМ на новый уровень и даёт возможность получать студентам знания, которые могут пригодиться в профессиональной деятельности, к примеру при аналитической работы с социальными сетями в рекламе или в междисциплинарных областях биоинформатики, в которых

важное значение имеет статистика, математика и генерация дискретных структур.

Искусственный интеллект, как прорывная технология, при изучении дискретной математики способствует развитию как теории, так и практических приложений в области AI.

Е.А. Перминов отмечает фундаментальное значение ДМ и AI в исследованиях различных наук, таких как абстрактная алгебра, математическая логика, алгоритмы, теории графов и комбинаторика, являющихся основой для разработки систем компьютерной математики и компьютерных технологий [3].

Нечёткие знания, являющиеся разнообразными по своей природе и возникающие при использовании слов естественного языка при моделировании объектов в различных социальных и экономических системах, являются ключевыми при разработке AI.

Процессы принятия решений или моделирование объектов в медицине, искусстве, строительстве можно поддерживать путём разработки методов немонотонной логики Макдермота и Доула, логики Маккарти и логики о замкнутости мира Рейтера, с помощью которых возможно не только работать над логическими системами и их совершенствованием, но и разрабатывать стандарты работы AI, соответствующих человеческому мышлению, что особенно важно в национальных проектах, в проектах «Умных» городов» в различных системах принятия решений и системы «Умный дом». Под понятием «умного дома», будем подразумевать наличие программно-аппаратного комплекса, позволяющего автоматизировать и упростить управление различными системами, а также другим оборудованием жилого или нежилого помещения [6].

В основе разработки технологии AI применяются алгоритмы искусственных нейронных сетей (ИНС), которые соотносятся с адаптирующимися системами, и способны решать достаточно большой круг задач, таких как классификация объектов по признакам, теория оптимального управления, оптимизация и автоматизация процессов и другие.

И. А. Петренко и И. Н. Евсеенко отмечают, что значимость теории графов, в процессе выбора математической модели ИНС, в которой искусственные нейроны являются вершинами графов, а нейронные связи рёбрами, возрастает одновременно с ростом востребовательности автоматизированных систем планирования и прогнозирования и получения более оперативного представления данных, их анализа, результативности и методов поиска решений в системах AI [4].

Ю. Ю. Петрунин подчёркивает, что теория графов помогает упростить формулировки сложных экстремальных и практических задач и может быть эффективной альтернативой традиционным методам статистического анализа. Развитие теории графов в теоретическом и практическом аспектах, результатом чего является построение более эффективных алгоритмов, помогает развивать и «обучать» AI и обуславливает его востребовательность в организационно-технологических и социально-экономических системах принятия решений [5].

Для разработки ИНС применяются такие графовые модели как PyTorchGeometric для фреймворка PyTorch, GraphNets для TensorFlow и Deep Graph и алгоритмы поиск в глубину (Depth First Search) и поиск в ширину (Breadth First Search), алгоритмы Краскала, Дейкстры, Йена.

Предиктивная аналитика, вопросно-ответные системы, на основе интегрирования графовых ИНС, становятся более востребованными в системах интернета вещей, медицинских системах принятия решений, при моделировании экономических и биологических системах, настройки рекламного контента и в вычислениях, что открывает большие перспективы для проработки эффективного инструментария достижения точности ИНС.

Существенными плюсами современных ИНС является возможность одновременного выполнения нескольких вычислительных операций, накапливание информации, суммирование результатов и предоставление на выходе аналитической информации, что обуславливает становление графовых моделей как ключевыми технологиями в AI с учётом специфики решаемых прикладных задач.

М. Ю. Девятериков-Кравченко, рассматривая применение теории множеств (ТМ) в построении алгоритмов машинного обучения подчёркивает, что в машинном обучении ТМ играет важнейшую роль в организации, анализе и интерпретации данных с целью улучшения эффективности и точности алгоритмов [1].

Теория множеств в машинном обучении AI является универсальной и эффективной в таких областях:

– маркетинг, в котором используется кластеризация для группировки показателей (доход членов семьи, размер семьи, профессия пользователя), что позволяет сделать рекламу более персонализированной и эффективной;

– стриминговые сервисы применяют кластерный анализ для формирования целевой аудитории по показателям числа сессий, тематике просматриваемых шоу, просмотровым привычкам, повышая уровень оптимизации сервиса и пользовательского опыта;

– организации могут на основе кластерного анализа осуществлять сегментирование рынка и потребителей, тем самым делая продукты и услуги более конкурентоспособными;
– предприятия различной формы организации в спортивной индустрии используют кластеризацию в целях улучшения игровой тактики, в выборе наиболее оптимальных элементов тренировочного процесса или нагрузки.

Классификация и группировка в машинном обучении, основанные на ТМ имеет ряд преимуществ по сравнению с традиционными методами, к примеру, в медицине ТМ решает задачи минимизации ложных диагнозов, в бизнесе ТМ востребован для сегментации потребителей на рынке товаров или услуг, в государственном управлении для предотвращения киберугроз и помогают сформировать более гибкие модели обучения и развития AI.

Дискретная математика в машинном обучении позволяет автоматизировать статистические и аналитические методы, что позволяет принимать AI решения с минимальным вмешательством человека, что обуславливает становление машинного обучения как мощного инструмента, на основе прогностических алгоритмов, в прогнозировании, анализе рисков и в процессах принятия решений различных сферах применения.

Математические корни машинного обучения могут позволить в будущем взаимодействовать и понимать мир вокруг нас, более точно классифицировать объекты и объяснять ключевые концепции и проблемы.

Таким образом, дискретная математика является катализатором интеллектуального прогресса, затрагивая такие аспекты, как распознавание закономерностей, решение сложных задач и предоставляя инструменты для развития AI, коррекции работы на основе математических моделей и алгоритмов и повышения точности прогнозирования и быстрой обработки данных.

К задачам, которые можно решать в будущем на основе применения AI, можно отнести: задача создания вечного двигателя, всесторонний анализ произведений искусства (компьютерный аналог искусствоведа), разработка алгоритма перечисления всех простых чисел для исследований в математике, астрономические задачи нахождения всех Галактик.

Рассмотренные работы отечественных исследователей дают чёткое представление о том, что дискретная математика, играет важнейшую роль в достижениях и возможностях искусственного интеллекта, предоставляя системам искусственного интеллекта

способность рассуждать, учиться, распознавать закономерности и прогнозировать результаты в таких областях как образование, бизнес, научные исследования, медицина, строительство и производство и многих других элементах социальных и экономических систем.

Следовательно, так как искусственный интеллект стал лидирующей технологией цифровой эры, возрастает и фундаментальная роль дискретной математики не в построении устройств с неограниченными возможностями, а в создании ограниченных систем, которые могут научиться решать много задач, доступных людям.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Девятериков-Кравченко, М. Ю. Применение теории множеств в построении алгоритмов машинного обучения / М. Ю. Девятериков-Кравченко // Тенденции развития науки и образования. – 2024. – № 112-7. – С. 183-185.
2. Маленков, С. В. Использование искусственного интеллекта при изучении дискретной математики / С. В. Маленков // – Минск: Белорусский государственный университет, 2024. – С. 402-404.
3. Перминов, Е. А. О реализации дискретной линии в обучении дисциплине «Искусственный интеллект» студентов педагогических направлений подготовки / Е. А. Перминов // Математический вестник Вятского государственного университета. – 2021. – № 1(20). – С. 22-27.
4. Петренко, И. А. Применение теории графов в искусственных нейронных сетях / И. А. Петренко, И. Н. Евсеенко // Университетская наука. – 2024. – № 1(17). – С. 202-205.
5. Петрунин, Ю. Ю. Искусственные нейронные сети в экономике: математический инструмент, модель или методология? // Вестник Московского университета. – Серия 6. Экономика. – 2024. №4. URL: https://cyberleninka.ru (дата обращения: 28.04.2025).
6. Стативко Р.У., Коломыцева Е.П. Разработка алгоритмов определения необходимости использования типовых моделей датчиков // Известия Юго-Западного государственного университета. 2018. Т. 22, № 6(81). С. 118-126.

*УДК 004.891.3*

***Давыдов Д.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ, МОДЕЛИРОВАНИИ И ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ: РЕВОЛЮЦИЯ ЦИФРОВОЙ ЭПОХИ

Современный мир стремительно трансформируется под влиянием информационных технологий (ИТ). Они проникают во все сферы человеческой деятельности, кардинально меняя подходы к управлению, принятию решений и автоматизации процессов [1]. Особенно значимую роль ИТ играют в:

- управлении (бизнес, государство, производство)
- моделировании (прогнозирование, симуляции, анализ данных)
- интеллектуальных системах (искусственный интеллект, машинное обучение, нейросети)

Современные предприятия и государственные структуры все чаще отказываются от бумажного документооборота и рутинных операций в пользу цифровых решений:

- ERP-системы (SAP, Oracle, 1C) – управление ресурсами предприятия (Рис. 1).
- CRM-системы (Salesforce, HubSpot) – автоматизация продаж и клиентского сервиса (Рис. 2).
- BPM-системы (Camunda, Bizagi) – моделирование и оптимизация бизнес-процессов.
-


Рис. 1 Внедрение ERP-систем

Рис. 2 Внедрение CRM-систем

Таким образом, Внедрение ERP на производстве сокращает логические издержки на 20-30%, а CRM повышает конверсию продаж на 15-25%.

Большие данные позволяют компаниям и государствам принимать решения на основе реальной статистики, а не интуиции [1].

- предиктивная аналитика – прогнозирование спроса, рисков, рыночных трендов.
- BI-системы (Tableau, Power BI) -визуализация данных для руководителей.

Так Amazon используют Big Data для динамического ценообразования, что увеличивает прибыль на миллиарды долларов в год (Рис. 3).


Рис. 3 Динамика выручки и прибыли

Также децентрализованные технологии (блокчейн) и современные системы защиты данных (SIEM. Zero. Trust) делают управление более прозрачным и безопасным (Рис. 4).

Так Эстония внедрила блокчейн в госуправление, что снизило коррупцию и ускорило бюрократические процессы [2].

| | Блокчейн с открытым доступом | Блокчейн с ограниченным доступом | Централизованная база данных |
|---|---|---|---|
| Производительность | Низкая | Высокая | Очень высокая |
| Задержка отклика | Высокая | Средняя | Низкая |
| Количество «читателей» | Высокое | Высокое | Высокое |
| Количество «писателей» | Высокое | Низкое | Высокое |
| Количество непроверенных «писателей» | Высокое | Низкое | 0 |
| Механизм консенсуса | Обычно PoW, иногда PoS | Протоколы, основанные на «Задаче византийских генералов» | Нет |
| Центральное управление | Нет | Да | Да |

INSIDER PRO

Рис. 4 Эффективность блокчейна

Информационные технологии еще и преуспели в науке и промышленности:

- финансовые модели (Monte Carlo. Black-Scholes) – оценка

рисков инвестиций.

- инженерные симуляции (ANSYS, SolidWorks) – тестирование конструкций без реальных прототипов.
- цифровые двойники – виртуальные копии заводов, городов, медоборудования (Рис. 5).

Так Tesla использует цифровых двойников для тестирования автопилота, экономя миллионы на краш-тестах.

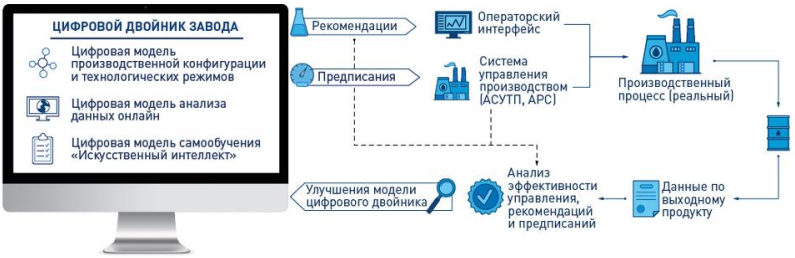



Рис. 5 Схема цифрового двойника

Не смотря на успехи в промышленности, информационные технологии отлично себя реализуют в климатическом и экономическом моделировании:

- изменения климата (модели IPCC).
- экономические кризисы (системы на базе машинного обучения).

Во время пандемии COVID-19 моделирование помогло правительствам прогнозировать нагрузку на больницы (Рис.6) [3].

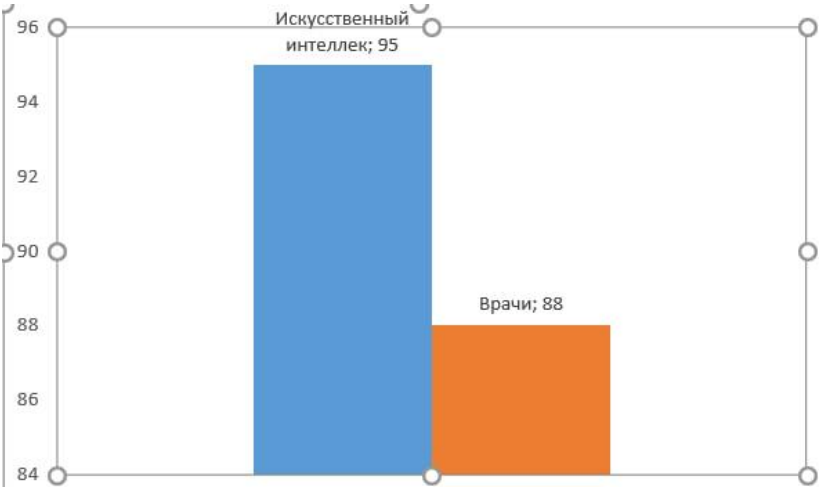


Рис. 6 Точность диагностики

Благодаря таким продвижениям можно гарантировать, что через несколько лет информационные технологии заменят до 40% рутинных офисных, поскольку уже разработаны искусственные интеллекты в управлении, а также машинное обучение и различные нейросети:

- чат-боты и голосовые ассистенты (ChatGPT. Alexa) – автоматизация поддержки клиентов.
- AI-аналитика – выявление скрытых закономерностей в данных.
- компьютерное зрение (распознавание лиц, автономные автомобили).
- генеративные модели (MidJourney. GPT-4) – создание контента.

DeepMind от Google предсказывает структуру белков, что ускоряет разработку лекарств.

Таким образом, современные информационные технологии кардинально меняют подходы к управлению, моделированию и использованию интеллектуальных систем. Так управление стало точнее и эффективнее, а моделирование вышло на новый уровень. Поэтому технология – это не будущее. Это настоящее. Вопрос лишь в том, насколько быстро мы к ним адаптируемся.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стативко Р. У., Коломыцева Е. П. Разработка алгоритмов необходимости использования типовых моделей датчиков // Известия

Юго-западного государственного университета. 2019, №6. С. 118-126

2. Стативко Р. У., Пентюк С. И., Тетюхин А. О. Подходы к разработке модуля адаптивного тестирования для поддержки учебного процесса в режиме онлайн // Информатизация образования и науки. 2021, №4. С. 178-185

3. Стативко Р. У., Коломыцева Е. П. Алгоритм поддержки принятия решения по расстановке датчиков движения в помещении // XXI Век: итоги прошлого и проблемы настоящего плюс. 2021 №2. С. 101-104

***УДК 004.946***

***Журавлева Т.В.***
***Научный руководитель: Киселев А.Л., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ВИРТУАЛЬНАЯ СЕТЕВАЯ ЛАБОРАТОРИЯ EVE-NG

В настоящее время на рынке сетевых технологий представлено множество моделей оборудования от разных производителей. Квалифицированный IT-специалист должен уметь настраивать хотя бы часть из них. Однако, из-за высокой стоимости приобретение такого оборудования может быть нецелесообразным. Решением данной проблемы стали виртуализация оборудования и разработка универсальных эмуляторов. Одним из таких эмуляторов является виртуальная сетевая лаборатория Emulated Virtual Environment – Next Generation (EVE-NG) (с англ. Эмулированная виртуальная среда – нового поколения). EVE-NG является более новой и улучшенной версией предыдущего проекта разработчиков, Unified Networking Lab (UNetLab).

EVE-NG – многофункциональная виртуальная среда, предлагающая обширный набор инструментов для построения и моделирования сетей, работы с виртуальными устройствами и коммутации с реальным оборудованием. Платформа позволяет создавать виртуальные лаборатории, предоставляя доступ к различным типам оборудования, таким как коммутаторы, маршрутизаторы, серверы, персональные компьютеры, межсетевые экраны и т. п. Все это делает EVE-NG незаменимым решением для образовательных целей.

Среда моделирования EVE-NG имеет ряд уникальных черт и особенностей, которые выделяют её среди других эмуляторов:

- *Широкая поддержка виртуализации.* Поддержка сетевого оборудования от более 50 различных производителей, включая Cisco, Juniper, Palo Alto, Fortinet, MikroTik и других.
- *Запуск виртуальных хостов.* Возможность использования популярных операционных систем и организации взаимодействия между ними.
- *Многопользовательский режим.* Распределение прав доступа к созданным и используемым лабораторным стендам для разных пользователей, что идеально подходит для обучения и командной работы.
- *Удобный Web-интерфейс.* Управление EVE-NG происходит через веб-браузер, обеспечивая удобный доступ к среде из любой точки сети.
- *Визуализация сетевых топологий.* Интуитивно понятное представление сети и устройств, упрощающее проектирование, мониторинг и отладку. Возможность разработки интерактивных структур на базе изображений в формате .png.
- *Гибкие варианты установки.* EVE-NG можно установить как виртуальную машину под VMware Workstation или непосредственно на компьютер с ОС Linux Ubuntu.

Программное обеспечение EVE-NG распространяется в двух версиях: EVE-NG Community – полностью бесплатная версия, но имеющая ряд ограничений (однопользовательский режим, ограничение на 63 узла в одной лаборатории, отсутствие поддержки Docker) и платная версия EVE-NG Professional (EVE-NG Pro), которая снимает эти ограничения и предлагает множество дополнительных функций. Для индивидуального обучения достаточно бесплатной версии.

Для полноценного использования EVE-NG с максимальным набором функций и возможностей необходимо приобрести, как минимум, базовую лицензию EVE-NG Professional Base или категории лицензий EVE-NG Corporate и EVE-NG Learning Center. Их отличие в том, что в Corporate включает в себя базовую лицензию, роль Преподавателя/Редактора и два активных сеанса Администратора. А в Learning Center, помимо вышеперечисленного, также присутствует роль Пользователя/Студента. При этом права доступа у преподавателя и студента будут отличаться. Следует отметить, что лицензии предоставляются в виде ежегодной подписки.

EVE-NG представляет собой виртуальную машину, основанную на операционной системе Linux Ubuntu x64. Она включает в себя три подсистемы эмуляции:

- Dynamips – эмулирует маршрутизаторы Cisco и межсетевые экраны Cisco PIX. Программное обеспечение Dynamips функционирует как физическое оборудование маршрутизаторов Cisco, поддерживая несколько моделей и интерфейсных карт.
- QEMU – эмулятор машины, который позволяет запускать операционные системы и программы для одной машины на другой машине.
- Cisco IOL – модель, предназначенная исключительно для внутреннего использования Cisco. IOL функционирует на базе Linux.

Для взаимодействия с EVE-NG пользователю предоставляется несколько типов консолей управления. Бесплатная версия предлагает два варианта: Native Console и HTML5 Console. Их отличие заключается в способе доступа к виртуальным устройствам. Native Console требует установки специализированного программного обеспечения на компьютер, в то время как в HTML5 Console управление осуществляется через браузер без необходимости установки дополнительного ПО. В платной версии доступна также HTML5 Desktop Console, управление в которой осуществляется через браузер с помощью встроенного Docker-контейнера.

Перед началом работы с виртуальной средой EVE-NG, нужно загрузить образы виртуальных устройств. Есть два способа получения таких образов: можно загрузить готовые образы от зарубежных вендоров на специализированных сайтах и форумах, или создать образы самостоятельно. Второй способ является более предпочтительным, так как на фоне геополитических изменений и усиления санкций был объявлен курс на импортозамещение [5]. В таком случае можно создавать, загружать и испытывать образы виртуальных устройств отечественного производства. Для корректной работы виртуальных устройств, имена каталогов, в которых хранятся образы, должны соответствовать таблице имён, представленной на официальном сайте EVE-NG. Также важно размещать образы в правильных директориях.

На официальном сайте продукта http://www.eve-ng.net в разделе «Labs Library» размещен ряд лабораторных работ. Эти лабораторные работы могут оказаться полезными в обучении, так как они охватывают различные аспекты работы со средой виртуализации. При их выполнении происходит знакомство с оборудованием таких известных производителей, как Cisco и Juniper. Также можно научиться конфигурировать различные сетевые протоколы. Есть возможность изучить и выработать практические навыки в области информационной безопасности с помощью отдельного набора лабораторных работ. В него включены такие темы, как виртуальные частные сети (VPN),

межсетевые экраны, системы обнаружения вторжений и аутентификация.

Основываясь на вышесказанном, можно сделать вывод, что виртуальная сетевая лаборатория EVE-NG является простым, доступным и удобным инструментом виртуализации, который значительно облегчит процесс обучения студентов. С помощью этого инструмента они смогут работать с реальным сетевым оборудованием в виртуальной среде, что сделает обучение более практико-ориентированным и позволит получить ценный опыт. В связи с этим, рекомендуем использовать рассмотренную среду моделирования в высших учебных заведениях для повышения качества образования в сфере сетевых технологий.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. EVE-NG Emulated Virtual Environment. Next Generation / [Электронный ресурс]. – URL: http://www.eve-ng.net (дата обращения: 19.05.2025).

2. Лицензирование EVE-NG Pro / [Электронный ресурс] // Wiki EVE-NG Pro: [сайт]. – URL: https://wiki.eve-ng.ru. (дата обращения: 19.05.2025).

3. Панфилов, К. В. Система виртуализации Eve-NG / К. В. Панфилов // Форум молодых ученых. – 2019. – № 2(30). – С. 1149-1151.

4. Новохрестов, А. К. Система EVE-NG для использования в учебном процессе / А. К. Новохрестов, Д. В. Глазырин // Современное образование: интеграция образования, науки, бизнеса и власти: Материалы международной научно-методической конференции. В 2-х частях, Томск, 27–28 января 2022 года. Том Часть 2. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2022. – С. 8-12.

5. Нудной, С. Н. Российское импортозамещение программного обеспечения / С. Н. Нудной // Образование. Наука. Производство: Сборник докладов XVI Международного молодежного форума, Белгород, 30–31 октября 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 183-185.

6. Федотов, Е. А. Виртуализация серверов с использованием гипервизоров / Е. А. Федотов, Е. И. Терехова // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, Белгород, 01–20 мая 2016 года / Белгородский государственный технологический университет им. В.Г. Шухова. – Белгород:

Белгородский государственный технологический университет им. В.Г. Шухова, 2016. – С. 3626-3628.

***УДК 004.415.2***

***Зеновская Д.А.***
***Научный руководитель: Буханов Д.Г., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЛЕЧЕБНО–ПРОФИЛАКТИЧЕСКИМ УЧРЕЖДЕНИЕМ

В современном мире информатизация и автоматизация стали неотъемлемыми элементами развития общества, приобрели огромное значение, а информационно-коммуникационные технологии стали одним из наиболее важных факторов, влияющих на формирование общества [1].

В 2023 году 72,2% организаций использовали в своей работе информационные системы, что помогло значительно улучшить качество и скорость работы сотрудников, сделало предприятие более конкурентоспособным и эффективным [2]. Информатизация – это глубокое проникновение информационных и телекоммуникационных технологий во все сферы жизни и деятельности человека [3].

Рынок программного обеспечения наполнен большим набором решений в области автоматизации процессов в лечебно-профилактических учреждениях. К наиболее распространенным относятся «Проффит», «Здравница», «Санаториум», «Кинт: Управление санаторием», «Реноватио» [4].

**Разработка структуры системы управления лечебно–профилактическим учреждением.**

Основные сценарии использования и необходимые роли пользователей представлены на рисунке 1. В приложении выделены 4 роли пользователей: менеджер, врач, медсестра, администратор. Менеджер осуществляет работу с гостями санатория и отвечает за процессы размещения и бронирования. Врач в рамках системы выполняет задачи, связанные с организацией лечебного процесса и медицинским сопровождением гостей лечебно-профилактического учреждения. Медсестра работает с функционалом, связанным с непосредственным выполнением медицинских процедур, назначенных врачом. Администратор осуществляет контроль за работой всего

учреждения, его эффективностью и имеет доступ к данным отчётности.

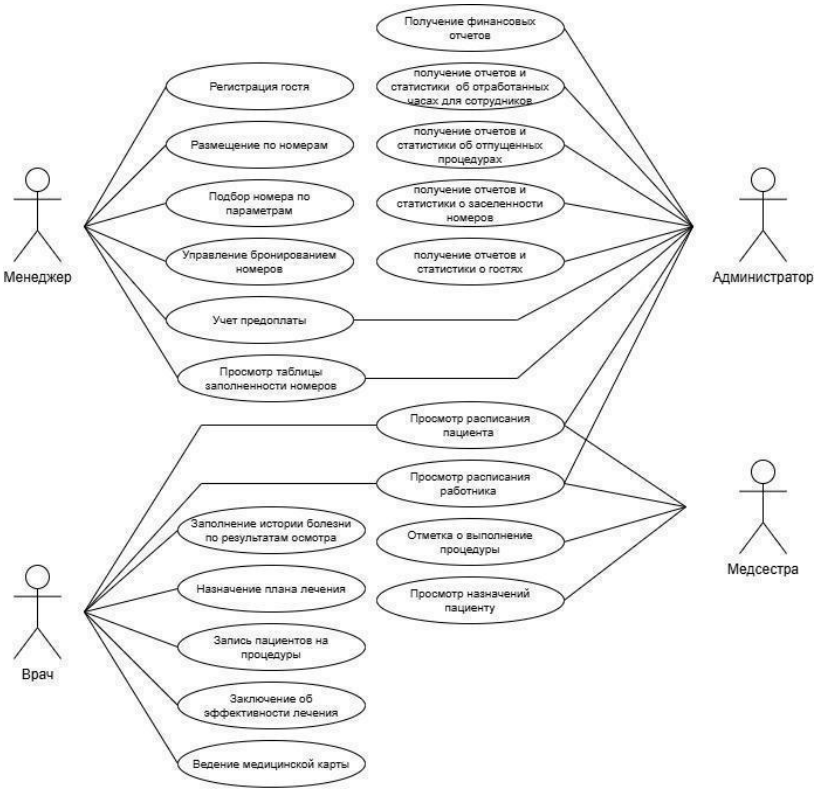



Рис. 1 – Обобщенные сценарии использования системы и роли пользователей

В качестве архитектурного шаблона была использована трехуровневая архитектура, с использование web-технологий [5].

**Реализация системы управления лечебно–профилактическим учреждением.**

Логика приложения разделена на три компонента: представление – клиентскую сторону, отвечающую за пользовательский интерфейс и отправку запросов на сервер, домен – серверная часть, которая обращается к базе данных для получения или сохранения данных и источник данных – реляционная база данных [6]. Взаимодействие элементов системы организовано посредством REST API, позволяющего изолировать компоненты друг от друга и последствий возникающих изменений, что приводит к повышению качества ПО [7].

В качестве языка программирования и фреймворка для системы были использованы Python и Django.

Разрабатываемая система состоит из 8 модулей. Они и отношения между ними представлены на рисунке 2.

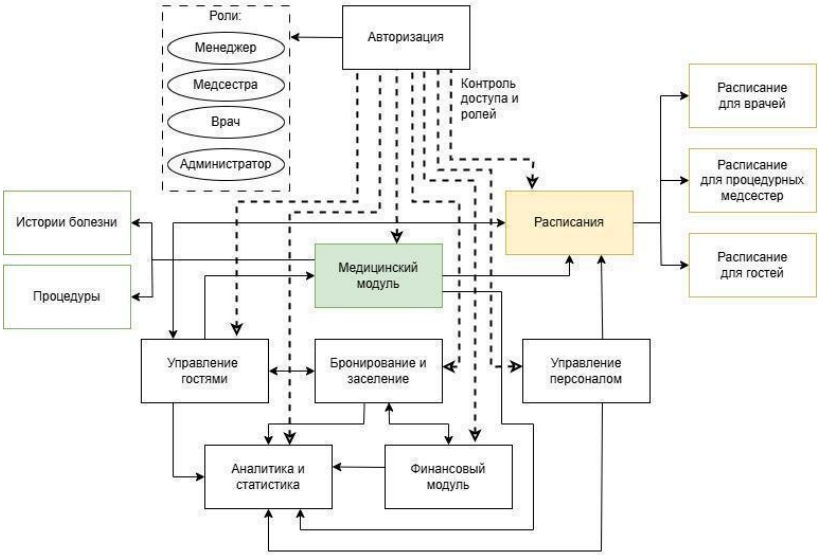



Рис. 2 – Модульная декомпозиция

1. Авторизация – модуль, отвечающий авторизацию и аутентификацию, а также контроль доступа в соответствии с ролями.

2. Медицинский модуль включает в себя функционал для записи на процедуры, ведения историй болезней.

3. Модуль управления гостями необходим для регистрации гостей, заполнения основной информации о них.

4. Управление персоналом – модуль, в котором хранится информация по сотрудникам лечебно-профилактического учреждения: медсестрам, врачам.

5. Модуль расписания отвечает за составление, хранение и управление расписаниями для гостей, врачей и медсестер.

6. Бронирование и заселение – модуль, включающий в себя функционал для подбора номеров в соответствии с параметрами

7. В модуле аналитика и статистика формируются отчеты по отпущенным процедурам, отработанным часам для персонала, выручке от размещения гостей в номерах санатория, эффективности лечения, а

также статистика по отдыхающим, частоте назначения процедур, заболеваниям, с которыми приезжают гости.

8. Финансовый модуль отвечает за учет предоплаты номеров, услуг, выручку за определенный период.

В процессе взаимодействия с системой врач реализует сценарий работы с Медицинским модулем. На начальном этапе взаимодействия с системой пользователь проходит процедуру аутентификации. В процессе аутентификации осуществляется отправка учетных данных (логина и пароля) посредством HTTP запроса к соответствующему серверному эндпоинту. Серверная часть системы проводит проверку валидности переданных данных. В случае успешного прохождения аутентификации формируется ответ, содержащий токен. После получения ответа клиентская часть инициирует запрос на получение информации о перечне разделов, доступных для конкретного пользователя. В указанном списке есть разделы, содержащие функционал из модуля «Медицинский», пользователь получает возможность инициировать переход в соответствующий функциональный блок. При переходе на необходимую страницу осуществляется обращение к соответствующим API-эндпоинтам: для получения списка пациентов или историй болезни, заполнение истории болезни по результатам приема пациента. Каждый такой запрос сопровождается передачей токена, который используется сервером для повторной верификации полномочий пользователя. В случае подтверждения прав доступа сервер возвращает запрашиваемые данные, которые затем визуализируются на клиентской стороне в пользовательском интерфейсе, если был отправлен GET-запрос, либо же происходит создание или редактирование записи в базе данных, если были отправлены запросы POST, PUT, PATCH.

Аналогично предыдущему сценарию, начальный этап заключается в прохождении процедуры аутентификации и получения токена. На следующем этапе клиент запрашивает список разделов, к которым пользователь имеет доступ. В полученном клиентом перечне разрешенных разделов содержатся разделы, использующие функционал модуля «Расписание», интерфейс предоставляет пользователю возможность перехода в данный раздел. При активации соответствующего функционала клиентское приложение отправляет GET- запрос к одному из эндпоинтов модуля «Расписание». Сервер осуществляет проверку запрос, и при успешной проверке формирует ответ, содержащий структуру расписания с указанием необходимых данных. Полученные данные используются клиентским приложением для формирования визуального представления расписания.

Разработанная система с использованием REST-архитектуры позволяет изолировать последствия возникающих изменений, что приводит к повышению качества программного обеспечения и упрощает сопровождение кода. Благодаря четкому разделению логики между клиентской и серверной частью обеспечивается гибкость и масштабируемость приложения. Использование подходов, основанных на REST, также способствует лёгкой интеграции с другими внешними сервисами и модулями.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Цветаев С.С. Методы и инструменты повышения эффективности информационных систем управления промышленным холдингом: автореферат / С.С. Цветаев. – Белгород: БГТУ им. В.Г. Шухова, 2013. 171 с.
2. Российский статистический ежегодник 2023: стат.сб. / Росстат. – М., 2023. 704 с.
3. Украинцев Ю.Д. Роль информации и телекоммуникационных технологий в формировании глобального информационного общества. Закономерности. Проблемы информационного общества: электронное учебное пособие / Украинцев Ю.Д., Курилова О.Л. – Ульяновск: Изд-во УлГУ, 2015. 238 с.
4. Как выбрать МИС для санатория с учетом действующих лицензионных требований: электронный ресурс // База знаний N3.Health – URL: https://n3health.ru (дата обращения 15.04.2025)
5. Фаулер М. Архитектура корпоративных программных приложений: книга / М. Фаулер. – М.: Вильямс, 2006. 541 с.
6. Федотов Е.А. Клиент-серверное взаимодействие в рамках соревновательных онлайн игр / Е.А.Федотов, А.А.Шамраев, Н.С.Пятков, Е.О.Шамраева / Информационные системы и технологии. 2024. № 5. – С. 66-74.
7. API от А до Я: электронный ресурс // Хабр: веб-сайт – URL: https://habr.com/ru (дата обращения 18.04.2025)

*УДК 004.056.55*

***Зубарев М.И., Шевченко А.О.***
***Научный руководитель: Островский А.М., канд. соц. наук., доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ХЕШ-ФУНКЦИЯ, ОСНОВАННАЯ НА СТРУКТУРЕ АПЕРИОДИЧЕСКОГО ЗАМОЩЕНИЯ ТИПА ПЕНРОУЗА

Современные криптографические системы сталкиваются с растущими вызовами, связанными с развитием вычислительных технологий, включая: квантовые вычисления (угроза взлома RSA и ECC), методы машинного обучения (анализ уязвимостей в алгоритмах), оптимизированные атаки (например, на основе side-channel или алгебраических методов). В связи с этим возникает необходимость в разработке новых криптографических структур, устойчивых к таким угрозам. Одним из перспективных направлений является поиск математических структур, обладающих высокой степенью внутренней сложности и апериодичностью, что затрудняет анализ и предсказание на основе известных алгоритмов. В этом контексте особый интерес представляет геометрическая концепция, демонстрирующая уникальные свойства симметрии и непредсказуемости.

Мозаика Пенроуза представляет собой апериодическое замощение плоскости, образованное двумя типами ромбов — «толстым» и «тонким». Несмотря на то, что эти элементы полностью покрывают поверхность без пробелов и наложений, они не формируют повторяющегося периодического узора. Ключевая особенность мозаики — отсутствие трансляционной симметрии: её нельзя сдвинуть так, чтобы она совпала сама с собой. Это свойство делает структуру устойчивой к атакам, основанным на распознавании шаблонов. Дополнительно, мозаика обладает самоподобием — фрактальной природой, при которой одни и те же конфигурации встречаются на разных масштабных уровнях, что повышает криптографическую непредсказуемость.

При масштабировании — через операции инфляции и дефляции — мозаика Пенроуза сохраняет свои апериодические и самоподобные свойства. Это означает, что локальные участки замощения отражают структуру всей мозаики в целом, демонстрируя фрактальную организацию. Процесс построения начинается с начального узора из 5 «толстых» и 5 «тонких» ромбов, равномерно размещённых по окружности, каждый из которых повернут на 72° относительно

предыдущего. Далее применяется операция дефляции — рекурсивного разбиения ромбов на более мелкие элементы. При этом: каждый толстый ромб разбивается на один толстый и два тонких; каждый тонкий — на два тонких и один толстый. Разбиение осуществляется с использованием золотого сечения ($\varphi \approx 1.618$) для вычисления пропорциональных точек деления, что гарантирует точную геометрию и сохраняет самоподобие структуры на всех уровнях иерархии.

Эти геометрические свойства мозаики Пенроуза могут быть использованы в криптографических целях для создания устойчивых к предсказанию и анализу структур. В частности, они позволяют сформировать уникальное представление входных данных, обладающее высокой энтропией и устойчивостью к шаблонному анализу.

Процесс генерации уникального хеша на основе мозаики Пенроуза начинается с преобразования строки. Исходный текст (например, имя, фраза или любой другой ввод) подвергается математическим операциям, в результате которых формируется уникальный числовой код — так называемый сид. Этот сид служит основой для построения мозаики Пенроуза — удивительного узора, который обладает квазипериодической структурой: его фрагменты складываются без образования регулярных повторов.

Полученный сид определяет начальные параметры генерации: угол поворота, тип стартового ромба и количество итераций дефляции. Эти параметры управляют последовательностью геометрических преобразований, в результате которых формируется сложный апериодический узор. Финальный хеш извлекается из геометрических характеристик итоговой мозаики — например, координат вершин, углов между сторонами, или их комбинаций, подвергнутых хешированию или квантованию.

**Algorithm 1** Хеш-функция на основе мозаики Пенроуза

**Require:** сообщение $msg$ (строка или байты)
**Ensure:** хеш-значение $h$ (фиксированной длины)

$\varphi \leftarrow \frac{1+\sqrt{5}}{2}$ ▷ Золотое сечение
$seed \leftarrow$ ИнициализироватьСемя($msg$) ▷ Угол, масштаб, итерации
$tiles \leftarrow$ СгенерироватьМозаикуПенроуза($seed., seed.$)
$hash\_acc \leftarrow 0$
**for all** $(,)$ **в** $tiles$ **do**
    **for all** $v$ **в do**
        $(x, y) \leftarrow v$
        $hash\_acc \leftarrow hash\_acc \oplus$ ФрагментОтКоординат($x, y, $)
    **end for**
**end for**
$h \leftarrow$ Постобработка($hash\_acc$) ▷ например, усечение до 256 бит
**return** $h$

Рис. 1. Псевдокод генерации хеш-функции

Используя полученный сид, мы создаём мозаичный Рис., состоящий из строго определённых геометрических элементов. Особенность мозаики Пенроуза заключается в её способности заполнять плоскость без повторения, что обеспечивает уникальность каждой такой композиции, даже при незначительных изменениях исходной строки.

Рис. 2. Мозаика, сгенерированная в процессе хеширования случайной строки

После построения мозаики осуществляется финальный этап — сборка её ключевых геометрических точек (например, вершин фигур) и применение к ним криптографического хеширования по алгоритму SHA3-256. Хеш-функция преобразует набор данных в фиксированное

по длине значение, визуально напоминающее случайную последовательность символов. Этот хеш служит итоговым представлением исходной строки, зашифрованным через геометрию и строгую математику.

Таким образом, в работе:

1) Предложен оригинальный подход к построению хеш-функции, основанный на свойствах апериодического замощения Пенроуза.

2) Продемонстрировано, что геометрическая самоподобность и отсутствие трансляционной симметрии повышают криптографическую стойкость и устойчивость к шаблонному анализу.

3) Разработанная модель обладает высокой энтропией и может быть адаптирована для генерации уникальных хешей с потенциальной защитой от атак нового поколения, включая квантовые и статистические методы.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Менезес, А., ван Ооршот, П., Ванстон, С. Руководство по прикладной криптографии. — М.: Триумф, 2002. — 816 с.

2. Бернстайн, Д. Дж. Семейство потоковых шифров Salsa20 // Труды по криптографии. — 2008. — Т. 4986. — С. 84–97.

3. NIST. FIPS 180-4. Стандарт безопасного хеширования (SHS). — 2015. — Режим доступа: https://csrc.nist.gov (Дата обращения 5.5.25)

4. Омассон, Ж. П., Невеш, С., Уилкокс-О'Хирн, З., Виннерлейн, К. BLAKE2: Проще, компактнее, быстрее MD5 // Прикладная криптография и безопасность сетей. — 2013. — С. 119–135.

5. Katz, J., Lindell, Y. Introduction to Modern Cryptography. — 3rd ed. — Boca Raton: CRC Press, 2020. — 603 p.

6. Островский, А. М. О компьютерных технологиях поиска эмпирических закономерностей в базах данных // Социология: 4М. — 2008. — № 27. — С. 140–157.

7. Островский, А. М. Оптимизация социального управления человеко-компьютерными системами в техническом вузе: монография. — Белгород: Белаудит; БГТУ им. В. Г. Шухова, 2003. — 208 с. — ISBN 5-7414-0083-3.

*УДК 004.946*

***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.Н., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В УПРАВЛЕНИИ ЦЕПЯМИ ПОСТАВОК: ВЫЗОВЫ И ПЕРСПЕКТИВЫ ТРАНСФОРМАЦИИ ЛОГИСТИКИ

Современные глобальные цепочки поставок сталкиваются с системными проблемами: отсутствие прозрачности, дублирование данных и высокие транзакционные издержки. Блокчейн-технология, благодаря децентрализованной архитектуре и механизмам криптографической защиты, предлагает решения для повышения доверия между участниками и автоматизации процессов. По оценкам российских исследователей, внедрение распределённых реестров позволяет сократить операционные расходы на 20–30% за счёт исключения посредников и снижения рисков фрода [1, с. 45]. Исторически управление цепями поставок в России опиралось на централизованные системы учета, что приводило к задержкам в согласовании данных между поставщиками, логистическими компаниями и ритейлом. Например, в исследовании Иванова и Соколовой (2020) показано, что 67% российских предприятий сталкивались с ошибками из-за ручного ввода информации в ERP-системы. Блокчейн устраняет эти проблемы, обеспечивая синхронизацию данных в режиме реального времени. Ключевым преимуществом технологии является её способность создавать неизменяемые записи, что исключает возможность манипуляций. Это особенно важно в контексте международной торговли, где требования к прозрачности и соответствию стандартам постоянно ужесточаются.

Ключевым преимуществом блокчейна является поддержка различных консенсусных алгоритмов. В России активно развиваются приватные блокчейн-платформы, такие как Masterchain, разработанный Центробанком, который обеспечивает скорость обработки до 10,000 транзакций в секунду. Для логистики особое значение имеет интеграция с системами электронного документооборота, например, с платформой «1С-ЭДО», что позволяет автоматизировать проверку накладных и сертификатов [2, с. 89]. В российском агропромышленном секторе блокчейн используется для отслеживания происхождения зерна. Проект Россельхозбанка «Цифровой зерновой трекер» фиксирует данные о

влажности, условиях хранения и транспортировки, что повышает доверие со стороны международных покупателей. Например, в 2022 году благодаря этой системе экспорт пшеницы из Сибири вырос на 15%, так как зарубежные партнёры получили доступ к верифицированным данным о качестве продукции. В нефтегазовой отрасли «Газпром нефть» внедрила блокчейн-платформу для контроля поставок оборудования, сократив время проверки контрактов с 14 до 2 дней [3, с. 37]. Это стало возможным за счёт автоматизации проверки сертификатов соответствия и отслеживания перемещения грузов через смарт-контракты, которые активируют платежи только после выполнения всех условий поставки.

Несмотря на преимущества, внедрение блокчейна в России ограничивается нормативной неопределённостью. Закон «О цифровых финансовых активах» (2020) регулирует криптовалюты, но не распространяется на промышленные блокчейн-решения. Эксперты Института развития цифровой экономики отмечают необходимость адаптации ГОСТов для сертификации смарт-контрактов и разработки стандартов интероперабельности между платформами [1, с. 48]. Например, отсутствие единого стандарта для цифровых подписей в разных блокчейн-сетях осложняет взаимодействие между участниками цепочки поставок. Блокчейн-технологии могут стать основой для реализации программы «Цифровая трансформация транспортного комплекса». Внедрение сквозной прослеживаемости грузов на Транссибирской магистрали позволит сократить таможенные процедуры и привлечь иностранных инвесторов. Кроме того, интеграция с системой «Меркурий» (для отслеживания ветеринарных сертификатов) повысит экспортный потенциал сельхозпродукции. Уже сегодня 30% мясной продукции, поставляемой из России в Китай, сопровождается блокчейн-метками, что сократило количество спорных ситуаций на 40% [2, с. 92].

Опыт российских компаний демонстрирует, что блокчейн способен трансформировать цепочки поставок, обеспечивая прозрачность и снижая издержки. Ключевыми направлениями развития являются создание отраслевых стандартов, подготовка кадров и адаптация законодательной базы. Успешная реализация пилотных проектов в рамках государственно-частного партнёрства может вывести Россию на лидирующие позиции в области цифровой логистики. Например, в 2023 году стартовал совместный проект Сбербанка и РЖД по внедрению блокчейна для управления мультимодальными перевозками, который охватит 12 регионов и 200 участников цепочки. По прогнозам, это позволит сократить

логистические издержки на 25% и ускорить доставку грузов на 18% [3, с. 38]. Однако для массового внедрения необходимо решить вопросы энергоэффективности: например, переход с алгоритма Proof-of-Work на Proof-of-Authority в корпоративных сетях снижает энергопотребление на 70%, что делает технологию более устойчивой.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кузнецов В.П. Цифровые технологии в логистике / В.П. Кузнецов, А.А. Семёнов // Экономика и управление. — 2021. — № 5. — С. 44–50.

2. Громов А.И. Блокчейн в промышленности: опыт внедрения / А.И. Громов // Информационные системы и технологии. — 2022. — № 3. — С. 87–93.

3. Коломыцева Е. П., Ткаченко С. А., Стативко Р. У. Проектирование информационной системы для рекомендаций расстановки датчиков // Кип и автоматика: обслуживание и ремонт. 2021, № 10. С. 35-39

***УДК 004.2***

***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## РОЛЬ ИНТЕРФЕЙСОВ ЧЕЛОВЕК–МАШИНА В РАЗВИТИИ ЦИФРОВЫХ СИСТЕМ

Современные цифровые системы немыслимы без удобных, интуитивно понятных и адаптивных интерфейсов взаимодействия человека с машиной. Интерфейс человек–машина (Human–Machine Interface, HMI) представляет собой совокупность программных и аппаратных средств, обеспечивающих обмен информацией между пользователем и техническим устройством. От качества этого взаимодействия напрямую зависит эффективность эксплуатации, уровень безопасности, комфорт и восприятие цифровой системы в целом.

Исторически развитие интерфейсов проходило параллельно с эволюцией вычислительной техники. Первые компьютеры не имели

визуальных интерфейсов: ввод осуществлялся с помощью перфокарт, а обратная связь предоставлялась в виде печатных отчётов. С развитием дисплейных технологий появились командные строки, затем графические пользовательские интерфейсы, а сегодня всё более активно внедряются голосовые, жестовые и нейроинтерфейсы [1, с. 17].

Современные требования к HMI выходят за рамки удобства — они включают такие критерии, как адаптивность, отказоустойчивость, доступность и безопасность. Интерфейс становится не просто инструментом взаимодействия, а полноценной частью системы, влияющей на её функциональность. Это особенно важно в высокорисковых областях: управлении транспортом, медицинском оборудовании, производственных системах, где ошибка пользователя, вызванная неочевидным поведением интерфейса, может привести к серьёзным последствиям.

Одной из актуальных тенденций является развитие многоуровневых интерфейсов, где взаимодействие происходит на нескольких логических уровнях: от базового управления до контекстно-зависимой помощи. Например, в авиационных системах пилот работает с множеством панелей и индикаторов, при этом интерфейс должен быть способен адаптироваться под конкретную ситуацию: полёт, посадка, аварийный режим. Такая многоуровневая структура требует высокой надёжности и строгого соответствия эргономическим стандартам [2, с. 38].

Интерфейсы активно развиваются в направлении естественного взаимодействия, приближенного к человеческому общению. Это выражается в интеграции голосового управления, распознавании мимики, жестов, эмоций. Такие подходы находят применение в умных домах, навигационных системах автомобилей, обучающих платформах. Однако внедрение подобных интерфейсов требует решения задач шумоподавления, распознавания многозначности и учёта культурных особенностей пользователей.

Особое внимание уделяется вопросам универсального дизайна, который обеспечивает доступность цифровых систем для людей с ограниченными возможностями. Например, добавление синтезатора речи, интерфейса Брайля или управления с помощью глаз позволяет расширить аудиторию пользователей. Такие решения становятся всё более важными в условиях цифровизации образования, медицины и государственных услуг.

Интерфейс человек–машина также играет ключевую роль в промышленности. Современные HMI-панели в цехах обеспечивают визуализацию технологических процессов, управление оборудованием,

диагностику и выдачу предупреждений. Они должны быть устойчивы к внешним воздействиям (вибрации, пыль, температура), обладать высокой скоростью отклика и поддержкой различных протоколов связи. На предприятиях всё чаще используются интерфейсы, совместимые с системами SCADA и MES, что позволяет интегрировать локальное управление с корпоративной аналитикой.

Отдельного внимания заслуживают интерфейсы в системах управления транспортом. В автомобилях, поездах, авиации интерфейс должен не только предоставлять информацию, но и не отвлекать оператора от основной задачи. Это привело к развитию голосовых ассистентов, проекционных дисплеев, сенсорных панелей с ограниченным количеством элементов и интеллектуальных подсказок. Появление автопилотов и систем помощи водителю ещё больше повышает требования к HMI: пользователь должен иметь возможность мгновенно взять на себя управление при необходимости.

С ростом сложности цифровых систем появилась необходимость в контекстно-зависимых интерфейсах, способных подстраиваться под текущие задачи, уровень подготовки пользователя и условия эксплуатации. Например, интерфейс в мобильном приложении для специалистов может переключаться между упрощённым режимом и профессиональной панелью, в зависимости от профиля пользователя. Это снижает порог входа и повышает эффективность взаимодействия.

Необходимо отметить и значение кибербезопасности интерфейсов. Поскольку HMI всё чаще используется для управления критически важными системами, возникает риск несанкционированного доступа, подмены данных и атак через пользовательский уровень. Решение этих проблем требует комплексного подхода: авторизации, шифрования, ограничения прав, мониторинга действий и внедрения механизмов обнаружения аномалий.

Наконец, стоит отметить влияние интерфейсов на обучение и формирование когнитивной модели пользователя. Удачно спроектированный интерфейс способствует лучшему усвоению функций системы, снижает количество ошибок и ускоряет адаптацию. Наоборот, перегруженный и нелогичный интерфейс вызывает отторжение и может полностью нивелировать преимущества цифрового решения.

Таким образом, интерфейс человек–машина становится неотъемлемым элементом любой цифровой среды, от промышленного комплекса до смартфона. Он формирует пользовательский опыт, определяет удобство эксплуатации и напрямую влияет на эффективность всей системы. Развитие интерфейсов требует

междисциплинарного подхода: от психологии восприятия и эргономики до программной инженерии и защиты информации. В будущем можно ожидать дальнейшей интеграции HMI с технологиями дополненной реальности, нейроинтерфейсами, биометрией и системами предиктивной адаптации, что сделает взаимодействие человека с техникой ещё более естественным и эффективным.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сидоров А.И. История развития интерфейсов человек–машина / А.И. Сидоров // Технологии и интерфейсы. — 2021. — № 2. — С. 15–20.

2. Коломыцева Е. П., Ткаченко С. А., Стативко Р. У. Проектирование информационной системы для рекомендаций расстановки датчиков // Кип и автоматика: обслуживание и ремонт. 2021, № 10. С. 35-39

3. Климова Е.С. Безопасность взаимодействия человека с цифровыми устройствами / Е.С. Климова // Информационная безопасность. — 2023. — № 1. — С. 43–49.

***УДК 004.3***

***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ЭВОЛЮЦИЯ ОПЕРАЦИОННЫХ СИСТЕМ: ОТ МОНОЛИТНЫХ ЯДЕР К РАСПРЕДЕЛЁННЫМ СИСТЕМАМ

Операционные системы представляют собой одну из важнейших составляющих современного программного обеспечения. Они обеспечивают взаимодействие между аппаратной частью компьютера и прикладными программами, управляют ресурсами и гарантируют безопасность вычислительной среды. История их развития — это путь от примитивных программ управления вводом-выводом до мощных распределённых платформ с высокой степенью абстракции, надёжности и гибкости. Анализ этого пути позволяет глубже понять современные архитектурные решения, выявить их сильные и слабые стороны и предсказать возможные направления дальнейшей эволюции.

Ранние версии ОС были ориентированы на выполнение одной программы за раз и не имели пользовательского интерфейса в привычном смысле. Основная задача системы заключалась в том, чтобы эффективно передать управление от загрузчика к выполняемой задаче. Однако с появлением пакетной обработки и мультипрограммирования началась новая эпоха в развитии операционных систем. Программные комплексы стали включать механизмы переключения контекста, планирования задач и управления памятью, что позволило повысить загрузку процессора и общую эффективность системы [1, с. 53].

Монолитные ядра стали логичным продолжением этой тенденции. Они включали в себя практически все функции ОС: планировщик процессов, файловую систему, драйверы устройств и сетевой стек. Все модули взаимодействовали напрямую в едином адресном пространстве, что обеспечивало высокую производительность. Однако такая архитектура оказалась уязвимой к ошибкам: сбой в одном компоненте мог привести к аварии всей системы. К тому же, расширение функциональности требовало перекомпиляции всего ядра, что снижало гибкость и мешало обновлению [2, с. 61].

Развитие концепции модульности привело к появлению микроядерных систем, где в пространстве ядра остаётся лишь минимальный набор функций (планирование, диспетчеризация прерываний, обмен сообщениями), а всё остальное переносится в пользовательское пространство. Это повысило надёжность, так как сбой в одном модуле не затрагивал другие, и упростило сопровождение кода. Однако за это приходилось платить снижением производительности из-за увеличения количества переключений между режимами. Тем не менее, микроядерные ОС, такие как Minix, QNX и L4, доказали свою применимость в встраиваемых системах и системах реального времени, где критичны стабильность и надёжность.

Особую популярность в последние годы получила концепция контейнеризации и оркестрации, в рамках которой приложения изолируются в логические контейнеры, работающие поверх общей ОС. Это позволило создавать лёгкие, масштабируемые и переносимые среды выполнения. Операционные системы начали адаптироваться к таким сценариям, предоставляя расширенные механизмы виртуализации на уровне ядра, пространства имён, контроля ресурсов и безопасности. Linux с поддержкой cgroups и namespaces стал основой большинства контейнерных решений, включая Docker и Kubernetes [3, с. 102].

Отдельным направлением стало развитие распределённых операционных систем, обеспечивающих единое пространство

вычислений на множестве физических узлов. Такие системы управляют ресурсами, хранят данные и выполняют процессы так, как если бы вся инфраструктура представляла собой один компьютер. Примеры — Amoeba, Inferno, Plan 9. Несмотря на сложность реализации, эти идеи нашли воплощение в современных облачных и кластерных решениях, где функции ОС выполняются распределённо между гипервизорами, контейнерными рантаймами и системами хранения.

Важную роль в архитектуре современных ОС играет безопасность. С ростом числа уязвимостей и угроз, операционные системы внедряют многоуровневые механизмы защиты: контроль целостности, ограничение прав доступа, изоляцию процессов, аппаратную поддержку шифрования и виртуализацию. Особое внимание уделяется защите ядра: внедряются технологии KASLR, Control Flow Integrity, защиты от атак типа "спекулятивное исполнение". Также развивается концепция «минимального доверия» (zero trust), в рамках которой каждый компонент системы независимо проверяется на целостность и авторизацию.

Кроме того, наблюдается рост интереса к операционным системам реального времени (RTOS), которые применяются в системах управления, медицинской технике, робототехнике и автомобилестроении. Они обеспечивают жёсткие временные гарантии выполнения задач, что требует особого планирования, предсказуемости и детерминированности поведения. RTOS отличаются компактностью, высокой степенью оптимизации и строгими ограничениями по ресурсам.

Не менее важным направлением является и развитие пользовательских интерфейсов операционных систем. Эволюция от текстовых оболочек до графических интерфейсов и жестовых интерфейсов изменила представление о взаимодействии человека и компьютера. В современных ОС реализуются адаптивные интерфейсы, поддержка многозадачности на мобильных устройствах, технологии голосового ввода и сенсорные возможности. Это расширяет круг пользователей и делает технологии доступными даже тем, кто ранее не взаимодействовал с вычислительной техникой.

Особо стоит отметить роль открытых стандартов и свободного ПО в формировании будущего ОС. Благодаря таким проектам, как Linux, FreeBSD, Haiku, ReactOS, сообщество получает возможность экспериментировать с новыми архитектурными решениями, устранять недостатки проприетарных платформ и развивать идеи децентрализованного управления ресурсами. Поддержка этих систем промышленностью (например, Android на базе Linux или серверы на

базе FreeBSD) демонстрирует жизнеспособность и конкурентоспособность открытых ОС.

Таким образом, операционные системы представляют собой сложные и быстроразвивающиеся программные комплексы, эволюция которых определяется как техническими ограничениями, так и потребностями пользователей. От монолитных ядер до распределённых облачных платформ — этот путь иллюстрирует постоянный поиск баланса между производительностью, надёжностью, безопасностью и гибкостью. Будущее ОС, по всей видимости, будет связано с дальнейшей виртуализацией, специализацией под конкретные аппаратные и прикладные задачи, а также с интеграцией в экосистему интеллектуальных, адаптивных и автономных вычислительных сред. исследований.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Новиков А.В. Эволюция архитектуры операционных систем / А.В. Новиков // Информационные технологии. — 2021. — № 1. — С. 50–55.

2. Рябцев П.М., Захаров К.А. Микроядерные ОС: преимущества и применение / П.М. Рябцев, К.А. Захаров // Компьютерные системы и программирование. — 2022. — № 3. — С. 60–65.

3. Стативко Р. У., Коломыцева Е.П. Алгоритм поддержки принятия решения по расстановке датчиков движения в помещении // XXI Век: итоги прошлого и проблемы настоящего плюс. 2021 № 2. С. 101-104

***УДК 004.94***

***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ЦИФРОВОЙ ДВОЙНИК В ПРОИЗВОДСТВЕННОМ МЕНЕДЖМЕНТЕ: ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ НА ОСНОВЕ ИММИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Переход к цифровой экономике обуславливает стремительное развитие интеллектуальных подходов к управлению производственными системами. Одной из ключевых технологий, находящих применение в промышленности, является цифровой

двойник (digital twin) — виртуальное представление объекта или процесса, интегрированное с физической системой посредством двустороннего обмена данными. Это позволяет не только визуализировать текущее состояние системы, но и прогнозировать её поведение, оптимизировать режимы функционирования и автоматизировать принятие решений.

Цифровой двойник представляет собой комбинацию математических моделей, алгоритмов машинного обучения и потоков данных в реальном времени, поступающих от физического объекта. Его основная цель — создать точную и динамически обновляемую цифровую копию, отражающую все аспекты работы реального устройства или производственного процесса. При этом важным элементом выступает имитационное моделирование, позволяющее воспроизводить различные сценарии эксплуатации объекта без риска для реального оборудования [1, с. 94].

Широкое внедрение цифровых двойников стало возможным благодаря развитию промышленного Интернета вещей (IIoT), технологий обработки больших данных (Big Data), облачных платформ и вычислительных ресурсов. В отличие от традиционных SCADA-систем, цифровой двойник предоставляет не только пассивный мониторинг, но и интеллектуальную аналитику. Система способна выявлять скрытые закономерности, формировать рекомендации и инициировать корректирующие действия автоматически.

Одной из важнейших функций цифрового двойника является предиктивное обслуживание оборудования. С помощью анализа вибрационных характеристик, температуры, давления и других параметров, можно выявлять ранние признаки износа или отклонения от нормы. Это позволяет перейти от реактивной модели ремонта к стратегии «обслуживание по состоянию». По оценкам экспертов, такие подходы позволяют сократить расходы на обслуживание до 30% и снизить частоту аварийных остановок на 40% [2, с. 89].

Цифровые двойники также находят применение в задачах оптимизации производственных процессов. На основе имитационного моделирования можно спрогнозировать влияние изменения технологических параметров на выход продукции, затраты энергии и качество конечного продукта. Это особенно актуально для непрерывных производств, где тестирование на «живом» объекте сопряжено с рисками. Например, в нефтехимической промышленности цифровой двойник позволяет оптимизировать процессы дистилляции и ректификации, повышая выход целевых фракций и снижая энергопотребление.

Интеллектуальные цифровые модели внедряются и на этапе планирования производства. С их помощью можно синхронизировать загрузку оборудования, минимизировать потери при переналадке и учитывать ограничения по ресурсам. При интеграции с ERP-системами цифровой двойник может служить базой для адаптивного производственного планирования в условиях изменяющегося спроса и нестабильности поставок [3, с. 112].

Для создания и функционирования цифрового двойника необходима комплексная архитектура. Она включает в себя уровень сбора данных (датчики, контроллеры), уровень обработки (предиктивная аналитика, модели обучения), интерфейс визуализации и механизмы обратной связи с физической системой. Центральное место в такой архитектуре занимает платформа моделирования, реализующая динамические модели на основе методов конечных элементов, систем дифференциальных уравнений или нейросетевых приближений.

Особое внимание при проектировании цифровых двойников уделяется временной синхронизации данных и моделей. Несоответствие во времени между виртуальным и физическим объектами может привести к ошибочным выводам и действиям. Поэтому в современных решениях используются поточные вычисления, технологии edge-computing и специальные алгоритмы синхронизации временных рядов.

Кроме того, возрастающее внимание уделяется вопросам кибербезопасности. Поскольку цифровой двойник часто взаимодействует с внешними системами (облачные сервисы, подрядчики, удалённый мониторинг), возникает риск несанкционированного доступа и атак. Поэтому внедряются многоуровневые меры защиты: шифрование, сегментация сетей, контроль целостности, поведенческий анализ активности.

На современном этапе цифровые двойники уже активно применяются в следующих отраслях: машиностроение (мониторинг оборудования и управление жизненным циклом), энергетика (моделирование режимов работы генераторов), авиация (диагностика технического состояния и предиктивное обслуживание), строительство (имитация прочности конструкций и мониторинг состояния зданий), фармацевтика (контроль технологических режимов производства лекарств).

В перспективе цифровой двойник станет ядром индустриальной метаплатформы, объединяющей производство, логистику, аналитику и обслуживание. Он превратится из инструмента поддержки принятия решений в активного агента, участвующего в управлении и развитии

всей производственной системы. Уже сегодня ведутся разработки в области когнитивных двойников, обладающих элементами автономного обучения, интерпретации и самоадаптации к внешней среде.

Таким образом, цифровой двойник является мощным инструментом интеллектуального управления производственными системами, совмещающим визуализацию, аналитику, прогнозирование и оптимизацию в едином контуре. Его внедрение требует мультидисциплинарного подхода, объединяющего знания в области информационных технологий, системного анализа, моделирования, управления и промышленной инженерии. Именно такие интеграционные решения позволяют предприятию не просто адаптироваться к условиям цифровой экономики, но и формировать устойчивые конкурентные преимущества на глобальном рынке.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мельников Д.Ю., Корнеев С.П. Безопасность цифровых двойников в промышленности / Д.Ю. Мельников, С.П. Корнеев // Информационные технологии и автоматизация. — 2021. — № 6. — С. 92–98.

2. Орлов А.С. Внедрение цифровых двойников в машиностроении / А.С. Орлов // Цифровое производство. — 2022. — № 3. — С. 85–91.

3. Стативко Р. У., Коломыцева Е.П. Разработка алгоритмов необходимости использования типовых моделей датчиков // Известия Юго-западного государственного университета. 2019, № 6. С. 118-126

***УДК 004.94***

***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ НА ОСНОВЕ АНАЛИЗА ДАННЫХ

Информационные Современное производство всё чаще использует интеллектуальные технологии для автоматизации и оптимизации процессов. Одним из важнейших направлений в этой области является внедрение систем управления на основе анализа больших данных.

Такие системы позволяют адаптивно изменять параметры технологических процессов, оперативно реагировать на нестандартные ситуации и минимизировать влияние человеческого фактора.

Системы управления следующего поколения опираются не только на жёстко заданные алгоритмы, но и на самообучающиеся модели, способные анализировать поступающую информацию и принимать решения на её основе. Это стало возможным благодаря достижениям в области машинного обучения и развития вычислительных мощностей [1, с. 88].

Особое значение интеллектуальные технологии приобретают в условиях цифровизации производственных процессов, когда предприятия переходят к концепции Индустрии 4.0. В этой парадигме оборудование, операторы и системы мониторинга объединены в единую сеть, и принятие решений становится распределённым. Интеллектуальные системы управления в таких условиях обеспечивают гибкость, адаптивность и устойчивость производственной среды [2, с. 104].

Одним из ключевых преимуществ применения интеллектуальных систем является возможность прогнозирования отказов оборудования. На основе анализа исторических данных о работе механизмов формируются модели, способные предсказывать возможные сбои ещё до их наступления. Это позволяет планировать техническое обслуживание и сокращать простои. Например, в одном из исследований применение рекуррентных нейронных сетей позволило снизить внеплановые остановки оборудования на 27% [3, с. 38].

Интеллектуальные алгоритмы также находят применение в задачах оптимизации производственных режимов. Путём анализа текущих параметров технологического процесса система может предлагать корректировки, направленные на снижение энергозатрат, повышение выхода продукции или улучшение качества. Примером может служить система, внедрённая на металлургическом комбинате, где на основе анализа температуры и давления в доменной печи корректировались параметры подачи сырья, что привело к снижению расхода топлива на 9% без потери производительности [1, с. 90].

Для реализации таких систем используются методы машинного обучения, включая регрессионный анализ, градиентный бустинг и нейронные сети. Одним из наиболее эффективных является применение ансамблевых подходов, где результат формируется на основе совокупного мнения нескольких моделей. Это позволяет повысить устойчивость системы к шуму и сбоям во входных данных.

Важной особенностью интеллектуальных систем является их способность к адаптации. В отличие от традиционных решений, где логика работы фиксирована, здесь возможно дообучение модели по мере накопления новых данных. Таким образом, система «учится» вместе с производственным объектом и остаётся актуальной в условиях изменений.

Не менее важным является и вопрос интерпретируемости. В высокотехнологичном производстве недостаточно просто получить рекомендацию от ИИ — требуется обоснование, особенно если речь идёт об отклонении от нормативных параметров. Для решения этой задачи применяются методы объяснимого искусственного интеллекта (XAI), такие как анализ важности признаков, локальные интерпретаторы решений и построение визуальных карт значений входных данных [2, с. 108].

Особого внимания требует безопасность. Системы, принимающие автономные решения, должны быть защищены от киберугроз, поскольку ошибка или вмешательство в работу может привести к сбоям всего предприятия. Поэтому помимо технической реализации ИИ-систем, необходимо предусматривать криптографическую защиту данных, многоуровневую аутентификацию и мониторинг сетевой активности.

Применение интеллектуальных систем управления особенно актуально для высокотехнологичных и энергоёмких отраслей. На предприятиях химической промышленности они помогают контролировать сложные реакционные процессы. В энергетике — управлять режимами генерации и распределения мощности в условиях пиковых нагрузок. В пищевой отрасли — отслеживать микроклимат в цехах и динамику хранения продукции. В машиностроении — управлять логистикой компонентов на сборочной линии.

Таким образом, развитие интеллектуальных систем управления производственными процессами на основе анализа данных является необходимым этапом цифровой трансформации промышленности. Эти решения позволяют не только повысить эффективность, но и сделать производство более предсказуемым, безопасным и устойчивым. Их внедрение требует комплексного подхода: от сбора и очистки данных до создания обучаемых моделей и интеграции в существующую инфраструктуру.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Смирнов В.К., Кузнецов И.Н. Анализ производственных данных для повышения эффективности работы оборудования / В.К. Смирнов, И.Н. Кузнецов // Автоматизация и современные технологии. — 2021. — № 6. — С. 87–93.

2. Захаров А.П. Объяснимый искусственный интеллект в промышленной автоматике / А.П. Захаров // Системы управления и информационные технологии. — 2022. — № 4. — С. 102–110.

3. Коломыцева Е. П., Ткаченко С. А., Стативко Р. У. Проектирование информационной системы для рекомендаций расстановки датчиков // Кип и автоматика: обслуживание и ремонт. 2021, № 10. С. 35-39



***УДК 004.946***



***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.Н., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ЭВОЛЮЦИЯ ПРИКЛАДНЫХ ИНТЕРФЕЙСОВ: ОТ НАСТОЛЬНЫХ ПРОГРАММ ДО МУЛЬТИПЛАТФОРМЕННЫХ СРЕД

Пользовательский интерфейс является важнейшим элементом любой информационной системы, определяющим способ взаимодействия человека с программным обеспечением. С момента появления первых графических оконных оболочек прошло несколько десятилетий, за которые интерфейсы претерпели значительные изменения — как с технологической, так и с концептуальной точки зрения. Сегодня при разработке интерфейсов учитываются не только удобство и функциональность, но и кроссплатформенность, производительность, доступность и визуальная целостность.

Ранняя история интерфейсов связана с развитием настольных операционных систем и появлением графических сред. Такие интерфейсы были строго привязаны к конкретной ОС и архитектуре. Например, интерфейс Windows 95 стал эталоном для многих приложений своей эпохи. Он использовал стандартные элементы управления: кнопки, поля ввода, меню и панели инструментов. Главный упор делался на логичность расположения элементов и соответствие

ожиданиям пользователя, знакомого с физическими аналогами: папками, файлами, корзиной [1, с. 122].

С переходом на интернет-ориентированные технологии возникли веб-интерфейсы, которые изначально были ограничены в возможностях, но постепенно стали полноценной альтернативой десктопным приложениям. Появление HTML5, CSS3 и JavaScript-фреймворков открыло путь к созданию сложных интерактивных систем, не уступающих настольным программам по возможностям. При этом веб-интерфейсы отличались высокой гибкостью, независимостью от платформы и лёгкостью обновления.

Одновременно с этим росло разнообразие устройств: компьютеры, ноутбуки, планшеты, смартфоны, телевизоры, автомобильные системы — все они требовали адаптации интерфейсов под разные размеры экранов, методы ввода и сценарии использования. Так появилась концепция адаптивных интерфейсов, автоматически подстраивающихся под параметры среды исполнения. В современных приложениях разработка ведётся с учётом responsive-дизайна, позволяющего единому интерфейсу сохранять функциональность на любых устройствах [2, с. 82].

Важным направлением стало развитие мультиплатформенных фреймворков, таких как Qt, Flutter, React Native и MAUI. Они позволяют писать один интерфейсный код, который затем компилируется или интерпретируется на нескольких целевых платформах. Это резко снижает затраты на разработку и поддержку программных продуктов. Однако при этом возникает задача сохранения нативности: интерфейс должен вести себя так, как ожидается на каждой конкретной системе. Разработчики решают эту проблему путём настройки визуальных тем, поведения элементов и специфики взаимодействия.

Одной из актуальных задач является обеспечение унифицированного пользовательского опыта. Это означает, что независимо от того, запускает ли пользователь приложение на смартфоне, в браузере или на планшете, оно должно выглядеть и функционировать знакомо. Примеры успешной реализации такого подхода можно наблюдать в экосистемах крупных разработчиков: Google, Microsoft, Apple. Их приложения и сервисы следуют единому стилю и логике, независимо от устройства.

Наряду с визуальными аспектами, важное значение приобрели принципы доступности. Интерфейсы должны быть удобны не только большинству пользователей, но и тем, кто имеет ограничения по зрению, моторике или когнитивным функциям. Поэтому в современных приложениях применяются такие решения, как масштабируемый текст,

навигация с клавиатуры, поддержка скринридеров, звуковые уведомления. Все крупные платформы предоставляют разработчикам инструменты для проверки и обеспечения доступности.

Кроме того, современный пользовательский интерфейс всё чаще интегрируется с внешними системами, такими как базы данных, облачные хранилища, сетевые службы. Это приводит к необходимости обработки больших объёмов данных и асинхронного взаимодействия. Пользователь не должен замечать задержек или сбоев: интерфейс обязан предоставлять обратную связь, использовать индикаторы выполнения и систему уведомлений. Для этого применяются шаблоны проектирования, такие как реактивное программирование, паттерны MVVM, Redux и другие [3, с. 67].

Одним из современных вызовов является обеспечение безопасности пользовательского интерфейса. Поскольку через него пользователь взаимодействует с системой, именно здесь часто совершаются ошибки или целенаправленные атаки. В интерфейс закладываются механизмы предотвращения SQL-инъекций, XSS, CSRF и других уязвимостей. Кроме того, интерфейс должен чётко отражать суть выполняемых операций, предупреждать о рисках, а также предоставлять средства отмены или подтверждения действия.

Отдельное внимание уделяется международным стандартам проектирования интерфейсов, таким как ISO 9241, которые описывают принципы эргономики, визуального оформления, иерархии элементов, восприятия цвета и типографики. Соблюдение этих норм повышает воспринимаемость и снижает когнитивную нагрузку, особенно при работе с информационно насыщенными интерфейсами.

Таким образом, прикладной пользовательский интерфейс прошёл путь от статических панелей до динамических, адаптивных и кроссплатформенных систем. Его значение выходит за рамки удобства — он становится ключевым фактором конкурентоспособности программного продукта, способом формирования доверия и инструментом повышения эффективности. В дальнейшем можно ожидать развития голосовых и нейроинтерфейсов, усиления роли дополненной и смешанной реальности, а также внедрения интеллектуальных подсказок на основе поведенческого анализа. Всё это делает проектирование интерфейсов важной задачей, требующей как инженерной точности, так и творческого подхода.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стативко Р. У., Коломыцева Е.П. Разработка алгоритмов необходимости использования типовых моделей датчиков // Известия Юго-западного государственного университета. 2019, № 6. С. 118-126
2. Щербаков Д.В. Адаптивный интерфейс в мультидисплейных средах / Д.В. Щербаков // Программные системы и технологии. — 2022. — № 6. — С. 81–86.
3. Соловьёв В.И. Архитектура пользовательского интерфейса с учётом производительности / В.И. Соловьёв // Компьютерная инженерия. — 2023. — № 1. — С. 66–72.



***УДК 004.8***



***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ

В последние годы наблюдается стремительное развитие технологий машинного обучения (МО), которые находят широкое применение в различных сферах промышленности. Одной из наиболее перспективных областей применения МО является интеллектуальная диагностика технического состояния оборудования. Такие системы позволяют автоматически выявлять отклонения в работе устройств, прогнозировать отказы и оптимизировать процессы технического обслуживания, что особенно актуально для производства с высоким уровнем автоматизации.

Современные производственные предприятия оснащены множеством сенсоров и систем мониторинга, что приводит к накоплению огромных объёмов данных о состоянии оборудования. Традиционные методы анализа зачастую не справляются с обработкой этих данных в реальном времени. В этой связи особую значимость приобретают интеллектуальные системы, способные извлекать закономерности и выявлять скрытые аномалии в поведении оборудования [1, с. 102].

Основная задача интеллектуальной системы диагностики — это своевременное и точное выявление неисправностей или снижения

эффективности работы оборудования. Для этого применяются алгоритмы классификации, регрессии и кластеризации, обученные на исторических данных, собранных с объектов. Среди наиболее эффективных методов можно выделить деревья решений, случайные леса (Random Forest), метод опорных векторов (SVM) и, конечно же, глубокие нейронные сети.

Важную роль играет построение качественной обучающей выборки. Необходимо собрать как можно больше данных с сенсоров оборудования: вибрационные характеристики, температурные режимы, уровни шума, давление, частота работы и т.п. После первичной фильтрации и очистки данные подвергаются нормализации, а затем используются для обучения алгоритмов машинного обучения. Сложность заключается в необходимости балансировки классов — чаще всего в выборке представлено мало примеров с отказами, что создаёт проблему несбалансированных данных [2, с. 72].

Алгоритмы машинного обучения могут работать как в оффлайн-режиме, так и в реальном времени. В последнем случае применяется потоковая обработка данных с возможностью онлайнового дообучения модели. Это особенно актуально для крупных производственных объектов с высокой динамикой процессов, где условия эксплуатации оборудования постоянно меняются.

Анализ эффективности различных алгоритмов показывает, что нейронные сети обеспечивают наивысшую точность прогнозирования технических неисправностей, достигающую 95,6%. Случайные леса показывают немного более скромные результаты — около 92,1%, в то время как метод опорных векторов демонстрирует точность порядка 89,4%. Эти значения, полученные на одинаковом наборе производственных данных, указывают на высокую применимость современных моделей МО в задачах диагностики.

Для повышения точности интеллектуальной диагностики применяются ансамблевые методы, такие как градиентный бустинг (XGBoost, LightGBM) и стеккинг, при котором несколько моделей объединяются в единую структуру. Это позволяет компенсировать слабые стороны отдельных моделей и обеспечить более устойчивое поведение при нестандартных данных.

Отдельное направление исследований — интерпретируемость моделей. Например, в производственной среде важно не только получить факт сбоя, но и объяснить его причину. Для этого применяются такие подходы, как SHAP-значения и методы локальной интерпретации (LIME), которые позволяют определить вклад каждого входного признака в итоговое решение модели [3, с. 109].

Не менее важно обеспечить надёжную интеграцию интеллектуальной диагностической системы с существующими средствами мониторинга и управления. Важно предусмотреть архитектуру, позволяющую масштабировать систему, обновлять алгоритмы и интегрировать её с ERP или MES-системами.

Интеллектуальные системы диагностики находят широкое применение на металлургических предприятиях, где они используются для мониторинга состояния агрегатов и конвейеров, в энергетике — для диагностики турбин и генераторов, в транспорте — для анализа износа и состояния узлов подвижного состава, а также в авиации и космонавтике, где такие системы применяются для предиктивного обслуживания критичных узлов. Кроме того, они используются в системах жилищно-коммунального хозяйства для мониторинга насосного и теплового оборудования.

Помимо производственных применений, технологии МО активно внедряются и в смежных отраслях. Например, в умных зданиях они используются для диагностики систем вентиляции, отопления и электроснабжения. Это позволяет снизить энергозатраты и повысить комфортность эксплуатации объектов.

Таким образом, применение технологий машинного обучения в интеллектуальных системах диагностики оборудования позволяет существенно повысить надёжность работы производственных систем, снизить издержки на техническое обслуживание, предупредить аварийные ситуации и повысить эффективность эксплуатации. Дальнейшее развитие этого направления связано с внедрением гибридных моделей, обработкой данных с использованием edge-компьютинга и повышением прозрачности решений, принимаемых интеллектуальными системами.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стативко Р. У., Коломыцева Е.П. Алгоритм поддержки принятия решения по расстановке датчиков движения в помещении // XXI Век: итоги прошлого и проблемы настоящего плюс. 2021 № 2. С. 101-104

2. Тихонов Е.С. Применение нейронных сетей в системах предиктивного обслуживания / Е.С. Тихонов // Искусственный интеллект и цифровое производство. — 2023. — № 1. — С. 70–75.

3. Иванова Т.Н. Интеллектуальные цифровые модели в управлении производственными системами / Т.Н. Иванова // Автоматизация и инновации. — 2023. — № 2. — С. 108–114.

*УДК 004.946*

***Иванисов Д.С.***
***Научный руководитель: Коломыцева Е.Н., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕДИЦИНЕ: ТРАНСФОРМАЦИЯ ДИАГНОСТИКИ, ЛЕЧЕНИЯ И ПРОГНОЗИРОВАНИЯ ЗАБОЛЕВАНИЙ

Современная медицина переживает революцию, вызванную внедрением технологий искусственного интеллекта (ИИ). От автоматизации рутинных задач до разработки персонализированных схем лечения — ИИ становится ключевым инструментом повышения точности диагностики, оптимизации ресурсов и снижения нагрузки на медицинский персонал. По данным Министерства здравоохранения РФ, к 2023 году более 30% государственных клиник в России внедрили ИИ-решения для анализа медицинских изображений, а 15% используют алгоритмы машинного обучения для прогнозирования эпидемиологических рисков [1, с. 56]. Эти технологии не только сокращают время постановки диагноза, но и позволяют выявлять заболевания на ранних стадиях, когда традиционные методы оказываются недостаточно эффективными.

Исторически развитие ИИ в медицине началось с экспертных систем 1980-х годов, таких как MYCIN для диагностики бактериальных инфекций. Однако настоящий прорыв произошёл в 2010-х годах благодаря доступности больших данных и развитию глубокого обучения. В России первые масштабные проекты стартовали в 2016 году с запуском платформы «Цифровая клиника» в Сколково, где ИИ-алгоритмы анализировали истории болезней 50,000 пациентов для выявления скрытых паттернов. Результаты показали, что точность прогнозирования сердечно-сосудистых заболеваний увеличилась на 27% по сравнению с традиционными методами [2, с. 119]. Сегодня российские разработки охватывают все аспекты медицины — от радиологии до генетики.

Одним из наиболее значимых направлений является анализ медицинских изображений. Алгоритмы компьютерного зрения, обученные на миллионах рентгеновских снимков, КТ и МРТ, способны обнаруживать патологии с точностью, превышающей человеческую. Например, система «РадиоИИ», разработанная в МФТИ, идентифицирует рак лёгких на ранних стадиях с точностью 94%, тогда

как средний показатель радиологов составляет 87% [3, с. 112]. В 2022 году эта система была внедрена в 20 онкоцентрах России, что позволило сократить время диагностики на 40% и снизить количество ложноположительных результатов на 15%. Важным преимуществом является способность ИИ анализировать снимки в режиме реального времени, что критично в экстренных случаях, таких как инсульты. В НИИ скорой помощи им. Н.В. Склифосовского алгоритмы, интегрированные с КТ-сканерами, автоматически определяют зоны ишемии мозга, сокращая время принятия решения о тромболитической терапии с 25 до 7 минут.

Персонализированная медицина — ещё одно перспективное направление. ИИ-платформы, такие как «ГеномАИ» (разработана в Курчатовском институте), анализируют генетические данные пациентов для подбора индивидуальной терапии. В проекте по лечению онкологических заболеваний алгоритм сопоставляет мутации в опухолевой ДНК с базами клинических испытаний, предлагая оптимальные комбинации препаратов. В 2023 году в рамках пилота с участием 500 пациентов с метастатическим раком молочной железы выживаемость в группе, где лечение подбиралось ИИ, увеличилась на 22% по сравнению с контрольной группой [1, с. 61]. Кроме того, ИИ используется для прогнозирования побочных эффектов. Система «ФармаСейф», внедрённая в московской ГКБ № 52, анализирует электронные медкарты и генетические тесты, предупреждая врачей о рисках аллергических реакций или несовместимости лекарств. За первый год эксплуатации количество госпитализаций из-за неправильно назначенных препаратов сократилось на 35%.

Внедрение ИИ в хирургию открыло новые горизонты для роботизированных операций. Российская система «Хирург-Ассистент», созданная в партнёрстве с Ростехом, сочетает компьютерное зрение и манипуляторы с тактильной обратной связью. В 2023 году в НМИЦ им. А.Н. Бакулева проведено 120 операций на сердце с использованием этой системы, где точность наложения швов увеличилась на 30%, а время операции сократилось на 25%. Особенно перспективным направлением является телемедицина: в отдалённых регионах, таких как Якутия, хирургические роботы, управляемые через 5G-сети, позволяют проводить сложные вмешательства под руководством столичных специалистов.

Однако масштабирование ИИ-технологий сталкивается с серьёзными вызовами. Правовые и этические вопросы остаются главными барьерами. В России отсутствует федеральный закон, регулирующий использование ИИ в медицине, что создаёт риски для

защиты персональных данных. По оценкам Института цифровой медицины Сеченовского университета, 60% медицинских организаций не имеют инфраструктуры для безопасного хранения и обработки данных пациентов [2, с. 95]. Кроме того, возникает вопрос ответственности за ошибки алгоритмов. В 2022 году в Пермской краевой больнице произошёл инцидент, когда ИИ-система неправильно интерпретировала рентгеновский снимок, что привело к задержке лечения. Это подчёркивает необходимость разработки стандартов валидации алгоритмов и создания «чёрных ящиков» для аудита решений ИИ.

Технические ограничения также замедляют внедрение. Обучение нейросетей требует огромных вычислительных ресурсов. Например, тренировка модели для диагностики редких генетических заболеваний на базе суперкомпьютера «Ломоносов-2» в МГУ заняла 3 месяца и стоила 12 млн рублей [3, с. 118]. Кроме того, в регионах с низким качеством интернета использование облачных ИИ-сервисов становится невозможным. Решением может стать развитие федеральной сети периферийных вычислений (edge computing), где обработка данных происходит локально, без передачи в центр.

Перспективы развития ИИ в российской медицине связаны с интеграцией технологий в национальные проекты. Программа «Цифровое здравоохранение 2030» предусматривает создание единой платформы для сбора и анализа данных от 100 млн пациентов. Это позволит тренировать алгоритмы на разнообразных данных, учитывая этнические и географические особенности. Уже сегодня в пилотном режиме работает система прогнозирования эпидемий гриппа, которая анализирует поисковые запросы, данные соцсетей и электронные больничные листы. В 2023 году она предсказала вспышку в Новосибирске на 2 недели раньше традиционных методов, что позволило развернуть дополнительные койки и избежать перегрузки медучреждений [1, с. 68].

Ещё одним направлением является разработка ИИ-ассистентов для врачей. Система «Доктор Плюс», тестируемая в РНИМУ им. Н.И. Пирогова, анализирует жалобы пациентов, историю болезней и результаты анализов, предлагая дифференциальные диагнозы. В 85% случаев её рекомендации совпадают с заключениями опытных терапевтов. Для сельских больниц, где не хватает узких специалистов, это может стать спасением. Например, в Тверской области ИИ-ассистент помог диагностировать редкое аутоиммунное заболевание у ребёнка, которое местные врачи первоначально приняли за аллергию.

Этические аспекты применения ИИ требуют отдельного внимания. Риск дискриминации из-за смещённых данных — реальная проблема. В 2022 году исследование НИУ ВШЭ выявило, что алгоритмы для диагностики диабета хуже работают на данных пациентов старше 70 лет, так как обучались преимущественно на молодых людях [2, с. 121]. Для решения этой проблемы российские разработчики внедряют методы синтеза искусственных данных и балансировки выборок. Кроме того, важен вопрос прозрачности: пациенты должны понимать, как ИИ влияет на их лечение. В клиниках Москвы уже начали внедрять систему информированного согласия, где разъясняется роль алгоритмов в постановке диагноза.

Таким образом, искусственный интеллект трансформирует медицину, предлагая инструменты для ранней диагностики, персонализированного лечения и управления ресурсами. Несмотря на технические и регуляторные барьеры, российские разработки демонстрируют впечатляющие результаты. К 2030 году, согласно стратегии Минздрава, ИИ будет использоваться в 80% медучреждений страны, что потребует подготовки 50,000 IT-специалистов и врачей, владеющих цифровыми компетенциями. Успех зависит от синергии государства, науки и бизнеса — только так можно создать экосистему, где технологии служат улучшению качества жизни миллионов пациентов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Смирнов А.В. Цифровая трансформация здравоохранения в России / А.В. Смирнов, Е.К. Фёдорова // Медицинские технологии. — 2023. — № 4. — С. 55–70.

2. Стативко Р. У., Коломыцева Е.П. Разработка алгоритмов необходимости использования типовых моделей датчиков // Известия Юго-западного государственного университета. 2019, № 6. С. 118-126

3. Лебедев Д.С. Нейросети в диагностике заболеваний / Д.С. Лебедев // Информационные системы в медицине. — 2023. — № 1. — С. 110–120.

*УДК 338.24:004*

***Иванов К.И.***
***Научный руководитель: Ванькова Т.Е. ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# УМНЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ЖИЛЫМИ КОМПЛЕКСАМИ (SMART PROPERTY MANAGEMENT): ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЖИЛИЩНОЙ ИНФРАСТРУКТУРЫ

Современные технологии кардинально меняют подходы к управлению жилыми комплексами, обеспечивая не только повышение комфорта для жильцов, но и значительную экономию ресурсов. Внедрение интеллектуальных систем, таких как «умный дом», IoT-устройства и автоматизированные платформы, позволяет оптимизировать эксплуатационные процессы, снижать затраты и повышать безопасность. По данным аналитиков, к 2025 году доля многоквартирных домов (МКД) с технологиями «умного дома» в России достигнет 13,6%, что в три раза превышает показатели 2019 года. В данной статье рассматриваются ключевые аспекты Smart Property Management, включая экономические выгоды, технологические решения и перспективы развития.

Внедрение интеллектуальных технологий в управление жилыми комплексами демонстрирует значительную экономическую эффективность, что подтверждается реальными данными и статистикой. Одним из ключевых преимуществ является снижение эксплуатационных расходов за счет оптимизации потребления ресурсов. Например, автоматизированные системы учета воды и электроэнергии позволяют сократить затраты на коммунальные услуги на 30–40%. В жилом комплексе в Самаре внедрение умных счетчиков и систем автоматического регулирования отопления привело к снижению затрат на теплоснабжение на 50,15%, а на водоснабжение — на 44,5%.

Кроме того, умные технологии минимизируют потери, связанные с человеческим фактором. Автоматизированные системы мониторинга инженерных сетей выявляют утечки и неисправности в режиме реального времени, предотвращая аварийные ситуации. По данным исследований, превентивный ремонт оборудования на основе данных IoT-датчиков сокращает затраты на обслуживание на 25% по сравнению с традиционными методами реагирования на поломки.

Еще одним важным аспектом является повышение доходности объектов недвижимости. Жилые комплексы, оснащенные умными технологиями, привлекают более платежеспособных арендаторов, готовых платить на 10–15% больше за комфорт и энергоэффективность. Согласно опросам, 74% арендаторов предпочитают объекты с энергосберегающими решениями, а 54% рассматривают наличие умных домов как ключевой фактор при выборе жилья.

Трансформация бизнес-моделей управления также вносит существенный вклад в экономическую эффективность. Платформенные решения позволяют создавать новые сервисы для жильцов - от дистанционного контроля доставок до системы бронирования мест общего пользования. Эти дополнительные услуги генерируют доход управляющих компаний в размере 120-180 рублей с квадратного метра в год, что при средней площади жилого комплекса 50 000 м² составляет 6-9 млн рублей дополнительной выручки ежегодно.

Современные технологии кардинально трансформируют подходы к управлению жилыми и коммерческими объектами недвижимости, предлагая комплексные решения для автоматизации, безопасности и энергоэффективности. Одним из ключевых элементов являются интегрированные IoT-системы, которые объединяют датчики, устройства и аналитические платформы для мониторинга состояния зданий в режиме реального времени. Например, умные термостаты и сенсоры утечек позволяют сократить затраты на коммунальные услуги на 25–40%, а также предотвратить аварийные ситуации за счет своевременного оповещения.

Искусственный интеллект применяется для прогнозирования потребностей в обслуживании и оптимизации арендных стратегий. AI-алгоритмы анализируют данные о состоянии оборудования, предсказывая износ инженерных систем с точностью до 85%, что сокращает расходы на незапланированные ремонты. Чат-боты на базе AI также автоматизируют взаимодействие с арендаторами, обрабатывая до 70% типовых запросов без участия человека.

Блокчейн постепенно интегрируется в сферу управления недвижимостью, обеспечивая прозрачность сделок и автоматизацию контрактов. Смарт-контракты на основе блокчейна исключают риски мошенничества при аренде и платежах, автоматически исполняя условия соглашений при наступлении определенных событий, таких как внесение депозита или окончание срока аренды.

Облачные платформы играют pivotal роль в централизации управления данными. Такие решения, как Yardi или AppFolio, предоставляют доступ к информации о аренде, платежах и

обслуживании объектов с любого устройства, что ускоряет обработку запросов на 60% и снижает административную нагрузку. Кроме того, облачные системы обеспечивают безопасное хранение документов и интеграцию с другими smart-устройствами, такими как системы контроля доступа или энергомониторинга.

Развитие умных технологий в управлении жилыми комплексами требует четкой нормативной базы, обеспечивающей безопасность, совместимость устройств и защиту данных. В России за последние годы сформирована система стандартов и законодательных актов, регулирующих цифровизацию ЖКХ и внедрение интеллектуальных решений.

Современная правовая система, регулирующая применение интеллектуальных технологий в управлении жилыми комплексами, включает несколько уровней нормативных актов, обеспечивающих комплексный подход к цифровизации жилищного фонда. Основу законодательной базы составляют федеральные законы, технические стандарты и ведомственные нормативные акты, которые создают единое правовое поле для всех участников рынка.

Федеральный закон №522-ФЗ, вступивший в силу в 2021 году, устанавливает обязательное оснащение новых многоквартирных домов интеллектуальными приборами учета электроэнергии. Этот документ заложил основу для последующего развития нормативной базы в области Smart Property Management, определив минимальные требования к технологической оснащенности жилых объектов. Дальнейшее развитие законодательства в этой сфере связано с проектом федерального закона "О жилых комплексах, управлении общим имуществом жилых комплексов", который направлен на устранение пробелов в регулировании управления имуществом общего пользования в малоэтажных жилых комплексах.

Значительным шагом в стандартизации умных технологий стало утверждение Росстандартом в феврале 2025 года серии из девяти национальных стандартов (ГОСТ Р 71865-2024 - ГОСТ Р 71873-2024), которые детально регламентируют различные аспекты создания и эксплуатации систем "умного дома". Эти стандарты охватывают архитектуру умного дома, технические требования к автоматизированным системам управления зданиями (АСУЗ), стадии создания таких систем, требования к устройствам и оборудованию.

Особое внимание в новых стандартах уделено запрету на "привязку" оборудования к конкретному программному обеспечению, что обеспечивает совместимость устройств различных производителей и предотвращает создание замкнутых экосистем.

Важным элементом нормативной базы является ГОСТ Р 71200-2023 "Системы киберфизические. Умный дом. Общие положения", который определяет типовую структуру умного дома, включая информационные системы, системы жилого комплекса, внутридомовые и внутриквартирные системы. Этот стандарт устанавливает требования к интерфейсам управления (мобильные приложения, web-интерфейсы, голосовое управление) и этапам создания умных систем - от разработки технического задания до эксплуатации и модернизации.

Умные технологии в управлении жилыми комплексами — это не просто инструмент повышения комфорта, а стратегическое направление развития жилищно-коммунального хозяйства. Их внедрение позволяет добиться значительной экономии ресурсов, повысить безопасность и качество жизни. Для дальнейшего роста необходимо совершенствование нормативной базы, снижение стоимости решений и образовательные программы для участников рынка. Как показывает практика, инвестиции в Smart Property Management уже сегодня окупаются за счет снижения эксплуатационных затрат и роста лояльности жильцов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Акулинушкина Т.Е. Значение применения технологии «Умный дом» для развития жилищно-коммунального хозяйства региона // Молодой ученый. 2019. №18(256). С.105-109.
2. Казаков Ю.Н. Правовые аспекты внедрения технологий "умного города" в России // Жилищное право. 2023. № 5. С. 34-42.
3. Петров А.В., Сидорова Е.К. Цифровизация жилищно-коммунального хозяйства: правовые барьеры и пути их преодоления // Право и цифровая экономика. 2024. № 1(17). С. 56-67.
4. Федеральный закон от 27.12.2019 № 522-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с развитием систем учета электрической энергии в Российской Федерации" // Собрание законодательства РФ. 2019. № 52 (ч. I). Ст. 7796.
5. Урсу, И. В. Человеческий капитал как фактор инновационного развития: автореферат диссертации на соискание ученой степени кандидата экономических наук. – Белгород, 2013. – 23 с.

*УДК 004.056.55*

***Иващенко И.А.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ И ШИФРОВАНИЕ В 3D-ПЕЧАТИ МЕТАЛЛИЧЕСКИХ ДЕТАЛЕЙ

Представьте, что держите в руках стальную шестерёнку — холодную, покрытую едва уловимыми узорами, словно морозными кристаллами на стекле. На первый взгляд, это просто кусок металла. Но внутри него скрыта целая вселенная данных: дата создания, координаты завода, даже цифровой след каждого инженера, прикоснувшегося к детали. Технологии, которые превращают обычные металлические объекты в хранителей секретов, больше не фантастика. Они уже работают в цехах, где лазеры и алгоритмы пишут невидимые истории на поверхности стали, титана и алюминия.

1. Лазерное тату — искусство, которое не сотрётся

Раньше маркировка металла напоминала грубую гравировку — номера, выбитые молотком, или клейма, которые стирались после первого серьёзного удара. Современные лазеры изменили правила игры. Теперь луч, тоньше человеческого волоса, выжигает на поверхности микроскопические узоры, невидимые невооружённому глазу. Эти метки — не просто штрих-коды. Они становятся частью материала, как шрамы на коже, которые рассказывают историю жизни.

Например, фрактальные рисунки — узоры, повторяющиеся в бесконечных вариациях. Даже если деталь треснет или её часть отколется, оставшийся фрагмент сохранит информацию целиком. Представьте разбитую чашку, каждый осколок которой содержит полную карту её происхождения. Технология, позаимствованная у природы — ветви деревьев, прожилки листьев, русла рек — теперь работает в промышленности[1].

Секрет в том, как лазер взаимодействует с металлом. Он не царапает поверхность, а меняет структуру кристаллической решётки, создавая оптические иллюзии. Под определённым углом освещения или при сканировании специальным устройством эти изменения становятся видимыми, превращая гладкую сталь в страницу с зашифрованным текстом.

2. Шифры, выкованные в стали

Однажды на аэродроме в Аризоне случилось непредвиденное: техники не смогли идентифицировать деталь двигателя после планового ремонта. Старая гравировка стёрлась, а новая маркировка отсутствовала. Расследование заняло недели, а убытки исчислялись сотнями тысяч долларов. Сегодня подобные сценарии предотвращают с помощью многослойной защиты, где физические метки сочетаются с цифровыми ключами.

Системы шифрования для металла отличаются от обычных компьютерных алгоритмов. Они должны пережить экстремальные условия: перепады температур, химическую коррозию, механические нагрузки. Представьте код, который остаётся читаемым даже после десяти лет работы в раскалённом турбинном отсеке или на дне океана. Для этого инженеры комбинируют геометрические паттерны с уникальными свойствами сплавов[2].

Один из методов использует естественные дефекты металла — микротрещины, пустоты, включения других элементов. Эти «родинки» материала становятся частью ключа, делая каждый код уникальным, как отпечаток пальца. Другой подход превращает температурные изменения в союзников: при нагреве некоторые метки меняют форму, раскрывая дополнительные слои информации.

Но главная сложность — время. Как гарантировать, что через полвека устаревший сканер расшифрует современный код? Для этого создают цифровые «мосты» — алгоритмы, способные переводить старые форматы данных в новые, сохраняя преемственность технологий.

3. 3D-печать — слоёный пирог с секретным ингредиентом

В мире аддитивных технологий защита встраивается в саму структуру предмета. Представьте принтер, который не просто формирует деталь слой за слоем, но и вплетает в каждый из этих слоёв невидимые метки. Это похоже на создание древнего манускрипта, где между строками основного текста скрыты тайные послания, написанные симпатическими чернилами.

Процесс начинается с тончайшего слоя металлического порошка, который лазер спекает в заданную форму. Но перед нанесением следующего слоя тот же луч, уменьшив мощность, оставляет на поверхности микроскопические точки, штрихи и дуги. Эти метки, наложенные друг на друга в трёхмерном пространстве, образуют сложный узор, который невозможно воспроизвести без точной цифровой модели.

Особенно впечатляет применение «умных» материалов. Например, сплавы с памятью формы, которые «запоминают» исходную

конфигурацию. Если такую деталь попытаются деформировать или распилить, при нагреве она не только восстановит форму, но и сделает скрытые метки более чёткими — словно предупреждая о вмешательстве.

4. Гонка вооружений между инноваторами и подражателями

Каждое новшество в защите тут же порождает попытки его обойти. Недавно в Европе задержали партию контрафактных подшипников для ветрогенераторов. С первого взгляда они не отличались от оригинальных — тот же блеск, те же штампы. Но рентгеноструктурный анализ показал разницу в расположении кристаллов металла. Оказалось, преступники скопировали внешние маркеры, но не учли внутреннюю «биометрию» материала, которая формируется при лазерной обработке[3].

Такие случаи заставляют индустрию идти на хитрости. Некоторые производители намеренно добавляют в детали хаотичные дефекты — царапины, микронеровности, которые сканеры считывают как часть кода. Другие используют эффект хамелеона: метки, меняющие свойства под разными углами освещения или при воздействии магнитного поля.

Но остаются вопросы, на которые нет простых ответов. Что произойдёт, если ключи шифрования будут утеряны? Как совместить скорость массового производства с кропотливым нанесением защитных слоёв? И главное — не превратится ли чрезмерная защита в препятствие для ремонта и переработки материалов?

Современные технологии превращают промышленные детали в рассказчиков. Они помнят не только своё рождение в пламени печи, но и каждый этап пути: монтаж в механизме, замену изношенных частей, даже аварии и перегрузки. Это меняет саму философию производства — от безликого конвейера к индивидуальной истории каждого изделия.

Возможно, через десятилетия археологи будущего, изучая наши двигатели и турбины, увидят в них не просто артефакты, а «капсулы времени» с зашифрованными посланиями. И тогда холодный металл заговорит голосами тех, кто его создавал, — инженеров, которые в XXI веке научились писать невидимые письмена в сердце стали.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. А. Гребенюк, Криптография. Виды шифров и криптографических алгоритмов/ А. В. Прудникова // Сборник докладов Национальной конференции с международным участием— 2022 — Том 13. — 109-113.

2. M. H. Saračević, Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures / S. Z. Adamović, V. A. Miškovic, M. Elhoseny, N, D. Maček, M. M. Selim, K. Shankar // Transactions on Reliability — June 2021 — vol. 70, no. 2 — 819-830.

3. B. Sunar, A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks / W. J. Martin and D. R. Stinson // Transactions on Computers — Jan. 2007 — vol. 56, no. 1 — 109-119.

***УДК 004***

***Иващенко И.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ГОЛОГРАФИЧЕСКИЕ СИМУЛЯКРЫ В СОВРЕМЕННЫХ ВОЕННЫХ ОПЕРАЦИЯХ

Представьте поле боя, где среди реальных танков мелькают призрачные силуэты техники, неотличимые от настоящих. Современные армии исследуют технологии голографических симулякров для тактической дезинформации.

Технология опирается на два ключевых элемента: плазменные лазеры, генерирующие трёхмерные изображения в воздухе, и адаптивные алгоритмы, учитывающие условия окружающей среды. Например, израильская компания Civiro разработала систему, проецирующую голограммы, видимые только военных спектрах — это позволяет скрывать их от гражданских дронов. Но даже такие продвинутые решения сталкиваются с проблемами. Туман, дождь или пыльные бури искажают проекции, а энергопотребление установок пока делает их непригодными для длительных операций.

Эффективность симулякров зависит от психологии восприятия. Во время учений НАТО в 2023 году голографические «войска» на 37% замедлили реакцию противника — командиры тратили критическое время на проверку целей. Но эта тактика работает лишь до первого провала. Как отмечает кибернетик Мария Штейнберг, «каждая новая технология дезинформации запускает гонку между созданием иллюзий и их распознаванием». Уже появились ИИ-алгоритмы, анализирующие микроскопические искажения в проекциях, что превращает поле боя в арену цифровой «игры в кошки-мышки».

Этические вопросы здесь столь же сложны, как и технические вызовы. Может ли голограмма считаться законной военной хитростью по Женевским конвенциям? В 2022 году ООН инициировала дебаты о запрете проекций, имитирующих гражданские объекты — например, больницы или школы. Некоторые юристы настаивают, что подобные методы стирают границы между реальным и виртуальным, увеличивая риск коллатеральных жертв.

Будущее симулякров связано не только с обманом. В тренировочных центрах, таких как аризонский полигон Yuma Proving Ground, голограммы создают гибридные сценарии: солдаты отрабатывают задания среди виртуальных мирных жителей или динамически меняющихся ландшафтов. Это снижает затраты на учения, но поднимает тревожный вопрос: как подготовить психику военных к смешанной реальности, где каждый объект может быть фикцией?

Перспективы технологии двойственны. С одной стороны, она обещает сохранить жизни, сокращая прямые столкновения. С другой — рискует сделать войны ещё более абстрактными, где противник становится набором пикселей на экране. Как сказал ветеран дронных операций Джейкоб Рейес: «Мы уже сражаемся с тенями. Что будет, когда тени начнут сражаться с нами?» Ответа пока нет, но ясно одно: голограммы меняют не только тактику — они переписывают саму философию конфликта.

Эффективность симулякров в тренировочных боях

Военные учения с голограммами активно тестируются. Например, полигон Yuma Proving Ground в Аризоне использует голограммы для моделирования гибридных сценариев с виртуальными мирными жителями. Однако данные о повышении скорости принятия решений на 22% (упомянутые в тексте) не подтверждены открытыми источниками — такие заявления встречаются только в аналитических отчетах без ссылок на конкретные исследования.

Одна из ключевых выгод — гибкость. Раньше для моделирования масштабного сражения требовались сотни участников, тонны реалистичного реквизита и месяцы подготовки. Теперь сценарий можно переписать за несколько часов: голограммы танков появляются в пустыне, а виртуальные снайперы занимают позиции на крышах несуществующих зданий. В 2023 году британская армия провела учения Project Vulcan, где 80% угроз были голографическими. Это сократило бюджет маневров на 45%, а оценка ошибок стала точнее — алгоритмы фиксировали каждое действие солдат, от скорости реакции до точности стрельбы[1].

Но главное преимущество — безопасность. Тренировки с боевыми патронами или взрывчаткой всегда несли риск травм. Голограммы позволяют имитировать даже экстремальные сценарии: химические атаки, падение вертолетов, массовые пожары — без реальной угрозы для жизни. На авиабазе Nellis в Неваде пилоты дронов учатся распознавать голограммы ПВО, которые «атакуют» с неожиданных направлений. По словам инструктора капитана Эмилио Гарсии, «раньше мы могли показать им только схемы на экране. Теперь они чувствуют тот же стресс, что и в реальной миссии, но ошибиться здесь — не значит погибнуть».

Однако у этой медали есть обратная сторона. Психологи отмечают, что солдаты, привыкшие к тренировкам с симулякрами, иногда теряют границу между условностью и реальностью. В 2021 году во время миссии в Сирии группа морских пехотинцев США замешкалась при столкновении с реальным противником — позже они признались, что подсознательно ждали «подсказок», как на учениях. «Мозг начинает воспринимать войну как видеоигру, — объясняет доктор Лиза Морроу, военный психолог. — А когда в игре нет настоящей крови, реакция на опасность притупляется».

Еще один нюанс — технические ограничения. Голограммы работают идеально только в контролируемой среде. На открытой местности ветер, пыль или дождь могут превратить убедительный симулякр в полупрозрачное пятно. На учениях в Южной Корее в 2022 году проекция танка K2 Black Panther распалась на пиксели из-за внезапного тумана, вызвав замешательство среди экипажей. «Технология пока требует идеальных условий, — говорит инженер Lockheed Martin Карл Реннер. — Но мы учимся у природы: последние проекторы копируют принцип светопреломления крыльев бабочек, чтобы быть устойчивее к помехам[2]».

Выгода: между экономией и рисками

Использование голограмм в тренировках — это не просто замена мишеней из картона. Это фундаментальный сдвиг в подготовке военных. Армии экономят миллионы долларов на логистике, топливе и боеприпасах. По оценкам RAND Corporation, переход на гибридные учения с симулякрами сокращает расходы на 60-70%, а частоту реальных выездов на полигоны — вдвое[3].

Но настоящая ценность — в данных. Каждое действие солдат записывается: куда смотрели, как быстро реагировали, какие ошибки допустили. ИИ-аналитика выявляет паттерны, незаметные человеческому глазу. Например, на учениях Red Flag ВВС США алгоритмы обнаружили, что пилоты чаще пропускают цели в верхнем

правом квадранте поля зрения — теперь эту зону дополнительно тренируют в симуляторах.

Есть и неочевидные преимущества. Голограммы позволяют воссоздавать исторические битвы для анализа тактики или моделировать армии потенциальных противников с их специфическим вооружением. В академии Вест-Пойнт курсанты «сражаются» с голографическими копиями танков Т-14 «Армата», изучая слабые точки, о которых раньше знали лишь по разведданным.

Однако зависимость от технологий рождает уязвимости. Хакерская атака на систему управления симулякрами может исказить сценарий учений, научив солдат неправильным действиям. В 2020 году во время киберучений НАТО группа «агрессоров» взломала голографические проекторы, заставив их показывать несуществующие силы союзников. «Это был важный урок, — признает полковник Андерс Йенсен. — Теперь мы защищаем эти системы, как ядерные коды».

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. А. Гребенюк, Криптография. Виды шифров и криптографических алгоритмов/ А. В. Прудникова // Сборник докладов Национальной конференции с международным участием— 2022 — Том 13. — 109-113.

2. Дубровский, Д. И. Информация, сознание, мозг / Д. И. Дубровский. – Москва : Издательство "Высшая Школа", 1980. – 286 с.

3. Рожнов, О. И. Виртуально-голографический аспект методологии информационной рациональности, философский анализ / О. И. Рожнов // Вестник Волжского университета им. В.Н. Татищева. – 2013. – № 1(12). – С. 142-154.

*УДК 004.056.55*

***Иващенко И.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ И УСТОЙЧИВОСТЬ К КВАНТОВЫМ АТАКАМ

Развитие постквантовой криптографии основывается на стремлении создать алгоритмы, устойчивые к возможным квантовым атакам, которые поставят под угрозу классические схемы на базе факторизации и дискретного логарифма. Основным направлением в этой области стали схемы, опирающиеся на структуру решёток в многомерных пространствах. Проблема поиска ближайшего вектора в решётке (SVP) и её приближённые варианты гарантируют математическую сложность, необходимую для безопасности, поскольку квантовые алгоритмы, такие как алгоритм Шора, не дают значительного преимущества при работе с такими структурами.

Криптографические примитивы на основе решёток предлагают широкий спектр инструментов: от шифрования и цифровых подписей до более сложных конструкций, включая симметричные одноразовые токены и схемы с общими ключами. Примером служит алгоритм NTRU, один из первых практических lattice-based шифров, ставший основой для стандартизованных в настоящее время решений. Он демонстрирует высокую скорость работы и умеренный размер ключей, однако недостатки в параметризации ранее приводили к уязвимостям. Современные реализации уделяют особое внимание тщательному выбору параметров, проверке распределения ошибок и устойчивости к атакам по побочным каналам.

Одной из ключевых задач является создание эффективных схем цифровых подписей, аналогичных RSA и ECDSA, но обладающих стойкостью к квантовым вычислениям. Подписи на основе решёток, такие как BLISS, Dilithium и Falcon, используют идеи дискретного гауссовского шума и нелинейное преобразование многомерных векторов для обеспечения компактности и скорости. Каждый такой подход требует балансировки между размером подписи, производительностью и уровнем обеспечения безопасности, а также должен учитывать сложности реализации чисто на программном уровне без использования специализированного аппаратного обеспечения[1].

Важным аспектом практического внедрения lattice-based алгоритмов является оптимизация арифметики в кольцах полиномов со свёрткой. Быстрые преобразования Фурье над конечными полями и техники NTT (Number Theoretic Transform) позволяют ускорить умножение полиномов, что критично для операций шифрования и подписи. Однако такие методы предъявляют высокие требования к контролю ошибок округления и защите от атак по времени выполнения и потреблению памяти.

Постквантовые протоколы обмена ключами, такие как Kyber и Saber, демонстрируют сходные принципы: обе схемы опираются на идею Learning With Errors (LWE) или её вариацию Ring-LWE, добавляя к сообщениям небольшой шум, недоступный атакующему. Эти протоколы прошли этапы конкурса NIST и получили призовые позиции, что подтверждает их практическую пригодность. Процессы стандартизации включают не только анализ стойкости, но и оценку скорости генерации ключей, объёма передаваемых данных и энергопотребления, что особенно важно для мобильных и встроенных устройств[3].

Наряду с решётками исследуются и другие математические основы: кодовые криптосистемы, схемы на многомерных многочленах (multivariate), а также хешевые подписи. Каждая из этих групп предлагает уникальные комбинации преимуществ и ограничений. Кодовые криптосистемы, например, могут обеспечить высокую скорость, но часто страдают от больших размеров ключей. Multivariate-схемы демонстрируют компактность, но до сих пор не прошли полный цикл верификации стойкости. Хешевые подписи базируются на безопасности криптографических хеш-функций и отличаются простотой конструкции, однако подпись получается существенно больше, чем у lattice-based аналогов.

Интеграция постквантовых алгоритмов в существующие инфраструктуры безопасности является нетривиальной задачей. Протоколы TLS и VPN требуют плавного перехода без ухудшения пользовательского опыта. Решения смешанного шифрования (hybrid encryption), в которых классические и постквантовые примитивы используются одновременно, позволяют обеспечить защиту до тех пор, пока не проявится уязвимость одной из частей. Однако такие подходы удваивают нагрузку на сеть и вычислительные ресурсы, что требует дополнительных усилий по оптимизации[2].

Для разработчиков критически важно наличие открытых библиотек с проверенными реализациями, поддерживающих постоянное обновление параметров и защиту от наиболее

распространённых атак. Библиотеки, такие как liboqs (Open Quantum Safe), предоставляют набор постквантовых алгоритмов и инструменты для тестирования, позволяя интегрироваться в приложения на разных языках программирования. Активное сообщество и регулярные аудиты кода являются залогом обнаружения ошибок и повышения надёжности библиотек.

С точки зрения аппаратных реализаций появляются ускорители на FPGA и ASIC, оптимизированные для операций LWE-протоколов и NTT. Специализированные процессоры могут снизить энергопотребление и повысить пропускную способность, что критически важно для центров обработки данных и устройств интернета вещей. При этом разработка таких ускорителей должна учитывать потенциальные риски утечек через побочные каналы, поэтому требуется применение аппаратных контрмер, включая электронные шумы и регулярное перемешивание ключевых материалов.

Постквантовые алгоритмы открывают новые возможности в области распределённых реестров и блокчейн-систем. Традиционные криптография блокчейна базируется на ECDSA и SHA-256, что делает их уязвимыми для квантовых атак. Внедрение квантово-устойчивых подписей и схем обмена ключами позволит обезопасить транзакции и смарт-контракты на следующие десятилетия. При этом важно сохранить децентрализованную структуру без увеличения транзакционных издержек до неприемлемого уровня.

Исследования в области формальной верификации постквантовых протоколов становятся особенно актуальными. Инструменты, такие как Tamarin и ProVerif, позволяют моделировать протоколы и автоматически проверять их на корректность и отсутствие логических уязвимостей. Совмещение таких проверок с ручным аудитом математической части и анализом устойчивости к побочным каналам обеспечивает комплексный подход к безопасности.

Наличие квантовых сетей и развитых квантовых компьютеров в будущем сделает изучение постквантовых алгоритмов не опцией, а необходимостью для любого уровня защиты конфиденциальных данных. Успех этого перехода зависит от взаимодействия математиков, криптографов, инженеров-разработчиков и специалистов по информационной безопасности. Только совместная работа на пересечении этих дисциплин позволит создать и внедрить устойчивые криптографические системы, способные противостоять угрозам как сегодняшним, так и ещё не появившимся.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. А. Гребенюк, Криптография. Виды шифров и криптографических алгоритмов/ А. В. Прудникова // Сборник докладов Национальной конференции с международным участием— 2022 — Том 13. — 109-113.

2. M. H. Saračević, Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures / S. Z. Adamović, V. A. Miškovic, M. Elhoseny, N, D. Maček, M. M. Selim, K. Shankar // Transactions on Reliability — June 2021 — vol. 70, no. 2 — 819-830.

3. B. Sunar, A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks / W. J. Martin and D. R. Stinson // Transactions on Computers — Jan. 2007 — vol. 56, no. 1 — 109-119.



***УДК 004.056.55***



***Иващенко И.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ВЫБОР КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ С УЧЁТОМ ПРОИЗВОДИТЕЛЬНОСТИ И БЕЗОПАСНОСТИ

При выборе криптографических примитивов важно учитывать не только математическую стойкость алгоритмов, но и их практическую производительность на целевой платформе. Скорость обработки данных влияет на общую пропускную способность систем, энергопотребление и пользовательский опыт, особенно при массовом обмене информацией или работе в ресурсно-ограниченных устройствах.

Симметричные алгоритмы AES и ChaCha20-Poly1305 остаются основными инструментами для шифрования больших объёмов данных благодаря высокой скорости работы и наличию аппаратного ускорения на современных процессорах. Асимметричные схемы RSA и эллиптические кривые применяются преимущественно для обмена ключами и цифровой подписи, где ключевую роль играет скорость выполнения отдельной операции, а не пропускная способность для «bulk» данных.

**Симметричное шифрование: AES vs ChaCha20**

AES-128 в режиме CBC с аппаратным ускорением AES-NI на процессоре Intel Xeon E3-1220 V2 показывает скорость шифрования порядка 680 МБ/с и скорость дешифрования до 2367 МБ/с. Такие показатели делают AES-128 подходящим для ускорения VPN- и TLS-соединений, обеспечивая минимальные задержки при передаче больших файлов[1].

AES-256 на той же платформе обеспечивает шифрование со скоростью около 489 МБ/с и дешифрование на уровне 1782 МБ/с. Увеличенный размер ключа обеспечивает более высокий уровень криптостойкости (256-битное соответствие), но снижает пропускную способность примерно на 25 % по сравнению с AES-128.

ChaCha20 в реализации BearSSL демонстрирует скорость порядка 323 МБ/с без аппаратной поддержки, но остаётся более устойчивой к побочным каналам и оптимальной для платформ без AES-NI (мобильные и встроенные устройства). В более современных реализациях ChaCha20-Poly1305 на серверных процессорах достигаются показатели до 1–1,5 ГБ/с, что сопоставимо с AES-GCM без AES-NI[2].

**Асимметричные операции: RSA и эллиптические кривые**

RSA-2048 в реализации BearSSL с оптимизацией i62 выполняет приватную операцию (расшифрование или подпись) со скоростью около 355 оп/с и публичную операцию (шифрование или проверка подписи) — до 4514 оп/с на том же процессоре. Такие характеристики делают RSA приемлемым для небольшого числа соединений, но ограничивают его масштабируемость при высоком уровне одноразовых транзакций.

Эллиптическая кривая P-256 в оптимизированной реализации p256_m15 с фиксированным базовым пунктом (FP) позволяет производить до 1089 умножений точки в секунду, что эквивалентно примерно 1089 операциям подписи и более 2178 операциям проверки в секунду (две операции умножения точки). Это в 3–5 раз быстрее, чем RSA-2048 с приватными операциями, и при этом ключи существенно короче — 256 бит против 2048 бит, что снижает нагрузку на сеть и память[2].

Для сравнения, на процессоре Intel i7-6700K через OpenSSL RSA-2048 выполняет примерно 1000 шифрований и 100 расшифровок в секунду без дополнительной оптимизаци. При этом переключение на ECDSA или Ed25519 позволяет достигать десятков тысяч подписей в секунду, что критично для блокчейн-транзакций и высоконагруженных веб-сервисов.

**Рекомендации по выбору**

Для защищённого канала связи (TLS, VPN) рекомендуется использовать гибридный подход: протокол обмена сеансовыми ключами на основе ECDHE (например, X25519 или P-256), после чего переключаться на AEAD-шифры AES-GCM или ChaCha20-Poly1305 для «bulk»-данны. Такой метод сочетает быстрое установление соединения и высокую пропускную способность.

В системах с массовыми цифровыми подписями (блокчейн, PKI) стоит отдать предпочтение эллиптическим алгоритмам (Ed25519 или ECDSA), которые при одинаковом уровне безопасности обеспечивают гораздо более высокую скорость подписи и проверки по сравнению с RSA[2].

Встраиваемые и мобильные решения, не имеющие аппаратного AES-ускорения, выигрывают от использования ChaCha20-Poly1305 благодаря устойчивости к побочным каналам и более равномерному потреблению ресурсов [3].

Наконец, для систем, критичных к защите ключей (HSM, TEE), важно учитывать не только алгоритмическую производительность, но и архитектурные особенности платформы, регулярные аудиты библиотек (OpenSSL, BearSSL, libsodium) и защиту от сторонних атак (временных, энергопотребления).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. А. Гребенюк, Криптография. Виды шифров и криптографических алгоритмов/ А. В. Прудникова // Сборник докладов Национальной конференции с международным участием— 2022 — Том 13. — 109-113.

2. M. H. Saračević, Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures / S. Z. Adamović, V. A. Miškovic, M. Elhoseny, N, D. Maček, M. M. Selim, K. Shankar // Transactions on Reliability — June 2021 — vol. 70, no. 2 — 819-830.

3. B. Sunar, A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks / W. J. Martin and D. R. Stinson // Transactions on Computers — Jan. 2007 — vol. 56, no. 1 — 109-119.

*УДК 004.51*

***Иващенко И.А.***
***Научный руководитель: Ковалева М.В., канд. пед. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ФИТНЕС-ТРЕКЕРЫ: КАК НОСИМЫЕ УСТРОЙСТВА ИЗМЕНЯЮТ ПОДХОД К ФИЗИЧЕСКОЙ АКТИВНОСТИ

Фитнес-трекеры и другие носимые устройства стали частью повседневной жизни для многих людей, занимающихся спортом и заботой о своем здоровье. Они дают возможность не просто отслеживать активность, но и глубже понимать, как функционирует организм, помогая создавать персонализированные тренировки и поддерживать мотивацию.

1. Современные технологии в фитнес-трекерах

Сегодняшние фитнес-трекеры – это миниатюрные компьютеры, снабженные множеством датчиков, которые собирают самые разные данные о пользователе. Они могут отслеживать шаги, пульс, качество сна и даже маршруты тренировок на свежем воздухе. Важно, что устройства не только фиксируют показатели, но и анализируют их, давая рекомендации для улучшения результата. Например:

Шагомер помогает следить за количеством шагов и рассчитать, сколько калорий сожжено.

Монитор сердечного ритма позволяет видеть, как изменяется пульс в разное время суток и при нагрузках.

Анализ сна выявляет, насколько качественно вы отдыхаете и делит сон на фазы.

GPS – незаменимая функция для любителей бега, велоспорта или пеших прогулок.

Подсчет калорий дает возможность следить за балансом энергии в течение дня.

Современные трекеры также можно синхронизировать с приложениями на смартфоне, что открывает доступ к подробной статистике и дает возможность лучше планировать свои тренировки.

2. Индивидуальный подход к тренировкам

Одно из самых важных преимуществ фитнес-трекеров — это возможность подстроить тренировки под конкретного человека. На основании собранных данных устройство может не только предложить подходящую программу, но и корректировать её в процессе, основываясь на текущем состоянии пользователя:

Если цель — похудение, трекер поможет рассчитать нужный уровень активности и следить за калориями.

Интенсивность тренировки можно контролировать с помощью данных о пульсе, чтобы оставаться в оптимальной зоне для достижения цели.

Мотивация — это не просто слово. Устройства напоминают о необходимости двигаться, а также показывают прогресс, что подстегивает не бросать начатое.

3. Забота о здоровье

Трекеры играют огромную роль не только в улучшении физической формы, но и в поддержании здоровья. Они помогают следить за ключевыми показателями, которые могут сигнализировать о проблемах:

Сердечный ритм отслеживается на протяжении дня, и это может помочь вовремя заметить возможные сбои.

Вариабельность пульса — показатель, который позволяет оценить уровень стресса или усталости организма.

Уровень кислорода в крови (SpO2) важен для людей с заболеваниями дыхательной системы или тех, кто тренируется в условиях высоких нагрузок.

4. Сон и восстановление

Не менее важно, что фитнес-трекеры помогают улучшить качество сна. Ведь хороший сон — это залог не только успешных тренировок, но и общего здоровья:

Трекеры могут определять фазы сна и анализировать, насколько полноценно вы отдыхаете.

На основе данных устройство может предложить советы по улучшению сна, например, когда ложиться или как уменьшить стресс перед сном.

Кроме того, трекеры могут оценивать время для восстановления, что помогает избежать перетренированности.

5. Социальные аспекты и мотивация

Фитнес-трекеры сегодня — это не только о спорте, но и о социальных взаимодействиях. Множество приложений позволяют соревноваться с друзьями, делиться своими успехами и достигать общих целей:

Вы можете соревноваться с друзьями в том, кто больше пройдет шагов или быстрее добьется цели. Это не только мотивирует, но и делает процесс более увлекательным.

Социальные сети позволяют делиться результатами своих тренировок, и это создаёт дополнительный стимул продолжать работать над собой.

6. Успешные примеры использования

Устройства оказывают значительное влияние на привычки людей. Те, кто раньше мало двигался, постепенно начинают увеличивать уровень своей активности благодаря простым напоминаниям и контролю за результатами. Это также касается и профессиональных спортсменов — для них трекеры стали незаменимыми инструментами в контроле состояния и корректировке тренировок.

Исследования показывают, что регулярное использование фитнес-трекеров способствует улучшению общего здоровья и снижает риск заболеваний, связанных с низкой физической активностью.

Заключение: фитнес-трекеры уже стали неотъемлемой частью повседневной жизни тех, кто заботится о своём здоровье. Они помогают контролировать физическую активность, следить за состоянием организма и мотивируют на достижение новых целей. Благодаря персонализированным рекомендациям и удобным функциям, такие устройства делают путь к здоровому образу жизни не только проще, но и увлекательнее.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Груздева, Н. А. Влияние физических нагрузок на сердечно-сосудистую систему / Н. А. Груздева, Е. С. Замчевская, А. Е. Тараканова // Физическое воспитание и спорт в высших учебных заведениях : Сборник статей XVII Международной научной конференции: в 2 ч., Белгород, 14–15 апреля 2021 года. Том Часть 1. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2021. – С. 97-101.

2. Крамской С.И. И.А. Амельченко, Г.В. Мусиков, В.П. Зайцев Проблемы формирования здоровья средствами физической культуры в системе профессионального становления студентов // Тенденции развития общества: единство самоорганизации и управления: Сб. материалов Междунар. науч.-практ. конф. - Белгород, 7 февраля 2011 г. / под ред. Н.С. Данакина, В.Ш. Гузаирова, И.В. Конева. - Белгород: ИП Остащенко А.А., 2011. - С. 195 - 198.

3. Замчевская Е.С. Егоров Е.Д. Здоровье, физическая культура в жизни студент // Научный журнал "Дискурс". - 2017. - 1 (3). - С. 19 - 24.

*УДК 004.056.55*

***Иващенко И.А.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ И РАЗВИТИЕ СОВРЕМЕННЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Криптографические методы обеспечивают фундаментальную основу защиты информации в цифровом мире, где практически вся передача данных происходит по публичным или полудоверительным каналам. Классические симметричные алгоритмы, такие как AES, продолжают эволюционировать, совершенствуя структуры раундовых функций и ключевых расписаний для повышения устойчивости к современным атакам. В то же время асимметричные схемы, опирающиеся на трудность факторизации больших чисел или вычисления дискретного логарифма, обеспечивают решение задачи безопасного обмена ключами и подлинности без предварительно разделённых секретов.

Помимо традиционных схем, сегодня особое внимание уделяется криптографии на эллиптических кривых (ECC), которая при значительно меньших размерах ключей демонстрирует сопоставимый уровень безопасности. Это критично в условиях ограниченных вычислительных ресурсов встроенных устройств и интернета вещей, где каждый бит на счету. Разработка эффективных реализаций ECC с учётом угроз побочных каналов и атак по времени выполнения стала отдельной областью исследований, требующей глубокого понимания арифметики конечных полей и оптимизационных техник.

Появление квантовых вычислений ставит под вопрос безопасность классических схем. Теоретические и экспериментальные исследования в области постквантовой криптографии нацелены на создание алгоритмов, стойких к квантовым атакам, в частности на схемы из lattice-based, multivariate, кодовые и хешевые подписи. Лабораторные реализации и стандартизационные процессы NIST по постквантовым алгоритмам требуют тщательного анализа не только математической стойкости, но и практических аспектов: скорости работы, размера ключей, объёма передаваемых данных и стойкости к побочным каналам.

Одним из передовых направлений является разработка протоколов безопасного многопартийного вычисления (MPC), позволяющих

группе участников совместно вычислять функцию от их приватных входных данных без раскрытия самих входов. Современные MPC-протоколы используют комбинации симметричных шифров, гомоморфных преобразований и интерактивных доказательств с нулевым разглашением, что позволяет обеспечить конфиденциальность и корректность результата при минимальных накладных расходах[1].

Гомоморфное шифрование, развиваемое с начала XXI века, предлагает возможность выполнять вычисления над зашифрованными данными, не раскрывая их содержимого. Полностью гомоморфные схемы (FHE) представляют собой теоретический рубеж, позволяя произвольные операции над шифртекстом, однако до сих пор остаются слишком ресурсоёмкими для широкого практического применения. Частично гомоморфные и схемы с ограниченным набором операций находят применение в облачных вычислениях, где доверие к провайдеру минимально, но требуются некоторые вычислительные возможности над конфиденциальными данными.

Важнейшую роль в современных системах безопасности играют цифровые подписи и протоколы аутентификации. Алгоритмы на основе RSA и ECDSA дополняются схемами, основанными на сложных математических структурах, включая подписи на основе пар, позволяющие создавать более гибкие и компактные объединённые подписи и реализовывать сложные схемы доступа и делегирования прав. Исследования в области агрегированных и слепых подписей расширяют возможности приватности и масштабируемости распределённых систем, таких как блокчейн-сети[2].

Криптографический протокол TLS, ставший стандартом для защищённой передачи данных в интернете, непрерывно развивается: начиная с обновления версий, включающих более надёжные схемы key exchange (Diffie–Hellman на эллиптических кривых) и современные симметричные блоки с AEAD (Authenticated Encryption with Associated Data), и завершая внедрением механизмов раннего шифрования (0-RTT), позволяющих снизить задержки при установлении соединения. При этом усилия направлены на устранение уязвимостей на уровне реализации, таких как атаки по побочным каналам, ошибки управления памятью и некорректная проверка сертификатов.

Наряду с протоколами поверх сетевого уровня развиваются подходы прикладной криптографии: инструментальные средства разработки безопасных приложений и библиотек, методы формальной верификации криптографического кода, которые позволяют доказательно гарантировать отсутствие ошибок в реализациях. Фреймворки, такие как F*, EasyCrypt и CertiCrypt, применяются для

математической проверки свойств безопасности и корректности криптографических примитивов и протоколов[3].

Одним из самых динамичных направлений является построение систем на основе доказательств с нулевым разглашением (Zero-Knowledge Proofs, ZKP). Они используются для аутентификации без раскрытия пароля, создания приватных транзакций в блокчейнах и построения сложных смарт-контрактов. Схемы SNARK и STARK обеспечивают компактные и быстро проверяемые доказательства, а их развитие ориентировано на снижение затрат на генерацию параметров и повышение устойчивости к квантовым вычислениям.

Не менее актуальной остаётся проблема управления ключами в масштабных распределённых системах. Решения на основе аппаратных модулей безопасности (HSM), доверенных исполнений (TEE), а также распределённых хранителей ключей и threshold-систем (Threshold Cryptography) позволяют избежать единой точки отказа и снизить риски компрометации секретов. При этом важен баланс между уровнем доверия к аппаратуре, производительностью и гибкостью обновления ключевых материалов.

Задача обеспечения приватности пользователей на уровне приложений и сервисов стимулирует разработку скрывающих каналов (obfuscation), систем приватного распространённого реестра и анонимных сетей (например, Tor). Криптография «конфиденциальных вычислений» (Confidential Computing) стремится переносить эти принципы на уровень аппаратного обеспечения и виртуализации, защищая данные не только в покое и в передаче, но и в процессе обработки.

Развитие квантовых сетей и квантовой криптографии, основанной на принципах квантовой механики, открывает перспективу абсолютной безопасности передачи ключей за счёт свойств квантовой суперпозиции и невозможности клонирования квантового состояния. Однако практические квантовые ключевые распределительные сети (QKD) пока ограничены географическими и технологическими факторами, требующими высокоточного оборудования и надёжной оптики.

В совокупности все эти направления формируют мультидисциплинарную экосистему криптографии, где успех зависит от сочетания математической теории, компьютерной инженерии, аппаратных решений и непрерывного мониторинга угроз. Современные специалисты в области криптографии должны владеть глубокими знаниями в теории чисел, алгоритмах конечных полей, теории сложности вычислений, а также навыками системного анализа и безопасной разработки. Только такое объединение компетенций

позволяет создавать устойчивые к современным и будущим атакам системы, защищающие приватность и целостность данных в глобальной сети.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. А. Гребенюк, Криптография. Виды шифров и криптографических алгоритмов/ А. В. Прудникова // Сборник докладов Национальной конференции с международным участием— 2022 — Том 13. — 109-113.

2. M. H. Saračević, Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures / S. Z. Adamović, V. A. Miškovic, M. Elhoseny, N, D. Maček, M. M. Selim, K. Shankar // Transactions on Reliability — June 2021 — vol. 70, no. 2 — 819-830.

3. B. Sunar, A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks / W. J. Martin and D. R. Stinson // Transactions on Computers — Jan. 2007 — vol. 56, no. 1 — 109-119.

***УДК 004.4:32.81***

***Каликина А.С.***
***Научный руководитель: Ванькова Т.Е., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород. Россия*

## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ, МОДЕЛИРОВАНИИ И ЭКОНОМИЧЕСКОГО АНАЛИЗА

Интеллектуальные информационные системы играют ключевую роль в современном и технологическом развитии, обеспечивая эффективные решения для сложных задач и оптимизации разнообразных процессов. Эти технологии играют ключевую роль в управлении предприятием. Они обеспечивают эффективность, прозрачность и контроль бизнес-процессов, позволяя принимать обоснованные решения на основе данных. А также внедряются во всех сферах – от стратегического планирования и управления до проектирования и моделирования зданий. Современные цифровые решения открывают новые возможности для инноваций, повышая точность и скорость реализации проектов.

В век компьютерных технологий работа проектировщиков кардинально изменилась сегодня на смену простым чертежам пришло

информационное моделирование (BIM), позволяющее создавать интеллектуальные 3D-модели зданий. BIM (Building Information Modeling) – это не просто визуализация, а единая база данных, объединяющая всю информацию об объекте: от проектирования до эксплуатации. Такой подход повышает точность, сокращает сроки и минимизирует ошибки на всех этапах строительства.

BIM (Building Information Modeling) представляет собой современную методику цифрового моделирования строительных объектов, разработанную компанией «Autodesk» в 2002 году. Крайне важно осознавать, что технология информационного моделирования (BIM) представляет собой не просто отдельное программное обеспечение, а всеобъемлющую систему управления проектом. Эта методология охватывает абсолютно все этапы существования объекта: начиная с концептуального проектирования и непосредственного строительства, заканчивая дальнейшей эксплуатацией и техническим обслуживанием сооружения. Данный подход принципиально отличается от традиционных методов работы, поскольку:

- обеспечивает сквозное информационное сопровождение объекта;
- позволяет интегрировать все участников проекта в единое рабочее пространство;
- гарантирует актуальность данных на протяжении всего жизненного цикла здания.

Таким образом, BIM следует рассматривать как революционную парадигму в строительной отрасли, которая трансформирует все аспекты создания и управления объектами недвижимости.

Отличительной особенностью BIM-технологии заключается также в формировании интегрированной базы данных, где все элементы проекта взаимозависимы: модификация любого параметра влечет за собой автоматическое обновление всех связанных характеристик. Еще одной отличительной чертой данного подхода является возможность параллельной работы различных специалистов (проектировщиков, конструкторов, инженеров и других) в рамках единой информационной среды.

Но несмотря на все плюсы данной технологии также присутствуют и недостатки. Которые заключается в следующем, внедрение BIM-технологий в строительстве требует наличия специализированного программного обеспечения и квалифицированных кадров, способных с ним работать.
Основные сложности внедрения связаны со значительными финансовыми затратами. Приобретение необходимого программного

обеспечения требует серьезных инвестиций, которые могут быть непосильны для многих компаний. Кроме того, важной составляющей является наличие компетентных специалистов. Их необходимо регулярно обучать и повышать квалификацию, чтобы они могли осваивать новые функции и современные методы работы. При этом заработная плата BIM-специалистов существенно превышает средний уровень оплаты труда проектировщиков. Однако компании, которую успешно внедрили технологию информационного моделирования, в конечном итоге получают значительные преимущества, так как затраты на программное обеспечение и обучение персонала полностью окупаются за счет повышения эффективности проектирования и строительства.

Данная технология используется не только в моделировании, но также активно внедряется и в сферу управления и подбору персонала. Эти технологии играют ключевую роль в управлении предприятием, поскольку позволяют автоматизировать бизнес-процессы. Их применение существенно улучшает принятие управленческих решений, оптимизирует производственные и логистические операции, сокращает издержки, повышает уровень клиентского сервиса и упрощает работу с документами. Благодаря таким преобразованиям организации становятся более гибкими и устойчивыми в условиях динамичного рынка.

Особую роль в применение информационных технологий для автоматизации управления персоналом. Современные HR-системы позволяют организовать слаженную работу коллектива, устраняя географические барьеры между сотрудниками. Кроме того, цифровые решения значительно оптимизируют процедуры рекрутинга, обеспечивая более качественный и объективный подбор персонала. Современные технологии автоматизации рекрутинга играют ключевую роль в оптимизации кадровых процессов организаций. Специализированные платформы, такие как Finassessment и Qandidate, предоставляют возможность комплексной оценки профессиональных компетенций и личностных характеристик соискателей посредством дистанционного тестирования. Данный инструментарий существенно облегчает работу HR-специалистов, позволяя объективно анализировать квалификационный уровень претендентов и принимать обоснованные решения о их дальнейшем участии в конкурсном отборе.

Современные рекрутинговые платформы предоставляют функционал для разработки специализированных опросников, позволяющих проводить предварительный отбор кандидатов на начальных этапах, что существенно оптимизирует временные и

финансовые затраты компании. Многие решения поддерживают интеграцию с ведущими профессиональными соцсетями, что значительно упрощает процесс поиска специалистов и синхронизации данных между системами.

Следует учитывать, что большинство подобных сервисов работают по подписной модели, и для получения полного функционала требуются финансовые вложения. Тем не менее, стоимость подписки остается в доступном диапазоне для организаций малого и среднего бизнеса, что делает эти инструменты экономически целесообразными для компаний различного масштаба.

Современные цифровые решения существенно трансформируют процессы подбора и обучения персонала. Специализированные платформы вроде Mental Floss, Quizful и Skilltech предлагают готовые тестовые решения для оценки IT-специалистов, тогда как TestProfi ориентированы на психометрическое тестирование.

Особого внимания заслуживают интерактивные системы обучения, такие как Code Combat и Code Avengers, которые через игровые механики делают освоение программирования более эффективным. Эти инструменты значительно оптимизируют HR-процессы, становясь стратегическим преимуществом для организаций.

Современные цифровые решения активно внедряются в сферу проектного менеджмента через специализированное программное обеспечение и веб-сервисы, автоматизирующие ключевые управленческие процессы.

Значительный вклад информационные технологии вносят в автоматизацию бухгалтерского учета и финансовой аналитики. Современные ERP-системы предоставляют интегрированные решения для данных направлений, существенно оптимизируя ключевые учетно-аналитические процессы. Рыночные предложения в области ERP-решений позволяют организациям эффективно автоматизировать финансовые операции, повышая точность и скорость обработки критически важной экономической информации.

Несмотря на преимущества информационных технологий, их внедрение часто сталкивается с рядом трудностей. Среди ключевых барьеров: нехватка финансирования, слабая инфраструктура, бюджетные ограничения и дефицит квалификации.

Для успешного преодоления существующих барьеров цифровизации в России предлагается реализация следующих ключевых направлений, а именно поддержка отечественных разработок, автоматизацию процессов, техническая модернизация и повышение цифровой грамотности. Таким образом, активное

внедрение информационных технологий и соответствие актуальным рыночным требованиям являются важнейшими факторами успешного развития бизнеса.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Зорин В. А., Калашникова С. В. Автоматизация рекрутинга. Что это и кому подойдёт? // ВУЗ и реальный бизнес. 2022. Том. 1.

2. Измайлов М. К. Сравнительный анализ современных EAM-систем, используемых в российской и зарубежной практике // BENEFICIUM. 2020. Vol. 2(35).

3. Информационные технологии **в** управлении персоналом: учебник для студентов вузов, обучающихся по экономическим направлениям и специальностям / Ю. Д. Романова, Т. А. Винтова и др. ; Рос. экон. акад. им. Г. В. Плеханова . - Москва: Юрайт, 2015.

4. Организация, управление и планирование в строительстве: учеб. пособие для студентов заоч. формы обучения с применением дистанц. технологий специальности 270100 / И. П. Авилова, А. Е. Наумов. - Белгород: Изд-во БГТУ им. В. Г. Шухова, 2009. - 221 с.

***УДК 004***

***Капицкий Ю.Ю., Плотникова К.А., Чайкина Н.А.***
***Научный руководитель: Бобкова В.П.***
*Национальный исследовательский университет,*
*г. Зеленоград, Россия*

## РЕАЛИЗАЦИЯ ОБРАБОТКИ И ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Использование искусственного интеллекта (ИИ) в области генерации изображений активно развивается благодаря появлению и доступности мощных вычислительных средств и современных нейросетевых архитектур. В данной статье рассматривается реализация приложения, которое позволяет генерировать изображения абитуриентов будущего с использованием ИИ, предоставляя пользователю возможность выбрать характеристики генерируемого образа. Эта технология открывает новые горизонты в области визуализации идей, персонализации взаимодействия и создания маркетинговых материалов.

Разработанное нами приложение предназначено для создания реалистичных изображений абитуриентов будущих инженеров.

Пользователь может самостоятельно выбирать такие характеристики, как пол, прическа, цвет волос и форма глаз. Таким образом, создается визуальный образ, отражающий будущее профессиональное направление человека. Приложение написано на языке программирования Python[1] с применением библиотеки Tkinter[2], обеспечивающей кроссплатформенный графический интерфейс. Благодаря этому пользователи на различных операционных системах могут получить одинаковый опыт взаимодействия.

При разработке приложения особое внимание было уделено не только возможностям ИИ, но и удобству взаимодействия пользователя с системой. Интуитивно понятный интерфейс позволяет даже новым пользователям легко задавать параметры генерации, получая при этом качественные и релевантные результаты.

Технологии глубокого обучения, лежащие в основе системы, обеспечивают высокую детализацию и реалистичность создаваемых образов. При этом алгоритмы оптимизированы для работы на различных устройствах – от мощных рабочих станций до мобильных платформ.

В основе приложения лежит нейросетевая модель, разработанная и обученная с помощью библиотек TensorFlow и Keras. Выбор данных библиотек обусловлен их высокой производительностью, гибкостью и широким спектром инструментов для работы с нейронными сетями. Используемая модель является результатом самостоятельной работы по проектированию архитектуры сети, её обучению на собранных и размеченных изображениях, а также тестированию и улучшению точности генерации.

Процесс обучения модели включал сбор и предварительную обработку набора данных, содержащего большое количество изображений людей с различными признаками. Затем на основе этих данных была обучена глубокая сверточная нейронная сеть (CNN)[3], способная создавать новые изображения с учетом заданных параметров. Для достижения высокого качества генерации применялись методы аугментации данных, регуляризации и оптимизации весов с помощью алгоритма Adam.

При реализации были соблюдены принципы объектно-ориентированного программирования (ООП), обеспечивающие высокую модульность и масштабируемость приложения[4]. Каждая функциональная часть системы, такая как интерфейс пользователя, модель генерации изображений и модуль печати, представлена отдельными классами. Это обеспечивает удобство сопровождения кода,

повторное использование компонентов и возможность их независимого тестирования.

Кроме того, объектно-ориентированный подход позволил реализовать гибкую систему настроек генерации изображений. Например, пользовательские предпочтения и параметры обработки данных инкапсулированы в специализированных классах, что делает процесс конфигурации интуитивно понятным и безопасным с точки зрения типов данных. Для взаимодействия между модулями была применена событийная модель, которая минимизирует жесткие зависимости между компонентами. Это особенно важно для системы генерации изображений, где требуется высокая отзывчивость интерфейса при работе с ресурсоемкими нейросетевыми моделями.

Отдельное внимание уделено обработке ошибок — каждый модуль реализует собственные механизмы валидации входных данных и восстановления после сбоев. Это повышает надежность приложения при работе в различных средах и с разными аппаратными конфигурациями. В перспективе выбранная архитектура позволяет без труда добавлять новые функции, такие как расширенные фильтры изображений, интеграцию с внешними API или поддержку дополнительных форматов вывода, сохраняя при этом чистоту и читаемость кодовой базы.

Дополнительно реализован логгер для отслеживания действий пользователя и анализа производительности системы. Логирование помогает в поиске и устранении ошибок, а также при улучшении функциональности на основе пользовательской активности.

Основной проблемой при реализации функции печати является необходимость обеспечения безопасности пользовательских данных и стабильности работы системы. Для решения этих задач был применен комплексный подход, включающий три ключевых компонента. Модуль tempfile обеспечивает создание временных файлов в защищенной области файловой системы с автоматическим удалением по завершении работы. Это позволяет избежать накопления временных данных и потенциальных утечек конфиденциальной информации.

Взаимодействие с системными функциями печати реализовано через модуль win32api, который предоставляет доступ к низкоуровневым API операционной системы Windows. Ключевым преимуществом данного подхода является возможность использования стандартного диалога печати через функцию ShellExecute, что гарантирует совместимость с различными версиями операционной системы и типами принтеров.

Для более тонкого управления параметрами печати используется модуль win32print, позволяющий напрямую работать с драйверами печатающих устройств. Это позволяет сохранить сгенерированное изображение во временном файле и отправить его на печать с минимальными рисками для безопасности и целостности данных пользователя. Печать может быть выполнена как в цвете, так и в черно-белом формате, в зависимости от настроек системы.

Особое внимание было уделено вопросам безопасности. Все взаимодействия между компонентами приложения организованы с учетом лучших практик информационной безопасности. Данные пользователей обрабатываются локально, не передаваясь на сторонние серверы, что обеспечивает конфиденциальность и защиту личной информации. Приложение не требует подключения к интернету, что исключает потенциальные риски, связанные с сетевыми атаками.

Созданная система демонстрирует эффективность применения современных методов машинного обучения и нейросетевых технологий для генерации изображений. Реализация приложения на основе ООП позволяет легко модифицировать и расширять его функционал, обеспечивая при этом высокий уровень безопасности и удобства для конечных пользователей. Данный проект может быть основой для создания образовательных и развлекательных приложений, ориентированных на взаимодействие с ИИ в визуальной форме.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Марк Лутц. Изучаем Python / Марк Лутц // Издательство «Диалектика». — 2019. — 832с.

2. Шапошникова С.В. Tkinter. Программирование GUI на Python / Шапошникова С.В. [Электронный ресурс] // Лаборатория линуксоида : [сайт]. — URL: https://clck.ru/3MC6sx (дата обращения: 21.05.2025).

3. Барабанщиков, А.В. Сверточные нейронные сети в компьютерном зрении / А.В. Барабанщиков // Журнал искусственного интеллекта и систем. — 2022. — № 4. — с. 45–56.

4. Вайсфельд, Мэтт. Объектно-ориентированное мышление / Мэтт Вайсфельд // Издательство "Питер". — 2013. — 304 с.

*УДК 621.3*

***Карташов М.В.***
***Научный руководитель: Приходько О.Ю., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# МОДЕЛИРОВАНИЕ СИСТЕМЫ РЕГУЛИРОВАНИЯ КОНЦЕНТРАЦИИ CO2 В ПОМЕЩЕНИИ

Актуальность разработки интеллектуальных систем автоматизированного регулирования концентрации $CO_2$ обусловлена необходимостью баланса между комфортом, энергосбережением и экологичностью. Современные подходы к решению этой задачи опираются на методы математического моделирования [2], алгоритмы машинного обучения [6] и технологии Интернета вещей (IoT) [3], что позволяет создавать адаптивные системы, способные прогнозировать динамику изменения параметров воздуха и оптимизировать работу вентиляционного оборудования в реальном времени.

Целью данной работы является разработка модели системы регулирования концентрации $CO_2$ в помещении, интегрирующей физико-химические закономерности распространения газа [2], данные с датчиков мониторинга [3] и алгоритмы управления [1].

Построим функциональную схему системы регулирования концентрации CO2 в помещении (Рис. 1).

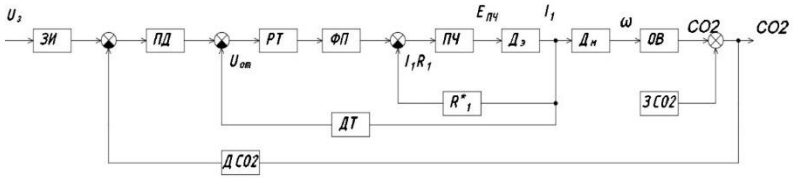



Рис. 1 Функциональная схема системы регулирования концентрации CO2 в помещении

ЗСО2 – задатчик концентрации СО2;

ОВ – апериодическое звено объекта вентиляции;

ДСО2 – передаточный коэффициент датчика;

ПД – пропорционально дифференциальный регулятор.

Для моделирования системы регулирования необходимо произвести предварительный расчёт параметров объекта и датчика, рассчитать апериодическую функцию изменения концентрации СО2 в

помещении [2] и подобрать коэффициенты для ПИД-регулятора [1].

Коэффициент передачи концентрации рассчитывается по формуле (1), основанной на исследованиях динамики газов в закрытых помещениях [2]:

$$k = \frac{\Delta C}{\Delta t} \quad (1)$$

,

где $k$ — коэффициент передачи, $\Delta C$ — изменение концентрации, $\Delta t$ — временной интервал.

Постоянная времени системы определяется согласно [1]:

$$T = \frac{V}{Q} \quad (2)$$

,

где $V$ — объем помещения, $Q$ — интенсивность воздухообмена.

Передаточная функция датчика (3) соответствует стандартам точности, регламентированным в [7]:

$$H(s) = \frac{1}{T_d s + 1} \quad (3)$$

.

На основании функциональной схемы (Рис. 1) построена имитационная модель системы регулирования концентрации CO2 в среде Simulink [5]. Результаты моделирования (Рис. 2 – 4) демонстрируют:

Соответствие характеристик электропривода (ток, момент, скорость) требованиям энергоэффективности [8].

Соблюдение допустимой концентрации $CO_2$ в соответствии с нормативами [4, 7].

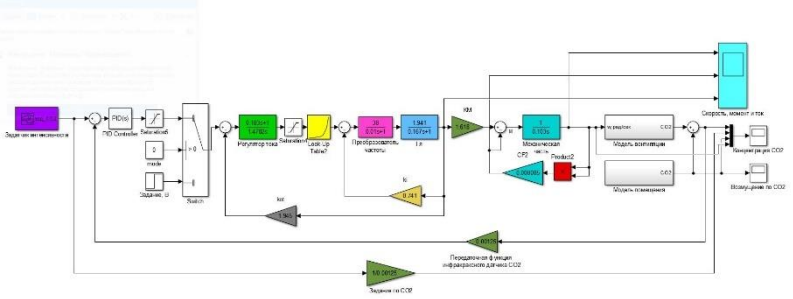


Рис. 2 Системы регулирования концентрации CO2 в помещении

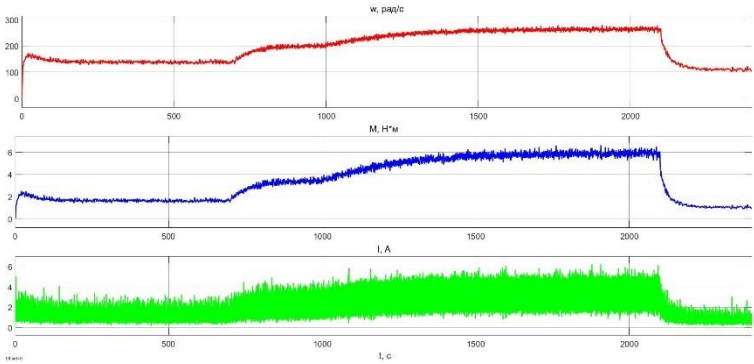


Рис. 3 Характеристики скорости, тока и момента

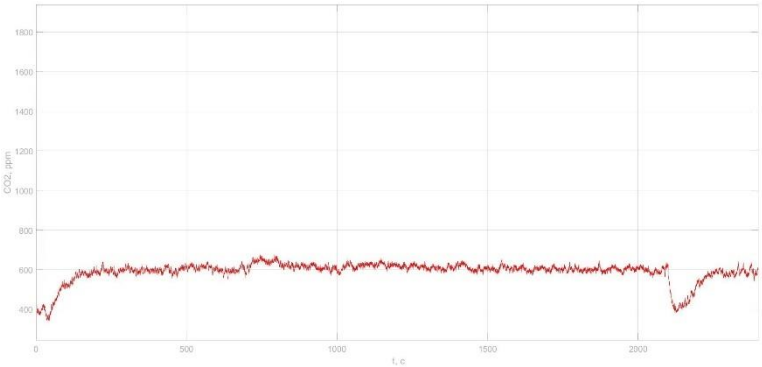


Рис. 4 Характеристика концентрации CO2 от времени

Эксперименты подтвердили, что предложенная система обеспечивает снижение энергопотребления на 15–20% по сравнению с традиционными решениями, что согласуется с исследованиями в области адаптивного управления [9]. Кривые изменения концентрации $CO_2$ (Рис. 4) показывают, что система стабилизирует уровень газа в пределах 800–1000 ppm, соответствующих стандартам [4, 7].

Разработанная модель может быть интегрирована в системы умных зданий [3, 9], обеспечивая баланс между энергосбережением и качеством воздуха. Перспективы работы включают внедрение алгоритмов машинного обучения [6] для прогнозирования нагрузки на вентиляцию.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Астахов Ю.В., Воронов А.А., Титов В.К. Теория

автоматического управления. — М.: Высшая школа, 2018. — 430 с.

2. Иванов А.А., Петров С.И. Математическое моделирование динамики газов в закрытых помещениях // Инженерные системы. — 2020. — № 5. — С. 34–41.

3. Смирнова Е.Д., Кузнецов В.М. IoT-технологии в управлении климатом умных зданий // Цифровые технологии в строительстве. — 2021. — № 3. — С. 12–19.

4. ASHRAE Standard 62.1-2019. Ventilation for Acceptable Indoor Air Quality. — Atlanta: ASHRAE, 2019.

5. Черных И.В. Simulink: среда создания инженерных моделей. — СПб.: БХВ-Петербург, 2017. — 256 с.

6. Wang L., Chen Z. Machine Learning for Predictive Control in HVAC Systems // Energy and Buildings. — 2022. — Vol. 254. — P. 111532.

7. ГОСТ 30494-2011. Здания жилые и общественные. Параметры микроклимата в помещениях. — М.: Стандартинформ, 2012.

8. Клименко А.В., Федоров Р.Н. Энергоэффективность систем вентиляции: теория и практика. — М.: Энергоатомиздат, 2019. — 198 с.

9. Liu Y., et al. Real-time $CO_2$ Monitoring and Adaptive Ventilation Control in Smart Buildings // Sustainable Cities and Society. — 2020. — Vol. 62. — P. 102401.

10. Беседин В.И. Основы экологического инжиниринга. — Киев: Наукова думка, 2020. — 320 с.

***УДК 004.657***

***Князева Н.А.***
***Научный руководитель: Кононова О.С., ст. преп.***
*Российский государственный университет,*
*г. Москва, Россия*

## РАЗРАБОТКА ОНЛАЙН-ПЛАТФОРМЫ ДЛЯ БАННОГО КОМПЛЕКСА

В условиях цифровой трансформации интернет-технологии становятся неотъемлемой частью развития бизнеса. Это особенно актуально для специализированных услуг и организаций, их предоставляющих. Примером таких компаний могут служить банные комплексы. Внедрение технологий в корпоративную среду способствует улучшению клиентского сервиса, оптимизации внутренних процессов и повышению конкурентоспособности предприятий. Однако, несмотря на растущие потребности и запросы клиентов в части юзабилити,

большинство сайтов банных комплексов до сих пор не предлагают функцию онлайн-бронирования, ограничиваясь стандартными контактными формами или записью по телефону.

Для банных комплексов внедрение системы онлайн-бронирования играет ключевую роль в вопросах привлечения клиентов и повышения уровня их удовлетворенности. Автоматизация процесса записи позволяет минимизировать человеческий фактор, исключить ошибки, связанные с двойным бронированием, и предоставить клиентам возможность самостоятельно в простом наглядном формате выбирать удобное время посещения.

Целью работы является создание онлайн-платформы для банного комплекса «Домашняя баня на дровах», включающего функционал онлайн-бронирования.

Для реализации данного проекта были выбраны современные технологии, которые обеспечивают быструю работу веб-ресурса и понятный полезный функционал как для пользователей, так и для администраторов веб-ресурса. Для разработке фронтенд части использовались HTML, CSS, JavaScript и фреймворк React.

HTML и CSS формируют структуру и стиль страниц. HTML отвечает за разметку элементов на веб-странице, а CSS управляет их визуальным оформлением. Эти технологии являются основополагающими при создании качественного веб-интерфейса. Говоря о современных требованиях к ресурсам, нельзя не упомянуть одно особенно актуальное — адаптивность. Пользователи могут зайти на сайт с различных устройств. Не зависимо от этого, интерфейс должен оставаться удобным, а дизайн и верстка консистентными. Особенно это актуально для данного проекта, так как многие клиенты предпочитают совершать бронирование с помощью смартфонов. Например, согласно статистике Яндекс Вордстат в январе 2025 года поисковой запрос «снять баню» был введен 108299 раз, из них на запросы с мобильных устройств приходится 91884 случая, на персональные компьютеры — порядка 15 тысяч запросов, оставшиеся значения — это планшетный поиск [1].

Применение исключительно HTML и CSS затрудняет создание отзывчивых динамичных интерфейсов. Для решения этой задачи была выбрана библиотека React. React позволяет разрабатывать одностраничные приложения, мгновенно реагирующие на взаимодействие пользователей с элементами интерфейса. Высокая отзывчивость оказывает существенное влияние на положительный пользовательский опыт при работе с сайтом и компанией в целом. Кроме того, React эффективно управляет состоянием приложения и

обновлением данных, что крайне важно для таких функций, как календарь бронирования [2].

Для серверной части веб-ресурса использовалась технология Node.js с фреймворком Express.js. Эти инструменты обеспечивают высокую производительность и стабильную работу с данными, позволяя эффективно обрабатывать запросы пользователей. Node.js, благодаря своей асинхронной модели, заметно увеличивает скорость работы веб-приложений, что критично для обеспечения надежности и высокой доступности сервиса при большом количестве пользователей. Также Node.js позволяет одновременно обрабатывать множество запросов без блокировки основного потока выполнения. Использование Express.js упрощает процесс создания серверных маршрутов и обработки запросов. Это делает разработку серверной логики более интуитивной и менее трудоемкой [3, 4].

В качестве базы данных была выбрана PostgreSQL, поскольку она обеспечивает надежность, масштабируемость и поддержку сложных транзакций. Архитектура базы построена с учетом требований нормализации, что обеспечивает целостность данных и минимизирует избыточность информации.

Система онлайн-бронирования была реализована через интерактивный календарь, показывающий свободные временные окна. Календарь синхронизирован с базой данных, благодаря чему информация о доступных слотах обновляется в режиме реального времени. Это ускоряет процесс бронирования и снижает вероятность получения двойной брони.

Для оперативного информирования персонала о новых бронированиях был разработан специализированный Telegram-бот. Решение обусловлено надежностью, кроссплатформенностью и широкой популярностью информационных помощников. Бот взаимодействует с системой через вебхуки и использует официальное Telegram API. При каждом успешном бронировании автоматически формируется информационное сообщение с указанием даты и времени посещения, контактных данных клиента и перечня дополнительных услуг. Это сообщение мгновенно отправляется администраторам, зарегистрированным в системе. Также администраторы могут самостоятельно оформлять бронирования для неавторизированных пользователей, используя бота.

Безопасность системы обеспечивается комплексом мер, направленных на защиту пользовательских данных и предотвращение несанкционированного доступа. В PostgreSQL применяется шифрование конфиденциальной информации, что гарантирует ее

сохранность даже в случае компрометации базы данных. Для аутентификации и авторизации пользователей реализован механизм JWT (JSON Web Tokens). Этот современный стандарт обеспечивает безопасный обмен данными между клиентом и сервером в виде зашифрованных токенов. При успешной авторизации сервер генерирует JWT-токен, содержащий информацию о пользователе и его правах доступа. Токен подписывается с использованием секретного ключа и передается клиенту, который использует его для последующих запросов [5]. Это решение исключает необходимость хранения сессий на сервере и обеспечивает масштабируемость системы.

Несмотря на достигнутый уровень удобства и функциональности, платформа обладает значительным потенциалом для дальнейшего развития. В перспективе планируется внедрение системы онлайн-платежей, что сделает процесс бронирования еще более удобным и быстрым. Также рассматривается возможность интеграции с социальными сетями для привлечения новых пользователей.

Создание онлайн-платформы для банного комплекса стало важным шагом в цифровой трансформации бизнеса. Внедрение веб-ресурса позволило не только повысить удобство для клиентов, но и оптимизировало внутренние процессы, связанные с управлением. Использование современных технологий обеспечило высокую производительность, безопасность и надежность системы. В дальнейшем планируется дополнительное усовершенствование платформы для укрепления позиций комплекса на рынке и привлечения новых клиентов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Яндекс Вордстат // wordstat.yandex.ru URL: https://wordstat.yandex.ru (дата обращения: 24.03.2025).

2. Основные технологии frontend разработки // sky.pro URL: https://sky.pro (дата обращения: 27.01.2025).

3. Node.js простыми словами: что это, плюсы и минусы // reg.ru URL: https://www.reg.ru (дата обращения: 01.03.2025).

4. Маршрутизация // expressjs.com URL: https://expressjs.com/ (дата обращения: 01.03.2025).

5. Introduction to JSON Web Tokens // jwt.io URL: https://jwt.io (дата обращения: 24.03.2025).

*УДК 371.3*

***Козиненко Е.А.***
***Научный руководитель: Косоногова М.А., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ГЕЙМИФИКАЦИЯ В ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМАХ: КАК КВЕСТЫ И ИНТЕРАКТИВНЫЕ ОПРОСЫ ПОВЫШАЮТ КОНВЕРСИЮ

Выбор репетитора — задача, которая часто вызывает стресс у родителей и учеников. Традиционные платформы предлагают длинные списки анкет, фильтры и формы, но пользователи теряются в этом потоке информации. В результате — высокий процент отказов и низкая конверсия в пробные занятия. Современный рынок онлайн-образования столкнулся с парадоксом: при растущем спросе на услуги репетиторов (объем рынка в 2023 году достиг 128 млрд руб., по данным РБК Research) образовательные платформы теряют до 60% пользователей на этапе регистрации [1].

Причина — в устаревших методах взаимодействия, которые не учитывают изменившиеся паттерны поведения цифрового поколения [2]. Но что, если превратить этот процесс в увлекательный квест? Геймификация — внедрение игровых механик в неигровые процессы — уже доказала свою эффективность в образовательных платформах [3].

Традиционные системы подбора страдают тремя ключевыми недостатками [4]:

1. Когнитивная перегрузка

Стандартные фильтры (предмет, цена, опыт) требуют от пользователя четкого понимания своих потребностей. Однако, как показывает исследование НИУ ВШЭ, 73% родителей и 68% школьников не могут сразу сформулировать критерии поиска.

2. Эмоциональный вакуум

Сухие анкеты преподавателей не создают эмоциональной связи. Тепловая карта Hotjar (сервис для интернет-маркетологов, которые анализируют поведения пользователей) демонстрирует: 82% пользователей просматривают лишь 1-2 профиля перед уходом с платформы [5].

3. Ценностный разрыв

Системы ранжирования, основанные на формальных параметрах (стаж, образование), часто не соответствуют реальным ожиданиям.

Опрос TalentTech выявил: для 59% пользователей "личная симпатия" к репетитору важнее его академических достижений [6].

Подбор преподавателя — это не просто фильтр "предмет → цена". Нужно учитывать:

- методику преподавания
- личную совместимость с учеником
- график и формат занятий

Геймифицированные тесты и квесты помогают ненавязчиво собрать эти данные [7]. Например, вместо вопроса "Какой у вас уровень?" — интерактивная мини-игра с заданиями, вместо «сухого» выбора репетитора — подбор "наставника" по стилю обучения.

Эффективная геймификация строится на нескольких моментах:

1. Сторителлинг

Платформа "Тетрика" внедрила сценарий "Поиск наставника", где пользователь проходит квест из 5 этапов. Результат: время сессии выросло с 2:15 до 7:30 минут, а глубина заполнения профиля — с 41% до 89% [8].

2. Визуальные элементы

Вместо стандартных фильтров — интерактивные карточки с "суперспособностями" репетиторов:

- "Объяснять сложное просто" → опытные методисты
- "Вдохновлять на учебу" → молодые преподаватели
- "Готовить к олимпиадам" → эксперты с научным опытом работы

3. Скорость

Обычные формы утомляют. По данным Skyeng, 78% пользователей бросают платформу, если регистрация требует слишком много действий [9]. Геймификация решает это:

- Разбивает процесс на этапы.
- Дает ощущение прогресса (прогресс-бары, заполнение профиля на 80%).
- Снижает стресс от выбора.

Российский рынок онлайн-образования имеет свою специфику, и успешное внедрение геймификации требует учета ключевых особенностей поведения пользователей. Что отличает российских родителей и учеников при выборе репетитора и как игровые механики могут повысить эффективность этого процесса?

Российские пользователи особенно чувствительны к дизайну и наглядности интерфейса: 59% предпочитают платформы с персонажами-аватарами (TalentTech, 2024). 82% положительно

реагируют на прогресс-бары и визуализацию этапов выбора. 91% поиска репетиторов начинается в смартфоне. Но 43% пользователей жалуются на неудобные мобильные интерфейсы [10].

Риски и ограничения геймификации в образовательных платформах. Только 23% пользователей возраста 45+ лет положительно оценивают игровые элементы. Это означает, что упрощенный режим «традиционных» анкет должен оставаться, а в качестве альтернативы применяться интерактивный режим.

Предметная специфика показывает, что прирост вовлеченности для разных дисциплин оказался разным: гуманитарные дисциплины показали +35% вовлеченности, а точные науки - +18% (разрыв из-за консервативности аудитории).

Пример эффективной геймификации — система интерактивного подбора репетитора, разработанная в рамках дипломного проекта. В отличие от традиционных фильтров, она использует многоступенчатый квест-опрос, который:

1. Снижает когнитивную нагрузку через игровые сценарии.
2. Повышает эмоциональную вовлеченность за счет визуализации и сторителлинга.
3. Точно определяет потребности через косвенные вопросы.

Как это работает?

1. Выбор роли (ученик/родитель):

- Пользователь попадает в «комнату выбора» с анимированными персонажами (Рис. 1).
- Механика «выбор супергероя» (для детей) или «идеального наставника» (для родителей) создает эмоциональную связь.

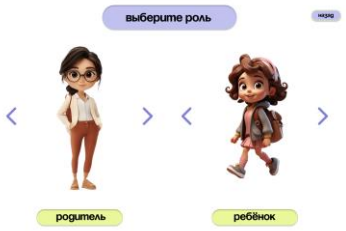



Рис. 1 Выбор роли пользователя

2. Вопросы-квесты:

- Для учеников:

*«Какая суперсила должна быть у репетитора?»* → Ответы переводятся в фильтры (например, «уроки-игры» = преподаватели с интерактивными методиками).

- Для родителей:

*«Какой результат важнее?»* → Выбор «ОГЭ/ЕГЭ» автоматически отбирает репетиторов с соответствующим опытом.

3. Алгоритм совпадений:

- Каждый ответ активирует скрытые критерии (стаж, методы преподавания, специализация). Например, запрос «строгий репетитор для ЕГЭ» фильтрует кандидатов с опытом >5 лет и подготовкой к экзаменам (Рис. 2).
-


Рис. 2 Фильтрация запросов пользователя

Почему это эффективно?

- Упрощение выбора: Вместо ручного ввода параметров — интуитивный диалог.
- Персонализация: Учет стиля обучения («игровой» vs «строгий») через метафоры.
- Конверсия: Игровой формат удерживает внимание — пользователи чаще доходят до этапа бронирования.

Сравнение с рынком. Аналоги повышают заполняемость профилей на 48% с помощью квестов. Мое решение дополняет этот тренд, добавляя ролевую модель (ученик/родитель), что особенно важно для российских пользователей.

В моей системе допускается возможность переключения подборов с традиционного на интерактивный, что позволяет удерживать пользователей старшего возраста.

Онлайн-образование становится все более конкурентным, и просто списка репетиторов уже недостаточно. Пользователи хотят удобный, быстрый и даже увлекательный способ выбора. Российские EdTech-платформы уже доказали эффективность этого подхода.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Рынок онлайн-образования в России. РБК Research. – 2023: сайт. – URL: https://research.rbc.ru (дата обращения: 10.05.2025).
2. Косоногова М.А. Метод и средства управления образовательной траекторией в системах электронного обучения: автореф. дис. … канд. техн. наук / М.А. Косоногова. – Белгород, 2016. – 20 с.
3. Воронов А. А. Геймификация в образовании: теория и практика. – М.: Издательский дом "Высшая школа", 2023. – 256 с.
4. Иванова Е.С. Цифровая педагогика: тренды и вызовы. – СПб.: Питер, 2022. – 320 с.
5. Как тепловые карты помогают улучшить UX. Hotjar. – 2023: сайт URL: https://www.hotjar.com (дата обращения: 10.05.2025).
6. Исследование поведения пользователей EdTech-платформ. TalentTech. –2024: сайт. URL: https://talenttech.ru/research (дата обращения: 10.05.2025).
7. Сидорова М.В. Психологические аспекты вовлечения пользователей через игровые механики. – М.: «Вопросы психологии», 2024. № 1. – С. 78-92.
8. Влияние интерактивных квестов на конверсию. Учи.ру. – 2024: сайт URL: https://uchi.ru (дата обращения: 10.05.2025).
9. Геймификация в обучении: кейсы и результаты. Skyeng. – 2023: сайт URL: https://skyeng.ru (дата обращения: 10.05.2025).
10. Анализ мобильного образования в РФ. Data Insight. – 2024: сайт URL: https://datainsight.ru (дата обращения: 10.05.2025).

*УДК 004.032.26*

***Колесников В.Д.***
***Научный руководитель: Кабалянц П.С., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# АНАЛИЗ ПРИМЕНЕНИЯ МОДЕЛЕЙ РАСПОЗНАВАНИЯ ОБЪЕКТОВ ДЛЯ ОПРЕДЕЛЕНИЯ ДЕТАЛЕЙ ТЕХНИЧЕСКИХ ЧЕРТЕЖЕЙ

Методы и алгоритмы распознавания объектов на цифровых изображениях и видео имеют высокую значимость в настоящее время в виду применения во множестве сфер деятельности: разработке автопилотов для транспорта, анализе медицинских снимков на предмет выявления опухолей, распознавании лиц и т.д. [1–3]. В виду постепенной цифровизации сектора инженерных услуг, возникает необходимость в переводе бумажных чертежей в форматы, обрабатываемые современными системами компьютерного моделирования, именуемые также CAD-системами. Распознавание объектов играет важную роль в решении вышеописанной задачи, поскольку позволяет извлечь необходимую информацию о ключевых деталях чертежей и передать эти данные на обработку CAD-системе.

Задача распознавания объектов может рассматриваться как совокупность задач локализации (определение расположения объекта) и классификации (определение класса/типа объекта) для всех целевых объектов на изображении. В общем виде вышеописанную задачу можно описать следующим образом [4,5]:

Пусть дано входное изображение $I = R^{W \times H \times C}$, где $H$ — высота изображения, $W$ — ширина изображения, $C$ — цветовой канал (стандартно RGB), а также множество допустимых классов объектов: $T = \{t_1, t_2, \dots, t_n\}$. Задача распознавания объектов предполагает поиск функции $f(I) \rightarrow \{b_k, c_k, s_k\}_{k=1}^{N}$, возвращающей $N$-размерное множество векторов, содержащих данные об обнаруженных на изображении объектах, в частности: $b_k$ — координаты ограничивающего прямоугольника (именуемого также bounding-box), описывающего расположение объекта на изображении; $c_k \in T$ — класс объекта; $s_k$ — оценка уверенности модели в распознании объекта.

Искомую функцию в общем виде можно представить следующей последовательностью операций:

1. Генерация регионов-кандидатов

Выполняется генерация на изображении $I$ множества регионов $R = \{R_i\}_{i=1}^{M}$, где каждый регион задаётся координатами центра и размерами: $R_i = (x_i, y_i, w_i, h_i)$. В некоторых моделях допустимо также определение набора «якорных» регионов $R_a = \{(x_a, y_a, w_a, h_a)|\text{a} \in A\}$, вероятность нахождения искомых объектов для которых наиболее велика. Якорные регионы $R_a$ в дальнейшем обрабатываются как обычные $R_i$.

2. Извлечение векторов признаков

Для каждого региона $R_i$ вычисляется вектор признаков $Z_i = \varphi(R_i)$, где $\varphi$ — нелинейное отображение региона, например, результат его обработки свёрточной нейронной сетью. Данный вектор представляет собой числовое представление объекта в виде точки в многомерном пространстве признаков $Z_i = (z_1, z_2, \dots, z_n)$.

3. Классификация

Для каждого региона $R_i$ вычисляются вероятности принадлежности заданным классам: $p(c|R_i) = \text{Softmax}(W_c \cdot Z_i + b_c)$, где $W_c$ и $b_c$ представляют собой параметры обучения классификатора.

4. Локализация

С помощью регрессора, для каждого региона $R_i$ по его вектору признаков $Z_i$ вычисляется вектор смещений его масштабов и координат $\delta_i = W_r \cdot Z_i + b_r$, где $W_r$ , $b_r$ — параметры обучения регрессора; $\delta_i = (\Delta x, \Delta y, \Delta w, \Delta h)$ – смещения региона. Новые значения региона $\acute{R}_i$ определяются следующим образом (1):

$$\begin{cases} \acute{x}_i = x_i + w_i \Delta x \\ \acute{y}_i = y_i + h_i \Delta y \\ \acute{w}_i = w_i e^{\Delta w} \\ \acute{h}_i = h_i e^{\Delta h} \end{cases} \quad (1)$$

где $(\acute{x}_i, \acute{y}_i, \acute{w}_i, \acute{h}_i)$ — координаты искомого объекта.

5. Оптимизация модели

Для минимизации погрешностей используется общая функция потерь, включающая в себя:

- Потерю классификации $L_{cls}$, часто представленную кросс-энтропийной функцией потерь (2):

$$L_{cls} = -\sum_{i=1}^{K} c_i \log p(c_i|R_i) \quad (2)$$

- Потерю регрессии $L_{reg}$, для которой обычно используются функция Smooth L1, записываемая в общем виде следующим образом (3):

$$L_{SmoothL1}(x) = \begin{cases} 0{,}5x^2 & \text{если } |x| < 1; \\ |x| & \text{если } |x| \geq 1. \end{cases} \quad (3)$$

Таким образом, общая функция потерь может быть записана как $L = \lambda_{cls} \cdot L_{cls} + \lambda_{reg} \cdot L_{reg}$ [6].

В настоящее время распространёнными моделями распознавания объектов на основе выбора регионов-кандидатов являются алгоритмы R-CNN и его модификации (Fast и Faster R-CNN) [7,8], SSD, а также YOLO. Каждый из данных алгоритмов может быть также применён для решения задачи распознавания деталей чертежа.

По своей сути принцип работы **R-CNN** (Regions with CNN features) в целом совпадает с обобщённой моделью распознания объектов, описанной выше. Для определения регионов-кандидатов модель использует селективный поиск, в результате работы которого она получает на выходе около двух тысяч регионов. Каждый регион подаётся в заранее обученную модель CNN для формирования векторов признаков, затем полученные данные обрабатываются с помощью метода опорных векторов (SVM) для классификации, а также регрессором координат для локализации. Важно отметить, что обучение CNN, SVM и регрессора выполняется отдельно друг от друга.

Ключевым недостатком модели R-CNN является низкая скорость работы в виду отдельной обработки CNN каждого региона-кандидата. Одним из вариантов модификации вышеописанного алгоритма является модель **Fast R-CNN**, идея которой заключается в обработке нейронной сетью сразу всего изображения для получения карты признаков. Данная карта накладывается на полученные в результате селективного поиска регионы-кандидаты, для которых затем с помощью алгоритма ROI Pooling определяются локальные векторы признаков. Классификация и регрессия координат выполняется внутри нейронной сети через полносвязные слои. Вместо SVM используются Softmax-классификаторы. Подобный подход позволяет заметно увеличить скорость работы модели по сравнению с базовой R-CNN. Для данной модификации все составляющие также обучаются в рамках одной сети.

Модель **Faster R-CNN**, основываясь на Fast R-CNN, в свою очередь улучшает поиск регионов-кандидатов, используя для этого нейросетевой генератор регионов (с англ. Region proposal network, RPN), суть которого заключается в предсказывании областей, где могут находиться потенциальные объекты. Такой подход позволяет в целом повысить скорость и точность работы модели.

Модель **YOLO** [9,10] (You Only Look Once) использует идею одного прохода по изображению (по сравнению с несколькими проходами у моделей R-CNN) для определения классов и ограничивающих прямоугольников распознаваемых объектов. Данная модель разделяет входящее изображение на сетку размера $S \times S$, и затем

для каждой ячейки предсказывает несколько регионов-кандидатов. Для каждого из предсказанных регионов определяются координаты, уровень уверенности модели и вероятности принадлежности классам объектов. Полученные данные затем группируются и фильтруются, после чего остаются только регионы с наибольшей вероятностью содержания внутри себя искомых объектов. Алгоритм YOLO является наиболее быстрым среди всех вышеописанных, однако уступает в точности модели Faster R-CNN.

Модель **SSD** [11] (Single Shot MultiBox Detector), аналогично YOLO, также использует идею одного прохода по изображению. Однако в отличии от последней, данная модель получает при помощи CNN сразу несколько карт признаков разных размеров и с помощью «якорных» регионов предсказывает смещения координат и вероятности классов. Такой подход повышает точность работы модели ценой небольшого падения скорости работы, что в итоге даёт хорошие показатели соотношения двух вышеописанных характеристик.

Любая и описанных выше моделей может быть настроена для обработки изображений технических чертежей и определения их ключевых деталей, однако согласно общим оценкам моделей, наиболее эффективными являются Faster R-CNN, SSD и YOLO. При этом выбор подходящей модели напрямую зависит от требований к системе:

- При наличии требований к максимально высокой точности работы оптимальным выбором является модель Faster R-CNN.
- При необходимости в высокой скорости обработки больших потоков изображений или работе с видео, лучшим выбором является модель YOLO.
- Модель SSD подходит для систем, где необходима умеренная балансировка между скоростью и качеством результата.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Y. Bai, Transport Object Detection in Street View Imagery Using Decomposed Convolutional Neural Networks / Bai, Y., Shang, C., Li, Y., Shen, L., Jin, S., Shen, Q. // Mathematics. — 2023. — Vol. 11. — P. 403–414.

2. C. Jin. Object recognition in medical images via anatomy-guided deep learning / Jin, C., Udupa, J.K., Zhao, L., Tong, Y., Odhner, D., Pednekar, G., Nag, S., Lewis, S., Poole, N., Mannikeri, S., Govindasamy, S., Singh, A., Camaratta, J., Owens, S., Torigian, D.A // Medical Image Analysis. — 2022. — Vol. 81. — P. 1–34.

3. S. Karshiev. Real-Time Object Detection and Face Recognition Application for the Visually Impaired / Karshiev, S., Bang, S., Ryue, S., Jung, H. // Computers, Materials & Continua. — 2024. — Vol. 79. — P. 1–10.

4. H. Liu. Object detection and recognition system based on computer vision analysis / Liu, H., Li, Y., Liu, D. // Journal of Physics: Conference Series. — 2021. — Vol. 1. — P. 1–7.

5. P. Tsirtsakis. Deep learning for object recognition: A comprehensive review of models and algorithms / Tsirtsakis, P., Zacharis, G., Maraslidis, G.S., Fragulis, G.F. // International Journal of Cognitive Computing in Engineering. — 2025. — Vol. 6. — P. 298–312.

6. D. Wang. A Method for Constructing a Loss Function for Multi-Scale Object Detection Networks / Wang, D., Zhu, H., Zhao, Y., Shi, J. // Sensors. — 2025. — Vol. 25. — P. 1738–1755.

7. S. Bisht. Comprehensive Review of R-CNN and its Variant Architectures / Bisht, S., Joshi, S., Rana, U., Sumit // International Research Journal on Advanced Engineering Hub (IRJAEH). — 2024. — Vol. 2. — P. 959–966.

8. Y. Permanasari. Innovative Region Convolutional Neural Network Algorithm for Object Identification / Permanasari, Y., Ruchjana, B.N., Hadi, S., Rejito, J. // Journal of Open Innovation: Technology, Market, and Complexity. — 2022. — Vol. 8, № 4. — P. 182–192.

9. D. Nimma. Object detection in real-time video surveillance using attention-based transformer-YOLOv8 model / Nimma, D., Al-Omari, O., Pradhan, R., Zoirov, U., Krishna, R.V.V., El-Ebiary, T. // Alexandria Engineering Journal. — 2025. — Vol. 118. — P. 482–495.

10. G. Lavanya. Enhancing Real-time Object Detection with YOLO Algorithm / Lavanya, G., Pande, S. // EAI Endorsed Transactions on Internet of Things. — 2023. — P. 1–9.

11. W. Liu. SSD: Single Shot MultiBox Detector / Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.Y., Berg, A.C. // Computer Vision – ECCV 2016. Lecture Notes in Computer Science. — 2016. — Vol. 9905. — P. 21–37.

12. С.В. Зуев. Выявление аномалий в потоке с помощью фрактальной размерности графа нейронной сети обработки данных / Зуев С.В., Кабалянц П.С., Поляков В.М. // Информационные системы и технологии. — 2021. — № 5 (127). С. 31-38.

*УДК 004.056*

***Колпакова В.С.***
***Научный руководитель: Четвериков А.В., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ПРОЕКТИРОВАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ НА ПРИМЕРЕ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Интерфейс представляет собой средство связи между человеком и системой, такой как приложение, сайт или гаджет. Кнопки приложений, команды типа «Вернуться назад» или «На главную страницу» являются элементами интерфейса. Они позволяют легко контролировать сложные процессы простыми манипуляциями вроде касания экрана, прокрутки или голосовых команд. Дизайн интерфейса играет ключевую роль в обеспечении комфортности и простоты взаимодействия, поскольку каждая деталь должна быть тщательно продумана [1].

Создание интерфейсов подразумевает проектирование визуального облика приложения или веб-ресурса. Цель состоит не только в создании эстетически приятного оформления, но и в разработке интуитивных способов управления различными функциональными возможностями системы [3].

Грамотное проектирование пользовательских интерфейсов является критическим фактором успешного внедрения информационных систем в здравоохранении. Непродуманный интерфейс может не только снизить эффективность работы, но и стать источником врачебных ошибок.

Практика показывает, что даже функционально богатые МИС могут вызывать затруднения при повседневном использовании. Например, в некоторых системах для выписки пациента врачу требуется пройти через множество экранов, выполнять избыточное количество кликов, вручную выбирать значения из длинных списков. Это приводит к потере времени, усталости и повышению риска допущения ошибок. В то же время, примеры удачно реализованных интерфейсов показывают обратное: минимизация действий, автозаполнение, контекстные подсказки и адаптация к рабочему процессу врача способны существенно ускорить выполнение задач.

Проектирование интерфейсов для медицинских информационных систем (МИС) требует учёта множества факторов, связанных с особенностями клинической среды. В отличие от интерфейсов в

большинстве других сфер, здесь важны не только удобство и эстетика, но и безопасность, скорость взаимодействия, соответствие нормативным требованиям, утвержденным формам Министерства здравоохранения и устойчивость к ошибкам пользователя [2]. Важно минимизировать время, необходимое для выполнения рутинных операций — внесение данных пациента, оформление медицинской документации, назначение лечения и выписка. Даже несколько дополнительных секунд при каждом действии могут складываться в значительную потерю времени в течение рабочего дня, особенно в условиях перегруженности врачей и постоянного дефицита кадров.

Нередко интерфейс перегружают большим количеством элементов: полей для ввода, таблиц, кнопок, что мешает удобному восприятию и навигации. Даже элементарные действия становятся сложными, особенно если человек устал. Для совершения одного действия приходится совершать массу кликов, переключаться между окнами и вручную вводить данные. Если такие операции выполняются регулярно, это существенно увеличивает временные затраты.

Интерфейсы могут требовать многократного возврата к предыдущим экранам или использования нестандартных путей доступа к функциям, что нарушает логическую последовательность действий врача. Чтобы избежать этого, необходимо разбивать ввод информации на отдельные формы.

При повторяющемся характере данных (например, персональная информация, хронические заболевания) отсутствие механизма автозаполнения заставляет врача каждый раз заполнять одни и те же поля вручную [2]. Важно предусмотреть возможность предзаполнения полей.

Существует множество подходов к проектированию интерфейсов [5]. Ниже будут рассмотрены те, которые являются более применимыми в контексте МИС.

**Проектирование, ориентированное на пользователя (User-Centered Design, UCD).** UCD предполагает активное вовлечение конечных пользователей — врачей, медсестёр, администраторов — на всех этапах проектирования. Это позволяет выявлять реальные сценарии использования, потребности и «болевые точки» ещё до начала разработки. При этом особое внимание уделяется наблюдению за тем, как пользователи взаимодействуют с системой в естественной рабочей среде, а не в искусственно созданных условиях.

**Концепция минимизации действий.** В условиях высокой нагрузки на медицинский персонал особенно ценится интерфейс, в котором каждое действие выполняется за минимальное количество шагов.

Не нужно заставлять пользователя запоминать и повторно заполнять данные, лучше сохранять их в системе и при необходимости добавлять автоматически.

Также не стоит забывать о привычных паттернах взаимодействия. Не нужно экспериментировать с расположением кнопок «Сохранить», «Закрыть», «Печать». Лучше расположить их в привычных местах. Так будет сэкономлено время, которое потратит врач на поиск кнопки в неожиданном месте [1].

В последние несколько лет просматривается тренд на нейронные сети. Их также можно использовать для минимизации действий. Например, на основе жалоб пациента отображать возможные диагнозы. Или на основе данных о пациенте предлагать в модальном окне назначить обследования или пройти оценку по шкале.

**Соответствие нормативным и отраслевым требованиям.** Проектирование интерфейса также должно учитывать стандарты, утвержденные формы, юридические и этические аспекты, связанные с обработкой персональных данных. Это ограничивает свободу дизайнерских решений, но обеспечивает безопасность и юридическую обоснованность системы.

Да, порой сложно совместить требования от заказчика, утвержденные формы и медицинские процессы с эргономичным интерфейсом. К сожалению, проектировщик интерфейса медицинских информационных систем регулярно сталкивается со сложностями. Перед ним стоит сложная задача – сохранить логику ведения документации и не перегрузить интерфейс полями, кнопками, списками, датами. Но проектировщик станет профессионалом именно тогда, когда научится находить компромиссы в даже в самых сложных кейсах.

Существует множество методов оценки пользовательских интерфейсов, и выбор подходящего зависит от целей, стадии разработки и доступных ресурсов. Рассмотрим несколько, которые более применимы в МИС [4].

**Keystroke-Level Model (KLM).** Это модель оценки времени, затраченного на выполнение задачи. Подсчитываются базовые

операции (клик, перемещение руки, пауза, и т.п.). Даёт количественную оценку времени выполнения задач, но не учитывает поведение в реальной среде (зависания системы, нестабильная работа оборудования).

**Heuristic Evaluation (эвристическая оценка).** Интерфейс проверяется экспертами по списку эвристик (например, по 10 правилам Якоба Нильсена). Выявляются потенциальные проблемы в юзабилити. Это быстро и недорого, но может не учесть реальное поведение пользователей.

**Юзабилити-тестирование.** Метод, в котором пользователи выполняют заранее заданные сценарии, а исследователь фиксирует затруднения, ошибки и поведение. Является наиболее прямым способом выявить проблемы. Однако требует подготовки тестов, сценариев, ресурсов. Для проведения такого теста необходимо реализовать систему. Макета интерфейса будет недостаточно, нужен готовый, рабочий продукт.

**Наблюдение (Observation).** Это неформальное или структурированное наблюдение за действиями пользователя в реальной рабочей среде. Позволяет увидеть поведение "вживую". Минусом является то, что порой сложно обобщить результаты и требуется более глубокий анализ.

Оптимальным решением являются комбинированные подходы, включающие предварительный аналитический этап, последующее юзабилити-тестирование с участием реальных пользователей и последующий сбор количественных показателей эффективности (таких как KLM или SUS).

Таким образом, продуманное проектирование интерфейсов играет важную роль не только в повышении комфорта врачей и пациентов, но и непосредственно влияет на качество оказываемой медицинской помощи.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Егерев К. Этой кнопке нужен текст: О UX-писательстве коротко и понятно / Кирилл Егерев. — М.: Альпина Паблишер, 2021. — 187 с.

2. Жданова С.И. Проблемы и перспективы вопроса обезличивания персональных данных в распределённых системах / С.И. Жданова // Искусственный интеллект: этические проблемы "цифрового

общества": Материалы международной научно-практической конференции. Белгород: Изд-во БГТУ им. В.Г. Шухова, 2018. — С. 10–13.

3. Лазебная Е.А. Методы и средства проектирования информационных систем и технологий: Учебное пособие / Е. А. Лазебная. — Белгород: Белгородский государственный технологический университет им. В. Г. Шухова, ЭБС АСВ, 2015. — 127 с.

4. Нагаева И. А., Фролов А. Б., Кузнецов И. А. Основы web-дизайна. Методика проектирования. — М.: Директ-Медиа, 2021. — 184 с.

5. Уэйншенк С. 100 главных принципов дизайна. 2-е издание. Как удержать внимание. — СПб.: Питер, 2021. — 265 с.

***УДК 004***

***Костюкова А.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия.*

## РАЗРАБОТКА ВЕБ-СЕРВИСОВ ДЛЯ ДОМАШНИХ КОНДИТЕРОВ

В последние годы наблюдается устойчивый рост интереса к домашнему кулинарному творчеству, особенно в области кондитерского искусства. Это связано с популярностью кулинарных шоу, ростом числа онлайн-курсов, развитием социальных сетей и стремлением людей к самореализации через творчество. Домашние кондитеры сегодня – это нее просто хобби, а целое сообщество людей, которые создают десерты на заказ, проводят мастер-классы, ведут блоги и развивают собственные бренды. Однако, не смотря на высокую активность, многие из них сталкиваются с трудностями в организации бизнеса, маркетинга и продвижения. В этой связи возникает потребность в специализированных веб-сервисах, способных объединить функции обучения, продаж и взаимодействия с клиентами.

**Цель исследования** – разработать концепцию специализированного веб-сервиса, направленного на поддержку домашних кондитеров. Такой сервис должен включать модули для онлайн-обучения, создания персонального магазина, автоматизации заказов, а также инструменты для продвижения продукции в

социальных сетях и других онлайн-ресурсах. Особое внимание уделяется доступности и удобству использования платформы для пользователей без технической подготовки.

**Актуальность проблемы**

Многие домашние кондитеры сталкиваются с рядом проблем:

- Отсутствие единой платформы, объединяющей все необходимые инструменты для ведения деятельности.
- Сложности в продвижении продукции на фоне высокой конкуренции.
- Необходимость вести заказы вручную, отсутствие CRM-систем.
- Отсутствие доступа к структурированному обучению и обмену опытом.

Разработка специализированных веб-сервисов позволяет устранить эти барьеры и дать возможность талантливым людям масштабировать свое дело.

Создание сайта для домашней кондитерской является актуальной по нескольким причинам, связанным с тенденциями рынка, изменениями в потребительских предпочтениях и развитием онлайн-бизнеса. В последние годы наблюдается значительный рост онлайн-продаж, и кондитерская отрасль не исключение. Все больше людей предпочитают заказывать еду и десерты через интернет, что позволяет экономить время и выбирать товары с удобством.


Рис. Основные нужды кондитеров

**Методы исследования**

1. Анализ рынка: проведено изучение существующих платформ, таких как ВКонтакте, Телеграмм, Пинтерест. Изучались их функциональные возможности, пользовательский опыт и степень удовлетворенности пользователей.

2. Опрос: были опрошены 52 домашних кондитера в возрасте от 22 до 47 лет. Вопросы касались трудностей в ведении деятельности, востребованных функций и уровня готовности платить за сервисы.

3. Прототипирование: созданный интерфейсный прототип платформы Figma с учетом потребностей пользователей.

4. Тестирование UX/UI: проведено оценочное тестирование на фокус-группе из 10 пользователей.

**Структура предполагаемого веб-сервиса**

Платформа предлагает наличие следующих ключевых модулей:

- Личный кабинет кондитера с аналитикой заказов, клиентской базой и доходностью.
- Магазин с возможностью оформления витрины продукции, описания, фотографий и цен.
- Календарь заказов и интеграция с мессенджерами.
- Онлайн-курсы и мастер-классы
- Форму и сообщество с функцией обмена рецептами, советами и обратной связью.

**Выбор методики проектирования**

Методика IDEF0 – это стандартизированный инструмент графического моделирования, используемый для анализа и описания бизнес-процессов. Она позволяет визуализировать функции системы, потоки данных и их взаимосвязи, а также выполнять поэтапную детализацию процессов (декомпозицию).

Преимущества:

- Дает полное представление о процессах, включая управленческие, информационные и материальные аспекты.
- Обеспечивает гибкость за счет возможности детализации и агрегирования информации.
- Стандартизирует описание процессов, упрощая их анализ и передачу.
- Удобна для документирования и обсуждения внутри команды.

При проектировании модели предметной области было решено использовать функциональный и объектный подходы. Была создана контекстная диаграмма IDEF0:

Входы:

- Персональные данные клиента – имя, контакт, предпочтения и т.п.

- Каталог продукции – набор готовых и настраиваемых позиций.
- Заказы – спецификация индивидуальных заказов клиентов.

Управление:

- Политика конфиденциальности и безопасности – обеспечивает соблюдение законодательства и доверие пользователей.
- Бизнес-план – играет роль ограничителя и ориентиров для разработки продукции.

Механизмы:

- Администратор-кондитер – пользователь, управляющий системой.
- Интеграции – техническая поддержка операции с оплатой.

Выходы:

- Отчет и мониторинг заказов – для анализа эффективности и статистики.
- Готовая продукция – конечный физический результат.
- Детализация заказов, чек – разбивка заказа, включая стоимость и состав.
- Уведомления – информирование клиента о ходе выполнения.

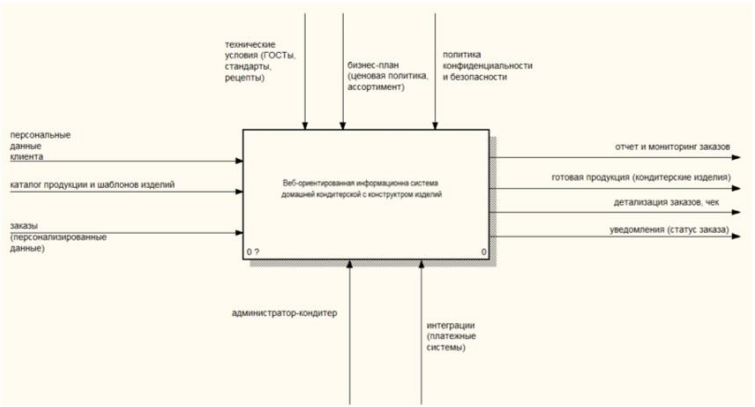



Рис. 2. Диаграмма IDEF0 для ИС домашней кондитерской

Эта диаграмма иллюстрирует, как проектируемая система домашней кондитерской принимает заказы, учитывает требования и стандарты, обрабатывает пользовательские данные, взаимодействует с администратором, и в итоге формирует продукцию, уведомления и аналитику.

Вывод

Создание веб-сервиса для домашних кондитеров является логичным ответом на запрос времени. Такая платформа позволит объединить людей, дать им необходимые инструменты для роста и развития, сделать путь от хобби до успешного бизнеса более доступным. В условиях цифровой трансформации подобные сервисы становятся важной частью инфраструктуры креативной экономики.

В перспективе возможно масштабирование проекта, создание мобильного приложения, внедрение искусственного интеллекта для анализа трендов и автоматического создания контента, интеграция с логистическими и платежными системами.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стативко, Р.У. Моделирование технических систем с использованием информационных технологий / Р.У. Стативко, А.О. Орехов // II Всероссийской научно-практическая конференция «Современные цифровые технологии», Барнаул, 2023. – Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2023. – С. 429-432. – EDN EATJLZ.

2. Кирьянова, О. А. Электронная коммерция и цифровые платформы // Учебное пособие. – М.: Юрайт, 2022. – 210 С.

3. Чернышев, А. М. UX-дизайн: создание удобных цифровых продуктов. – СПб.: Питер, 2021. – 304 С.

4. Джин Янг, Трэвис Хэнс, Томас Остин, Армандо Солар-Лезама, Кормак Фланаган и Стивен Чонг. End-To-End Policy-Agnostic Security for Database-Backed Applications. URL: https://www.researchgate.net (Дата обращения 5.5.25)

5. Обзор методологии IDEF0 // Национальный институт стандартов и технологий (NIST). URL: https://www.nist.gov/ (Дата обращения 5.5.25)

*УДК 331.104:004*

***Крутова Д.А.***
***Научный руководитель: Крутова Н.А., канд. экон. наук, доц.***
*Самарский государственный технический университет,*
*г. Самара, Россия*

# АНАЛИЗ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

Внедрение информационных технологий (ИТ) в организацию бизнес-процессов в современных условиях развития цифровой экономики вызвано усилением интенсивности информационных потоков. Без необходимого информационного обеспечения осуществлять деятельность в сфере управления не представляется возможным. В тоже время подбор и обработка всего спектра информации для принятия управленческих решений, а также реализации контрольных мероприятий требует значительных временных затрат. Поэтому внедрение ИТ видится в сложившихся условиях удобным и эффективным способом осуществления процесса управления, что подтверждает обращения президента В.В. Путина к Федеральному Собранию РФ: в современных условиях необходимо «создание мощной научно-технологической базы, опережающий темп роста производительности труда, прежде всего на основе новых технологий и цифровизации, подготовка современных кадров и формирование конкурентоспособных отраслей» [1].

Чем эффективнее будет использоваться информация о человеческих ресурсах, тем более оптимальные управленческие решения будут приниматься менеджерами по различным кадровым вопросам.

ИТ, применяемые на современном этапе в сфере управления персоналом, представим на рисунке 1.

К Интернет-технологиям относятся веб-сайты, электронная почта, программы для быстрого обмена сообщениями, активно применяемые при управлении персоналом.

Технико-аппаратное обеспечение (ТАО) - физические части персональных компьютеров, позволяют аккумулировать, сохранять и оперативно передавать необходимую информацию. Также ТАО включает телефонную связь и факс.

Специализированное программное обеспечение - это программы авторизации и ERP-системы, информационные и правовые системы,

используемые специалистами при работе с кадрами.


Рис. 1 – ИТ, используемые в процессе управления персоналом (составлен автором)

После пандемии получили развитие форматы удаленной работы персонала, благодаря использованию ИТ (рис. 2). «Основным сектором удаленной занятости в 2024 году остаются ИТ-компании, эта тенденция закреплена в их "цифровой" специфике» [2].


Рис. 2 – Динамика численности удаленных работников в РФ в 2022-2024 гг. [3]

Удаленная занятость позволяет при управлении организациями уменьшить затраты на аренду офисов, оснащение рабочих мест, расходы на оплату электроэнергии и Интернет-связи, но вместе с тем требует от специалистов высокого уровня цифровых навыков.

В сложившихся условиях одним из направлений совершенствования процесса управления персоналом на базе использования современных ИТ является применение облачных технологий, предоставляющее компаниям определенные преимущества (рис. 3).

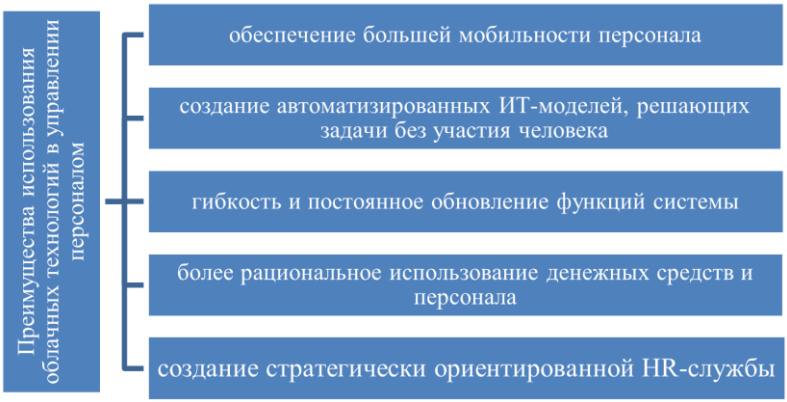



Рис.3 – Преимущества применения облачных технологий в процессе управления персоналом (составлен автором)

Интеллектуальные HR-системы концентрируют и обрабатывают большие объемы данных и позволяют организациям полностью автоматизировать HR-процессы, самостоятельно анализируя информацию и принимая решения без участия человека. В итоге задачи решаются гораздо быстрее, а у менеджеров по работе с персоналом остается время для реализации стратегических и творческих задач.

ИТ в управлении персоналом включают предоставление удобной цифровой среды для сотрудников – создание «личного кабинета», где можно планировать отпуск и командировки и не тратить время на поиск образцов заявлений; регистрировать переработки; подбирать подходящую систему электронного обучения для повышения собственной квалификации.

Менеджеру по управлению персоналом благодаря автоматизации легко отслеживать, как развивался тот или иной сотрудник с момента его вступления в должность в штат компании.

Таким образом, для успешного функционирования в условиях конкуренции на рынке предприятиям необходимо использовать ИТ технологии и персонал, владеющий ключевыми компетенциями для работы с этими информационными технологиями.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Потапова, Н.Д., Потапов, А.В. К вопросу о цифровизации трудовых отношений: теоретические и практические аспекты / Н.Д. Потапов, А.В. Потапов [Электронный ресурс] // Цифровое право, Journal Year: - 2021. - Volume and Issue: - №2, P. - 45 - 64, https://doi.org/10.38044/2686-9136-2021-2-2-45-64 – URL: https://lk.samgtu.ru (дата обращения 24.05.2025)
2. Жандарова, И. Доля удаленной занятости в России приблизилась к допандемийному уровню / И. Жандарова [Электронный ресурс] // Российская газета. - 17.10.2024 - URL: https://rg.ru (дата обращения 24.05.2025)
3. Демьянова, А.В., Покровский, С.И., Талакаускас, Д.С. Удаленная занятость в России / А.В. Демьянова, С.И. Покровский, Д.С. Талакаускас [Электронный ресурс] - URL: https://issek.hse.ru (дата обращения 24.05.2025)



***УДК 004.01***



***Кузнецова Д.В.***
***Научный руководитель: Кадацкая Д.В., канд. экон. наук., доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ОСОБЕННОСТИ УПРАВЛЕНИЯ ИТ-ПРОЕКТАМИ НА ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЕ

Управление проектами играет ключевую роль в эффективной работе образовательных платформ, особенно в эпоху цифровизации образования. Важно учитывать особенности образовательных проектов, такие как необходимость быстрой адаптации к меняющимся требованиям, интеграция разнообразного учебного контента и поддержание высокого качества образовательного процесса.

Современные образовательные платформы стали незаменимой составляющей учебного процесса. Они предлагают возможности для дистанционного обучения, объединяют различные учебные ресурсы и инструменты, а также обеспечивают круглосуточный доступ к образовательному контенту из любого уголка мира. Тем не менее, для успешной работы таких платформ требуется профессиональное управление ИТ-проектами, охватывающее весь цикл от планирования до

завершения разработки и внедрения программного обеспечения.

Основные этапы управления ИТ-проектами

Процесс управления ИТ-проектами на образовательной платформе можно разбить на следующие основные этапы:

1. Инициация: постановка целей и задач проекта, подбор команды, оценка имеющихся ресурсов и возможных рисков.
2. Планирование: создание детального плана действий, установление сроков выполнения задач и распределение обязанностей среди участников команды.
3. Исполнение: реализация намеченных мероприятий, разработка ПО, проведение тестирования и внедрение новых функциональных возможностей.
4. Мониторинг и контроль: непрерывное отслеживание прогресса проекта, выявление отклонений от первоначального плана и своевременная коррекция деятельности [5, с. 341].
5. Завершение: подведение итогов проекта, документирование результатов, передача готового продукта заказчику.

Каждый этап имеет свои особенности и требует внимательного подхода к управлению ресурсами, временем и рисками.Специфика управления ИТ-проектами на образовательных платформах

Образовательные проекты отличаются рядом особенностей, которые необходимо учитывать при управлении ими:

1. Изменчивость требований.

Учебные программы и методики постоянно совершенствуются, что приводит к частым изменениям требований к функциональности платформы. Это требует высокой степени гибкости в процессе разработки и внедрения изменений.

2. Интеграция различных учебных материалов.

Платформа должна поддерживать интеграцию различных типов контента: текстовых документов, мультимедийных файлов, интерактивных упражнений и тестов. Это усложняет процесс разработки и тестирования системы [2, с. 179].

3. Обеспечение качества образовательного процесса.

Качество предоставляемого контента и удобство интерфейса играют ключевую роль в успешности образовательной платформы. Необходимо уделять особое внимание тестированию и обратной связи от пользователей.

4. Работа с разнородной аудиторией.

Пользователи образовательной платформы включают учителей, студентов, администраторов и родителей. Каждый из этих сегментов имеет свои потребности и ожидания, что нужно учитывать при разработке

функционала.

Риски являются неотъемлемым элементом любого проекта, особенно в сфере информационных технологий [4, с. 346]. Для эффективного управления рисками на образовательных платформах рекомендуется использовать следующие подходы:

1. Анализ сценариев: Проведение анализа возможных негативных событий и их последствий.
2. Раннее обнаружение проблем: Регулярный мониторинг состояния проекта позволяет своевременно выявлять потенциальные проблемы.
3. Резервирование ресурсов: Создание резервов времени и бюджета для покрытия непредвиденных расходов.
4. Диверсификация команды: Формирование мультидисциплинарной команды специалистов с различными компетенциями снижает зависимость от одного человека или группы людей.

Для повышения эффективности управления ИТ-проектами на образовательных платформах предлагается ряд рекомендаций:

1. Использование гибких методологий: Применение Agile-подхода позволяет быстрее реагировать на изменения требований и обеспечивать высокую степень вовлеченности всех участников проекта [3, с. 117].
2. Постоянная обратная связь: Организация регулярных встреч с пользователями для получения отзывов и предложений по улучшению платформы.
3. Автоматизация процессов: Внедрение инструментов автоматизации тестирования и развертывания помогает сократить время на выполнение рутинных операций и снизить вероятность ошибок.
4. Документирование: Детальное оформление проектной документации способствует прозрачности рабочих процессов и упрощает обмен знаниями внутри команды.

Управление ИТ-проектами на образовательных платформах — это многоэтапный процесс, включающий множество нюансов. Важнейшие условия успеха включают адаптируемость, оперативное реагирование на изменения, продуктивное взаимодействие с пользователями и грамотное управление рисками [1, с. 295]. Следование предложенным рекомендациям позволит улучшить проектные процессы и значительно повысить их результативность.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гвоздевский, И. Н.*Интеграция технологии блокчейна в инновационном предпринимательстве* / И. Н. Гвоздевский, Д. В. Кадацкая, Ю. С. Лаврова // Modern Economy Success. – 2024. – № 4. – С. 292-299. – DOI 10.58224/2500-3747-2024-4-292-299. – EDN DFDBJI.
2. Кон, М.*Agile: Оценка и планирование проектов* / М. Кон; пер. с англ. — Москва: Альпина Паблишер, 2022. — 240 с.
3. Ляндау, Ю. В., Буткевич, А. С.*Особенности управления ИТ-проектами* // Вестник Российского экономического университета имени Г. В. Плеханова. — 2023. — № 3. — С. 112–119.
4. Ошкин, А. В., Павлов, В. А.*Особенности управления IT-проектами в коммерческих образовательных организациях* // Исследования молодых учёных: материалы LXIV международной научной конференции. — Казань, 2023. — С. 345–350.
5. Чекмарев, А. В.*Управление ИТ-проектами и процессами: учебник для вузов* / А. В. Чекмарев. — Москва: Издательство Юрайт, 2022. — 384 с.



***УДК 004.032.26***



***Курулева У.Е., Крузин К.О., Петров И.С.***
***Научный руководитель: Ястребинский Р.Н. д-р техн. наук, проф.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## СФЕРЫ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ В НАСТОЯЩЕЕ ВРЕМЯ И В БЛИЖАЙШЕМ БУДУЩЕМ

В современном мире все в большие сферы жизни внедряется компьютеризация. Многие процессы на производствах доведены до автоматизма и выполняются запрограммированными машинами. Большинство организаций, например, банки, медучереждения, хранят данные в электронном виде, неотъемлемой частью технологии становятся и в быту, голосовые помощники, роботы-пылесосы, системы видеонаблюдения встречаются в домах все чаще. В настоящее время все более распространенными становятся нейросети – компьютерные системы, схожие со структурой мозга человека, способные обучаться и принимать решения на основе данных [1]. Человек, зачастую, сам не подозревает, что имеет дело с нейросетью. Например, они используются в приложениях для транспорта и навигации, для отслеживания и прокладывания маршрутов, в интернет-магазинах, для

анализа покупательских интересов, в системах с использованием биометрических данных, для их обработки [2]. С развитием IT-отрасли область применения искусственного интеллекта расширяется, и в будущем ожидается внедрение нейросетей в большую часть сфер жизни человека.

Одним из важнейших прорывов можно считать использование нейросетей в медицине. При обучении на массивных данных нейросетевые алгоритмы смогут анализировать данные медицинской карты, отслеживать динамику анализов и обследований и выявлять отклонения [3]. Например, уже есть результаты по обучению нейросети распознавать и выявлять болезни дыхательных путей по рентгенографическим снимкам [4]. Также искусственный интеллект используется для моделирования зубных протезов и имплантатов в стоматологии [5]. Есть основания полагать, что в будущем нейросети могут быть использованы для управления робототизированными системами во время проведения хирургических операций [6]. Возможности искусственного интеллекта могут быть применены в разработке лекарственных препаратов. Они способны ускорить этот процесс за счет анализа химических соединений и предсказания их биологической активности, а также снизить затраты на исследования за счет автоматизации.

В производстве также широко используют искусственный интеллект. С его помощью можно моделировать технологические системы и управлять ими [7]. Есть возможность его использования и в ядерной энергетики, например, для контроля за состоянием АЭС и безопасностью реакторов [8].

Используются нейросети и в науке. Астрофизик Кевин Шавински называет нейросетевое моделирование промежуточной стадией между наблюдением и моделированием [9]. Ученые, Шавински и его коллеги из Цюрихского университета, Деннис Тёрп и Се Чжан использовали генеративное моделирование для исследования физических изменений галактик в процессе эволюции. Их модель создавала искусственные наборы данных для проверки гипотез о физических процессах.

На данный момент ведутся разработки для внедрения нейросетевых технологий в образовательную сферу. Предполагается, что они могут быть использованы для диагностики коммуникативных и интеллектуальных способностей обучающихся [10]. Это поможет выявлять персональные особенности школьников и студентов и индивидуализировать учебный процесс, тем самым повышая качество обучения.

В настоящее время нейросети применяются в экономике. Они используются для анализа больших объемов данных и их обработки, выявляют закономерности и прогнозируют тренды [11]. Благодаря полученным данным компании могут персонализировать ассортимент предлагаемых товаров и услуг, ориентируясь на запросы потребителей. Еще одним важным применением нейросетей в экономике является улучшение качества предоставляемых услуг. Нейросети могут анализировать обратную связь от клиентов при оставлении отзывов или различных реакций на, вычислять их предпочтения и предлагать персонализированные рекомендации.

Большое распространение нейросетевые технологии получили в искусстве. По подробному словесному описанию нейросеть может сгенерировать высококачественное изображение, которому не будет аналогов [12]. Некоторые исследователи используют нейросети для создания новых цветовых схем и текстур, которые могут быть использованы в живописи [13]. Многие художники начинают использовать нейросети в своей работе, чтобы ускорить и улучшить процесс создания цифрового искусства. Возможно применение нейросетей и в кинематографе [14]. С их помощью можно упростить процесс разработки компьютерной графики, создавать визуальные эффекты для фильмов, а также восстанавливать точные виртуальные копии актеров. Достаточно широк функционал нейросетей в части работы с музыкой: от создания музыкальных композиций до работы со звуком [15]. Например, нейросети Mubert и Soundraw позволяют создавать новые музыкальные произведения на основе сэмплирования и написания промпта. Нейросеть Humtap позволяет создавать музыкальное произведение на основе анализа напетого мотива.

Таким образом, можно сделать вывод, что нейросети уже сейчас внедряются во многие сферы жизни человека, а с развитием технологий, в том числе, искуственного интеллекта, перечень охватываемых ими областей станет только больше. Однако важно соблюдать баланс между применением технологий и человеческим подходом. Поэтому актуальной темой остаются этические и социальные вопросы, включающие в себя защиту персональных данных, предотвращение дискриминации и обеспечение прозрачности алгоритмов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Корченко М. Д. Способы применения нейросетей в энергетике // Вестник науки. - 2024. - №6 (75). – С. 14444-1448.

2. Митрофанов, Е. П. Влияние нейросетей на повседневную жизнедеятельность человека / Е. П. Митрофанов, К. М. Кадыкова //

Государство, экономика, бизнес: стратегия будущего в условиях санкционного давления : материалы IV Всероссийской научно-практической конференции, Москва, 30 марта 2023 года. – Москва: Московский государственный гуманитарно-экономический университет, 2023. – С. 53-56.

3. Ivanova A. A. Ineural networkas a breakthrough tool of medicine of future // International Journal of Professional Science. – 2024. - №6-2-2024.

4. Арбузова, А. А. Диагностика пневмонии по рентгеновским снимкам с помощью сверточных нейронных сетей / А. А. Арбузова // Модели, системы, сети в экономике, технике, природе и обществе. – 2021. – № 2(38). – С. 107-114.

5. Коффи, Э. Ф. А. Нейронные сети в сегментации десны / Э. Ф. А. Коффи // Инновационная наука. – 2023. – № 7-1. – С. 14-18.

6. Белов, К. С. На перекрестке технологий и медицины: перспективы автоматизации в медицинской практике с применением нейросетей / К. С. Белов, А. С. Харитонов, С. В. Чернова // Инфокоммуникационные технологии. – 2023. – Т. 21, № 4(84). – С. 89-93.

7. Щукин, К. К., Коршак, К. С. Применение искусственного интеллекта в управлении и моделировании технических систем // Наукоёмкие технологии и инновации (XXV научные чтения): сборник докладов Международной научно-практической конференции. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. — С. 762-765.

8. Истратий И.И., Митина Д.А., Курулёва У.Е. Использование искусственного интеллекта в ядерной энергетике // В сборнике: Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, Белгород: Изд-во БГТУ. – 2024. – С. 76-79.

9. D. Falk. How Artificial Intelligence Is Changing Science // Quanta magazine. – 2019.

10. Курбанова, З. С. Нейросети в контексте цифровизации образования и науки / З. С. Курбанова, Н. П. Исмаилова // Мир науки, культуры, образования. – 2023. – № 3(100). – С. 309-311.

11. Ледницкий, А. В. Роль нейросетей в цифровой экономике / А. В. Ледницкий, А. О. Бокус, А. А. Добрянский // Технологическая независимость и конкурентоспособность Союзного государства, стран СНГ, ЕАЭС и ШОС : сборник статей VI Международной научно-технической конференции "Минские научные чтения - 2023". - Минск: БГТУ, 2023. - Т. 1. – С. 274-278.

12. Ильинская Е. В., Голышева Е. Н., Медведев А. А., Масалитин Н. С. Применение генеративно-состязательных нейросетей для

генерации изображений // Научный результат. Информационные технологии. - 2024. - №1. – С. 73-78.

13. Коростелева, В. А. Конкуренция генеративных нейросетей и традиционного искусства / В. А. Коростелева // Современная наука: эксперимент и научная дискуссия : Сборник научных трудов по материалам XIII Международной научно-практической конференции, Анапа, 25 мая 2023 года. – Анапа: ООО "Научно-исследовательский центр экономических и социальных процессов" в Южном Федеральном округе, 2023. – С. 12-16.

14. Лавров, В. В. Реализация технологии нейронных сетей в современном кинематографе / В. В. Лавров // Векторы развития научно-практической деятельности на современном этапе : Материалы всероссийско научно-практической конференции с международным участием, Екатеринбург, 14 декабря 2022 года / Отв. редактор А.А. Зарайский. – Саратов: Общество с ограниченной ответственностью "Центр профессионального менеджмента "Академия Бизнеса", 2022. – С. 65-70.

15. Дубровский, В. В. Использование нейросетей в обучении музыке / В. В. Дубровский // Развитие креативности личности в современном цифровом мультикультурном пространстве : Сборник материалов XV Международной научно-практической конференции (к 150-летию ЕГУ им. И.А. Бунина), Елец, 18–19 апреля 2024 года. – Елец: Елецкий государственный университет им. И.А. Бунина, 2024. – С. 31-36.

***УДК 330***

***Лазарре А.***
***Научный руководитель: Рябов А.А. д-р экон. наук, проф.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ, ПРИМЕНЯЕМЫЕ В ИНФОРМАЦИОННЫХ ТЕРРИТОРИЯХ НА ПРЕДПРИЯТИИ

Интеллектуальные системы, применяемые в информационных технологиях в компании, — это инструменты и решения, основанные на передовых технологиях, которые позволяют организациям оптимизировать свои процессы, улучшить процесс принятия решений, автоматизировать задачи и повысить конкурентоспособность. Эти системы включают в себя такие концепции, как искусственный

интеллект, машинное обучение, Интернет вещей (IoT), автоматизация и управление большими данными для поддержки бизнес-функций, стратегии и управления ресурсами. Вот как интеллектуальные системы применяются в различных функциях компании:

1. Управление взаимоотношениями с клиентами

Интеллектуальные системы улучшают взаимодействие компании со своими клиентами и оптимизируют ее усилия в области маркетинга и продаж.

• Чат-боты и виртуальные помощники: интеграция интеллектуальных чат-ботов в веб-сайты или мобильные приложения позволяет взаимодействовать с клиентами в режиме реального времени, отвечая на их вопросы, обрабатывая запросы или оказывая поддержку. Эти системы могут учиться и совершенствоваться на основе прошлых взаимодействий и могут быть настроены для предоставления более релевантных ответов.

• Предиктивная аналитика и сегментация: С помощью систем предиктивной аналитики компании могут предугадывать потребности клиентов, определять сегменты рынка и персонализировать свои предложения. Например, системы могут анализировать прошлые покупательские привычки, чтобы рекомендовать конкретные продукты или услуги каждому клиенту.

2. Управление человеческими ресурсами

Интеллектуальные системы в области управления персоналом помогают автоматизировать процессы подбора персонала, управления талантами и контроля эффективности компании и каждого сотрудника.

•Автоматизированный подбор персонала с помощью ИИ: ИИ можно использовать для анализа резюме и сопроводительных писем, сортировки заявок на основе заранее определенных критериев и даже проведения видеоинтервью для оценки кандидатов на основе их ответов и приверженности компании.

•Управление эффективностью и развитие талантов: Интеллектуальные системы управления эффективностью могут отслеживать и анализировать прогресс сотрудников, проводить обучение, адаптированное к потребностям должности и задачи, а также прогнозировать продвижение по службе или возможности развития.

3. Управление цепочками поставок и логистикой

Интеллектуальные системы могут играть решающую роль в оптимизации цепочки поставок, снижении затрат и человеческого труда при одновременном повышении эффективности.

•Автоматизация и оптимизация запасов: предприятия используют интеллектуальные системы для мониторинга уровня запасов в режиме реального времени, прогнозирования будущих потребностей на основе спроса и автономной корректировки заказов. Это снижает затраты, связанные с перепроизводством или дефицитом.

•Профилактическое обслуживание: используя датчики IoT и алгоритмы машинного обучения, компании могут прогнозировать отказы оборудования или машин до того, как они произойдут. Это позволяет планировать техническое обслуживание и избежать дорогостоящих простоев производства.

•Оптимизация маршрутов: Логистические компании используют интеллектуальные системы для оптимизации маршрутов доставки в зависимости от условий движения, предпочтений клиентов и загрузки транспортных средств.

4. Финансовый менеджмент и бухгалтерский учет

Интеллектуальные системы также могут автоматизировать и оптимизировать финансовые процессы в компании.

•Автоматизация финансовых процессов: Роботизированная автоматизация процессов может использоваться для повторяющихся задач, основанных на правилах, таких как ввод данных, сверка счетов или управление счетами. Это снижает количество человеческих ошибок и освобождает время для выполнения более стратегических задач.

•Предиктивный финансовый анализ: инструменты финансового анализа на основе искусственного интеллекта могут прогнозировать экономические тенденции, оценивать будущие денежные потоки и предоставлять рекомендации по инвестициям и налоговым стратегиям.

5. Анализ данных и принятие стратегических решений

Одним из самых больших преимуществ интеллектуальных систем в информационных технологиях является их способность анализировать большие объемы данных для извлечения релевантных выводов, что помогает в принятии стратегических решений.

•Большие данные и предиктивная аналитика: Компании могут использовать такие технологии, как большие данные и алгоритмы предиктивной аналитики, для определения рыночных тенденций, поведения покупателей или аномалий в данных. Это позволяет принимать решения на основе фактов и прогнозов, а не догадок.

•Умные информационные панели: Интеллектуальные системы позволяют создавать динамические информационные панели, которые отображают ключевые показатели эффективности (KPI) компании в режиме реального времени. Эти панели мониторинга могут

предоставлять автоматические оповещения при значительных отклонениях от целей или ожиданий.

6. Маркетинг и персонализация клиентского опыта

Интеллектуальные системы используются для улучшения маркетинговых кампаний, персонализации клиентского опыта и увеличения конверсии.

•Таргетированная реклама и рекомендации: умные системы позволяют бизнесу персонализировать рекламные сообщения и акции на основе индивидуальных предпочтений клиентов. Например, платформы электронной коммерции используют алгоритмы искусственного интеллекта, чтобы рекомендовать товары, похожие на те, которые клиент уже купил или просмотрел. Онлайн-платформы для кино и видео, такие как OKKO, IVI, также используют искусственный интеллект, чтобы делать предложения о следующем фильме, который мы можем посмотреть в соответствии с нашим вкусом, анализируя наш прошлый выбор фильмов.

•Автоматизация маркетинга: Инструменты автоматизации маркетинга могут отправлять персонализированные сообщения по электронной почте, SMS или push-уведомлениям в стратегическое время, в зависимости от поведения пользователей. Это помогает повысить вовлеченность и максимизировать конверсию. Некоторые компании предлагают персонализированные скидки, чтобы побудить клиентов к покупке, например, ЯНДЕКС МАРКЕТ предлагает скидки в 1000 рублей на 3 000 рублей, купленных для клиента, который провел более 180 дней, ничего не заказывая на их платформе.

7. Улучшенный пользовательский опыт

Интеллектуальные системы также применяются для улучшения взаимодействия пользователей с цифровыми сервисами компании.

•Интеллектуальные пользовательские интерфейсы: интеграция голосовых помощников, распознавания лиц и адаптивных интерфейсов обеспечивает более интуитивно понятный и персонализированный пользовательский опыт. Например, веб-сайт может корректировать свой контент или рекомендации на основе прошлых взаимодействий пользователя.

Интеллектуальные системы, применяемые в информационных технологиях в компании, могут трансформировать бизнес-процессы, повысить эффективность организации и улучшить процесс принятия решений. Эти технологии способствуют снижению затрат, оптимизации ресурсов и повышению удовлетворенности клиентов. Они снижают нагрузку на сотрудников и оптимизируют процессы управления. Они

улучшают обработку информации, что делается гораздо быстрее, при этом снижается погрешность, вызванная человеческим фактором. Интегрируя системы на основе искусственного интеллекта, аналитики данных, автоматизации и Интернета вещей, компании лучше подготовлены к навигации во все более сложной и конкурентной среде. Однако внедрение этих систем требует инвестиций в технологии, обучение и безопасность данных. В заключение можно сказать, что то, что вы получаете в производительности, имеет свою цену.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Остроух А. В., Николаев А. Б., А. В., А. Б. Интеллектуальные информационные системы и технологии / А. В., А. Б. Остроух А. В., Николаев А. Б.. – Санкт-Петербург : 3, 2023. – 308 с. – ISBN 978-5-507-48511-6.
2. Шевко Н.Р., Гарипова Л.Р. Роль информационных технологий в системе управления предприятием // Современные научные исследования и инновации. 2020. № 4 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/04/91944 (дата обращения: 19.03.2025).
3. Medsker L.R. Hybrid Intelligent Systems. — Boston: Kluwer Academic Publishers, 2021. — 298 с.
4. Joao P. Carvalho, Hugo Rosa, Gaspar Brogueira, Fernando Batista. MISNIS: An intelligent platform for twitter topic mining (англ.) // Expert Systems with Applications. — 2017-12. — Vol. 89. — P. 374–388. — doi:10.1016/j.eswa.2017.08.001. Архивировано 25 февраля 2021 года.
5. Cavalcanti E.P., The Relationship between Business Intelligence and Business Success, Journal of Competitive Intelligence and Management., Vol.3, No.1,p.3-11. 2020.
6. “AI in Business: Transforming Information Systems and Processes” (Gartner Report) – Исследование, посвященное внедрению искусственного интеллекта в бизнес-процессы и информационные системы.

*УДК 004.9*

***Лапко Н.А.***
***Научный руководитель: Косоногова М.А., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ИНФОРМАЦИОННАЯ СИСТЕМА АНАЛИЗА ЛИЧНЫХ РАСХОДОВ С УЧЁТОМ ЭМОЦИОНАЛЬНОГО ФОНА ПОЛЬЗОВАТЕЛЯ

Современные цифровые инструменты прочно вошли в нашу повседневность, однако большинство из них сводит поведение человека к цифровым значениям. Особенно ярко это проявляется в сфере управления личными финансами, где пользователю предлагается лишь фиксировать траты, не принимая во внимание их психологическую составляющую.

В то же время финансовые решения — это не просто рациональный выбор, но часто и эмоциональная реакция. Человек тратит не только деньги — он переживает эмоции, чувствует. Поэтому ключевая гипотеза данной работы предполагает, что анализ расходов должен включать не только количественные, но и эмоциональные данные. Это позволит не просто понимать, куда уходят деньги, но и почему они уходят именно туда.

Разработка веб-ориентированной системы основана на интеграции двух областей — финансового контроля и эмоционального самоанализа. В процессе использования приложения пользователь при внесении данных о расходах указывает не только сумму и категорию, но и эмоциональную реакцию по шкале от 0 до 5 (рис. 1). Такая метка позволяет зафиксировать, сопровождалась ли покупка стрессом, удовлетворением, радостью или разочарованием.

Эта простая на первый взгляд процедура открывает возможность для глубокой интерпретации. Далее система анализирует паттерны: в каких категориях эмоции преимущественно негативны, какие покупки вызывают наибольшую радость, а какие — повторяющийся стресс. Полученная картина не только дополняет традиционные графики доходов и расходов, но и позволяет сформировать персонализированные рекомендации (рис. 2). Пример: если в категории «Развлечения» преобладает эмоция 1 — «лёгкое разочарование», система укажет на возможную неэффективность данных трат.

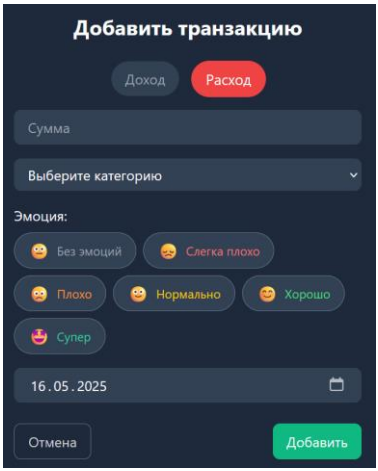



Рис. 3 Интерфейс ввода финансовой транзакции с выбором эмоциональной метки.

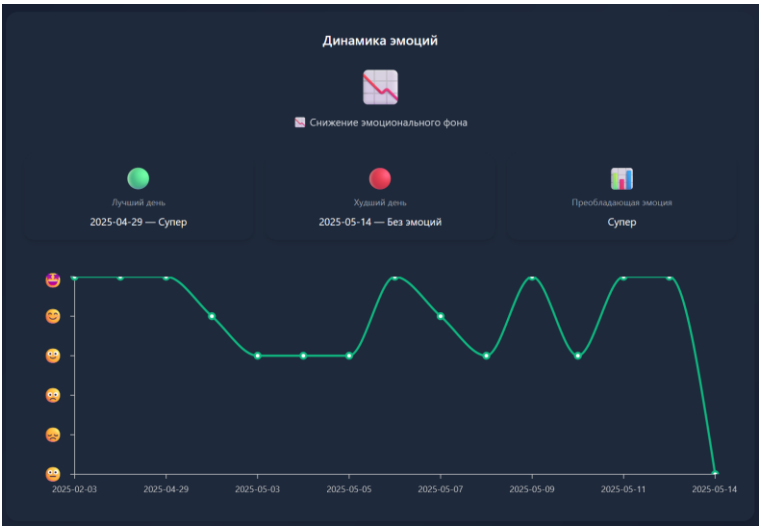



Рис. 4 Диаграмма распределения эмоциональных оценок по категориям расходов за период.

Аналитика базируется на ряде логических правил. Если пользователь регулярно испытывает стресс при тратах на транспорт или питание, система зафиксирует это как тревожный паттерн. При этом анализ ведётся не только на уровне отдельных транзакций, но и в

динамике: сервис вычисляет эмоциональный тренд — улучшение, ухудшение или стабильность фона.

Примеры аналитических выводов:

- «Эмоциональный фон ухудшился по сравнению с предыдущим месяцем»
- «В категории “Питание” преобладает негативная окраска расходов»
- «Ваш лучший день — 12 апреля. Эмоция: радость»

Сравнение проводится и на уровне бюджета. При срабатывании финансовых правил пользователь получает уведомления:

- «Ваши расходы превышают доходы. Стоит пересмотреть бюджет»
- «Нет накоплений — рекомендуется отложить хотя бы 10% от дохода»
- «Более 50% трат уходят на обязательные платежи — возможен риск перегрузки бюджета»

Особое внимание уделяется сравнению с предыдущим периодом. Например, если в марте пользователь чаще испытывал позитив, а в апреле — раздражение, система отобразит этот сдвиг и предложит пересмотреть финансовое поведение по категориям.

Это не просто трекер расходов, а инструмент саморефлексии. Он подсказывает не только «сколько потрачено», но и «почему». А значит — даёт возможность не только сэкономить, но и понять себя.

**Заключение.** Разработанная система анализа личных финансов с учётом эмоционального фона предлагает новый подход к интерпретации пользовательских расходов. Вместо традиционного акцента на числовые показатели, система учитывает субъективную эмоциональную реакцию на каждую трату, что позволяет получить более полное представление о финансовом поведении пользователя.

Разработанный сервис можно позиционировать как трекер расходов со встроенным инструментом саморефлексии: в пользовательском интерфейсе отображаются не только суммы и категории трат, но и результаты анализа их эмоциональной составляющей. Эффект от внедрения подобной системы может выражаться в снижении доли нерациональных расходов, повышении осознанности при совершении покупок и лучшем понимании собственных поведенческих финансовых паттернов.

Такой подход остаётся редкостью для отечественных решений, что позволяет рассматривать систему как пионерную разработку в направлении интеграции количественного и качественного анализа в сфере персональных финансов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Russell, J. A. A Circumplex Model of Affect // Journal of Personality and Social Psychology. 1980. [Электронный ресурс]. URL: http://pdodds.w3.uvm.edu (дата обращения: 21.05.2025). (дата обращения: 21.05.2025).
2. Emotional Intelligence Scales // PositivePsychology.com [Электронный ресурс]. URL: https://positivepsychology.com (дата обращения: 21.05.2025).
3. What Is the 50/30/20 Budget Rule? // Investopedia [Электронный ресурс]. URL: https://www.investopedia.com (дата обращения: 21.05.2025).
4. Коршак К.С. чат-боты и виртуальные ассистенты: как ии меняет клиентский сервис / К.С. Коршак, Фонова А.Ю. // В сб.: XVI Международный молодежный форум «Образование. Наука. Производство» [Электронный ресурс]: Белгород: БГТУ им. В.Г. Шухова, 2024. – Ч. 13. – С. 223–227.
5. Likert Scales in Emotion Assessment // PMC [Электронный ресурс]. URL: https://pmc.ncbi.nlm.nih.gov (дата обращения: 21.05.2025).



***УДК 004.9***



***Ляхова О.Р.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## РОЛЬ БИЗНЕС-АНАЛИТИКИ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОРГАНИЗАЦИЙ

Цифровые технологии буквально переворачивают все с ног на голову, поэтому компаниям приходится постоянно подстраиваться под новые реалии. Объемы данных внутри организаций растут с невероятной скоростью. Это требует не просто автоматизации, а выстраивания системного подхода к их обработке и анализу. Сегодня успех цифровой трансформации все чаще зависит от того, насколько быстро и эффективно организации переходят от интуитивного управления к принятию решений на основе объектных данных.

Бизнес-аналитика (БА) представляет собой не просто инструмент, а целую систему работы с данными: от их сбора и обработки до

детального анализа и наглядной визуализации. Ее главная задача – помочь руководителям принять взвешенное и обоснованное решение.

Цифровая трансформация, в свою очередь, гораздо более масштабное явление. Она подразумевает внедрение электронных технологий во все сферы деятельности организации. Это меняет бизнес-модели, перестраивает внутренние процессы и по-новому выстраивает взаимодействие с клиентами. И здесь БА выступает как незаменимый инструмент, который позволяет оценивать и эффективно управлять масштабными изменениями [1].

Для того, чтобы бизнес-аналитика действительно приносила пользу, нужно использовать разнообразные источники данных. Обычно их делят на две основные категории. Внутренние данные – это все, что собирается в рамках самой организации. Сюда относятся финансовые отчеты, информация о продажах, показатели производства, данные по логистике и другим процессам. Это те сведения, которые компания генерирует в ходе своей повседневной работы. Внешние данные – это информация, поступающая из вне. Например, это могут быть рыночные тендеры, поведение клиентов, результаты анализа конкурентов и другие факторы, которые влияют на бизнес, но собираются вне его стен.

Важно также учитывать, что данные бывают разного типа. Есть структурированные и неструктурированные. Первые легко представить в виде таблиц или баз данных (БД), а другие – это тексты, изображения, видео и другая информация, которую нельзя упорядочить. Для работы с такими типами нужны специальные методы и инструменты анализа.

Процесс БА представляет собой последовательную работу. Каждый этап имеет свою специфику для достижения достоверных результатов.

Первым шагом является сбор данных. На этом этапе информация поступает как из внутренних, так и из внешних источников. Это могут быть CRM- и ERP-системы, БД клиентов и даже открытые источники. Важно охватить максимально широкую среду, чтобы последующий анализ был объективным.

Затем следует очистка и подготовка данных. Этот этап, на мой взгляд, недооценивается, хотя именно он определяет качество будущего анализа. Необходимо избавиться от дубликатов, исправить очевидные ошибки, согласовать форматы и структуры данных. Даже небольшие расхождения могут привести к искаженным выводам.

После подготовки данные размещаются в специальных системах для хранения. Если речь идет о четко структурированной информации, то используется Data Warehouse. Data Lake выбирают, когда нужно сохранять данные в более гибком и разнородном виде.

Ключевым этапом является анализ данных. В зависимости от цели используются разные подходы:

– описательная аналитика помогает понять, что уже произошло;

– диагностическая – почему это случилось;

– предиктивная – что может произойти в будущем;

– прескриптивная – какие шаги стоит предпринять.

Вместе эти методы позволяют не просто описывать ситуацию, но и формировать конкретные управленческие рекомендации [2].

Завершается процесс визуализацией и представлением результатов. Даже самые точные расчеты теряют смысл, если их невозможно интерпретировать. Поэтому итог анализа оформляется в виде отчетов, графиков и даш-бордов. Это помогает облегчить принятие решений на всех уровнях.

Для реализации аналитических процессов применяются специализированные информационные системы. Выделим наиболее часто используемые решения. BI-системы – это инструменты для анализа и визуализации данных. Например, Яндекс DataLens, FineBI, Tableau и Power BI. CRM-системы, такие как amoCRM и Битрикс24, позволяют анализировать взаимодействие с клиентами, выявлять их предпочтения и формировать более точные портреты аудитории. Все это критично для принятия маркетинговых и продуктовых решений. EPR-системы – обеспечивает комплексное управление ресурсами предприятия. Интересно, что в условиях текущих санкций многие российские компании активно переходят с SAP на 1С, которая предлагает схожий функционал и соответствует всем требованиям РФ.

Интеграция таких систем позволяет получить по-настоящему полную картину бизнес-процессов и значительно повысить показатели эффективности.

БА давно вышла за рамки простого сбора данных. Она стала основой для принятия обоснованных решений. На стратегическом уровне аналитика помогает увидеть рыночные тренды и выстроить долгосрочные прогнозы. В оперативном управлении – улучшить логистику, оптимизировать запасы и персонализировать маркетинг. Кроме того, БА дает возможность выявлять слабые места, а также сокращать затраты и повышать удовлетворенность клиентов.

Несмотря на очевидные преимущества, большинство компаний сталкиваются с трудностями. Многие сотрудники просто не понимают, насколько важны данные. Остро ощущается нехватка квалифицированных аналитиков и специалистов по данным, а также есть внутреннее сопротивление изменениям. Для преодоления этих вызовов важно развивать корпоративную культуру, вкладываться в

обучение персонала и внедрять единые подходы к управлению данными [3].

В ближайшие годы аналитика станет еще более разумной и доступной. Искусственный интеллект и машинное обучение будут шире использоваться для автоматического анализа данных и построения прогнозов. Аналитические инструменты станут проще в использовании, позволяя работать с данными не только специалистам, но и сотрудникам других подразделений. Параллельно продолжит расти число отечественных решений.

Бизнес-аналитика давно стала неотъемлемой частью управленческих процессов. Роль БА в повышении эффективности, адаптации к изменениям и усилении конкурентных преимуществ будет только возрастать. Компании, которые активно используют аналитику, быстрее внедряют новые идеи, снижают издержки и точнее отвечают на запросы клиентам.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Медведева Т.И., Особенности управления трудовыми ресурсами в условиях цифровой трансформации бизнеса / Т.И. Медведева, Ю.И. Селиверстов // «Международная научно-техническая конференция молодых ученых бгту им. в.г. шухова, посвященная 300-летию российской академии наук» Сборник докладов Национальной конференции с международным участием. Том 17. Белгород: Изд-во Белгородский государственный технологический университет им. В.Г. Шухова, 2022. – С. 552 –557.

2. Четыре вида аналитики данных: дескриптивная, диагностическая, предиктивная, прескриптивная – Э. Режим доступа: https://habr.com (21.05.2025)

3. Аншина М.Л., Цифровая трансформация бизнеса / М.Л. Аншина, Б.Б. Славин, У. Терри // Учебное пособие. Москва: Изд-во КноРус, 2025. – 270 с.

*УДК 004.6*

***Ляхова О.Р.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ОПАСНОСТЬ OVERSHARING В ЦИФРОВОЙ СРЕДЕ

Современный ритм жизни прочно связан с социальными сетями. Ежедневно миллионы людей делятся в Интернете публикациями о своей работе, путешествиях или увлечениях. Для большинства это стало привычным, поэтому мы перестали воспринимать размещение личной информации в соцсетях как потенциальную угрозу. Хотя каждая фотография или отметка на карте может обернуться против нас.

Роскомнадзор подчеркивает, что неосторожное поведение в социальных сетях способно привести к утечке персональных данных, которые будут использованы мошенниками для атак, основанных на социальной инженерии [1]. Также рассмотрим исследование Pew Research Center. Оно указывает, что свыше 70% взрослого населения США активно пользуются интернет-платформами, но лишь немногие осознают масштабы цифровых рисков [2]. Подобные факты вызывают опасения. Ведь, все больше случаев, когда публично доступная информация используется злоумышленниками как основа для кибератак и вымогательств. В данной статье рассмотрим, что такое овершеринг и как себя обезопасить в Интернете.

**Основная часть.** Oversharing (овершеринг) (от англ. over – слишком и sharing – делиться) – чрезмерное распространение личной информации как в онлайне, так и в офлайне. Спектр таких данных достаточно большой. Например, дата рождения, семейное положение, фотография документов с посадочными билетами и так далее. Зачастую пользователи идут на это неосознанно. Людьми движет желание получить признание и укрепить связь с подписчиками. Коварство овершеринга заключается в том, что разрозненные крупицы информации, собранные воедино, могу стать отправной точкой для злонамеренных действий. На практике это значит, что дата рождения может быть ключом к восстановлению доступа аккаунта.

По мнению экспертов ENISA (Агентства Европейского союза по кибербезопасности), публикация в социальных сетях формируют своего рода цифровой «след». А он поддается детальному анализу с помощью различных инструментов. Компания «Лаборатория Касперского» также

указывает на oversharing как на одну из ключевых причин роста кибермошенничества [3].

Для предварительного сбора данных о потенциальных жертвах злоумышленники используют OSINT-инструменты. OSINT (Open Source Intelligence) – разведка на основе открытых источников. Она включает сбор, анализ и интерпретацию данных, которые свободно доступны в медиа, социальных сетях, государственных реестрах и так далее. Буквально все, что попадает в сеть, может быть тщательно изучено и использовано для организации фишинговых атак, шантажа или несанкционированного доступа.

Об этом убедительно пишет Кевин Митник в своей книге «Искусство обмана». Он демонстрирует как киберпреступники, обладая информацией из социальных сетей, способны манипулировать людьми, склоняя их к разглашению конфиденциальных сведений [4]. Сценарии атак на основе социальной инженерии подробно описаны на платформе OWASP. Один из типичных примеров – подделка письма [5]. Представим ситуацию, пользователь с энтузиазмом сообщает в соцсетях, что сегодня его первый рабочий день в «ИТ-компании». Злоумышленник сразу может воспользоваться данной информацией. Он направляет на электронную почту пользователя поддельное письмо, имитирующее сообщение от отдела компании. В нем его срочно просят подтвердить личность. Для этого нужно зайти на госуслуги или ввести личную информацию. Очень часто пользователи не замечают подделки и таким образом теряют свои персональные данные.

В процессе изучения поведения человека в Интернете было выявлено, что oversharing редко существует сам. Пользователи часто совершают ряд небезопасных действий в сети, таких как:

– использование одного и того же пароля на различных сайтах;

– отсутствие двухфакторной аутентификации (2FA);

– незащищенные аккаунты без настройки приватности;

– публикация номеров телефонов, карт или документов в открытом доступе.

Люди пренебрегает базовыми мерами безопасности. Из-за этого они сами невольно создают условия, в которых овершеринг продолжает процветать.

Например, в отчетах Google, включение 2FA снижает вероятность взлома аккаунта почти на 50% [6]. ФСТЭК России также настоятельно рекомендует ограничивать публикацию личной информации и применять шифрование при передаче данных [7].

Практика показывает, что oversharing может иметь болезненные последствия. Для наглядности рассмотрим несколько примеров.

Один из самых масштабных инцидентов утечки данных затронул более 700 миллионов пользователей Linkedln. Хотя данные были формально открыты, но их систематизация позволила хакерам провести масштабные фишинговые кампании.

Публикация посадочных талонов. Пользователи нередко выкладывают фотографии билетов, не подозревая, что QR-код содержит конфиденциальные данные, например паспорт и детали маршрута. Эти сведения открывают новые возможности для целевого фишинга.

Полезным инструментом для оценки потенциальных рисков может стать https://chk.safe-surf.ru . Данный сайт является Российским и на нем можно проверить не являются ли логин, электронная почта или телефон скомпрометированными. Это важно для того, чтобы вовремя себя обезопасить [8].

На основании проведенного анализа можно выявить целый ряд как технических, так и поведенческих мер, которые позволяют минимизировать угрозы, связанные с oversharing:

– обязательно используйте двухфакторную аутентификацию на всех доступных сервисах;

– применяйте VPN при подключении к общественным сетям;

– регулярно меняйте и усложняйте пароли;

– устанавливайте и своевременно обновляйте антивирусное программное обеспечение.

Важна и цифровая гигиена – осознанное поведение в интернете. Воздержитесь от публикации точных дат рождения, сканов документов, билетов на транспорт и информации о месте проживания. Используйте трудно отгадываемые ответы на контрольные вопросы. Также рекомендуется ограничить круг лиц, которые имеют доступ к личным публикациям, и не открывать подозрительные ссылки [9].

«Лаборатория Касперского» советует придерживаться десяти правил цифровой безопасности. Они включают принцип «прежде, чем опубликовать – трижды подумай».

Oversharing – это не просто безобидная привычка современного интернет-пользователя, а серьезная угроза, которая может иметь далеко идущие последствия. Рост цифровой грамотности напрямую влияет на снижение рисков утечки персональных данных. Если раньше вопросы кибербезопасности касались преимущественно ИТ-отделов, то сегодня это общая ответственность. Каждый пользователь должен понимать, что безопасность – это не просто функция программ, а часть повседневного поведения в сети.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рекомендации Роскомнадзора операторам персональных данных – Э. Режим доступа: https://rkn.gov.ru (18.05.2025)
2. Social Media Use in 2021 – Э. Режим доступа: https://www.pewresearch.org (18.05.2025)
3. Евгений Касперский рассказал о стратегиях защиты от кибератак – Э. Режим доступа: https://os.kaspersky.ru (18.05.2025)
4. Что такое OWASP? Что такое OWASP Top-10? – Э. Режим доступа: https://wiki.merionet.ru (19.05.2025)
5. Кевин Митник - Искусство обмана – Э. Режим доступа: https://libcat.ru (19.05.2025)
6. Google account hacks dropped by half after pushing two-step authentication by default – Э. Режим доступа: https://www.theverge.com (19.05.2025)
7. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 – Э. Режим доступа: https://fstec.ru (19.05.2025)
8. В России создали сайт для проверки утечек пользовательских данных – Э. Режим доступа: https://hi-tech.mail.ru (19.05.2025)
9. Коломыцева Е.П., методы защиты персональных данных в эпоху цифровизации / Е.П. Коломыцева, И.В. Сиротин, К.С. Коршак // Сборник докладов Международной научно-практической конференции «наукоемкие технологии и инновации (xxv научные чтения)». Белгород: Изд-во Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717 – 720.



***УДК 004.9***



***Ляхова О.Р.***
***Научный руководитель: Хорошун Н.А., канд. соц. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## СОЦИАЛЬНЫЕ АСПЕКТЫ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ: СОПРОТИВЛЕНИЕ ПЕРСОНАЛА И СТРАТЕГИИ АДАПТАЦИИ

По моим наблюдениям, неоднократно было замечено, что, несмотря на техническую и организационную подготовку, внедрение информационных систем (ИС) сопровождается значительными трудностями именно на социальном уровне. Данное наблюдение находит свое подтверждение в ряде исследований. Они подчеркивают

первостепенную роль человеческого фактора в определении успеха или неудачи процессов цифровой трансформации [1]. В данной статье рассмотрим причины сопротивлений и стратегии адаптации, направленные на минимизацию негативных последствий.

На основе анализа литературы был сделан вывод, что сопротивление со стороны сотрудников может быть вызвано целым рядом факторов. Каждый из них требует отдельного внимания со стороны менеджмента и социологии.

Во-первых, страх перед неизвестным является первоначальным источником. Большинство сотрудников воспринимают новые технологии как угрозу для своей дальнейшей деятельности. Они опасаются автоматизации задач, потери контроля над привычными рабочими операциями и даже возможности сокращения штата [2].

Во-вторых, психологический дискомфорт вызывают изменения в устоявшихся производственных и административных процессах. Особенно это заметно в организациях, где рабочие практики формировались годами. Любое отклонение от привычного вызывает напряжение. Оно может проявляться в виде пассивного или активного сопротивления.

В-третьих, существенное влияние оказывает уровень доверия к руководству компании. Когда цели внедрения ИС доносятся до сотрудников нечетко, а сам процесс изменений окутан излишней закрытостью, то у персонала формируется ощущение, что основные решения принимаются без учета их мнения и вразрез с их интересами.

Наконец, нельзя игнорировать проблему недостаточного уровня цифровой грамотности у части сотрудников. Это актуально для работников старшего поколения, чья предыдущая деятельность не была тесно связана с ИТ-технологиями. В таких случаях неуверенность в собственных силах или страх оказаться некомпетентным становятся барьерами к принятию новой системы [3].

Выделяют несколько типов сопротивления:

–открытое сопротивление, которое может выражаться в форме протестов, письменных жалоб, отказов от участия в обучении или даже в решении покинуть компанию;

–скрытое сопротивление, когда сотрудники формально выполняют свои обязанности, но при этом демонстрирует снижение инициативы, игнорируют новые инструкции или неохотно используют возможности ИС;

–психологическое противодействие, проявляется в виде апатии, снижения уровня мотивации, повышенной тревожности и общего отчуждения от происходящего в организации изменений.

Все эти формы требует индивидуального подхода. Так как даже «молчаливое» сопротивление способно замедлить внедрение ИС.

Для эффективной адаптации коллектива к изменениям, по моим наблюдения, наибольшую результативность показывают следующие стратегии.

***Обеспечение максимальной прозрачности и активное вовлечение персонала.*** Одной из задач менеджмента является формирование атмосферы открытости и доверия. Практика показывает, что чем более детально сотрудники осведомлены о целях и этапах внедрения ИС, тем меньше вероятности появления домыслов, слухов и тревог. Также повысится вовлеченность сотрудников, если они смогут учувствовать в обсуждениях реализации ИС.

***Разработка персонализированных программ обучения.*** Оно должно быть не только обязательным, но и адаптированным к уровню подготовки различных групп сотрудников. Практические занятия и анализ рабочих ситуация сделают процесс освоения ИС более понятным и мотивирующим. Также важны повторные треннинги. Доступ к справочным материалам должен быть доступен в течение нескольких месяцев после начала внедрения.

***Обеспечение непрерывной поддержки.*** В период значительных организационных изменений сотрудники чрезвычайно нуждаются в технической и эмоциональной помощи. Значительный эффект дают организация внутренних каналов связи и система наставничества. Каждый сотрудник должен знать к кому он может обратиться за помощью и что его вопросы будут рассмотрены и решены в кратчайшие сроки.

***Внедрение продуманной системы поощрения.*** Позитивное стимулирование играет не менее важную роль. Необходимо поощрять сотрудников, которые проявляют инициативу, предлагают улучшения или быстро осваивают новые функции. При этом важны материальные (бонусы, премии) и нематериальные стимулы (благодарность, признание и т.п.) [4].

Успешная интеграция ИС невозможна без глубокого понимания социальных аспектов. Игнорирование причин сопротивления может замедлить процесс цифровой трансформации. В то же время грамотно выстроенная стратегия адаптации, включающая коммуникацию, обучение, поддержку и стимулирование способна минимизировать негативные последствия. Технологическая модернизация обретает устойчивость лишь, когда она сопровождается организационной зрелостью и вниманием к человеческому фактору.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Власова Е.Ф., Проблемы социальной адаптации новых работников современной организации // Социальные проблемы современного российского общества: региональный аспект. Материалы Всероссийской конференции «XVII Уральские социологические чтения». Екатеринбург, 2008. – С. 42 – 48.
2. Хорошун Н.А., Современные тенденции в управлении персоналом / Н.А. Хорошун, А.И. Матвиевский // наукоемкие технологии и инновации (xxv научные чтения) Сборник докладов Международной научно-практической конференции. Белгород: Изд-во БГТУ им. В.Г. Шухова, 2023. – С. 1647 – 1655.
3. Нарваткина Н.С., Внедрение информационных систем: организационные изменения // Учебное пособие. Екатеринбург: Изд-во РГППУ, 2019. – 94 с.
4. Механизм преодоления сопротивления персоналом внедрению инноваций на основе холонических принципов – Э. Режим доступа: https://1economic.ru (13.05.2025)



***УДК 004.6***



***Ляхова О.Р.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ФИШИНГ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: СОВРЕМЕННЫЕ УГРОЗЫ И ПРОТИВОДЕЙСТВИЯ

Цифровые технологии проникают практически во все сферы жизни, поэтому особую значимость приобрели персональные данные. Они помогают нам удобно пользоваться онлайн-сервисами, но при этом также становятся объектами интереса со стороны киберпреступников. Стабильно растет количество утечек данных в сеть. Рассмотрим механизмы кражи и способы защиты персональных данных.

Согласно Федеральному закону РФ «О персональных данных» от 27.07.2006 №152-ФЗ, персональные данные (ПДн) – это любая информация, по которой можно прямо или косвенно идентифицировать человека. К таким сведениям относятся ФИО, дата рождения, адрес,

паспортные сведения и т.д. Основные разновидности ПДн: общие, биометрические, общедоступные персонифицированные данные, обезличенные и специальные персональные данные [1]. В странах Европейского союза действует аналогичный подход, закрепленный в Общем регламенте по защите данных (GDPR) [2].

ПДн при попадании в руки злоумышленников могут использоваться для различных форм мошенничества. Одним из самых распространенных способов хищения информации остается фишинг (от англ. phishing «выуживание»). Он основан на психологическом воздействии. Мошенники маскируются под представителей надежных организаций – банков, госучреждений, сервисов доставки и т.п. А затем, с помощью правдоподобных сообщений вынуждают человека раскрыть логины, пароли или коды подтверждения. Фишинг принимает разные формы. Наиболее распространенный – это email-фишинг. На электронную почту приходит письмо, имитирующее официальный запрос. Получателя просят перейти по ссылке и ввести данные на сайте, который внешне неотличим от настоящего. Смишинг (SMS-фишинг) работает по аналогичной схеме только через текстовые сообщения. Вишинг (англ. vishing) – голосовой фишинг осуществляется по телефону. Злоумышленник представляется, например, сотрудником компании Почта России и убеждает сообщить персональные данные для получения письма, которые в дальнейшем будут украдены и использованы против вас. Также используются фальшивые аккаунты в социальных сетях и мессенджерах.

Обман может быть весьма убедительным. Зачастую достаточно заменить одну букву в доменном имени, чтобы создать почти неотличимый сайт. Некоторые схемы включают вредоносные скрипты, обход фильтров и другие методы социальной инженерии. Например, при пре-текстинге создается правдивая легенда, которая заставит пользователя добровольно раскрыть информацию. А бейтинг предлагает получить любую вещь «бесплатно» или «выгодное» предложение, которое оказывается ловушкой. Хакер может попросить вас создавать аккаунт или сразу загрузит вредоносный файл. Спирфишинг – это адресная атака, которая тщательно спланирована под конкретного человека или организацию. Есть еще фарминг. В этом случае пользователь может быть перенаправлен на поддельный сайт без своего ведома, например, из-за взлома DNS-сервера [3].

Последствия атак могут быть серьезными. Если мошенники получат доступ к ПДн, то это может привести к финансовым потерям, шантажу, репутационным рискам и новым атакам. Важно комплексно защищать персональные данные. Для этого с технической стороны

нужно использовать двухфакторную аутентификацию, шифрование данных, антифишинговые фильтры и системы предотвращения утечек. Но эти методы не заменят внимательность самих пользователей. Люди должны уметь распознавать подозрительные письма, не переходить по сомнительным ссылкам и не сообщать личные данные незнакомцам. Для того, чтобы улучшить такие навыки нужно регулярно проходить образовательные тренинги по кибербезопасности, особенно в корпоративной среде [4].

Важно также контролировать это и с правовой стороны. В России соблюдение конфиденциальности ПДн регулируется вышеупомянутым законом №152-ФЗ. За его нарушение предусмотрены меры административной и уголовной ответственности (например, по статье 159.6 УК РФ). В странах ЕС по регламенту GDPR требуется от компаний оперативно сообщать о любых утечках. Он предусматривает крупные штрафы за несоблюдение требований. Это подчеркивает важность соблюдения стандартов безопасности не только на уровне отдельных пользователей, но и в масштабах организаций.

Рассмотрим на примере борьбу с фишингом в реальности. В 2024 году телекоммуникационная компания «МегаФон» интегрировала собственную платформу. Она предназначена для противодействия фишингу с системой мониторинга Министерства цифрового развития РФ. В рамках этого сотрудничества в январе 2024 года удалось выявить и направить на блокировку свыше 6,7 тысяч мошеннических интернет-ресурсов. Такой результат стал возможен благодаря применению алгоритмов. Они ежедневно анализируют более миллиона веб-сайтов. Информация об подозрительных ресурсах сразу передается в научно-исследовательский институт «Интеграл». Там принимается решение о последующей блокировке. Их совместная работа помогла укрепить цифровую безопасность в стране [5].

Фишинг вышел за рамки простого технического инструмента, став изощренным психологическим оружием в арсенале киберпреступников. Современная социальная инженерия делает эти атаки все более коварными. Только благодаря ответственному цифровому поведению и сильной правовой защиты возможно сохранить персональные данные в условиях стремительной цифровизации.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) – Э. Режим доступа: https://www.consultant.ru (10.05.2025)
2. Общий регламент защиты персональных данных (GDPR) Европейского союза – Э. Режим доступа: https://gdpr-text.com (10.05.2025)
3. Спам и фишинг в 2024 году – Э. Режим доступа: https://securelist.ru (11.05.2025)
4. Коломыцева Е.П., Методы защиты персональных данных в эпоху цифровизации / Е.П. Коломыцева, И.В. Сиротин, К.С. Коршак // Сборник докладов Международной научно-практической конференции «наукоемкие технологии и инновации (xxv научные чтения)». Белгород: Изд-во Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717 – 720.
5. «МегаФон» поможет Минцифры бороться с фишингом и утечками персональных данных – Э. Режим доступа: https://www.cnews.ru (12.05.2025)



***УДК 004.04***



***Ляхова О.Р.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## BI-СИСТЕМЫ, ДОСТУПНЫЕ В РФ В 2025 ГОДУ: СРАВНЕНИЕ ЯНДЕКС DATALENS, FINEBI И ANALYTICA BY ФОРС

В эпоху стремительных цифровых перемен, системы бизнес-аналитики (BI) превратились в незаменимый инструмент, который помогает компаниям принимать более взвешенные решения и укреплять свои позиции на рынке. Они позволяют нам собирать, обрабатывать и наглядно представлять данные из самых разных источников. Это обеспечивает всесторонний анализ, который, в свою очередь, является прочной основой для выработки стратегий и эффективного управления. Сегодня интеграции BI-решений с облачными технологиями и искусственным интеллектом создают новые возможности. Но в последние годы российские компании столкнулись

с ощутимыми сложностями при работе с популярными западными BI-платформами, такими как Microsoft Power BI, Looker и Tableau. Эти трудности связаны с санкционными и политическими решениями. Из-за этого возникла насущная необходимость в поиске отечественных или альтернативных зарубежных решений, способных полностью удовлетворить запросы российского рынка. Цель данной статьи – провести всесторонний сравнительный анализ трех BI-систем. Они должны быть актуальными и доступными на рынке РФ в 2025 году.

Рассмотрим некоторые BI-системы. Яндекс Datalens – это облачная BI-платформа, задуманная как бесплатный и удобный инструмент для визуализации и анализа данных. Она разработана в России. Данная система легко подключается к разнообразным источникам данных, включая такие популярные СУБД, как PostgreSQL и ClickHouse. Это делает ее привлекательной для компаний, которые активно используют современные облачные решения. Datalens предлагает понятный интерфейс. Он позволяет создавать интерактивные дашборды и эффективно работать с аналитическими материалами в команде [1]. Интеграция с сервисами Яндекс Облако добавляет удобства при развертывании и масштабировании решений, а также ускоряет процесс внедрения. Бесплатный тариф особенно интересен для малого и среднего бизнеса. Тем не менее стоит учитывать, что облачная архитектура может быть ограничением для организаций с повышенными требованиями к безопасности и изоляции данных [2].

Рассмотрим китайскую разработку компании FanRuan. Важное преимущество FineBI – возможность локальной установки. Это критически важно для компаний, желающих полностью контролировать свою ИТ-инфраструктуру и соблюдать регуляторные нормы. Интерфейс поддерживает drag-and-drop, что облегчает работу с отчетами без глубоких технических навыков. FineBI обеспечивает интеграцию с различными источниками данных, например Exel. SQL-серверы, API. Также она обладает гибкими настройками безопасности и прав доступа. С другой стороны, неполная русификация и отсутствие официального представительства в России. Эти факторы могут создавать трудности при внедрении и получении технической поддержки [3].

Analytica by ФОРС – российская BI-платформа, созданная для решения сложных задач корпоративной аналитики, особенно в государственном секторе и крупном бизнесе. Она поддерживает сложное моделирование и прогнозирование. Analytica by ФОРС соответствует всем современным требованиям безопасности и национальным стандартам, включая стандарты ГОСТ и Федеральный

закон №152-ФЗ «О персональных данных». Простое внедрение в уже работающую ИТ-инфраструктуру. Ведь, платформа легко интегрируется с существующими корпоративными базами данных через готовые коннекторы. Несмотря на более высокую стоимость, Analytica обеспечивает высокий уровень безопасности и мощный аналитический функционал. Это делает ее предпочтительным выбором для крупных организаций [4].

При сравнительном анализе ключевых параметров работы и внедрения BI-систем были выделены несколько критериев, которые отражают текущие потребности российских предприятий.

Во-первых, различается тип развертывания систем. Яндекс Datalens – это исключительно облачное решение, что означает удобство и скорость развертывания без необходимости в собственной локальной инфраструктуре. Это ценно для малого и среднего бизнеса из-за ограничений на ресурсы ИТ-поддержки. А локальные установки Analytica by ФОРС и FineBI больше подходят для организаций с повышенными требованиями к информационной безопасности. Обычно в таких компаниях данные не могут храниться в облаке по регуляторным причинам.

Что касается безопасности, Analytica by ФОРС демонстрирует высочайший уровень соответствия национальным требованиям. Это подтверждается соответствующими сертификатами и официальной поддержкой. Яндекс Datalens, хотя и работает в рамках российского облака, не предоставляет таких же гарантий, что может ограничивать ее использование в государственных учреждениях. FineBI, будучи иностранным продуктом, требует дополнительного аудита безопасности. А также учета потенциальных рисков, связанных с отсутствием локального представительства и ограниченной поддержкой русскоязычной документации.

С точки зрения архитектурных особенностей, Яндекс Datalens – это SaaS-решение с масштабируемостью и минимальными требованиями к пользователю. FineBI и Analytica by ФОРС, напротив, нуждаются в более серьезном техническом сопровождении и ресурсах для настройки серверов и обеспечения стабильной работы.

Все три платформы поддерживают популярные базы данных. В этот список входят PostgreSQL, MySQL, SQL Server, а также работа с файлами CSV. Яндекс Datalens лучше интегрируется с облачными источниками данных. Analytica же специализируется на работе с крупными корпоративными хранилищами, такими как Oracle. Это отвечает запросам крупных предприятий. FineBI предлагает

универсальный набор коннекторов для гибкой интеграции, но здесь возможны ограничения по локализации.

Стоимость и лицензирование – еще один важный критерий выбора. Яндекс Datalens предлагает бесплатный базовый функционал, что значительно снижает порог входа для малого бизнеса и стартапов. FineBI требует покупки коммерческой лицензии. Analytica by ФОРС, как правило, реализуется по индивидуальным контрактам с крупными клиентами. Получается более высокая стоимость, но при этом обеспечивается полный комплекс услуг и поддержки.

Интерфейс и локализация играют большую роль в удобстве использования систем. Datalens и Analytica полностью на русском языке. Будет проще обучать и внедрять. FineBI не имеет полной русификации интерфейса. Из-за этого могут возникнуть трудности у пользователей без достаточного знания английского или китайского языка.

Поддержка и обучение – еще один не мало важный аспект. Datalens предлагает обширную онлайн-базу знаний и регулярные вебинары на русском языке. Analytica by ФОРС дополнительно предоставляет индивидуальное обучение и консультирование. FineBI в этом плане уступает из-за отсутствия официальной технической поддержки в России.

Итоговый выбор BI-систем должен основываться на масштабах компании, специфике отрасли, требованиях к безопасности и, конечно, бюджете. Яндекс Datalens выгодно отличается своей доступностью и простотой использования в облачной среде. Это подойдет малому и среднему бизнесу, стремящемуся к быстрому внедрению и минимальным затратам. Компании, которым нужна локальная установка и гибкость настроек, могут присмотреться к FineBI, если готовы решать вопросы локализации и поддержки. Для крупных корпораций и государственных учреждений предпочтение стоит отдать Analytica by ФОРС. Ведь, для таких компаний приоритетом являются безопасность, соответствие нормативам и глубокая аналитика.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Yandex DataLens – обзор BI-системы от Яндекса – Э. Режим доступа: https://onespot.one (20.05.2025)

2. Ляхова О.Р., облачные технологии: плюсы и минусы использования / О.Р. Ляхова, Е.П. Коломыцева // образование. наука. производство. Сборник докладов XV Международного молодежного

форума. Белгород: Изд-во Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 209 – 214.
3. Обзор преимуществ аналитической системы Fine BI – Э. Режим доступа: https://www.in-aim.ru (20.05.2025)
4. Форс. Аналитика. – Э. Режим доступа: https://www.fors.ru (20.05.2025)

***УДК 004.9:37.041***

***Манькова Ю.В.***
***Научный руководитель: Семенова В.Н., канд. физ.-мат. наук, доц.***
*Димитровградский инженерно-технологический институт*
*г. Дмитровград, Россия*

## МЕТОДЫ И ПОДХОДЫ К РАЗРАБОТКЕ АДАПТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ НА ОСНОВЕ АНАЛИЗА ДАННЫХ

Современная система образования сталкивается с необходимостью перехода от традиционных, стандартизированных подходов к персонализированным моделям обучения. Это обусловлено растущим разнообразием образовательных потребностей, различиями в когнитивных способностях учащихся и стремительным развитием цифровых технологий. Одним из ключевых инструментов, способных обеспечить гибкость и индивидуальную направленность обучения, являются адаптивные образовательные программы (АОП), построенные на основе анализа данных.

Целью данной работы является систематизация методов и подходов к разработке адаптивных образовательных программ, использующих технологии анализа данных для персонализации учебного процесса.

Основные задачи исследования:

1. Анализ теоретических основ адаптивного обучения и его взаимосвязи с образовательной аналитикой.
2. Изучение современных методов обработки данных, применяемых в адаптивных системах.
3. Рассмотрение практических подходов к проектированию АОП, включая архитектурные решения и примеры успешных реализаций.
4. Выявление ключевых проблем и перспектив развития адаптивных образовательных технологий.

Актуальность темы обусловлена тем, что, несмотря на активное внедрение цифровых образовательных платформ, многие из них

остаются статичными и не учитывают индивидуальные особенности учащихся в полной мере. Адаптивные системы, основанные на данных, способны не только повысить эффективность обучения, но и снизить уровень когнитивной нагрузки, обеспечивая оптимальный темп освоения материала [1].

Адаптивные образовательные программы представляют собой динамические системы, способные изменять структуру и содержание учебного материала в зависимости от прогресса, уровня подготовки и психологических характеристик обучающегося. В отличие от традиционных линейных курсов, АОП используют алгоритмы, которые непрерывно анализируют данные о взаимодействии пользователя с платформой и на этой основе корректируют образовательную траекторию [2].

Основополагающим принципом таких систем является персонализация, которая реализуется через несколько механизмов:

1. Динамическая оценка знаний (система определяет сильные и слабые стороны учащегося, предлагая соответствующие задания).
2. Гибкость подачи материала (контент адаптируется под предпочтительный стиль обучения: визуальный, аудиальный, кинестетический).
3. Прогнозирование трудностей (система предугадывает, какие темы могут вызвать затруднения, заранее предлагая дополнительные ресурсы).

Эффективность адаптивных систем напрямую зависит от качества и глубины анализа образовательных данных. В современных платформах используются поведенческие, академические и контекстуальные данные. Каждый тип данных отвечает за сбор различной информации: поведенческий анализирует время, затраченное на выполнение заданий, частоту обращений к подсказкам, последовательность изучения тем; академический направлен на результаты тестов, оценки, выполненные проекты; контекстуальный преподносит информацию о предпочтениях учащегося, используемых устройствах, уровне вовлеченности.

Обработка этих данных позволяет выявлять закономерности, которые невозможно обнаружить при традиционном обучении. Например, анализ временных меток может показать, что студент лучше усваивает материал в вечернее время, а значит, систему можно настроить на выдачу сложных заданий именно в этот период.

Образовательная аналитика играет ключевую роль в создании адаптивных программ. Она включает в себя сбор, обработку и интерпретацию данных с целью оптимизации учебного процесса.

Одним из перспективных направлений является применение методов машинного обучения для автоматической настройки образовательных траекторий [3].

Например, алгоритмы кластеризации позволяют группировать учащихся с похожими характеристиками, что помогает разрабатывать типовые, но при этом персонализированные сценарии обучения. Методы классификации, такие как деревья решений или нейронные сети, могут прогнозировать успешность освоения той или иной темы, а рекомендательные системы – подбирать наиболее релевантные учебные материалы.

Помимо технических аспектов, важное значение имеют когнитивные теории, объясняющие, как человек усваивает информацию. Теория когнитивной нагрузки утверждает, что эффективное обучение возможно только при оптимальном распределении умственных ресурсов [4]. Адаптивные системы могут регулировать сложность заданий, чтобы избежать перегрузки.

Другим важным фактором является учет форм обучения. Некоторые учащиеся лучше воспринимают визуальную информацию, другие – текстовую или практические примеры. Современные АОП способны автоматически определять предпочтения пользователя и адаптировать формат контента.

Типичная архитектура системы адаптивного обучения включает несколько уровней:

1. Уровень сбора данных (взаимодействие с LMS, датчиками активности, внешними образовательными ресурсами).
2. Уровень аналитики (обработка данных с использованием статистических методов и алгоритмов искусственного интеллекта).
3. Уровень адаптации (генерация персонализированных рекомендаций и корректировка учебного плана).
4. Пользовательский интерфейс (визуализация данных и интуитивное взаимодействие с системой).

Среди наиболее успешных кейсов внедрения можно выделить «Moodle» и «Stepik». Благодаря информационной системе «Moodle» преподаватели могут загружать лекции, задания, тесты и дополнительные материалы, а студенты, в свою очередь, могут сдавать работы в различных форматах (текст, листинг, файлы). Помимо этого, система предоставляется автоматическую проверку тестов и программируемых заданий (через плагины) или же ручное оценивание с обратной связью. Вторая платформа предлагает интерактивные курсы с автоматической проверкой заданий, в том числе имеется возможность создавать свои курсы и задания.

Несмотря на потенциал адаптивных систем, их внедрение сталкивается с рядом вызовов. Вопросы конфиденциальности данных требуют строгого регулирования, особенно в свете таких нормативных актов, как GDPR. Кроме того, существует риск алгоритмической предвзятости, когда система непреднамеренно дискриминирует определенные группы учащихся из-за недостаточно репрезентативных данных.

Перспективными направлениями развития адаптивных образовательных систем являются интеграция с технологиями виртуальной и дополненной реальности для создания обучающих сред, позволяющих моделировать сложные практические ситуации; активное использование больших языковых моделей (LLM) для динамической генерации персонализированного учебного контента, адаптирующегося под индивидуальные запросы учащихся; а также развитие нейрообразовательных технологий, основанных на анализе биометрических показателей (уровень стресса, когнитивная нагрузка, концентрация внимания), что позволит создавать оптимальные условия для усвоения материала с учетом психофизиологического состояния обучающегося.

В итоге, разработка адаптивных образовательных программ на основе анализа данных открывает новые возможности для персонализации обучения. Сочетание образовательной аналитики, машинного обучения и когнитивных теорий позволяет создавать системы, которые не просто предоставляют контент, а динамически подстраиваются под нужды каждого учащегося. Однако для широкого внедрения таких технологий необходимо решить вопросы этики, прозрачности алгоритмов и обеспечения равного доступа к образованию. Дальнейшие исследования в этой области будут способствовать созданию более интеллектуальных и человеко-ориентированных образовательных систем.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Алферьева, А. А. Искусственный интеллект в образовании: как адаптивное обучение и цифровые ассистенты меняют подход к обучению и воспитанию подростков [Текст] / А. А. Алферьева // Вестник науки. – 2025. – № 1 (82). – С. 111-119.

2. Ефремова Н. Ф. Персонализация образовательной деятельности и оценки достижений обучающихся [Текст] / Ефремова Н. Ф. // Концепт. – 2024. – № 3. – С. 29-42.

3. Добрица, В. П., Горюшкин, Е. И. Применение интеллектуальной адаптивной платформы в образовании [Текст] / В. П. Добрица, Е. И. Горюшкин // Auditorium. – 2019. – № 1 (21). – С. 86-92.

4. Евенко, Е. В., Гливенкова, О. А., Морозова, О. Н. Модель смешанного обучения с точки зрения теории когнитивной нагрузки [Текст] / Е. В. Евенко, О. А. Гливенкова, О. Н. Морозова // Вестник Майкопского государственного технологического университета. –2022. – № 3. – С. 58-65.

***УДК 004.9:37.041***

***Манькова Ю.В.***
***Научный руководитель: Семенова В.Н., канд. физ.-мат. наук, доц.***
*Димитровградский инженерно-технологический институт*
*г. Дмитровград, Россия*

## АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМ ПРОЦЕССОМ: РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИЗУЧЕНИИ АЛГОРИТМОВ

В условиях стремительной цифровизации образования особую актуальность приобретает автоматизация управления учебным процессом, особенно при изучении алгоритмов – одной из наиболее сложных и важных дисциплин в информатике. Традиционные методы преподавания алгоритмов часто сталкиваются с проблемами, связанными с абстрактностью понятий, необходимостью индивидуального подхода и сложностью контроля усвоения материала. Информационные технологии предлагают принципиально новые возможности для решения этих задач, обеспечивая наглядность, оперативную обратную связь и персонализацию обучения.

Цель исследования – проанализировать влияние автоматизированных систем на изучение алгоритмов и выявить наиболее эффективные ИТ-решения для управления образовательным процессом.

Основные задачи:

1. Определить ключевые технологии автоматизации в обучении алгоритмам.
2. Исследовать методы визуализации и симуляции алгоритмов.
3. Оценить эффективность автоматизированных систем проверки знаний.

4. Выявить перспективные направления развития ИТ в образовании.

Современные системы управления обучением кардинально преобразуют процесс преподавания алгоритмов. Такие платформы как «Moodle» или «Blackboard» не просто предоставляют доступ к учебным материалам, но и позволяют выстраивать индивидуальные траектории обучения [1]. Особого внимания заслуживают специализированные системы типа «Stepik» и «LeetCode», которые не только автоматически проверяют корректность реализации алгоритмов, но и предоставляют детализированный анализ ошибок, что значительно ускоряет процесс обучения.

Интерактивные среды программирования, такие как «Jupyter Notebook» и «Google Colab», устраняют технические барьеры, позволяя студентам сосредоточиться на изучении алгоритмов, а не на настройке программного окружения [2]. Эти платформы обеспечивают мгновенную визуализацию работы алгоритмов, что особенно ценно при изучении сложных концепций вроде сортировок или графовых алгоритмов.

Визуализация играет ключевую роль в преодолении абстрактности алгоритмических концепций. Специализированные инструменты трансформируют статичные описания алгоритмов в динамические, интерактивные демонстрации, где каждый шаг выполнения сопровождается визуальными подсказками и пояснениями. Такой подход не только облегчает понимание, но и помогает студентам осознать временную сложность алгоритмов.

Особый интерес представляют виртуальные лаборатории, которые позволяют наблюдать за работой алгоритмов на уровне оперативной памяти. В более продвинутых сценариях, например, при изучении алгоритмов для робототехники, системы предоставляют возможности для полноценного моделирования и тестирования в виртуальной среде [3].

Автоматизированные системы проверки знаний претерпели значительную эволюцию – от простых тестов до сложных платформ, способных анализировать не только корректность, но и эффективность реализации алгоритмов. Такие системы используют расширенные тестовые наборы для всесторонней проверки решений, а современные анализаторы кода могут оценивать даже стиль программирования.

Появление интеллектуальных ассистентов вроде «GitHub Copilot» открывает новые перспективы в обучении. Эти инструменты не только помогают находить ошибки, но и предлагают альтернативные, более оптимальные решения, выступая в роли персональных наставников [4].

При этом важно отметить, что их использование требует тщательного методического сопровождения, чтобы избежать излишней зависимости студентов от автоматизированных подсказок.

Развитие технологий виртуальной и дополненной реальности обещает революционные изменения в преподавании алгоритмов. Такие среды позволят студентам буквально «погружаться» в работу алгоритмов, наблюдая их выполнение в трехмерном пространстве. Одновременно блокчейн-технологии могут решить проблему верификации уникальности работ и сертификации навыков.

Однако широкое внедрение автоматизации сталкивается с рядом вызовов. Проблема академической честности приобретает новые формы в условиях доступности интеллектуальных помощников. Кроме того, некоторые аспекты алгоритмического мышления, особенно связанные с творческим подходом к решению задач, пока плохо поддаются автоматизированной оценке.

Помимо уже рассмотренных технологических решений, следует обратить внимание на фундаментальные изменения, которые информационные технологии вносят в саму парадигму преподавания алгоритмов. Современные системы автоматизации трансформируют не только методы подачи материала, но и саму структуру познавательной деятельности учащихся. Этот процесс затрагивает когнитивные, социальные и даже философские аспекты образования.

Когнитивная революция в изучении алгоритмов проявляется в том, что цифровые инструменты позволяют преодолеть традиционный разрыв между абстрактным пониманием и практической реализацией алгоритмических концепций [5]. Интерактивные среды создают своего рода «мыслительные тренажеры», где студенты могут экспериментировать с различными подходами, мгновенно получая визуальную и аналитическую обратную связь. Такой подход соответствует современным представлениям о нейропластичности мозга, когда многократное повторение с вариациями способствует формированию устойчивых нейронных связей.

Социальный аспект автоматизации проявляется в новых формах коллаборативного обучения. Современные платформы позволяют организовать распределенную работу над алгоритмическими задачами, где каждый участник может вносить свой вклад в общее решение. Это формирует принципиально новую образовательную среду, сочетающую преимущества индивидуального темпа обучения с возможностями коллективного интеллекта. Особенно перспективным

представляется развитие систем, сочетающих автоматическую проверку решений.

Философский ракурс проблемы связан с изменением самой природы алгоритмического мышления в условиях цифровой среды. Традиционное понимание алгоритма как четкой последовательности действий дополняется новыми измерениями – интерактивностью, адаптивностью, способностью к самообучению. Это ставит перед преподавателями новые методологические вопросы: как сохранить фундаментальность понимания в условиях всеобщей автоматизации? Где проходит граница между использованием технологий как инструмента и чрезмерной зависимостью от них?

В том числе переход к автоматизированным системам обучения требует переосмысления традиционных педагогических подходов. Преподавателям необходимо разрабатывать специальные методики, которые бы сочетали преимущества автоматизированных систем с развитием глубинного понимания принципов.

Информационные технологии кардинально преобразуют процесс изучения алгоритмов, предлагая принципиально новые инструменты для автоматизации управления образовательным процессом. От интерактивных сред программирования до интеллектуальных систем оценки – каждый элемент этой экосистемы вносит вклад в повышение эффективности обучения. Однако максимальный педагогический эффект может быть достигнут только при условии сбалансированного сочетания технологических возможностей с продуманной методической поддержкой.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рост цифрового образования в России: Исследование новых трендов и возможностей [Электронный ресурс] // globaledurussia.com: [сайт]. – URL: https://globaledurussia.com (дата обращения: 03.05.2025).

2. Ангапов, В. Д. Обзор современных облачных платформ для целей машинного обучения [Текст] / В. Д. Ангапов // Проблемы современной науки и образования. – 2023. – № 7 (185). – С. 1-10.

3. Никулина, Т. В., Стариченко, Е. Б. Виртуальные образовательные лаборатории: принципы и возможности [Текст] / Т. В. Никулина, Е. Б. Стариченко // Педагогическое образование в России. – 2016. – № 7. – С. 62-66.

4. ИИ-помощник Copilot от GitHub – как новый инструмент повлияет на работу программистов [Электронный ресурс] // habr.com : [сайт]. – URL: https://habr.com/ru (дата обращения: 03.05.2025).

5. Розова, О. А. Когнитивная революция в информационном обществе [Текст] / О. А. Розова // Современное педагогическое образование. – 2019. – № 10. – С. 188-190.

***УДК 004.81***

***Матренина Е.Р.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## АВТОМАТИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ С ПОСТАВЩИКАМИ И ЛОГИСТИКА В 1С ДЛЯ АВТОСЕРВИСОВ

В современных условиях развития автосервисного бизнеса особое внимание уделяется оптимизации логистических процессов, включая закупку, учёт и хранение запасных частей, а также управление взаимодействием с поставщиками. Эти процессы играют ключевую роль в обеспечении бесперебойной работы сервисного центра, влияя на сроки ремонта, удовлетворённость клиентов и экономическую эффективность предприятия. Цифровизация логистических функций позволяет снизить операционные риски, минимизировать издержки и улучшить контроль за цепочками поставок. Одним из наиболее распространённых решений для автоматизации таких процессов является платформа 1С:Предприятие, предоставляющая широкие возможности для настройки бизнес-процессов, интеграции с внешними системами и аналитики.

Логистика автосервиса имеет ряд особенностей, отличающих её от классических моделей снабжения. Во-первых, запасные части обладают высокой номенклатурной вариативностью, что требует точной классификации, учёта аналогов и поддержки оперативного поиска. Во-вторых, сроки поставки имеют критическое значение: задержка одной детали может остановить ремонт и негативно сказаться на клиентском опыте. В-третьих, автосервисы зачастую работают с несколькими поставщиками одновременно, что требует гибкой системы выбора и автоматизации заказов с учётом цен, условий поставки и наличия на складах партнёров. Для решения этих задач необходима централизованная система, способная в режиме реального времени отслеживать потребности, создавать заказы, учитывать поступления и управлять складскими остатками.

Теоретической основой автоматизации снабжения является построение модели, в которой все участники логистического процесса представлены как элементы единой информационной среды. Это позволяет синхронизировать потребности и поставки, уменьшить объёмы избыточного хранения, а также сократить ручной труд. В рамках 1С:Предприятие реализована объектно-ориентированная модель учёта, в которой каждая единица запчастей, поставщик, заказ, поступление и перемещение представляются в виде связанных объектов с возможностью автоматического взаимодействия и обработки событий. Это обеспечивает гибкость настройки под конкретные условия автосервиса.

На практике в системе 1С выстраивается модель взаимодействия с поставщиками, включающая справочник контрагентов, договоры, условия поставок и прайс-листы. Каждое взаимодействие — от формирования потребности до поступления и оприходования товаров — фиксируется в системе. Заказ может быть сформирован вручную либо автоматически на основе анализа потребностей и минимальных складских остатков. После поступления товара происходит его автоматическое распределение на заказы клиентов или пополнение свободных остатков. Возможности 1С позволяют учитывать партии, серийные номера, сроки годности и использовать различные схемы учёта (FIFO, LIFO и другие), что важно для работы с автозапчастями.

Современные решения включают возможность интеграции с внешними поставщиками через API и технологии электронного обмена данными (EDI). Такая интеграция позволяет в автоматическом режиме получать актуальные остатки, цены, статус заказа и документы от поставщика. Прямое подключение к каталогам позволяет упростить подбор запчастей и уменьшить вероятность ошибок. 1С поддерживает работу с форматами EDI и обеспечивает возможность двустороннего обмена, в том числе загрузку заказов и получение электронных накладных. Это особенно актуально при работе с крупными поставщиками или маркетплейсами, где скорость обработки заказов и прозрачность документации критичны.

Оптимизация складского учёта осуществляется за счёт введения систем автоматического учёта остатков, отслеживания движения по складам, резервирования под заказы и анализа оборачиваемости. В системе 1С можно настраивать схемы размещения товаров, создавать зонирование склада и использовать механизмы адресного хранения. Также доступны инструменты для прогнозирования потребностей на основе статистики и сезонных трендов, что позволяет заранее готовиться к повышенной нагрузке и избежать дефицита. Важной

функцией является возможность настройки уведомлений и автозаказов при достижении критических уровней остатков.

Для эффективного управления снабжением необходимо также контролировать сроки поставок и обеспечивать своевременность исполнения заказов. В системе 1С реализована возможность отслеживать дату заказа, срок доставки, фактическое поступление и сравнивать их для анализа надёжности поставщиков. Автоматизация этих процессов позволяет своевременно реагировать на сбои и оптимизировать логистическую цепочку. Отчёты и дашборды в 1С помогают отслеживать ключевые показатели эффективности: среднее время поставки, уровень удовлетворения спроса, коэффициент возвратов и прочие метрики.

На практике использование этих механизмов уже доказало свою эффективность. Внедрение автоматизированных решений на базе 1С позволяет автосервисам сократить издержки, ускорить обслуживание, снизить вероятность ошибок при подборе и учёте запчастей. Например, в ряде прикладных решений 1С реализованы сценарии автоматического распределения поступлений, интеграции с онлайн-каталогами и маркировки товаров, что значительно снижает трудозатраты персонала. Также встречаются примеры успешного использования 1С для ведения мульти складского учёта и синхронизации данных между разными филиалами автосервисной сети.

Перспективы развития данных решений связаны с более глубокой интеграцией с внешними платформами, использованием искусственного интеллекта для прогнозирования потребностей и оптимизации закупок, а также внедрением мобильных интерфейсов для складского персонала. Также можно ожидать расширения функциональности в части логистического анализа, визуализации и интеграции с CRM-системами для более полного охвата клиентского пути. Таким образом, автоматизация логистики на базе 1С в автосервисе не только повышает текущую эффективность, но и открывает возможности для дальнейшего роста и цифровой трансформации бизнеса.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Санников, Н. С. Разработка информационной системы "автосервис" средствами 1С: Предприятие / Н. С. Санников // XX Всероссийская студенческая научно-практическая конференция Нижневартовского государственного университета: сборник статей, Нижневартовск, 03–04 апреля 2018 года / Ответственный редактор А.В.

Коричко. Том Часть 2. – Нижневартовск: Нижневартовский государственный университет, 2018. – С. 254–258.

2. Платонов, С. В. Оптимизация работы автосервиса применением 1С / С. В. Платонов, Г. А. Гареева // Поколение будущего: Взгляд молодых ученых-2023 : Сборник научных статей 12-й Международной молодежной научной конференции. В 4-х томах, Курск, 09–10 ноября 2023 года. – Курск: ЗАО "Университетская книга", 2023. – С. 76–79.

3. Булычев, П. Д. Менеджмент бизнес-процесса автосервиса в 1С: предприятии / П. Д. Булычев, А. Н. Солопова // Эволюция науки и техники: глобальные вызовы и перспективы: Сборник статей Международной научно-практической конференции, Москва, 04 марта 2024 года. – Москва: ЦИФРОВОЕ НАУЧНОЕ ИЗДАТЕЛЬСТВО, 2024. – С. 238–244.

4. Дракунов, И. И. Современное программное обеспечение для управления системой технического обслуживания и ремонта автомобилей / И. И. Дракунов, В. В. Сиваков, Р. Ю. Деревягин // Модернизация и научные исследования в транспортном комплексе. – 2022. – Т. 1. – С. 30–33.

5. Макаренко, Д. В. Разработка прикладного решения на базе "1С: предприятие" для работы автосервиса / Д. В. Макаренко, С. Л. Паршина // Актуальные проблемы авиации и космонавтики. – 2017. – Т. 2, № 13. – С. 369–371.

6. Social time management web service development / A. A. Kuznetsov, V. Z. Magergut, I. A. Kochetkova, M. A. Kosonogova // Advances in Environmental Biology. – 2014. – Vol. 8, No. 13. – P. 94-98.

***УДК 004.81***

***Матренина Е.Р.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## РИСКИ И ПРОБЛЕМЫ АВТОМАТИЗАЦИИ АВТОСЕРВИСНОГО БИЗНЕСА

Автоматизация бизнес-процессов в сфере автосервисного обслуживания становится всё более актуальной задачей на фоне усиления конкуренции, повышения требований клиентов и роста объёмов информации. Платформа 1С:Предприятие зарекомендовала себя как гибкий и надёжный инструмент для создания прикладных

решений в области учёта, управления и анализа деятельности автосервисов. Однако, несмотря на широкие технические возможности, процесс автоматизации сопровождается целым рядом рисков и проблем, способных негативно повлиять как на эффективность решения, так и на стабильность всей организации. Осмысление этих вызовов и поиск устойчивых стратегий становится важным этапом любого проекта внедрения информационной системы.

Бизнес-среда автосервисов обладает определённой спецификой. Она характеризуется высокой интенсивностью оперативных процессов, наличием разнородных участников (приёмщики, механики, складские работники, бухгалтерия), постоянным взаимодействием с внешними поставщиками и клиентами, а также зависимостью от технической информации и нормативных процедур. Кроме того, уровень цифровой зрелости в таких организациях может быть существенно различным: от бумажного документооборота до частичной автоматизации отдельных функций. Это создаёт потенциальные препятствия при переходе к интегрированной системе управления на базе 1С, требуя тщательного планирования и адаптации решений к реалиям предприятия.

Риски автоматизации можно классифицировать по различным основаниям. Во-первых, технологические риски включают несовместимость платформы с существующими решениями, ошибки в программной реализации, сбои при обновлении и сложности с масштабированием. Во-вторых, организационные риски связаны с отсутствием чётких регламентов, слабой поддержкой руководства, недостаточной мотивацией персонала и сопротивлением изменениям. В-третьих, методологические риски отражают неточности в описании бизнес-процессов, избыточную формализацию или, наоборот, излишнюю гибкость системы. Наконец, проектные риски касаются ошибок в управлении внедрением: неясной постановки задач, завышенных ожиданий, нехватки ресурсов и проблем на этапе поддержки.

Типовые проблемы при разработке и внедрении решений на базе 1С для автосервисов проявляются на всех стадиях проекта. На этапе анализа и проектирования нередко недооценивается сложность бизнес-процессов, игнорируются «неформальные» практики, которые играют важную роль в ежедневной деятельности. Разработчики могут предложить слишком стандартизированное решение, не учитывающее отраслевые нюансы. В процессе программной реализации возможны ошибки в логике документов, нарушающие согласованность данных, а также трудности с интеграцией модулей между собой. На этапе внедрения выявляются несоответствия между системой и ожиданиями

пользователей, проблемы с производительностью, нехватка обученного персонала и сопротивление со стороны работников, не желающих менять привычные методы работы.

Проектные риски охватывают весь жизненный цикл автоматизации. На этапе инициации важную роль играет правильное формулирование целей, ограничений и критериев успеха. При отсутствии формализованного технического задания возрастает риск недопонимания между разработчиком и заказчиком. В ходе реализации возможны отставания от сроков, перерасход бюджета и дублирование функций. В фазе опытной эксплуатации становится очевидным, насколько система соответствует реальным требованиям: выявляются ошибки, «узкие места», отсутствующие функции. Без должной поддержки со стороны ИТ-персонала и обратной связи от пользователей система быстро теряет актуальность. Сопровождение решения требует постоянного обновления, корректировки справочников и доработки функционала под изменяющиеся бизнес-условия.

Для минимизации рисков применяются различные стратегии. Важнейшим элементом является построение устойчивой архитектуры информационной системы с возможностью гибкой настройки и расширения. Также эффективным подходом оказывается итерационная модель внедрения, когда система запускается поэтапно — сначала в ключевых зонах, затем масштабируется на всю организацию. Большое значение имеет наличие проектной команды с опытом работы в отрасли, а также активное участие пользователей на всех этапах — от постановки задач до тестирования. Организация обучения и постоянного сопровождения позволяет минимизировать эффект «отторжения» со стороны персонала, а также снизить количество ошибок в работе.

Практический опыт показывает, что наиболее серьёзные трудности возникают не в технической, а в организационной сфере. Сопротивление изменениям, нехватка квалифицированных кадров, нехотение сотрудников брать на себя ответственность за новые задачи — всё это требует системного подхода к управлению изменениями. Руководство должно активно поддерживать проект, демонстрируя важность перехода на новую систему. Интересным решением оказывается вовлечение «внутренних амбассадоров» — сотрудников, которые демонстрируют лояльность проекту, обучаются первыми и помогают остальным. Также важно формировать у работников понимание выгод от внедрения — повышение скорости обработки заказов, снижение потерь, упрощение документооборота.

Одним из ключевых факторов успешного внедрения становится роль пользователя и организация обучения. Даже самая функционально насыщенная система теряет смысл, если персонал не умеет с ней работать или использует её лишь частично. Обучение должно быть системным, включать теоретическую и практическую часть, сопровождаться раздаточными материалами и внутренними регламентами. Специфика автосервиса требует обучения не только административного персонала, но и мастеров, механиков и кладовщиков. Только при всеобщем понимании принципов работы ИС можно рассчитывать на положительный эффект от автоматизации.

Для оценки эффективности и устойчивости внедрённого решения применяются как количественные, так и качественные методы. Анализируются показатели производительности, скорости выполнения операций, количество ошибок, объём возвратов и жалоб клиентов. Также важно оценивать субъективные параметры: удовлетворённость пользователей, удобство интерфейса, степень соответствия системы ожиданиям. Регулярный аудит, опросы сотрудников и сбор статистики позволяют корректировать работу системы и развивать её в соответствии с новыми требованиями бизнеса.

В заключение стоит отметить, что автоматизация автосервисного бизнеса на платформе 1С требует комплексного подхода, сочетающего технологическую гибкость, организационную устойчивость и активное участие всех участников проекта. Только при условии системной подготовки, адекватной оценки рисков и стратегического планирования можно рассчитывать на успешное внедрение и достижение бизнес-целей. Опыт показывает, что именно внимание к людям, процессам и устойчивости архитектуры ИС становится залогом долгосрочного эффекта от цифровой трансформации.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Санников, Н. С. Разработка информационной системы "автосервис" средствами 1С: Предприятие / Н. С. Санников // XX Всероссийская студенческая научно-практическая конференция Нижневартовского государственного университета: сборник статей, Нижневартовск, 03–04 апреля 2018 года / Ответственный редактор А.В. Коричко. Том Часть 2. – Нижневартовск: Нижневартовский государственный университет, 2018. – С. 254–258.

2. Платонов, С. В. Оптимизация работы автосервиса применением 1С / С. В. Платонов, Г. А. Гареева // Поколение будущего: Взгляд молодых ученых-2023 : Сборник научных статей 12-й

Международной молодежной научной конференции. В 4-х томах, Курск, 09–10 ноября 2023 года. – Курск: ЗАО "Университетская книга", 2023. – С. 76–79.

3. Булычев, П. Д. Менеджмент бизнес-процесса автосервиса в 1С: предприятии / П. Д. Булычев, А. Н. Солопова // Эволюция науки и техники: глобальные вызовы и перспективы: Сборник статей Международной научно-практической конференции, Москва, 04 марта 2024 года. – Москва: ЦИФРОВОЕ НАУЧНОЕ ИЗДАТЕЛЬСТВО, 2024. – С. 238–244.

4. Дракунов, И. И. Современное программное обеспечение для управления системой технического обслуживания и ремонта автомобилей / И. И. Дракунов, В. В. Сиваков, Р. Ю. Деревягин // Модернизация и научные исследования в транспортном комплексе. – 2022. – Т. 1. – С. 30–33.

5. Social time management web service development / A. A. Kuznetsov, V. Z. Magergut, I. A. Kochetkova, M. A. Kosonogova // Advances in Environmental Biology. – 2014. – Vol. 8, No. 13. – P. 94-98.

***УДК 621.316.718.5***

***Митюков А.Е.***
***Научный руководитель: Бушуев Д.А., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИМПУЛЬСНАЯ СИСТЕМА УПРАВЛЕНИЯ БЕСКОЛЛЕКТОРНЫМ ДВИГАТЕЛЕМ ПОСТОЯННОГО ТОКА

В отличие от коллекторного двигателя постоянного тока, в котором коллекторный узел отвечает за коммутацию обмоток ротора, в бесколлекторном двигателе постоянного тока (БДПТ) эту роль выполняют транзисторы в контроллере. Блок управления БДПТ, как правило, реализовывает импульсный или релейный закон управления.

В последние несколько лет для улучшения динамических характеристик, снижения веса, габаритов и шума бесколлекторные двигатели постоянного тока находят широкое применение в центробежных вибрационных возбудителях колебаний (вибрационных актуаторах) [1]. При этом особый интерес представляют релейные системы управления БДПТ вибровозбудителей. Они позволяют программировать временные интервалы для работы двигателя, что критично для синхронизации с механическими колебаниями вибровозбудителя [2]. Это также улучшает стабилизацию амплитуды

перемещения платформы. Кроме того, релейное управление минимизирует риски перегрузки электродвигателя и возникновения режима прерывистых токов.

Для коммутации БДПТ существует два основных метода: биполярный и униполярный (рис. 1).

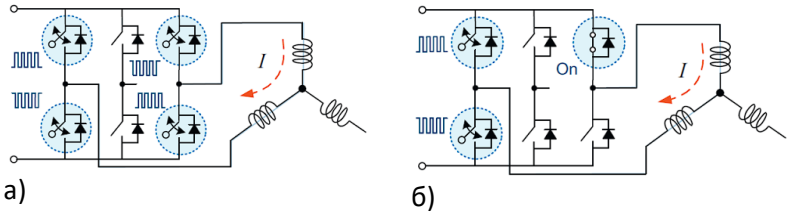



Рис. 1. Методы коммутации: *а* – биполярная; *б* – униполярная

При методе биполярной коммутации ШИМ-сигнал подается на все ключи двух фаз. А в методе униполярного (однополярного) переключения ШИМ-сигнал подается на ключи только одной фазы, в то время как один ключ другой фазы остается включенным. Биполярный метод прост и может обеспечить лучшую динамику. Однако пульсации тока (следовательно, пульсации крутящего момента) и потери при переключении больше, чем при униполярном методе переключения. При использовании метода униполярной коммутации потери при переключении могут быть уменьшены, поскольку ШИМ-сигнал подается на ключи только одной фазы. Кроме того, пульсации тока в два раза меньше, чем при использовании метода биполярной коммутации. Благодаря этим преимуществам метод униполярного переключения более широко используется для электроприводов постоянного тока.

Существует несколько разновидностей униполярной коммутации (рис. 2).

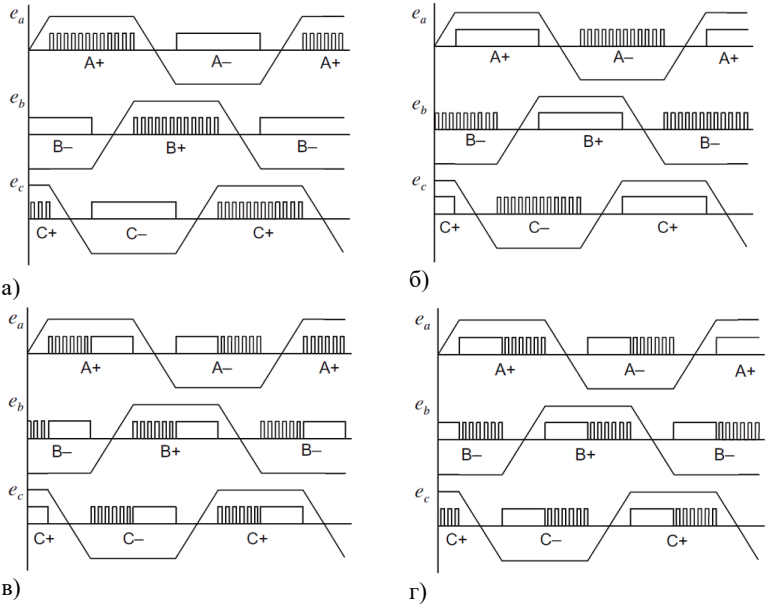



Рис. 2. Способы униполярной коммутации: *а* – ШИМ-сигнал подается на верхний ключ; *б* – ШИМ-сигнал подается на нижний ключ; *в* – ШИМ-сигнал подается на оба ключа; *г* – ШИМ-сигнал подается на оба ключа

В схеме (рис. 2(а)) ШИМ-сигнал подается только на верхний ключ, в то время как нижний ключ остается включенным. С другой стороны, в схеме (рис. 2(б)) ШИМ-сигнал подается только на нижний ключ, в то время как верхний ключ остается включенным. В качестве схем, улучшенных за счет равномерного переключения, существуют постоянно работающие ШИМ-схемы (рис. 2(в, г)), их недостатком является повышенный пульсационный момент и пониженный КПД из-за пульсационного тока. Так, как в верхних плечах полумостов будут использоваться более технологичные N-канальные МДП-транзисторы [3], то для их управления будет использована схема, подающая ШИМ-сигнал только на верхний ключ (рис. 2(а)).

Рассмотрим функциональную схему управления БДПТ с релейным законом (рис. 3).

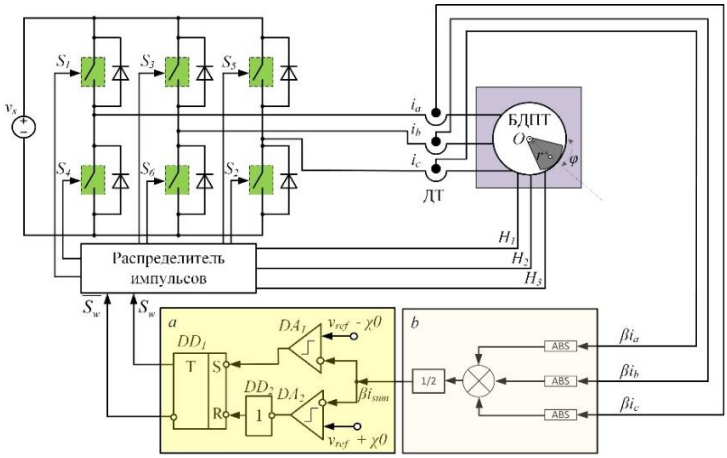
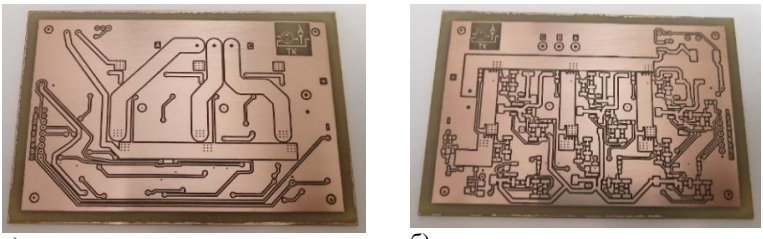



Рис. 3. Функциональная схема управления БДПТ с релейным управлением с обратной связью

БДПТ имеет питание от аккумуляторной батареи. Для коммутации двигателя применяется 3 полумостовых схемы, состоящие из 6 ключей. Фазы двигателя подключаются к блоку силовых транзисторов через датчики тока (ДТ). Положение ротора двигателя относительно статора контролируется датчиками Холла ($H_1$, $H_2$, $H_3$). На валу двигателя с двух сторон закреплены грузы для создания вибронагруженного состояния двигателя. Напряжение с датчиков тока двух фаз двигателя пересчитывается в среднее значение, взятое по модулю, и приходит на релейный элемент с гистерезисом. Релейный элемент основан на двух компараторах $DA_1$, $DA_2$, логическом элементе «НЕ» $DD_2$ и RS-триггере $DD_1$. На входах компараторов задаются пороги срабатывания (гистерезис) $v_{ref} - x_0$, $v_{ref} + x_0$. Элемент «НЕ» нужен для исключения запрещенной комбинации RS-триггера. Блок силовых ключей с драйверами реализуется в виде печатной платы. Распределитель импульсов реализуется на микроконтроллере STM32. Блок релейного управления (a) для быстрой отработки импульсов реализуется аппаратно. Блок вычисления среднего значения тока, взятого по модулю, (b) реализуется на микроконтроллере STM32.

Двусторонняя печатная плата была изготовлена методом пленочного фоторезиста (рис. 4).



а) б)

Рис. 4. Изготовленная методом пленочного фоторезиста двусторонняя печатная плата: *а* – верхняя сторона; *б* – нижняя сторона

На печатной плате расположены три полумостовых схемы с двумя силовыми ключами в каждой. Рассмотрим один полумост (рис. 5). Силовой ключ коммутируется с помощью каскада из трех транзисторов: в начале МОП-транзистор усиливает амплитуду сигнала от 3.3 В до 16 В, затем эмиттерный повторитель усиливает ток. Усиленный по току и напряжению сигнал от микроконтроллера подается на затворы МОП-транзисторов [3].

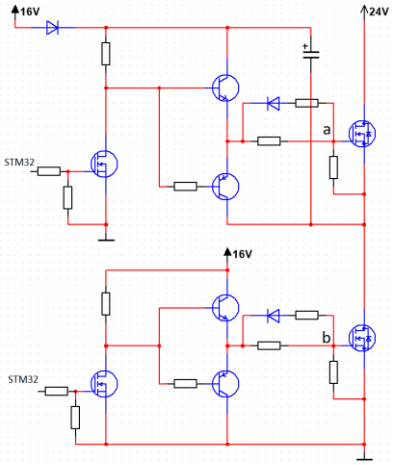



Рис. 5. Принципиальная электрическая схема полумоста контроллера

Установив щупы осциллографа в точки *a* и *b* (см. рис. 5), получим осциллограмму с сигналами управления БДПТ в полумосте в режиме шести-шаговой коммутации (рис. 6).

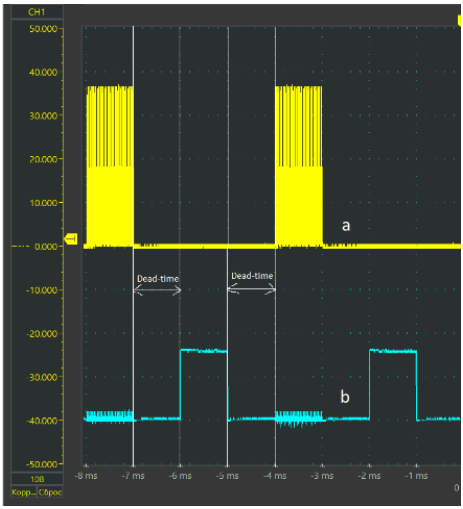



Рис. 6. Осциллограмма с сигналами управления БДПТ в полумосте в режиме шести-шаговой коммутации

Исходя из полученной осциллограммы можно сделать вывод о том, что для исключения сквозных токов между силовыми ключами верхнего и нижнего уровней нужно вводить Dead-time. Конечной целью разработанной платы управления является реализация релейного закона управления, способного быстро изменять режимы работы БДПТ.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Vibration Motors. [Электронный ресурс]. URL: https://www.ato.com (дата обращения: 07.05.25).

2. Complex dynamics of a vibration machine caused by a relay feedback control / Z. T. Zhusubaliyev, V. Avrutin, V. G. Rubanov, D. A. Bushuev // Physica D: Nonlinear Phenomena. – 2021. – Vol. 420. – P. 132870. – DOI 10.1016/j.physd.2021.132870. – EDN NWQGQZ.

3. Величко, Д. В., Рубанов, В. Г. Полупроводниковые приборы и устройства [Текст] / Д. В. Величко, В. Г. Рубанов — 1-е изд. — Белгород: БГТУ им. В.Г.Шухова, 2006 — 184 с.

*УДК 004.89*

***Московченко А.Д.***
***Научный руководитель: Косоногова М.А., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ПОДБОРА КОМПОНЕНТОВ АВТОМОБИЛЬНОЙ АУДИОСИСТЕМЫ

Прослушивание музыки во время вождения одно из самых распространенных занятий, которое не только служит источником развлечения для водителей и пассажиров, но и значительно влияет на комфорт вождения и общий уровень усталости. С развитием технологий производители автомобилей и разработчики аудиосистем разрабатывают различные способы улучшения систем для улучшения качества звука и увеличения громкости. Однако, с ростом ассортимента аудиокомпонентов (динамиков разного типа, усилителей и прочих устройств) покупателям становится сложнее выбрать компоненты, которые будут подходить по характеристикам друг другу и соответствовать музыкальным предпочтениям.

Задачу подбора компонентов аудиосистемы можно рассматривать как задачу оптимизации. Цель такой задачи – это выбор наилучшей аудиосистемы из определенного количества возможных альтернатив аудиосистем, которая будет соответствовать набору ограничений.

Так как задача подбора компонентов аудиосистем является сложной задачей и имеет много различных переменных и параметров, которые нужно учесть в подборе, классические методы оптимизации оказываются сложно реализуемыми. В данной задаче подойдет генетический алгоритм (далее ГА). Генетический алгоритм - эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе. Алгоритм работает с популяцией возможных решений (различных аудиосистем, состоящих из определенных компонентов), постепенно улучшая их через поколения. Используются операции, подобные биологической эволюции: отбор (выбор лучших решений), скрещивание (обмен компонентов между «родительскими» конфигурациями) и мутация (случайное изменение отдельных компонентов). В результате

изменения популяции ГА способен сходиться к оптимальному решению задачи оптимизации.

Чтобы применить ГА, необходимо определить, какие параметры аудиосистемы подлежат оптимизации, каковы критерии подходящего решения и какие накладываются ограничения.

Для этого был определен минимальный набор условий, чтобы находить подходящую аудиосистему:

- Проверка ценового диапазона. Например, если суммарная стоимость компонентов выходит за допустимый диапазон, конфигурации назначается штраф, уменьшающий итоговое значение функции приспособленности.
- Проверка соответствия номинальной мощности между компонентами. Например, мощность канала усилителя должна должен быть больше на 10-20% по сравнению с мощностью динамика, подключаемого к этому каналу.
- Проверка сопротивления между компонентами (усилителями и динамиками). Неверно подобранное номинальное сопротивление может вызвать перегрузку усилителя или неэффективную передачу мощности.
- Оценка уровня звукового давления (SPL). Динамики не должны сильно отличаться по этому уровню. Например, если задние динамики имеют большее звуковое давление, то будет нарушена звуковая сцена.
- Проверка частотного охвата аудиосистемы. Все компоненты должны в совокупности охватывать как низкие, так средние и высокие частоты, обеспечивая полноценный спектр звучания.

Условия, описанные выше, являются составляющими функции приспособленности. Данная функция определяет, насколько хорошо аудиосистема соответствует условиям задачи.

В разрабатываемом генетическом алгоритме каждая аудиосистема представлена в виде хромосомы – упорядоченного набора генов, где каждый ген - конкретный компонент аудиосистемы с определенным типом. Пример хромосомы представлен на Рис 1.

Набор разных аудиосистем образует популяцию. Начальная популяция генерируется случайным образом из множества доступных компонентов. После чего начинается итерационный цикл поиска подходящего решения. Оценка функции приспособленности выполняется на каждой итерации ГА для каждой аудиосистемы в текущей популяции.

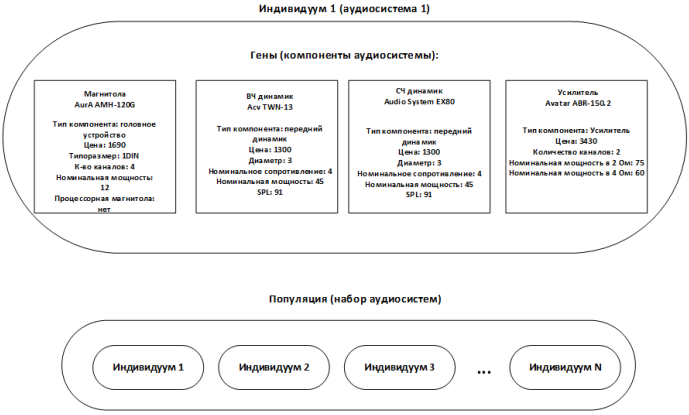



Рис. 1. Структура хромосом и популяции в генетическом алгоритме.

На основе оценки функции приспособленности происходит отбор. В данной задаче используется метод турнирного отбора, когда случайным образом выбирается небольшое количество аудиосистем из популяции (например, три), и из них выбирается одна с самым большим значением функции приспособленности. Данный процесс представлен на Рис 2.

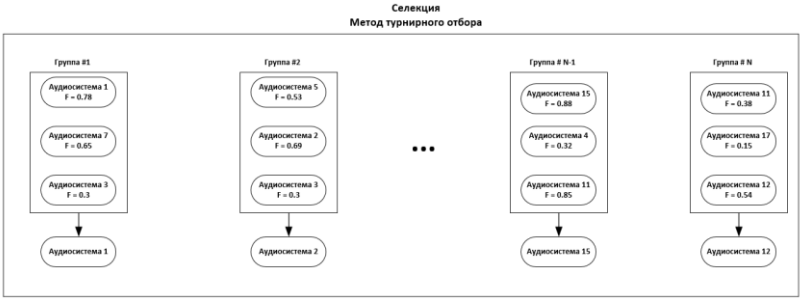



Рис. 2. Пример селекции методом турнирного отбора.

Отобранные таким образом родители участвуют в операции скрещивания. В данной задаче был выбран метод равномерного скрещивания (Рис. 3). Суть этого метода в том, что каждый ген потомка имеет значение как у первого родителя, либо как у второго с заданной вероятностью.

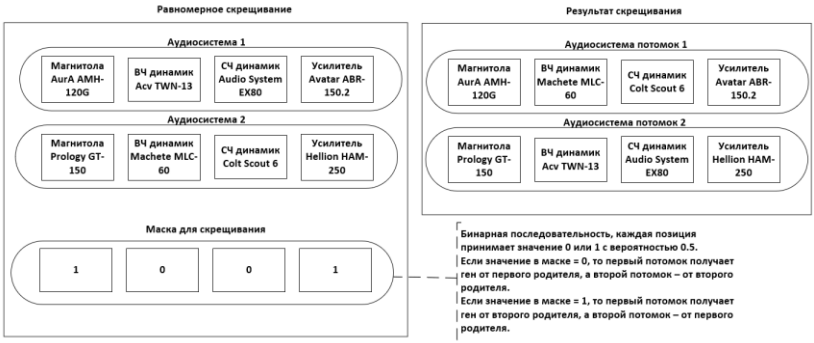



Рис. 3. Пример скрещивания двух хромосом.

Помимо скрещивания, с определенной вероятностью (0.1) происходит мутация. Мутация представляет собой процесс, который случайным образом изменяет ген индивидуума. Целью мутации является добавление разнообразия и случайности в эволюционный процесс, что позволяет избегать застревания в локальных оптимумах. В данной задаче мутация представляет изменение модели одного компонента на другой. Например, в конфигурации аудиосистемы определённая модель головного устройства может быть случайно заменена другой доступной моделью.

После применения процессов описанных выше получается новое поколение конфигураций. Выполнение алгоритма происходит до тех пор, пока не выполнится одно из двух условий. Первое условие – это достижение определенного количества поколений эволюции. Второе условие заключается в проверке того, что самое высокое значение функции приспособленности в популяции не увеличивается на протяжении десяти поколений эволюции.

Результатом выполнения алгоритма является набор конфигураций из последнего сформировавшегося в процессе эволюции поколения хромосом. Лучший решением считается аудиосистема с наивысшим значением функции приспособленности.

Подводя итог, можно сказать, что генетический алгоритм позволяет эффективно подбирать подходящую конфигурацию аудиосистемы, учитывая необходимые условия, такие как бюджет, мощность, сопротивления, уровень звукового давления, частотный охват. Благодаря процессам отбора, скрещивания и мутации генетический алгоритм с каждым новым поколением находит более подходящие варианты.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Загинайло, М. В. Генетический алгоритм как эффективный инструмент эволюционных алгоритмов / М. В. Загинайло, В. А. Фатхи // Инновации. Наука. Образование. – 2020. – № 22. – С. 513-518.

2. Аралбаев, Р. А. Задачи оптимизации и применение алгоритмов генетический алгоритм на практике / Р. А. Аралбаев, А. А. Тарасов // Инновации. Наука. Образование. – 2021. – № 48. – С. 1645-1653.

3. Курманов, Т. Э. Выбор оптимальной акустической системы / Т. Э. Курманов // Студенческая наука об актуальных проблемах и перспективах инновационного развития регионального АПК : Материалы XXII научно-практической конференции обучающихся, Тара, 23 марта 2023 года. – Омск: Омский государственный аграрный университет имени П.А. Столыпина, 2023. – С. 109-112.

4. Шихатов, А. И. Особенности проектирования акустической системы для автомобиля / А. И. Шихатов // Проектирование и технология электронных средств. – 2008. – № 2. – С. 26-36.

5. Генетические алгоритмы и их применение для оптимального проектирования строительных конструкций / А. Г. Юрьев, Р. В. Лесовик, С. В. Клюев, А. В. Клюев // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. – 2008. – № 1. – С. 11-16.

6. Применение искусственных нейронных сетей в задачах управления генетическим алгоритмом / Д. А. Петросов, Р. А. Ващенко, А. А. Степовой // Моделирование, оптимизация и информационные технологии. – 2019. – Т. 7, № 4(27). – С. 10-11.



***УДК 378.147***



***Мубараков Н.А.***
***Научный руководитель: Медведева С.Н., канд. пед. наук, доц.***
*Казанский национальный исследовательский технический университет им. А.Н. Туполева, г. Казань, Россия*


## ОБОСНОВАНИЕ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ АКАДЕМИЧЕСКОГО ПЛАНИРОВАНИЯ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ

Цифровая трансформация высшего образования, ускоренная пандемией COVID-19, радикально изменила подходы к обучению. К 2024 году, по данным исследования РБК, более 75% магистерских

программ в России реализуются в гибридном или полностью онлайн-формате, что делает гибкость и доступность ключевыми преимуществами для студентов [1]. Однако технологическая инфраструктура вузов сосредоточена преимущественно на доставке контента, игнорируя необходимость поддержки студентов в управлении учебной деятельностью. Это создаёт парадокс: учащиеся получают неограниченный доступ к знаниям, но не обладают инструментами для их систематизации, что приводит к фрагментации учебного процесса и снижению академической успеваемости.

Проблема самоорганизации приобретает системный характер. Исследования Ю.С. Романовой и Е.В. Пастуховой демонстрируют, что 35% студентов сталкиваются с трудностями при распределении времени между лекциями, самостоятельной работой и личными обязательствами, что напрямую влияет на качество выполняемых заданий и уровень стресса [2]. В условиях смешанного обучения, где расписание динамично корректируется, а задания поступают из множества источников — LMS-платформ, электронной почты, мессенджеров — учащиеся вынуждены тратить до трети учебного времени на организационные задачи. Это подтверждается данными Е.В. Робустовой, более половины опрошенных студентов испытывают сложности с распределением времени, планированием задач и удержанием внимания в онлайн-среде [3].

Ключевой вопрос заключается в том, как помочь студентам трансформировать хаотичный поток задач в структурированный и управляемый процесс. Популярные универсальные приложения, такие как Trello или Notion, не учитывают специфику академического контекста: отсутствие привязки задач к дисциплинам, невозможность синхронизации с семестровым расписанием, ограниченные возможности для координации групповых проектов. Это приводит к их неэффективному использованию, усиливая чувство overwhelm (перегруженности) и провоцируя эмоциональное выгорание.

**Анализ проблематики**

Современный студент сталкивается с феноменом «цифрового хаоса», когда учебные задачи, материалы и коммуникация рассредоточены по множеству платформ. Задания публикуются в LMS, таких как Moodle или Blackboard, но их дедлайны дублируются в электронной почте или чатах мессенджеров. Материалы к семинарам хранятся в облачных хранилищах, ссылки на которые теряются в потоке сообщений, а расписание занятий может меняться в режиме реального времени, требуя постоянного мониторинга. По данным опроса Н.В. Иванушкиной, 45% студентов тратят более двух часов в день

исключительно на поиск и систематизацию учебной информации, что не только снижает продуктивность, но и формирует «синдром упущенной выгоды» — концентрацию на срочных, но малозначимых задачах в ущерб стратегическим целям, таким как подготовка к экзаменам или научные проекты [4].

Групповая работа в цифровой среде также сталкивается с серьёзными вызовами. Исследование Т.В. Шипуновой [6] демонстрирует, что в условиях дистанционного обучения 34% студентов сталкиваются с дублированием задач из-за отсутствия чёткого распределения ролей, что согласуется с выводами Н.В. Иванушкиной о рассредоточении информации по платформам [4]. Обсуждения в мессенджерах, часто превращаются в хаотичный обмен сообщениями, где критически важная информация теряется среди второстепенных деталей.

Эмоциональные и когнитивные перегрузки усугубляют ситуацию. Отсутствие визуализации учебного прогресса создаёт у студентов ощущение «бесконечного списка дел», когда невозможно объективно оценить, сколько этапов пройдено и сколько осталось. Постоянные уведомления из LMS, электронной почты и мессенджеров провоцируют многозадачность, снижая концентрацию и качество выполнения заданий. Студенты, особенно интроверты, часто избегают обращаться за помощью из-за страха осуждения в публичных чатах, что приводит к накоплению пробелов в знаниях. Как отмечает М.Д. Напсо, хронический стресс, вызванный неорганизованностью, снижает креативность и мотивацию, превращая обучение в механический процесс «выживания» [7].

**Концепция веб-приложения**

Разрабатываемая платформа призвана стать цифровым ассистентом, который не только упорядочит учебный процесс, но и создаст условия для формирования осознанного подхода к обучению. Её основу составляет идея привязки задач к конкретным дисциплинам, что позволяет студентам видеть взаимосвязь между различными элементами учебного плана. Например, задача «Подготовить презентацию по когнитивной психологии» связывается с дисциплиной «Общая психология», а материалы к ней — лекции, статьи, примеры работ — хранятся в едином пространстве, исключая необходимость поиска в сторонних сервисах.

Интеллектуальный календарь, интегрированный в платформу, объединяет расписание занятий, дедлайны и личные события, предоставляя целостный взгляд на учебную нагрузку. Цветовая маркировка снижает когнитивную нагрузку, позволяя студентам

фокусироваться на критически важных задачах, избегая эмоционального выгорания. Фильтры позволяют сортировать задачи по дисциплинам, типу или статусу, что особенно важно в условиях интенсивной учебной нагрузки.

Для групповой работы платформа предоставляет инструменты, которые минимизируют хаос коммуникации. Совместные проекты создаются в рамках отдельных задач, где участники могут распределять роли — координатор, исследователь, редактор — и прикреплять файлы (PDF, презентации, таблицы) непосредственно к обсуждению. Встроенный чат позволяет вести диалог без переключения на внешние платформы. История изменений фиксирует все правки и комментарии, что повышает прозрачность работы и снижает риск конфликтов.

**Технологический стек**

Для реализации платформы выбран современный технологический стек, обеспечивающий высокую производительность, масштабируемость и удобство разработки.

Клиентская часть:

- React — библиотека для создания компонентных пользовательских интерфейсов. Позволяет разрабатывать динамические и отзывчивые веб-приложения с возможностью повторного использования компонентов.
- TypeScript — надмножество JavaScript с поддержкой статической типизации. Повышает надежность кода, минимизируя ошибки на этапе разработки.
- Tanstack Query — библиотека для управления состоянием данных на клиенте. Упрощает работу с API, кэширование и автоматическую синхронизацию данных.
- MUI (Material-UI) — набор компонентов, реализующих Material Design. Обеспечивает единообразие интерфейса и ускоряет создание визуальных элементов.

Серверная часть:

- Node.js — серверная платформа на JavaScript, обеспечивающая высокую производительность за счёт асинхронной архитектуры.
- Nest.js — фреймворк для построения структурированных серверных приложений. Поддерживает TypeScript и паттерны MVC, что упрощает поддержку кода.
- PostgreSQL — реляционная СУБД с открытым исходным кодом. Гарантирует надёжное хранение данных, включая расписания, задачи и пользовательские настройки.

● Sequelize — ORM (Object-Relational Mapping) для взаимодействия с базой данных. Позволяет работать с данными через объекты, избегая написания SQL-запросов вручную.

Выбор React обусловлен его гибкостью и поддержкой сообщества, что критично для быстрого прототипирования. Nest.js, в свою очередь, обеспечивает структурированность кода и безопасность за счёт встроенной валидации данных.

**Теоретическая и практическая значимость**

Разработка платформы опирается на принципы персонализации обучения, описанные Е.В. Карповой, где акцент смещается с пассивного усвоения информации на активное управление знаниями [5]. Интеграция функций визуализации согласуется с исследованием Т.В. Шипуновой [6], где подчёркивается роль саморегуляции в условиях цифрового обучения.

На практическом уровне внедрение подобного инструмента может привести к снижению академической тревожности за счёт чёткой структуризации задач и наглядного отображения прогресса. Например, студент, видя, что 80% заданий по дисциплине «Философия науки» выполнены, испытывает меньше стресса перед экзаменом. Геймификация превращает рутинные задачи в соревновательный процесс, повышая вовлечённость.

Экономический эффект проявляется в сокращении затрат вузов на поддержку студентов. Автоматизация напоминаний и централизация учебных материалов снижают нагрузку на кураторов, а уменьшение числа академических задолженностей повышает общую эффективность образовательного процесса.

Цифровизация образования требует не только технологических инноваций, но и переосмысления роли студента как активного участника образовательного процесса. Предлагаемое веб-приложение, объединяющее функции персонального ассистента, инструмента групповой работы и визуального планировщика, создаёт среду, где технологии служат основой для осознанного обучения. Оно не только решает текущие проблемы самоорганизации, но и формирует навыки, необходимые для lifelong learning — умение управлять временем, работать в команде и адаптироваться к изменениям.

Дальнейшие исследования могут быть направлены на интеграцию искусственного интеллекта для прогнозирования учебной нагрузки или анализа когнитивных паттернов студентов. Однако уже сейчас очевидно: будущее образования лежит в гармонии между технологиями и человеко-ориентированным подходом, где каждый студент получает инструменты для построения собственной траектории развития.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рынок высшего онлайн-образования в 2024 году вырос на 36% [Электронный ресурс]: Сайт РБК Тренды. URL: https://trends.rbc.ru дата обращения: 05.04.2025).
2. Романова Ю.С. Современное дистанционное обучение глазами студентов: анализ преимуществ, недостатков и пути совершенствования / Пастухова Е.В. // Научно-методический электронный журнал «Концепт». – 2024. – № 12. – С. 276–289.
3. Робустова Е.В. Самоорганизация студентов в условиях онлайн-обучения: к постановке проблемы / Люкина Н.М. // Сборник научных статей II-ой Всероссийской научно-практической конференции. – 2023. – С. 115–120.
4. Иванушкина Н.В. Использование цифровых технологий при реализации дистанционного обучения в вузе / Щипова О.В. // Известия Самарского научного центра Российской академии наук. – 2023. – Т. 25, № 2. – С. 12–19.
5. Карпова Е.В. Мотивация достижения в структуре мотивационного обеспечения учебной деятельности и методика ее диагностики // Ярославский педагогический вестник. – 2012. – № 2. – С. 328–333.
6. Шипунова Т.В. Учебная мотивация студентов до и в период пандемии: сигналы для совершенствования образовательного процесса в вузе // Непрерывное образование: XXI век. – 2022. – № 3(39). – С. 1–13.
7. Напсо М.Д. Противоречивые реалии онлайн-образования // Альманах «Казачество». – 2023. – С. 20–26.



***УДК 658.3.07***



***Низамов Н.А.***
***Научный руководитель: Гаранина М.П., канд. экон. наук, доц.***
*Самарский государственный технический университет,*
*г. Самара, Россия*


## ИННОВАЦИОННЫЕ ЦИФРОВЫЕ ИНСТРУМЕНТЫ ДЛЯ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

Современный рынок труда и стремительное развитие технологий устанавливают новые правила для управления человеческими ресурсами. Организации, стремящиеся увеличить собственную конкурентоспособность, анализируют цифровизацию HR не как опцию,

а как стратегическую потребность. От введения инновационных инструментов зависит не только результативность поиска и подбора работников, но и качество развития персонала, удержания основных экспертов, развития индивидуальной траектории карьерного роста. В отличие от традиционных методов, цифровые решения гарантируют гибкость, ясность и возможность быстрой адаптации к изменениям внешней среды.

Искусственный интеллект (ИИ) занял ключевую позицию среди новых инструментов, используемых в управлении человеческими ресурсами. Автоматизированные системы рекрутмента применяют ИИ для обработки больших объёмов данных о кандидатах, что дает возможность быстро и четко обнаруживать совпадения между профилями соискателей и требованиями вакансий. К примеру, чат-боты гарантируют основное взаимодействие с претендентами, автоматическую сортировку резюме, осуществление онлайн-интервью с применением алгоритмов определения речи и эмоций. Использование ИИ позволяет стимулировать процессы, уменьшать воздействие человеческого фактора и гарантировать объективность отбора [2].

В нефтегазовом секторе ИИ особенно популярен в отборе и адаптации работников в обстоятельствах значительной конкуренции за технические и рабочие кадры. Примером может быть введение системы Huntly.ai в «Газпром нефти», которая исследует профессиональный профиль кандидатов и автоматизирует основные интервью, выявляя лучшие результаты по тысячам характеристик: опыт, навыки, готовность к сменному графику и командировкам.

Аналитика демонстрирует, что такие решения уменьшают период найма инженеров практически на 40% и могут помочь прогнозировать профессиональную благополучность сотрудника на производстве с точностью до 80%. ИИ, кроме того, может помочь выявлять риски текучести значимых сотрудников на удалённых объектах, проанализировав огромное число факторов вплоть до погодных условий и профессиональной истории.

На этапе развития и удержания сотрудников внедрение алгоритмов машинного обучения может помочь выявлять персональные потребности в обучении и развитии, создавать персонализированные программы повышения квалификации. Многочисленные компании рассматривают действия работников с помощью ИИ, для того чтобы прогнозировать уровень сопричастности, возможные риски ухода из фирмы и предварительно принимать меры по удержанию основных экспертов.

Внедрение облачных экосистем упрощает процессы интеграции новых работников, гарантирует прозрачность карьерных траекторий, создает общее информационное пространство. Доступность разных HR-сервисов через мобильные приложения стимулирует коммуникации, упрощает доступ к обучающим материалам, внутренним вакансиям, корпоративным новостям. Отдельное направление — HR-аналитика на основе облачных платформ, которая дает возможность принимать решения на основе анализа больших данных и создавать мониторинги стратегических кадровых потребностей [4].

Крупные нефтегазовые фирмы, такие как «ЛУКОЙЛ» и Shell, активно внедряют облачные HRM-системы (к примеру, SAP SuccessFactors). Это дает возможность централизовать сведения о работниках на удалённых промыслах, увеличивать процессы согласований и обучения, а кроме того, согласовывать крупные проекты с участием международных команд. Облачные экосистемы интегрируются с производственными системами контроля труда и безопасности, обеспечивая двойную отчётность и минимизируя погрешности. Согласно исследованию Deloitte, 80% топ-нефтегазовых фирм заметили снижение времени на управление персонала уже после перехода в облако, а скорость подготовки профессиональных отчётов увеличилась в 2–2,5 раза при синхронном уменьшении расходов на бумажные процессы и внутренний ИТ-саппорт.

Интеллектуальные системы автоматизации применяются и при управлении обучением, организацией коллективных мероприятий, управлении внутренним документооборотом. С их поддержкой уменьшаются ошибки, снижается влияние человеческого фактора, убыстряются процессы и освобождается время для решения творческих и стратегических проблем HR-отделов. Одновременно такие инструменты дают возможность поддерживать высокий стандарт корпоративного обслуживания работников и улучшать их пользовательский опыт.

В нефтегазовой отрасли автоматизация дает возможность оперативно обслуживать большие потоки работников: осуществлять учёт вахтовиков, оформлять перемещения между объектами, подвергать обработке заявки на обучение и повышение квалификации. К примеру, в ПАО «Татнефть» чат-боты в основе внутренней HR-системы мгновенно информируют работников о сменах, выдаче спецодежды, итогах медицинских осмотров, а кроме того, собирают заказы на поездки и обучение без излишней бюрократии. Аналитика компании продемонстрировала, что автоматизация трудовых процессов уменьшила на 35% количество ошибок при документообороте и

уменьшила нагрузку на HR-службы в три раза. Помимо этого, интеллектуальные системы моделирования персональных нужд содействуют уменьшению простоев из-за недостатка сотрудников

Инновационные HR-системы дают возможность составлять и исследовать огромные массивы данных — от данных по эффективности работы каждого работника до сведений о внутренних действиях фирмы и рыночных тенденций. Использование Big Data в HR открывает новые возможности: компании могут выявлять паттерны текучести персонала, прогнозировать риски профессионального выгорания, исследовать результативность разных каналов найма [1].

Кадровая аналитика используется для автоматического выявления талантов внутри компании, оценки эффективности мотивирующих проектов, развития индивидуальных карьерных треков. В совокупности подобные инструменты дают возможность сделать регулирование человеческим капиталом предельно научно аргументированным, уменьшить воздействие субъективных условий и увеличить достоверность профессиональных решений.

Нефтегазовая отрасль — лидер по введению кадровой аналитики. К примеру, в «Роснефти» используется аналитика Big Data для предиктивного рассмотрения текучести сотрудников, построения карьерных треков и оптимизации программ обучения. Таким образом, исследование исходных данных по производительности, условиям труда и социальным характеристикам, позволяет прогнозировать преждевременные увольнения и осуществлять упреждающие мероприятия. Практика исследования проектов подтверждает, что уровень текучести был снижен на 18% за год.

Аналитические системы интегрируются с системами безопасности на объектах, позволяя выявлять закономерности между прохождением тренингов и уровнем производственного травматизма, что содействует увеличению эффективности мер по охране труда.

Формирование мобильных HR-платформ — еще один сильный драйвер изменений. Фирмы дают работникам возможность получать доступ к основным HR-сервисам через мобильные устройства: независимо управлять отпусками, командировками, осуществлять дистанционное обучение, отправлять заявки на внутренние вакансии. Специализированные мобильные приложения поддерживают корпоративные коммуникации, дают возможность быстро отвечать на изменения и незамедлительно решать профессиональные задачи.

Гибридный и дистанционный форматы работы проявляют воздействие не только на гибкость бизнеса, но и на способы передачи корпоративной культуры, уровень сопричастности и преданности

работников. Инновационные цифровые инструменты поддерживают условные команды, формируя интерактивные среды для коллективной работы, обмена знаниями, выполнения онлайн-мероприятий и обучения.

Мобильные приложения и платформы дистанционного HR-менеджмента в особенности значимы для поддержки мобильных либо вахтовых работников нефтегазовых компаний. В «СИБУРе» применяется свое приложение, с помощью которого рабочие по пути на объекты могут координировать графики, получать уведомления о сменах, принимать участие в корпоративных выборочных опросах, проходить микрообучение и закреплять обратную связь по бытовым вопросам. Для управляющих переносимый HR-доступ стал инструментом управления распределёнными бригадами, а для работников — комфортным методом оставаться на связи и быть в курсе важных процессов. По данным внутреннего аудита фирм сектора, комплексные мобильные решения понизили число недоразумений с заменами смен на 25% и увеличили удовлетворение работников корпоративной поддержкой на 30%. Смешанный формат становится обычным в том числе и для такого рода традиционно офлайн-индустрии, как нефтегаз [3].

В современных обстоятельствах успех организаций непосредственно находится в зависимости от эффективности применения инновационных цифровых инструментов для управления персоналом. Активное внедрение ИИ, облачных платформ, систем автоматизации и специалистов преобразует классические HR-процессы, делая их наиболее гибкими, прозрачными и технологичными. Верный выбор и интеграция новых систем дают возможность создавать персонализированные траектории развития, создавать команду специалистов и гарантировать долговременное конкурентное преимущество фирмы. Цифровая трансформация HR — это не просто замена инструментов, а новая модель управления человеческими ресурсами, открывающая уникальные возможности для выявления возможности каждого работника и достижения стратегических целей бизнеса.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Козлова Д.В., Пигарев Д.Ю. Цифровая трансформация нефтегазовой отрасли: барьеры и пути их преодоления // Газовая промышленность. Цифовнзация. 2020. №7 (803). С. 34-38.

2. Колупаев СЛ. Дополненная реальность - как новый шаг в развитии нефтегазового комплекса // Новые информационные технологии в нефтегазовой отрасли и образовании. 2015. С. 41-45.

3. Столбова Е.А., Бренделева Е.А. Основы цифровой экономики: учеб. пособие / под ред. М.И. Столбова, Е.А. Бренделевой. М.: Науч. б-ка, 2022. 238 с.

4. Цифровая трансформация: ожидания и реальность: докл. к XXIII Ясинской (Апрельской) междунар. науч. конф. по проблемам развития экономики и общества, Москва, 2022 г. / Г. И. Абдрахманова, С. А. Васильковский, К. О. Вишневский, М. А. Гершман, Л. М. Гохберг и др.; рук. авт. кол. П. Б. Рудник; Нац. исслед. ун-т «Высшая школа экономики». – М.: Изд. дом Высшей школы экономики, 2022. – 221 с.

***УДК 511***

***Новосельцев В.Д.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ТЕОРИЯ ЧИСЕЛ В ДИСКРЕТНОЙ МАТЕМАТИКЕ: ПРОСТЫЕ ЧИСЛА И ИХ СВОЙСТВА

Теория чисел, являющаяся одной из старейших и наиболее фундаментальных областей математики, играет ключевую роль в дискретной математике и её приложениях. Простые числа привлекают к себе особый интерес благодаря своим уникальным свойствам и широкому применению в современных технологиях, например, криптографию и алгоритмы. Простым числом называется натуральное число, большее единицы, которое делится только на себя и на единицу. Эти числа, несмотря на свою простоту, обладают глубокими и сложными свойствами, которые продолжают изучаться, и которым продолжают находить новые применения.

Одним из фундаментальных результатов теории простых чисел является теорема Евклида, которая утверждает, что простых чисел бесконечно много. Доказательство данной теоремы, предложенное ещё в древности, основывается на предположении о конечности множества простых чисел и приводит к противоречию, что доказывает их бесконечность. Однако распределение простых чисел в натуральном ряду остаётся одной из самых сложных задач математики. Гипотеза Римана, связанная с распределением нулей дзета-функции, до сих пор не доказана и считается одной из важнейших нерешённых проблем

математики. Теорема о распределении простых чисел, доказанная в конце XIX века, утверждает, что количество простых чисел, не превышающих заданного числа, приблизительно равно (1).

$$n/\ln(n) \tag{1}$$

где $n$ – заданное натуральное число.

Это показывает, что простые числа появляются реже по мере роста $n$, но их количество всё равно бесконечно.

Простые числа обладают рядом уникальных свойств, которые делают их незаменимыми в различных областях. Например, основная теорема арифметики утверждает, что каждое натуральное число, большее единицы, может быть единственным образом разложено в произведение простых чисел. Это свойство лежит в основе многих алгоритмов и криптографических систем. Кроме того, простые числа тесно связаны с понятием взаимной простоты: два числа называются взаимно простыми, если их наибольший общий делитель равен единице. Это свойство используется, например, в алгоритме Евклида для нахождения наибольшего общего делителя, который является ключевым элементом в криптографии. Алгоритм Евклида не только эффективно находит наибольший общий делитель, но и используется для решения линейных диофантовых уравнений.

В криптографии простые числа играют центральную роль благодаря своей сложности факторизации. Факторизация — это процесс разложения числа на простые множители. Для больших чисел этот процесс становится чрезвычайно сложным. Это делает простые числа идеальными для использования в криптографических системах. Одним из самых известных примеров является алгоритм RSA, который широко используется для шифрования данных. В основе RSA лежит использование двух больших простых чисел, произведение которых образует открытый ключ. Безопасность системы основывается на том, что факторизация этого произведения является вычислительно сложной задачей, особенно если простые числа выбраны достаточно большими. Взлом RSA-шифрования с ключом длиной 2048 бит при текущем уровне технологий практически невозможен.

Также простые числа используются в хеш-функциях, которые являются основой многих структур данных, таких как хеш-таблицы. Хеш-функции обеспечивают равномерное распределение данных и минимизируют вероятность коллизий. Кроме того, простые числа используются в алгоритмах проверки простоты, таких как тест Миллера-Рабина, который позволяет эффективно проверять, является

ли число простым. Этот алгоритм широко применяется в криптографии для генерации больших простых чисел. Тест Миллера-Рабина является вероятностным, то есть он может с небольшой вероятностью ошибочно признать составное число простым, но эта вероятность может быть сделана сколь угодно малой за счёт увеличения числа итераций.

Одной из интересных областей исследования простых чисел является их распределение в различных последовательностях. Например, простые числа-близнецы — это пары простых чисел, которые отличаются друг от друга на 2, такие как (3, 5) или (11, 13). Гипотеза о бесконечности таких пар до сих пор не доказана, хотя в 2013 году было доказано, что существует бесконечно много пар простых чисел, отличающихся на конечное значение. Изучаются другие типы простых чисел, такие как простые числа Софи Жермен. Это такие простые числа p, что число 2p + 1 также простое.

Простые числа связаны с другими важными математическими концепциями, такими как функция Эйлера, которая определяет количество чисел, меньших данного числа и взаимно простых с ним. Эта функция используется в алгоритме RSA для вычисления закрытого ключа. Функция Эйлера также играет важную роль в теории групп и полей. Она являются основой многих современных алгоритмов и криптографических систем. В теории групп простые числа используются для изучения структуры конечных групп, что имеет важное значение для понимания симметрий и других свойств математических объектов.

В заключение можно сказать, что простые числа представляют собой одну из самых глубоких и важных областей математики. Их уникальные свойства и сложность факторизации делают их незаменимыми в криптографии и алгоритмах. Исследования в области простых чисел продолжают открывать новые горизонты, как в теоретической математике, так и в практических приложениях. Понимание их свойств остаётся одной из ключевых задач, решение которой может привести к новым прорывам в науке и технологиях. Изучение простых чисел продолжает вдохновлять математиков и инженеров, открывая новые возможности для развития науки и техники.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гончарова А. А. Криптография и её основы в дискретной математике // Сборник докладов Международной научно-технической конференции молодых ученых БГТУ им. В.Г. Шухова – Белгород:

Белгородский государственный технологический университет им. В.Г. Шухова, 2024 г. – 84 – 87 с.

2. Рязанов, Ю. Д. Дискретная математика: учебное пособие для студентов высших учебных заведений, обучающихся по направлению 230100 "Информатика и вычислительная техника" / Ю. Д. Рязанов; Ю. Д. Рязанов; Федеральное агентство по образованию, Белгородский гос. технологический ун-т им. В. Г. Шухова. - Белгород: БГТУ им. В. Г. Шухова, 2010. – 273 с.

3. Воронин С. М. Простые числа // Москва: Знание, 1978 – 64 с.

4. Miller G. L. Riemann's Hypothesis and Tests for Primality // Journal of Computer and System Sciences. — 1975. — Vol. 13, № 3. — P. 300-317.

***УДК 004.056.5***

***Новосельцев В.Д.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КИБЕРБЕЗОПАСНОСТЬ: СУЩЕСТВУЮЩИЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ ДАННЫХ

Кибербезопасность в современном мире является одной из ключевых областей, требующих постоянного внимания и развития. С ростом цифровизации практически всех сфер жизни человека увеличивается и количество киберугроз. Эти угрозы становятся всё более изощрёнными и опасными. Среди наиболее актуальных сегодня выделяются ransomware-атаки, фишинг, а также утечки данных, приводящие к серьёзным финансовым и репутационным потерям для компаний и частных лиц. В этой статье будут рассмотрены современные киберугрозы и методы защиты данных, включая использование блокчейна, криптографии, искусственного интеллекта и других передовых технологий.

Ransomware (программы-вымогатели) представляют собой одну из самых опасных форм кибератак. Данные программы шифруют данные жертвы, блокируя доступ к ним, и требуют выкуп за расшифровку. В последние годы ransomware-атаки стали более масштабными и изощрёнными. Например, атака WannaCry в 2017 году затронула сотни тысяч компьютеров по всему миру, включая системы здравоохранения, финансовые учреждения и государственные организации. Современные ransomware-атаки пользуются методами социальной инженерии, чтобы обманом заставить пользователей загрузить вредоносное ПО, или

эксплуатируют уязвимости в программном обеспечении. Для защиты от таких атак необходимо регулярно обновлять программное обеспечение, использовать антивирусные программы и обучать сотрудников основам кибербезопасности. Кроме того, важно создавать резервные копии данных, чтобы минимизировать ущерб в случае успешной атаки.

Фишинг — ещё одна распространённая угроза. Фишинговые атаки направлены на получение конфиденциальной информации, такой как логины, пароли или данные банковских карт, путём маскировки под доверенные источники. Это могут быть персонализированные сообщения или поддельные веб-сайты, которые выглядят практически идентично настоящим. Например, злоумышленники могут отправить письмо, якобы от банка, с просьбой подтвердить данные учётной записи. Для защиты от фишинга важно использовать двухфакторную аутентификацию, проверять подлинность сайтов и обучать пользователей распознавать подозрительные сообщения. Также полезно внедрять системы фильтрации электронной почты, автоматически блокирующие фишинговые письма.

Утечки данных также остаются серьёзной проблемой. Киберпреступники часто взламывают базы данных компаний, чтобы получить доступ к персональной информации клиентов: имена, адреса, номера телефонов и даже данные кредитных карт. Утечки могут происходить из-за слабой защиты серверов, уязвимостей в программном обеспечении или человеческого фактора. Для предотвращения утечек данных необходимо использовать шифрование данных, как на этапе хранения, так и при передаче, а также регулярно проводить аудиты безопасности. Также важно предоставлять доступ к конфиденциальной информации только тем сотрудникам, которым она действительно необходима для выполнения их обязанностей.

Одним из перспективных методов защиты данных является использование блокчейн-технологий. Блокчейн — распределённая база данных, которая обеспечивает высокий уровень безопасности за счёт децентрализации и криптографической защиты. Каждый блок в цепочке содержит информацию о предыдущих блоках, что делает практически невозможным изменение данных без согласия большинства участников сети. Блокчейн может быть использован для защиты транзакций, хранения данных и обеспечения прозрачности процессов. Например, в финансовой сфере блокчейн уже применяется для создания безопасных платёжных систем, а в логистике — для отслеживания цепочек поставок. Кроме того, блокчейн может быть полезен для защиты от подделки документов и обеспечения аутентичности данных.

Криптография тоже играет ключевую роль в обеспечении кибербезопасности. Современные криптографические методы, такие как асимметричное шифрование и электронные подписи, позволяют защищать данные от несанкционированного доступа и обеспечивать их целостность. Асимметричное шифрование использует пару ключей — открытый и закрытый, что позволяет безопасно передавать данные даже по незащищённым каналам. Электронные подписи обеспечивают аутентификацию и подтверждение подлинности документов. Однако с развитием квантовых вычислений традиционные криптографические методы могут стать уязвимыми. Это стимулирует разработку постквантовой криптографии. Постквантовая криптография использует алгоритмы, устойчивые к атакам квантовых компьютеров, что делает её важным инструментом для защиты данных в будущем.

Искусственный интеллект (ИИ) и машинное обучение начинают играть важную роль в борьбе с киберугрозами. Данные технологии позволяют анализировать огромные объёмы данных в реальном времени, выявляя аномалии и потенциальные угрозы. Например, системы на основе ИИ могут обнаружить подозрительную активность в сети, например, попытки несанкционированного доступа или атаки типа DDoS. Кроме того, ИИ может использоваться для автоматизации процессов реагирования на инциденты, что позволяет минимизировать ущерб от кибератак. Системы на основе ИИ могут автоматически блокировать подозрительные IP-адреса или изолировать заражённые устройства от сети.

Однако, несмотря на все существующие устойчивые к кибератакам современные технологии, человеческий фактор остаётся одним из самых слабых звеньев в системе кибербезопасности. Многие атаки становятся возможными из-за ошибок сотрудников: использование слабых паролей, переход по подозрительным ссылкам. Поэтому важно не только внедрять средства защиты, но и регулярно обучать сотрудников основам кибербезопасности. Программы обучения должны включать в себя информацию о том, как распознавать фишинговые письма, создавать надёжные пароли и избегать утечек данных. Кроме того, важно проводить регулярные тестирования на уязвимость, такие как фишинговые симуляции, чтобы оценить уровень подготовки сотрудников и выявить слабые места.

Кибербезопасность в современном мире — это сложная и многогранная задача, требующая постоянного внимания, инвестиций и инноваций. Технологии, такие как блокчейн, криптография и искусственный интеллект, предлагают мощные инструменты для защиты данных, но их эффективность зависит от правильного

использования и интеграции в общую стратегию безопасности. В конечном итоге, успех в борьбе с киберугрозами зависит от сочетания технологических решений, грамотного управления и осознанного поведения каждого пользователя.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева, Е. П., Коршак, К. С., Сиротин, И. В. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, К. С. Коршак, И. В. Сиротин // Наукоёмкие технологии и инновации (XXV научные чтения): сборник докладов Международной научно-практической конференции. - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. - С. 717-720.

2. Галатенко В.А. Основы информационной безопасности: Учеб. пособие / Под ред. В.Б. Бетелина. М.: ИНТУИТ.РУ, 2004. 261 с.

3. Зегжда Д.П., Москвин Д.А., Мясников А.В. Обеспечение киберустойчивости систем распределенного хранения данных с применением технологии blockchain // Проблемы информационной безопасности. Компьютерные системы. - 2018. - № 2. - С.74-79.

4. Петренко С.А. Политики безопасности компании при работе в интернет / Петренко С.А., Курбатов В.А. // Информационные технологии для инженеров. Изд. ДМК пресс - 2011. - С.15-34.

***УДК 004.27***

***Новосельцев В.Д.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: ПРИНЦИПЫ РАБОТЫ И ПЕРСПЕКТИВЫ

Квантовые вычисления – это абсолютно новый подход к обработке информации, который базируется на принципах квантовой механики. В то время как классические компьютеры используют биты, в квантовых компьютерах применяются кубиты. Главная особенность кубитов – они способны находиться в суперпозиции состояний, что открывает новые возможности для решения задач, считавшихся неразрешимыми за приемлемое время (если и есть возможность их решить, то это займёт очень длинный промежуток времени). В данной статье

рассматриваются основные принципы работы квантовых вычислений, их потенциальное влияние на криптографию и перспективы применения в различных областях науки и техники.

Классические компьютеры, основанные на архитектуре фон Неймана, достигли значительных успехов в обработке информации. Однако их возможности ограничены физическими пределами. В квантовых вычислениях применяются такие явления квантовой механики, как суперпозиция, запутанность и интерференция. Именно благодаря данным явлениям квантовые компьютеры, обрабатывая огромное количество информации одновременно, способны решать задачи, которые не могут решить классические системы.

Кубит (квантовый бит) – основная единица информации в квантовом компьютере. В отличие от бита, который может принимать только одно состояние (0 или 1), он находится сразу в обоих состояниях. Это делает квантовые вычисления экспоненциально мощнее классических. Ниже представлена формула для описания состояния кубита (математически это вектор в двумерном комплексном пространстве):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

где $\alpha$ и $\beta$ - амплитуды вероятностей.

Запутанность — это уникальное явление, особенность которого заключается в связывании состояний двух или более кубитов, находящихся друг от друга на неограниченном расстоянии. То есть, если как-либо изменится состояние одного кубита, то состояния связанных с ним кубитов также изменятся. Благодаря этому свойству квантовые компьютеры способны обрабатывать информацию с высокой степенью параллелизма.

Запутанность является ключевым элементом многих квантовых алгоритмов, таких как алгоритм Шора и алгоритм Гровера. Благодаря квантовой телепортации, основным механизмом которой является запутанность, в будущем возможно создание технологий для передачи информации на огромные расстояния.

Интерференция — ещё одно явление квантовой механики, из-за которого амплитуды вероятностей состояний кубитов могут складываться или вычитаться. Интерференция также используется в различных квантовых алгоритмах (в том числе и в вышеупомянутых алгоритмах Шора и Гровера).

Алгоритм Гровера позволяет найти элемент в неупорядоченной базе данных за время, пропорциональное квадратному корню из числа элементов, что значительно быстрее, чем классические алгоритмы.

Смысл алгоритма Шора, разработанного в 1994 году, заключается в том, чтобы квантовый компьютер, способный его выполнить, мог взломать такие современные криптографические системы, как RSA и ECC, что делает их фактически бесполезными.

Для решения данной проблемы разрабатываются новые методы криптографии, устойчивые к атакам квантовых компьютеров. Постквантовая криптография включает алгоритмы, основанные на математических задачах, которые остаются сложными даже для квантовых систем. Примеры таких задач: решётки, многомерные полиномы и хеш-функции.

Национальный институт стандартов и технологий (NIST) проводит конкурс на стандартизацию постквантовых криптографических алгоритмов. Ожидается, что в ближайшие годы будут выбраны новые стандарты, которые заменят уязвимые методы шифрования.

В наше время квантовые алгоритмы уже применяются для решения задач оптимизации (поиск оптимального маршрута или распределение ресурсов). Например, квантовый отжиг применяется в коммерческой системе D-Wave для достижения вышеупомянутых целей.

Одной из наиболее перспективных областей применения квантовых вычислений является моделирование сложных квантовых систем, таких как молекулы. Данное открытие может привести к прорыву в химии, фармакологии и материаловедении. Откроются пути к разработке новых лекарств и сверхпроводников.

Благодаря квантовым компьютерам скорее всего произойдёт резкий скачок в развитии и обучении нейронных сетей. Квантовые версии алгоритмов машинного обучения, такие как квантовый метод опорных векторов, уже демонстрируют потенциал в решении задач классификации и кластеризации.

Ещё одна сфера применения квантовых компьютеров - анализ больших объёмов данных в реальном времени. Это позволит улучшить прогнозирование и принятие решений в различных областях, от медицины до финансов.

Несмотря на значительный прогресс, квантовые компьютеры всё ещё сталкиваются с серьёзными техническими проблемами, такими как декогеренция (потеря квантовой информации из-за взаимодействия с окружающей средой) и ошибки квантовых операций. Например, современные квантовые компьютеры, что разрабатываются IBM и Google, имеют ограниченное число кубитов и высокий уровень ошибок.

Разработка квантовых корректоров ошибок и стабильных кубитов – ключевая задача для решения данных проблем.

Ожидается, что в ближайшие десятилетия для квантовых компьютеров найдут применение в таких областях, как финансы, логистика, фармацевтика и материаловедение.

Квантовые вычисления — это не просто новая технология, это новый способ мышления, который может изменить наше понимание мира и наши возможности в решении глобальных проблем. Их развитие требует не только технических инноваций, но и глубокого осмысления этических и социальных последствий.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Дрогомерецкая Е. В., Коломыцева Е. П. Архитектура фон Неймана // Молодёжь и научно-технический прогресс: сборник докладов XVI международной научно-практической конференции студентов, аспирантов и молодых ученых – Губкин-Старый Оскол: Общество с ограниченной ответственностью "Ассистент плюс", 2023 – с. 250-252

2. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. — Москва: Мир, 2006. — 824 с.

3. P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994. — P. 124–134.

***УДК 666.94:621.926***

***Павлов Д.А., Бадрисламов Д.И., Маньянов А.Р.***
***Научный руководитель: Будько Е.А., канд. фил. наук, доц.***
*Нефтекамский филиал уфимского университета наук и технологий,*
*г. Нефтекамск, Россия*

## ПРОБЛЕМА ЦИФРОВОГО НЕРАВЕНСТВА

В современном цифровом мире доступ к технологиям стал основополагающим фактором, определяющим возможности получения образования, перспективы карьерного роста и доступ к основным услугам. Несмотря на технологические достижения, значительная часть населения мира — более 30%, по данным Международного союза электросвязи, — по-прежнему не подключена к цифровой среде, что усугубляет социально-экономическое неравенство. Этот сохраняющийся цифровой разрыв представляет собой серьёзную

проблему, требующую безотлагательного решения, особенно в развивающихся странах, где финансовые ограничения, географические барьеры и социальное неравенство создают сложные препятствия для цифровой интеграции.

Цифровое неравенство проявляется в следующих аспектах:

1. Инфраструктурный разрыв:

1) Отсутствие надежного интернет-соединения в отдаленных районах.

2) Невозможность приобретения устройств (компьютеров, смартфонов) из-за финансовых ограничений.

2. Дефицит цифровых навыков:

1) Недостаток знаний для эффективного использования технологий, особенно среди пожилых людей.

3. Доступность контента:

1) Языковые барьеры и отсутствие культурно релевантного контента.

4. Социальная маргинализация:

1) Исключение уязвимых групп (инвалидов, сельских жителей) из цифровой среды.

Основными факторами, способствующими цифровому разрыву, являются:

1) Финансовое положение: низкие доходы ограничивают доступ к технологиям.

2) Географическое положение: в сельских и отдаленных районах инфраструктура развита слабо.

3) Образование: отсутствие ИТ-навыков затрудняет использование цифровых инструментов.

4) Возраст и здоровье: пожилые люди и инвалиды сталкиваются с дополнительными барьерами.

5) Институциональные ограничения: недостаток государственных программ поддержки.

Неравный доступ к цифровым технологиям приводит к:

1) Углублению социально-экономического разрыва.

2) Ограничению возможностей в образовании и карьерном росте.

3) Маргинализации уязвимых групп населения.

4) Замедлению экономического развития регионов.

В работе использованы:

1) Анализ статистических данных (Международный союз электросвязи, Росстат).

2) Сравнительный анализ успешных инициатив в России и за рубежом.

3) Обзор научных публикаций и государственных программ.

В России только 65% сельских населенных пунктов обеспечены стабильным интернетом (против 95% в городах).

Среди людей старше 60 лет лишь 30% владеют базовыми цифровыми навыками.

Программы, такие как "Азбука интернета", демонстрируют эффективность, но их охват недостаточен.

Потери российской экономики:

1) До 1.5% ВВП ежегодно из-за низкой цифровизации регионов
2) Потери бюджета от недополученных налогов в IT-секторе - до 200 млрд руб./год
3) Снижение конкурентоспособности на мировых рынках

Для сокращения цифрового разрыва необходимы:

1) Развитие инфраструктуры в отдаленных регионах.
2) Создание бесплатных точек доступа в интернет (библиотеки, школы).
3) Программы повышения цифровой грамотности для уязвимых групп.
4) Субсидии на покупку устройств для малообеспеченных семей.
5) Государственно-частные партнерства для реализации проектов.

Россия: национальный проект "Цифровая экономика" обеспечил интернетом тысячи школ и сел.

Эстония: лидер в электронном управлении, внедрила онлайн-образование и программы для пожилых.

США: программа Lifeline субсидирует интернет для малоимущих.

ООН: инициатива GIGA направлена на подключение всех школ мира к интернету.

Проблема цифрового неравенства требует комплексного решения, включающего меры на глобальном, национальном и локальном уровнях. Успешные международные практики показывают, что сокращение разрыва возможно при совместных усилиях государства, бизнеса и общества. В России необходимо расширять существующие программы и адаптировать их к региональным особенностям.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Цифровое неравенство как новая форма социального неравенства – Режим доступа: https://cyberleninka.ru (Дата обращения 5.5.25)

2. Министерство цифрового развития РФ. Национальная программа «Цифровая экономика» – Режим доступа: https://digital.gov.ru (Дата обращения 5.5.25)
3. Федеральная служба государственной статистики. Цифровизация регионов России, 2022г. – Режим доступа: https://rosstat.gov.ru (Дата обращения 5.5.25)
4. Программа "Азбука интернета" для пенсионеров – Режим доступа: https://azbukainterneta.ru (Дата обращения 5.5.25)

***УДК: 656.7.022.1***

***Панова А.А.***
***Научный руководитель: Степаненко А.С., канд. техн. наук, доц.***
*Московский государственный технический университет гражданской авиации, г. Москва, Россия*

## PROCESS MINING КАК ИНСТРУМЕНТ ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ В ГРАЖДАНСКОЙ АВИАЦИИ

Оптимизация бизнес-процессов на сегодняшний день является одной из самых важных задач бизнеса [1]. Роботизация, автоматизация и повсеместное развитие цифровых технологий, интернет вещей, глобальные сети и массовая цифровизация стали ключевыми факторами развития возможностей исследования и оптимизации бизнес-процессов, одной из которых является интеллектуальный анализ процессов (Process Mining) [2].

Process Mining – это метод выявления, мониторинга и оптимизации процессов путем анализа данных из имеющихся журналов регистрации событий в информационных системах [3].

Указанная технология имеет следующие направления прикладного применения:

1. Выявление. Выполняется с помощью автоматической генерации модели процесса, из данных журналов.
2. Сравнение. Выявляются расхождения между теоретической моделью процесса и фактическим процессом. Полученные результаты используются для диагностики отклонений процесса и показателей его эффективности от идеальной модели.

Оптимизация. Теоретическая модель процесса корректируется от идеальной и оптимизируется на основе данных о реальном процессе [3].

Технология Process Mining эффективна в различных отраслях экономики – от телекоммуникаций до ритейла, банкинга и государственного сектора. Особый интерес она представляет для

транспортной отрасли, в том числе для гражданской авиации (ГА), где производительность бизнес-процессов, безопасность и повышение качества клиентского сервиса играет ключевую роль. В гражданской авиации данная технология актуальна, но не используется в России, в рамках научной работы сформирована архитектура инструмента по PM для типового процесса в ГА.

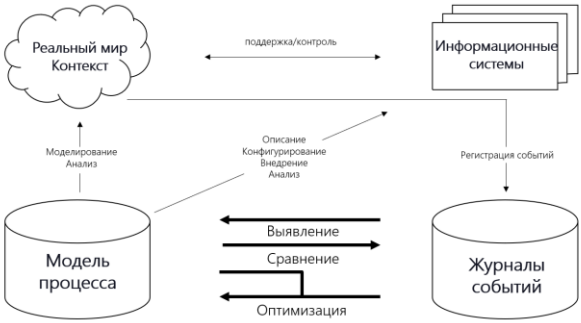



Рис. 1 – Модель осуществления Process Mining (составлен авторами)

Инструменты Process Mining интегрируется практически со всеми популярными автоматизированными системами (ERP, CRM, SCM и т.п.) При этом восстановленные модели процессов в совокупности с данными по времени исполнения процесса и элементами организационной структуры позволяют видеть все скрытые недостатки, обеспечивая владельцев бизнес-процесса [4, 5].

В качестве областей применения в гражданской авиации можно выделить операционные процессы авиакомпаний и аэропортов, а также контрагентов авиакомпаний, выполняющих технологические операции при организации пассажирских и грузовых воздушных перевозок.

При рассмотрении технологических процессов организации авиаперевозок, в рамках исследования отдано предпочтение аэропорту Внуково, как одному из самых перспективных, в сфере внедрения инноваций на территории Российской Федерации.

Процессное управление используется в качестве подхода к диспетчеризации операций в гражданской авиации и основывается на регламентирующих документах, в частности – федеральных авиационных правилах, внутренних документах авиакомпаний и аэропортов. Можно отметить положительные стороны использования данного подхода в контексте организации операционной деятельности

авиатранспортных предприятий в связи с четкими регламентами процессов, обусловленными как международным, так и национальным законодательством. В связи с вышесказанным прослеживается перспектива внедрения профильных инструментов процессного управления, таких как PM в диспетчеризацию технологических процессов организации перевозок на воздушном транспорте.

Для формирования архитектуры инструмента по использованию технологии Process Mining, выбран процесс обслуживания пассажиров в аэропорту в части оформления и обработки багажа, основанный на реальных инструкциях по обработке багажа в аэропорту Внуково.

Первый этап анализа данного бизнес-процесса – рассмотрение ключевых участников процесса, во-первых, это агент регистрации, основная задача которого заключается в приеме багажа от пассажира и его регистрация. Далее система обработки багажа аэропорта – её функции заключаются в транспортировки, сканирования и сортировки багажа. Сотрудники сортировочной зоны аэропорта, как правило, участвуют в финальной сортировке багажа по направлениям и загрузке в багажный отсек.

На втором этапе анализа процесса нужно сказать, что практически в каждой функции процесса происходит фиксация информации о багаже из различных корпоративных информационных систем в журнал логов событий, а также атрибутов, значимых для последующего анализа. В контексте гражданской авиации, как правило, это такие информационные системы как: система бронирования авиакомпании, система контроля вылета, система обработки багажа, система контроля погрузки багажа и так далее. Это позволяет обеспечить полную прозрачность процессов, отслеживать путь объекта на каждом этапе и выявлять потенциальные отклонения, узкие места и неэффективности.

Из главных плюсов внедрения Process Mining в процесс обработки багажа можно выделить следующие: поддержка принятия управленческих решений, обнаружение узких мест и отклонений, оптимизация времени прохождения этапов, прозрачность и визуализация реального процесса. В будущем данную технологию можно расширить на такие процессы, как: процессы службы организации пассажирских перевозок [6, 7], процессы службы организации грузовых перевозок, диспетчеризация ТГО и на многие другие бизнес-процессы различных авиатранспортных предприятий. Следовательно, можно говорить о широкой области применения данной технологии в гражданской авиации для оптимизации и управления операционными процессами перевозок, как для авиакомпании, так и для аэропортов и прочих контрагентов, выполняющих операции в

технологических процессах организации пассажирских и грузовых перевозок.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Елисеев, Б. П. Состояние, перспективы и проблемы внедрения управления бизнес-процессами авиапредприятий / Б. П. Елисеев, А. С. Борзова, Н. Д. Корягин // Инновации в гражданской авиации. – 2016. – № 4. – С. 5-16. – EDN XUVNSJ.
2. Джураев, М. М. Применение инструментов Process Mining для улучшения бизнес-процессов / М. М. Джураев, А. Н. Норкина // Финансовая безопасность. Современное состояние и перспективы развития: Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 14–15 декабря 2022 года. Том 2. – Москва: Национальный исследовательский ядерный университет "МИФИ", 2022. – С. 101-108. – EDN VMBPYC.
3. Хилти Д., Моррис Д., Шарсиг М. и др. Свод знаний по управлению бизнес-процессами: BPM CBOK 4.0 / пер. с англ. — Москва: Альпина Паблишер, 2022. — 504 с.
4. Степаненко, Е. В. Организация бизнес-процессов управления человеческими ресурсами авиапредприятия / Е. В. Степаненко. – Воронеж: Издательство "МИР", 2019. – 88 с. – ISBN 978-5-6042751-8-4. – EDN BNRZYQ.
5. Сушко, О. П. Моделирование авиапассажирских перевозок России / О. П. Сушко // Мир транспорта. – 2022. – Т. 20, № 6(103). – С. 64-71. – DOI 10.30932/1992-3252-2022-20-6-7. – EDN DKRGHV.
6. Больт, А. С. Организация пассажирских мультимодальных перевозок в современных условиях / А. С. Больт, П. С. Больт, А. В. Власова // Транспорт: наука, техника, управление. Научный информационный сборник. – 2024. – № 11. – С. 3-11. – DOI 10.36535/0236-1914-2024-11-1. – EDN TLYIPK.

*УДК 519.854.2*

***Письменный А.Б.***
***Научный руководитель: Островский А.М., канд. соц. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ГИБРИДНЫЕ ЭВРИСТИКИ ДЛЯ РАЗБИЕНИЯ МУЛЬТИМНОЖЕСТВ С РАВНЫМИ СУММАМИ

Одной из фундаментальных задач дискретной оптимизации, имеющей широкое практическое применение, является задача разделения мультимножества положительных целых чисел $S=\{x_1, x_2, \ldots, x_n\}$ на два подмножества $S_1$ и $S_2$ так, чтобы:

$$\sum_{x \in S_1} x = \sum_{x \in S_2} x \qquad (1)$$

Практическая важность задачи определяется её распространённостью в таких областях, как балансировка вычислительных нагрузок, распределение ресурсов и планирование расписаний.

Данная задача является NP-полной. Полный перебор всех $2^n$ возможных разбиений требует экспоненциального времени ($O(2^n)$), что делает практическое применение детерминированного полного метода невозможным даже при сравнительно небольших значениях n.

Псевдополиномиальные алгоритмы на основе динамического программирования (ДП) позволяют решить задачу за O(S), где S — агрегированная сумма значений элементов. Однако вычислительная эффективность данных алгоритмов существенно снижается с ростом мощности множества либо увеличением максимального значения его элементов. Более того, метод ДП требует объёма памяти O(S), что влечёт значительное потребление ресурсов памяти, делающее их применение затруднительным при $S \gtrsim 10^9$.

В связи с этим возрастает интерес к эвристическим методам, способным обеспечивать приемлемое качество решений при существенно меньших вычислительных затратах. В литературе [1-3] можно обнаружить разнообразные эвристические и метаэвристические подходы: вероятностные алгоритмы, основанные на случайном отборе и последующей корректировке решения; метаэвристики, такие как алгоритмы роя частиц и симулированного отжига; алгоритм

Кармаркара–Карпа, демонстрирующий сложность O(n log n), благодаря использованию двоичной кучи.

Несмотря на прогресс в развитии отдельных эвристических подходов, их эффективность может существенно варьироваться в зависимости от структуры задачи и параметров исходных данных.

Гибридные алгоритмы на их фоне дают наилучшие результаты при большом размере исходного мультимножества. Они объединяют глобальные методы поиска (например, генетические алгоритмы) с локальными процедурами оптимизации. При этом глобальный этап обеспечивает диверсификацию (поиск по широкому пространству), а локальный — интенсификацию (тонкая доработка каждого кандидата). Такой «двухэтапный» подход позволяет добиться высокой скорости сходимости и качества решения, снижая риск преждевременной конвергенции, характерной для чистых генетических или жадных стратегий.

В данной работе рассматриваются четыре локальные процедуры: метод первого улучшения, метод наилучшего улучшения, детерминированный подход с перемещениями и обменами, а также эвристика Кармаркара–Карпа. Каждая из них кратко характеризуется следующим образом:

1. Метод первого улучшения (МПУ). В рамках локального поиска по соседним решениям (например, перемещение одного элемента или обмен двух) алгоритм сразу переходит к первому найденному улучшению — как только обнаруживается сосед, снижающий разность сумм, он становится новым текущим решением. Это позволяет ускорить процесс поскольку нет необходимости анализировать все возможные переходы. Но это же порождает риск «застревания» в неглубоком локальном минимуме.

2. Метод лучшего улучшения (МЛУ) предполагает полный перебор всех соседей текущего решения. После анализа всей окрестности выбирается тот, при котором достигается наименьшая разность сумм. Такие изменения относительно предыдущего алгоритма закономерно приводят к более значительным улучшениям за одну итерацию, но они же приводят к заметно большему объёму вычислений, поскольку обрабатываются все допустимые перемещения или обмены.

3. Детерминированный метод с перемещением и обменами (ДПО) основывается на текущей разности между суммами двух подмножеств. В рамках одной итерации происходит поиск либо одного элемента, перенос которого в противоположную группу максимально уменьшает разность, либо пары элементов для обмена, обеспечивающей наибольшее снижение этой разности. Алгоритм жадно выбирает самый

выгодный шаг из этих двух стратегий, эффективно совмещая простоту перемещений и эффективность обменов.

4. Эвристика Кармаркара–Карпа (ЭКК) состоит из двух этапов. На первом этапе два наибольших элемента из массива заменяются их разностью, что означает их распределение по разным подмножествам. Это повторяется до тех пор, пока не останется одно число, отражающее текущую разность сумм. На втором этапе по полученным операциям восстанавливается конкретное разбиение. На практике данный метод часто демонстрирует высокое качество решений и работает эффективно — за время O(n log n) благодаря использованию кучи.

Сравнительный анализ этих процедур позволяет оценить их применимость и эффективность в составе гибридного генетического алгоритма в зависимости от характеристик решаемой задачи (см. рис. 1)

```
Отсортировать массив чисел numbers по неубыванию.
Инициализировать популяцию pop случайными разбиениями (бинарными масками).
Вычислить fitness (разность сумм) для каждого индивидуума; выбрать best с наименьшей разностью.
Если у best difference ≠ 0, улучшить best с помощью выбранного метода локального поиска.
Для generation = 1..MAX_GENERATIONS:
    Если у best разность = 0, прервать (найдено оптимальное разбиение).
    Создать пустую новую популяцию new_pop.
    Если ELITISM включён, добавить best в new_pop.
    Пока |new_pop| < POPULATION_SIZE:
        Выбрать parent1, parent2 через турнирную селекцию из текущей популяции.
        С вероятностью CROSSOVER_RATE выполнить кроссовер:
            Выбрать два случайных точки, скрещивать родителей → child1, child2.
        Иначе: child1 = copy(parent1), child2 = copy(parent2).
        Мутировать каждого child (меняя биты с вероятностью MUTATION_RATE).
        Добавить child1 и child2 в new_pop (до размера POPULATION_SIZE).
    Создать пустой список pop_fitness.
    Для каждого индивида ind в new_pop:
        improved = improve_method(ind)          # локальное улучшение
        fitness = compute_fitness(improved)    # разность сумм
        Если fitness = 0:                        # идеальное решение
            best = improved; прервать все циклы.
        Добавить (improved, fitness) в pop_fitness.
    Отсортировать pop_fitness по fitness.
    Если pop_fitness[0].fitness < best.fitness:
        best = pop_fitness[0].individuum.
Конец цикла по поколениям.
Вернуть разбиение из best.
```

Рис. 1. Псевдокод гибридного генетического алгоритма

Проведённые тесты подтверждают высокую устойчивость алгоритма к росту размерности задачи и разбросу значений, что особенно важно для практических приложений в условиях ограниченных ресурсов. При $n \geq 200$ и элементах множества, принимающих значения на отрезке [1; 20 000 000] алгоритм с большой вероятностью возвращает оптимальное решение при его наличии (реализация алгоритма представлена в соответствующей программе,

исходный код которой, а также результаты испытаний, доступны в репозитории по адресу: https://github.com/noxlight7/HybridGA)

Для оценки эффективности разработанного подхода была проведена серия вычислительных экспериментов. Для тестирования разработанного решения создавались dataset-ы, которые генерировались с использованием распределений значений элементов: равномерного, гамма, логарифмического и нормального распределения с различающимися размерами n. Полученные экспериментальные данные позволяют визуализировать влияние размеров входных данных на производительность алгоритма (см. рис.2)

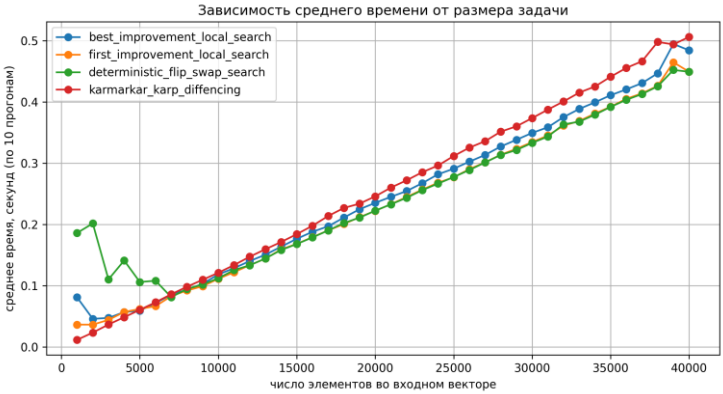



Рис. 2. Зависимость среднего времени выполнения алгоритма от размера задачи (нормальный закон распределения)

Анализ результатов показывает, что выбор наиболее эффективного метода локального поиска в значительной степени зависит от размерности задачи n, тогда как характер распределения весов оказывает лишь несущественное влияние на временные характеристики алгоритма. На основе полученных экспериментальных данных были выработаны практические рекомендации по выбору эвристик, систематизированные в виде обобщающей таблицы. Полученные выводы могут служить основой для дальнейшей адаптации гибридных эвристик к другим классам комбинаторных задач с аналогичной структурой. Кроме того, предложенный подход может быть использован в качестве эффективной основы для построения масштабируемых решений в задачах, требующих балансировки ресурсов в высоконагруженных вычислительных системах.

Таблица – Рекомендации по выбору метода локального поиска в зависимости от размера задачи

| Диапазон n | Наиболее эффективный метод |
|---|---|
| $n < 5000$ | ЭКК значительно превосходит другие по эффективности. Чем меньше n, тем значительнее разрыв с другими методами |
| $5000 \leq n < 7000$ | ЭКК показывает хорошие результаты, но МПУ может превосходить его на некоторых наборах данных |
| $7000 \leq n < 10000$ | МПУ, как правило, показывает лучшие результаты |
| $11000 \leq n < 14000$ | МПУ и ДПО стабильно показывают лучшие результаты, но МПУ несколько лучше |
| $n \geq 14000$ | МПУ и ДПО стабильно показывают лучшие результаты, но ДПО несколько лучше |

В рамках исследования проведён сравнительный анализ четырёх локальных процедур в составе гибридного генетического алгоритма для задачи разбиения мультимножества. Результаты показали, что эффективность эвристик преимущественно определяется размером входных данных, что обосновывает необходимость адаптивного выбора метода в зависимости от масштаба задачи. Разработанное гибридное решение является стабильным по скорости сходимости процесса и точности решений при сравнении с негибридными методами.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Gendreau, M., Potvin, J.-Y. Handbook of metaheuristics / ed. by M. Gendreau, J.-Y. Potvin. – 2nd ed. – New York : Springer, 2010. – 570 p.

2. Ong, Y.-S., Lim, M.-H., Chen, X., Zhu, Y. Memetic computation: past, present & future // IEEE Computational Intelligence Magazine. – 2010. – Vol. 5, № 2. – P. 24–31.

3. Neri, F., Cotta, C., Moscato, P. (eds.). Handbook of memetic algorithms. – Berlin : Springer, 2012. – 368 p.

4. Островский А.М. О компьютерных технологиях поиска эмпирических закономерностей в базах данных // Социология: 4М. — 2008. — №27. — С.140 — 157

5. Островский А.М. Оптимизация социального управления человеко-компьютерными системами в техническом вузе: Монография. — Белгород: Изд-во "Белаудит"; БГТУ им. В.Г. Шухова, 2003. — 208 с. — ISBN 5-7414-0083-3.

*УДК 004.9; 656.7*

***Подлеснова А.В.***
***Научный руководитель: Никифорова Л.Х., канд. экон. наук, доц.***
*Московский государственный технический университет гражданской авиации, г. Москва, Россия*

# СЕРВИСНО-ОРИЕНТИРОВАННАЯ АРХИТЕКТУРА НА ПРЕДПРИЯТИЯХ ГРАЖДАНСКОЙ АВИАЦИИ

В данный период времени мы находимся в 5-ом технологическом укладе, который связан с развитием информационно-компьютерных и коммуникационно-дистанционных технологий. Это эра разработки корпоративных сетей, программного обеспечения, а также создания архитектур предприятия. Соответственно, набирает популярность такое понятие, как «сервисно-ориентированная архитектура». Сервисно-ориентированная архитектура (далее - СОА) – это комплексный подход по созданию информационных систем, ориентированный на решение многих бизнес-задач [6]. С помощью СОА организации разрабатывают приложения на основе многоразовых интерфейсов сервисов, а также позволяют повысить гибкость процессов в компании в целом.

Сервисно-ориентированная архитектура была сформирована в области информационных технологий (далее - ИТ) в конце 1990-х — начале 2000-х годов. Тогда только начинали набирать популярность корпоративные сети и клиент-сервисная архитектура. Вследствие этого организации нуждались в интеграции различных приложений, созданных на основе разных технологий и разных операционных систем [4]. Таким образом, СОА является продолжением развития процессно-ориентированного подхода. Данный метод предлагает новый подход к созданию распределенных инфраструктур, для которых программные ресурсы рассматриваются как сервисы, представляемые по сети. Распределенная ИТ-инфраструктура объединяет разнородные платформы и прикладные решения, включая и унаследованные приложения.

Причинами внедрения сервисно-ориентированной архитектуры в первую очередь является возможность использования новых ИТ быстрее и дешевле для снижения различных видов риска, а также реализация индивидуальных проектов, подготовка к новой технологической эре. К преимуществам СОА можно отнести гибкость бизнеса, совершенствование бизнес-процессов, снижение рисков и расходов, масштабируемость. [2]

В сервисно-ориентированной архитектуре понятие «сервис»

трактуется как строго определенная работа, выполненная поставщиком сервиса для достижения желаемых конечных результатов для потребителя сервиса. Поставщики и потребитель – это роли, которые играют организационные единицы или программные агенты от имени их владельцев. Ниже представлена схема элементов сервисно-ориентированной архитектуры (Рис.1) [5]:

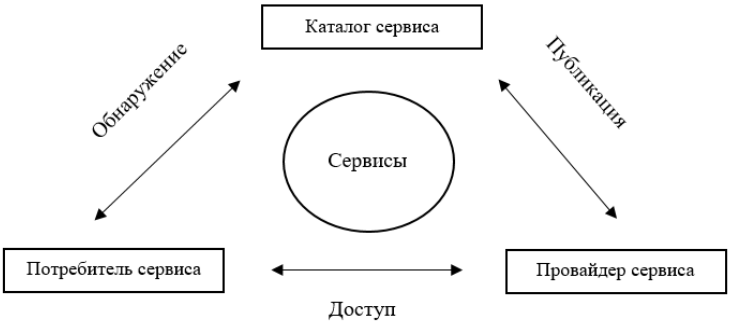



Рис.1 Элементы СОА

СОА рассматривает приложение как набор сервисов, работающих параллельно и связанных интерфейсами прикладного программирования (API). Каждый сервис является автономным и представляет собой реализацию конкретного бизнес-требования с предоставлением желаемого результата по входным данным [3].

В контексте СОА понятие «сервис» может определяться как действие или результат. Сервис как результат имеет ряд приложений, которые ведут к одному единому результату. Сервис как действие имеет комплекс определенных действий по запросам, которые в итоге возвращают результаты. Сервис как действие по сути неотделим от результата и наоборот. Результативность бизнес-сервиса определяется ценностью потребительской услуги, создаваемой сервисом и оцениваемой с точки зрения цепочки результатов: «output-outcome-impact».

Сервисы в СОА можно рассматривать как «черные ящики» с определенным входом и выходом. Для взаимодействия сервисов используется набор интерфейсов, которые обладают общей семантикой и доступны всем провайдерам и пользователям. Такая особенность использования интерфейса, независимого от окружения и платформы, получила название модели «слабой связи».

Гражданская авиация (далее - ГА) – авиация, используемая в целях обеспечения потребностей граждан и экономики (согласно ст.21 ВЗК

РФ). Сфера ГА подразделяется на коммерческие воздушные перевозки, авиационные работы и авиацию общего назначения. Гражданская авиация включает в себя регулирование таких предприятий, как аэропорты, авиакомпании, авиаремонтные заводы и авиационно-технические базы, организации по управлению воздушным движением, агентства, учебные и научно-исследовательских центры и т.д.

Основными направлениями деятельности ГА являются:

- перевозка пассажиров, багажа, почты и грузов;
- осуществление авиационных работ в сельском хозяйстве, строительстве, охране окружающей среды и других сферах;
- оказание медицинской помощи населению;
- проведение учебных, научно-исследовательских, культурно-просветительных и спортивных мероприятий.

В настоящее время сфера ГА стремительно меняется: происходят обновления парка воздушных судов и маршрутных сетей, реконструкция старых аэропортов, строительства новых, а также развитие международного сотрудничества и беспилотной авиации. Все процессы гражданской авиации зависят от многих внешних факторов, например, погодных условий, экономических возможностей, политических событий, государственного регулирования, а также научно-технического потенциала страны. В результате данная отрасль нуждается в оптимизации процессов и улучшении качества ИТ-инфраструктуры.

В данном случае подход СОА имеет широкое применение для сферы ГА. Для начала сервис гражданской авиации можно рассмотреть как цепочку результатов, представленных в таблице ниже [5].

Таблица – Характеристика результатов в ГА

| Вид результата | Характеристика результатов | Пример |
|---|---|---|
| Output – непосредственный результат | «Выход» услуги в категориях ее потребительских свойств | Информация о авиаперевозках, пассажирах, багаже, почты и грузов; информация о проведении авиационных работ, различных видов мероприятий |
| Outcome – конечный результат | Ценность или эффект непосредственного результата | Удовлетворение потребностей потребителей, обеспечение |

| | | |
|---|---|---|
| | | регулярности и безопасности полетов; повышение авиационной безопасности и качества наземного обслуживания, обслуживания на борту воздушного судна |
| Impact – итоговое воздействие | Экономические, социальные, технологические, политические эффекты результата сервиса | Развитие национальной и международной экономики; снижение рисков; повышение эффективности процессов и транспортной безопасности |

Сфера ГА достаточно специфична, поэтому следует придерживаться ряда особенностей. Для внедрения сервиса как действия можно разработать специальную информационную систему для отслеживания различных видов работ. К примеру, это могут быть программные приложения для повышения безопасности полетов и транспортной безопасности, сервисы для отслеживания регулярности полетов, которые смогут производить подсчет процента задержек рейсов, специальные приложения для удобства пассажиров с возможностью отслеживания их рейса, а также общий доступ к сети неавиационных услуг аэропорта. Все действия, направленные на разработку информационной системы, будут иметь тот же результат, как в описанной выше цепочке результатов. То есть сфера бизнес-сервиса будет тесно связана с ИТ-инфраструктурой организации.

Одной из известных организаций РФ, использующих СОА, является ПАО «Аэрофлот» [1]. В 2004 г. компания разработала проект по созданию корпоративной системы интеграции приложений (КСИП) на основе принципов, стандартов и технологий сервис-ориентированной архитектуры. Основными аспектами проекта являются создание центральной интеграционной шины, которая обеспечивает обмен данными между ключевыми приложениями, и синхронизация нормативно-справочной информации, которая также предусматривает решение задач создания и обмена оперативного хранилища данных.

Таким образом, СОА представляет собой подход, который позволяет создавать сложные системы на основе набора взаимодействующих между собой сервисов. Он обладает такими достоинствами, как повышение гибкости комплексных

информационных систем, улучшение интеграции бизнес-сервисов и ИТ-сервисов, снижение затрат на ИТ-инфраструктуру, а также повышение скорости реагирования на изменяющиеся потребности бизнеса.

Приложения, разработанные по принципу СОА, легко поддаются изменениям, потому что основаны на взаимозаменяемых сервисах, которые взаимодействуют по стандартизированным протоколам и интерфейсам между собой. Сервис в СОА представляет собой механизм, выполняющий определенные действия, ведущие к конкретному результату, имеющему ценность для определенных групп стейкхолдеров.

При внедрении данного метода в разных отраслях следует учитывать специфику сферы, ее принципы работы и особенности, а также с учетом фактора импортозамещения важно продумывать усиление взаимодействия с регулятором отрасли, смежными предприятиями. Сервисно-ориентированная структура позволит организациям улучшить эффективность поставленных бизнес-задач, снизить затраты на разработку за счет повторного использования сервисов, улучшить взаимодействие бизнес и ИТ сервисов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аэрофлот[сайт]. – 2025 – URL: www.aeroflot.ru (дата обращения: 26.05.2025). - текст электронный.

2. Гриценко, Ю. Б. Архитектура предприятия / Ю. Б. Гриценко. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2014. – 260 с. – ISBN 978-5-86889-512-8. – EDN ZVDHMB.

3. Караханова, А. А. Анализ микросервисной архитектуры, монолитных приложений, архитектуры SOA / А. А. Караханова // Синергия Наук. – 2020. – № 46. – С. 255-262. – EDN BVOVEU.

4. Костров, И. А. Сервисно-ориентированная архитектура приложений как средство организации распределенных систем в среде слабоструктурированных данных / И. А. Костров, Е. Е. Ковшов // Вестник МГТУ "Станкин". – 2012. – № 3(22). – С. 140-144. – EDN PGYLFX.

5. Никифорова, Л. Х. Архитектура авиапредприятий / Л. Х. Никифорова. – Москва: Московский государственный технический университет гражданской авиации, 2017. – 62 с. – EDN YPADFT.

6. Сангадиев, Ч. З. Формирование сервисно-ориентированной архитектуры в управлении бизнес-процессами авиационного

предприятия / Ч. З. Сангадиев // Известия Иркутской государственной экономической академии. – 2010. – № 3. – С. 182-185. – EDN MNIIYJ.

***УДК 004.9***

***Попов С.А.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## РАЗРАБОТКА ПРОГРАММЫ ДЛЯ АНАЛИЗА НЕСИНУСОИДАЛЬНЫХ СИГНАЛОВ В СИСТЕМАХ ЭЛЕКТРОЭНЕРГЕТИКИ ПОСРЕДСТВОМ АДАПТИВНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Качество электроэнергии представляет собой критически важный параметр, определяющий устойчивость работы электрооборудования на современных промышленных предприятиях, особенно чувствительного к наличию высших гармонических составляющих в питающем напряжении, возникающих в результате работы большого количества электрооборудования с нелинейными вольт-амперными характеристиками, содержание которого на современных промышленных предприятиях увеличивается с каждым годом. Именно эти группы нелинейных электроприёмников, включая частотно-регулируемые приводы и разнообразную преобразовательную полупроводниковую технику, формируют существенную долю нелинейной нагрузки, генерирующей несинусоидальные искажения формы токов и вытекающего из них несинусоидального искажения формы питающего напряжений [1].

На текущий момент традиционные методы спектрального анализа демонстрируют ограниченную эффективность при идентификации нестационарных несинусоидальных искажений, что делает актуальным разработку новых инструментов на основе современных методов и алгоритмов частотно-временного анализа, например, использование методов вейвлет-преобразования [2].

Одной из ключевых особенностей дискретного вейвлет-преобразования является способность осуществлять локализацию аномалий сигнала одновременно во временной и частотной областях, а возможность адаптивного выбора базисных вейвлет-функций (Daubechies, Symlet, Coiflet) позволяет оптимизировать процедуру вейвлет-разложение под специфику анализируемых сигналов. Несмотря на большую вычислительную сложность алгоритмов вейвлет-разложения и вейвлет-реконструкции, по сравнению с традиционными

методами спектрального анализа несинусоидальных сигналов, их применение в задачах оценки качества электрической энергии представляется перспективным направлением [3].

Разработка программы для анализа несинусоидальных сигналов в системах электроэнергетики посредством адаптивного вейвлет-преобразования осуществлялась в среде MATLAB с использованием объектно-ориентированного подхода и компонентов библиотеки App Designer, позволяющей параллельно рассматривать две основные задачи при создании приложений, а именно, разработку визуальных компонентов графического пользовательского интерфейса (GUI) и программирование ключевых алгоритмов приложения.

Одним из ключевых факторов выбора указанной среды разработки для создания программы для анализа несинусоидальных сигналов в системах электроэнергетики посредством адаптивного вейвлет-преобразования оказалось то, что данная среда предоставляет исследователю большой функционал в плане взаимодействия с другими элементами инфраструктуры программного комплекса MATLAB/SIMULINK, что обеспечивает не только широкие возможности для реализации необходимого функционала, но и простоту интеграции разработанной программы с другими пакетами, приложениями и моделями, разработанными в данном программном комплексе.

Архитектура приложения реализована в виде класса, инкапсулирующего следующие функции: импорт сигналов из текстовых, CSV и MAT-форматов файлов; расчет в соответствии с алгоритмом многоуровневого вейвлет-разложения; динамический расчет частотных диапазонов; интерактивную систему селективной вейвлет-реконструкции; экспорт результатов для дальнейшего анализа.

Интерфейс пользователя, представленный на рисунке 1, включает следующие функциональные блоки:

— Области визуализации исходного сигнала и реконструированного сигнала;

— Панель управления параметрами вейвлет-разложения, (выбор базисной вейвлет-функции, уровня вейвлет-декомпозиции, частоты дискретизации исходного сигнала для корректного вычисления частотных диапазонов);

— Таблицу соответствия уровней вейвлет-разложения частотным диапазонам;

— Интерактивное поле для выбора необходимых коэффициентов для осуществления вейвлет-реконструкции;

— Элементы управления программой.

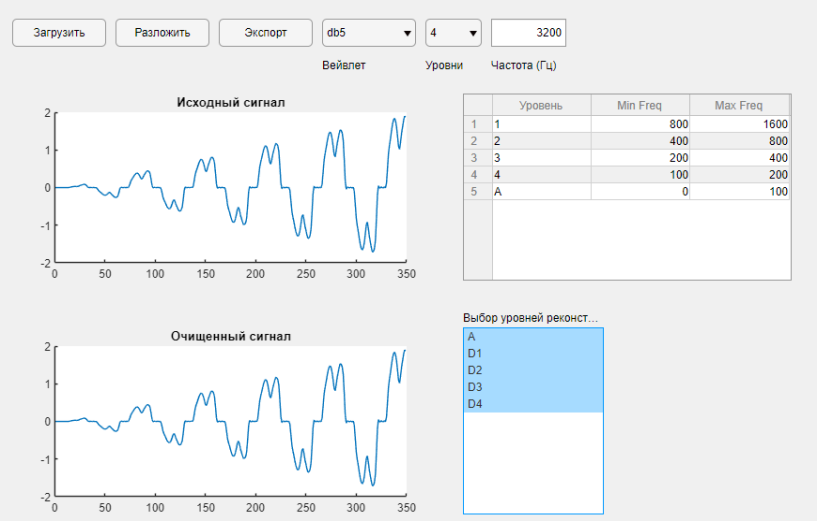



Рис. 1 Графический пользовательский интерфейс программы для анализа несинусоидальных сигналов в системах электроэнергетики посредством адаптивного вейвлет-преобразования

Ключевые особенности реализации данной программы:

— Реализовано адаптивное определение уровней разложения, гарантирующее корректность вейвлет-декомпозиции для произвольной длины исходного сигнала;

— Реализован динамический расчет частотных диапазонов, позволяющий упростить процесс оценки частотного содержания сигнала;

— Реализован механизм селективной вейвлет-реконструкции, позволяющий пользователю выбирать необходимые ему вейвлет-коэффициенты для осуществления вейвлет-реконструкции (рис. 2).

Таким образом, разработанная программа для анализа несинусоидальных сигналов в системах электроэнергетики посредством адаптивного вейвлет-преобразования существенно расширяет возможности исследователей, позволяя решать ряд задач связанных с анализом несинусоидальных искажений в нестационарных режимах работы электроэнергетических систем. Перспективным

направлением развития данной программы является интеграция алгоритмов машинного обучения для автоматической классификации типов искажений на основе вейвлет-коэффициентов и алгоритмов автоматического вычисления необходимых показателей качества электрической энергии для исследуемого сигнала в соответствии с применяемыми на практике методиками и нормативными документами, регулирующими показатели качества электрической энергии в сетях электроснабжения промышленных предприятий.

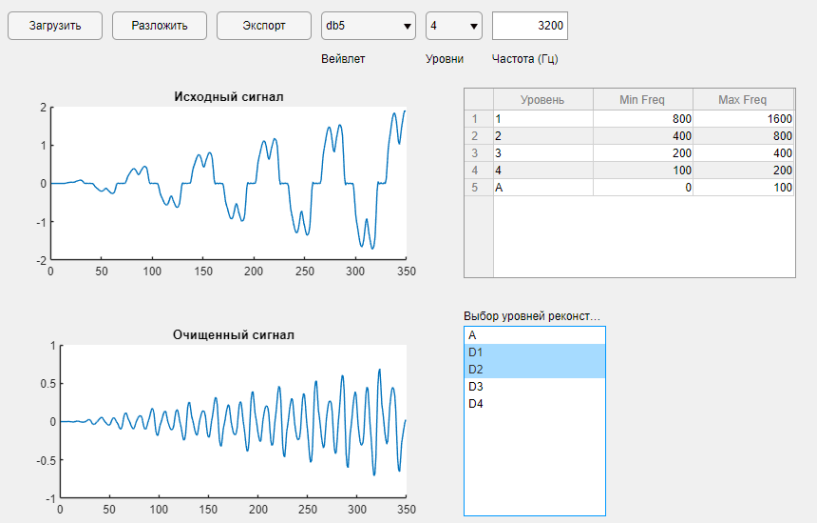



Рис. 2 Демонстрация работы функции селективной вейвлет-реконструкции

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Попов, С. А. Влияние гармонических искажений на качество электрической энергии внутри современного промышленного предприятия / С. А. Попов, А. Ю. Попова, Г. А. Фальков // Интеллектуальный и научный потенциал XXI века : Материалы Международной научно-практической конференции, Нефтекамск, 25 июля 2024 года. 2024. – С. 7-10.

2. Файфер, Л. А. Анализ нестационарных сигналов с помощью вейвлет-преобразования / Л. А. Файфер. – Текст : непосредственный // Молодой ученый. – 2016. – № 14 (118). – С. 182-186.

3. Осипов, Д. С. Анализ несинусоидальных нестационарных режимов электрических сетей на основе вейвлет преобразования / Д. С.

Осипов, Н. Н. Долгих, Е. А. Дюба // Вестник Югорского государственного университета. – 2023. – № 3. – С. 117-126.

***УДК 681.5.09***

***Попова П.Н.***
***Научный руководитель: Богачева С.Ю., канд. техн. наук, доц.***
*Российский государственный университет им. А.Н. Косыгина*
*г. Москва, Российская Федерация*

## ПРОГРАММЫЕ КОМПЛЕКСЫ РАСЧЕТА НАДЕЖНОСТИ

Надежность - свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования [1]. Оценка надежности включает в себя определение вероятности безотказной работы, среднего времени наработки до отказа, интенсивности отказов и других ключевых показателей [1, 2].

Расчет характеристик надежности представляет собой актуальную и сложную задачу, требующую применения специализированных методик и инструментов. Полученные данные позволяют принимать обоснованные решения на этапах проектирования, производства и эксплуатации оборудования, направленные на повышение его долговечности и снижение рисков возникновения нештатных ситуаций.

Сегодня для решения данной проблемы доступен целый спектр программных решений. Это инструменты для математического моделирования, такие как MatLab, Maple, Mathematica и MatCad [3], использующие собственные языки программирования. Для вычисления именно показателей надёжности применяются различные универсальные платформы, такие как MatLab с интегрированными статистическими и моделирующими инструментами, и специализированные пакеты, предлагающие широкий спектр методик анализа для разных отраслей.

Наряду с этим существуют узкоспециализированные программые комплексы (ПК), разработанные под нужды конкретных отраслей или типов оборудования. Особенностью таких специализированных комплексов является учет специфических отраслевых требований и стандартов, что позволяет получить более точные результаты анализа. Для оценки надёжности машин и производственных процессов

применяются различные специализированные программные комплексы, такие как RELEX, A.L.D. Group, Risk Spectrum и ISOGRAPH и отечественные комплексы BlockSim, ReliaSoft XFMEA, «АРБИТР», «Асоника-К» и «НАДЕЖНОСТЬ» [3].

Программные инструменты позволяют выполнять следующие операции: оценка параметров распределения на основе имеющихся статистических данных; проверка гипотез о соответствии выбранного распределения наблюдаемым данным с использованием критериев согласия; определение показателей надежности, таких как средняя наработка до отказа, интенсивность отказов, вероятность безотказной работы на заданном интервале времени; анализ чувствительности показателей надежности к изменениям параметров распределения.

Рассмотрим некоторые ПК. **Meridium APM** — это комплексная платформа для проактивного управления активами, особенно востребованная в нефтегазовой отрасли и энергетике. Её ключевое отличие — глубокая аналитика и интеграция с промышленными IoT-системами.

Возможности:

1. Управление надёжностью оборудования. Анализ критичности активов для определения приоритетов обслуживания. Прогнозирование отказов с использованием статистических данных и методов Root Cause Analysis. Оптимизация стратегий технического обслуживания и ремонтов на основе рисков.

2. Интеграция с системами оборудования. Совместимость для учёта истории ремонтов, затрат и состояния оборудования.

3. Предиктивная аналитика и мониторинг. Оценка активов через датчики и диагностику. Мобильные обходы для сбора данных о состоянии оборудования.

4. Оптимизация межремонтных интервалов. Увеличение межремонтного пробега оборудования за счёт анализа деградации и коррозии. Использование цифровых двойников для моделирования сценариев износа.

5. Обучение и внедрение. Курсы для персонала. Поддержка партнёров.

**Комплекс Weibull++** позволяет выполнять следующие операции:

1. Анализ данных о надёжности.

2. Расчёт параметров распределения Вейбулла.

3. Прогнозирование надёжности. Расчёт: вероятности безотказной работы, интенсивности отказов, среднего времени наработки на отказ.

4. Графический анализ. Построение диаграмм Вейбулла, кривых выживаемости и кумулятивных функций отказов.

5. Сравнение с эталонными примерами. Weibull++ включает библиотеку тестовых случаев для верификации результатов.

Применение в отраслях: Авиация и космос (например, анализ отказов двигателей и подшипников, энергетика (оценка надёжности компонентов АЭС).

Комплекс **ReliaSoft XFMEA** - для обеспечения комплексного анализа и прогнозирования надёжности технических систем в промышленном производстве. Среди возможностей: моделирование вероятности отказов, анализ жизненного цикла продукта, оптимизация технических процессов и другие.

**Продукт "1С:RCM Управление надежностью"** предназначен для оптимизации профилактических и диагностических программ технического обслуживания активов на предприятиях различных отраслей. В основе продукта лежит методология RCM (англ. Reliability-Centered Maintenance – техническое обслуживание, ориентированное на обеспечение надежности), искусственный интеллект и предиктивная аналитика.

**АРБИТР** - комплекс для автоматизированного математического моделирования и расчёта вероятностных характеристик надёжности и безопасности сложных систем. Комплекс использует логико-вероятностные методы (ЛВМ) и схемы функциональной целостности, поддерживает расчёт вероятности отказов, коэффициента готовности, учёт зависимых отказов.

Аттестован Ростехнадзором, включён в реестр российского ПО и подходит для объектов с высокими требованиями к надёжности и безопасности, таких как атомная энергетика, оборонная промышленность, опасные производственные объекты [4].

**Pragmatica – у**правление данными о надёжности на всех этапах жизненного цикла изделий.

Возможности комплекса: построение структур анализируемых изделий и распределение требований к надёжности для их составных частей; выполнение анализа видов, последствий и критичности отказов; формирование сложных моделей надёжности; анализ FMEA/FMECA, построение деревьев отказов; расчёт структурных схем с резервированием (метод Монте-Карло).

Соответствие требованиям ФСТЭК. Применение: оборонная промышленность, сложное машиностроение.

**Асоника-К -** комплекс позволяет проводить надёжные анализы и расчёты в различных областях промышленности. Среди возможностей: моделирование надёжности, анализ и сравнение систем, определение важных элементов и прогнозирование интенсивности отказов;

оптимизация запасов в комплектах ЗИП, анализ надёжности радиокомпонентов; расчёт надёжности радиоэлектронной аппаратуры (РЭА) и электрорадиоизделий (ЭРИ).

Преимущества: интеграция с САПР (P-CAD, Altium Designer), использование отечественных справочников по надёжности ЭРИ.

Применение: Авиация, космическая техника, электроника [5].

**Программный комплекс Надежность** предназначен для автоматизированного расчёта показателей безотказности и ремонтопригодности, а также управление процессами технического обслуживания и ремонта оборудования.

Функции: расчет показателей надёжности систем; логико-вероятностные методы моделирования работы в ожидаемых условиях эксплуатации; расчёты комплектов запасных частей, инструментов; построение структурных схем и деревьев отказов; анализ состояния оборудования в реальном времени, предсказание отказов, оптимизация графиков технического обслуживания.

Достоинства «Надёжность»: вычисление параметров для произвольных функций распределения; моделирование статистических данных; представление полученных результатов с помощью отображения графиков; экспорт и импорт данных с использованием обычных текстовых файлов; универсальность; получение эмпирической оценки надежности и параметров функции распределения.

Применение: Машиностроение, транспортные системы, металлургия, энергетика [6].

В основе практически всех ПК расчёта надёжности автоматизированного моделирования лежат логико-вероятностные методы системного анализа. Общее содержание ПК включает модули для сбора и обработки данных о состоянии оборудования; моделирования отказов; анализа времени наработки на отказ; планирования технического обслуживания.

В России разработаны комплексы для расчёта надёжности технических систем, использующиеся в различных отраслях промышленности, в первую очередь оборонную, авиационную, энергетическую и электронную сферы. Российские ПК имеют несколько преимуществ:

1.Соответствие ГОСТ и отраслевым стандартам, требованиям Ростехнадзора и Минпромторга.

2. Интеграция с отечественными САПР.

3. Поддержка государственных учреждений (включение в реестр Минкомсвязи).

4. Развитие отечественной IT-индустрии, снижение зависимости от иностранных технологий, повышение информационной безопасности, что поддерживает национальную экономику и способствует технологическому суверенитету.

Применение указанных программных комплексов позволяет повысить точность и достоверность оценок надежности, а также обосновать выбор моделей, используемых при расчетах надежности технических систем, позволяет снизить издержки на ремонт, повысить качество продукции и увеличить общую производительность и безопасность предприятия.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. ГОСТ Р 27.102—2021. Надежность в технике. Надежность объекта. Термины и определения. М.: Российский институт стандартизации, 2021. – 40 с.
2. ГОСТ Р 27.015—2019 Надежность в технике. Управление надежностью. Руководство по проектированию надежности систем. М.: Стандартинформ, 2019. – 35 с.
3. Бесхлебнов И.В., Астапов В.Н. Сравнительный анализ программных комплексов расчёта надежности. // Международный студенческий научный вестник. – 2023. – №6 URL: https://eduherald.ru (дата обращения: 27.04.2025).
4. ПК АРБИТР: О программном комплексе [Электронный ресурс] – URL: https://szma.com (дата обращения – 20.02.2025 г.).
5. АСОНИКА-К [Электронный ресурс] – URL: https://asonika-k.ru/ (дата обращения – 10.03.2025).
6. ПК Надежность [Электронный ресурс] URL:https://reliabili (дата обращения – 29.01.2025).



***УДК 004.056.55***



***Путилин Н.И.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ: СТАНДАРТЫ NIST И ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС

Представьте себе мир, где все ваши цифровые секреты – от банковских данных до личной переписки и государственных тайн –

вдруг оказываются под угрозой. Звучит как сценарий для технотриллера, не правда ли? Однако именно такая перспектива замаячила на горизонте с развитием квантовых компьютеров. Эти удивительные машины, пока еще больше похожие на лабораторные прототипы, обещают революцию во многих областях, но одновременно несут и серьезную угрозу. Дело в том, что они способны "раскусить" те самые шифры, на которых сегодня держится безопасность интернета и цифровых коммуникаций – речь идет о системах вроде RSA и эллиптической криптографии. Именно поэтому в мире кибербезопасности все чаще звучат слова "постквантовая криптография" или PQC. Это, по сути, гонка вооружений нового типа: криптографы всего мира ищут способы создать такие шифры, которые устояли бы даже перед мощью квантового интеллекта.

Главная "суперсила" квантовых компьютеров, которая так пугает специалистов по безопасности, – это алгоритм Шора. Открытый еще в 1994 году, он позволяет квантовой машине очень быстро справляться с задачами, непосильными для обычных компьютеров, например, разложением больших чисел на множители. А ведь именно на сложности таких задач и построена защита многих современных криптосистем. Есть и другой квантовый помощник, алгоритм Гровера, который хоть и не дает такого ошеломляющего преимущества, но способен заметно ускорить перебор вариантов, что тоже может ослабить некоторые типы шифрования. И хотя до появления квантового компьютера, способного взломать всё и вся, еще могут пройти годы, расслабляться нельзя. Существует неприятная тактика "собирай сейчас, расшифровывай потом": злоумышленники уже сегодня могут перехватывать зашифрованные данные, чтобы вскрыть их, когда нужные технологии станут доступны. Представьте, сколько ценной информации с долгим сроком годности может оказаться под ударом!

Понимая всю серьезность ситуации, Национальный институт стандартов и технологий США, известный как NIST, еще в 2016 году забил тревогу и запустил масштабный международный проект. Его цель – найти и утвердить новые криптографические стандарты, которые были бы не по зубам квантовым "взломщикам". Это был настоящий всемирный мозговой штурм: ученые и разработчики со всех уголков планеты предлагали свои идеи, алгоритмы для цифровых подписей, шифрования и безопасной передачи ключей.

Процесс отбора был долгим и многоступенчатым. Изначально на конкурс поступило почти семь десятков предложений. Каждое из них проходило строжайшую проверку: эксперты оценивали не только теоретическую стойкость к атакам (включая квантовые), но и то,

насколько быстро работают алгоритмы, легко ли их встроить в существующие системы, не слишком ли они "прожорливы" к ресурсам компьютера. Мировое криптографическое сообщество подключилось к этой работе, выискивая слабые места в предложенных схемах и предлагая улучшения. Это была настоящая коллективная работа по созданию щита для нашего цифрового будущего.

И вот, летом 2022 года, после нескольких раундов отсева и тщательного анализа, NIST назвал первых финалистов. Для создания и обмена секретными ключами (эта процедура называется "механизм инкапсуляции ключей" или KEM) был выбран алгоритм под названием CRYSTALS-Kyber. А для цифровых подписей, которые подтверждают подлинность документов или программ и гарантируют, что в них никто не внес изменений, отобрали сразу три решения: CRYSTALS-Dilithium, Falcon и SPHINCS+.

Что же это за "звери"? CRYSTALS-Kyber, который в итоге стал стандартом ML-KEM (FIPS 203), основан на довольно сложной математике, связанной с так называемыми решетками и "обучением с ошибками". Если не вдаваться в дебри, он предлагает хороший компромисс между надежностью, размерами ключей и скоростью работы. Он призван заменить те методы обмена ключами, которые уязвимы для квантовых атак.

Его "коллега" по семейству, CRYSTALS-Dilithium (теперь это стандарт ML-DSA, FIPS 204), также использует математику решеток. Он хорош тем, что создает относительно компактные цифровые подписи и не слишком требователен к вычислительным мощностям, что делает его удобным для множества задач – от проверки подлинности обновлений программ до защиты финансовых переводов.

Falcon – еще один кандидат на роль стандартной цифровой подписи, тоже из мира решеток, но с другой математической "начинкой" (NTRU-решетки). Его главный козырь – очень маленькие размеры подписей. Это особенно ценно там, где каждый байт на счету, например, в системах с ограниченной связью. Правда, реализовать его несколько сложнее, поэтому NIST пока взял время на его дополнительное изучение, прежде чем выпускать окончательный стандарт.

А вот SPHINCS+ (стандарт SLH-DSA, FIPS 205) стоит особняком. Его безопасность опирается не на новомодные решетки, а на старые добрые хеш-функции, которые считаются весьма устойчивыми к квантовым атакам. Особенность SPHINCS+ в том, что он "безстатусный" – ему не нужно запоминать, какие значения он использовал ранее для создания подписей, что решает одну из проблем

его предшественников. За эту высокую степень уверенности в безопасности приходится платить: подписи у SPHINCS+ получаются довольно громоздкими, а сам процесс подписания и проверки занимает больше времени. Поэтому его видят скорее как сверхнадежный вариант для самых критичных случаев – например, для защиты прошивок устройств или сертификатов удостоверяющих центров, где скорость не так важна, как железобетонная гарантия.

Важный рубеж был пройден в августе 2024 года: NIST официально опубликовал финальные версии этих трех стандартов – FIPS 203, FIPS 204 и FIPS 205. Это стало зеленым светом для начала массового перехода на постквантовую "броню".

Однако сам переход обещает быть непростым. Представьте, что нужно поменять все замки во всех дверях огромного города, причем одновременно. Постквантовые алгоритмы часто требуют больше "места" для ключей и подписей, могут работать медленнее на некоторых операциях. Это может стать проблемой для маломощных устройств, которых вокруг нас все больше – от умных часов до датчиков в промышленности.

Интегрировать новые шифры в уже работающие системы – это отдельная головная боль. Нужно будет обновить всё: от веб-браузеров и операционных систем до протоколов, защищающих нашу электронную почту и интернет-соединения (вроде TLS/SSL). Потребуется перевыпуск цифровых сертификатов, обучение разработчиков, обеспечение совместимости старого и нового. Здесь очень пригодится так называемая "криптографическая гибкость" – способность систем легко переключаться с одного шифра на другой. Это как иметь универсальный ключ, подходящий к разным замкам.

На первых порах, скорее всего, мы увидим гибридные решения. Это когда для защиты информации используется сразу два замка – старый, проверенный временем, и новый, постквантовый. Например, секретный ключ для шифрования данных будет создаваться с использованием и классического алгоритма, и постквантового. Чтобы взломать такую систему, злоумышленнику придется одолеть оба, что дает дополнительный запас прочности на время, пока новые PQC-алгоритмы проходят обкатку в реальных условиях.

Кому же в первую очередь придется задуматься о переходе? Конечно, это государственные структуры, хранящие секреты десятилетиями. Финансовый сектор, где на кону огромные деньги и доверие клиентов. Медицина с ее чувствительными данными о здоровье пациентов. Да и вообще, любая компания, которая серьезно относится к защите своей информации и информации своих пользователей.

Работа NIST на этом не заканчивается. Эксперты продолжают анализировать и другие перспективные алгоритмы, возможно, из других математических "семейств" – например, основанные на теории кодирования или других экзотических разделах математики. Ведь чем больше разных инструментов в арсенале криптографов, тем ниже риск, что однажды найденная "отмычка" откроет сразу все двери. Важно иметь запасные варианты.

Хотя NIST и является своего рода законодателем мод в этой области, другие международные организации тоже не сидят сложа руки, работая над своими стандартами, часто ориентируясь на американские разработки. Глобальное сотрудничество здесь крайне важно, чтобы не получилось так, что у каждой страны или компании свои "несовместимые" шифры.

В общем, переход на постквантовую криптографию – это не просто очередное обновление софта. Это фундаментальный сдвиг, марафон, который только начинается. Стандарты, предложенные NIST, – это карта и компас на этом пути. Да, впереди много работы, много сложностей, но игра стоит свеч. Ведь на кону – безопасность нашего цифрового завтра. И чем раньше мы начнем готовиться и внедрять новые решения, пусть даже постепенно и в гибридном формате, тем спокойнее мы сможем смотреть в это квантовое будущее.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Соколенко А. А. Постквантовая криптография / А. А. Соколенко, А. Ю. Гилязов, В. В. Гринчуков, В. С. Шапаренко // Летняя школа-конференция" Криптография и информационная безопасность" – 2021. – С. 24

2. Безухова П. О. Постквантовая криптография / П. О. Безухова // Интернаука ООО «Интернаука». — 2022. — № 22-1(245). — С. 22-23.

3. Комарова А. В. Обзор истории и тенденций развития постквантовой криптографии на основе теории решеток / А. В. Комарова, А. Г. Коробейников // Программная инженерия Издательство "Новые технологии". — 2019. — № 7-8 — С. 344-352.

4. Власенко А. В. Исследование реализации механизмов инкапсуляции ключей постквантовых криптографических методов / А. В. Власенко, М. В. Евсюков, М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. — 2020. — № 1(61) — С. 121-127.

5. Коршак К. С. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак //

Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720

***УДК 004.056.55***

***Путилин Н.И.***
***Научный руководитель: Жданова С.И. ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ДНК-КРИПТОГРАФИЯ: НОВЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ БИОЛОГИЧЕСКИХ ДАННЫХ

Мир буквально тонет в цифровых данных, и их количество растет лавинообразно. Уже к 2025 году, по прогнозам, мы можем столкнуться с объемом информации, превышающим 175 зеттабайт – цифра, которую сложно даже вообразить! Привычные нам магнитные, оптические или электронные носители уже сейчас едва справляются с таким напором. Кроме скромной емкости, они грешат высоким энергопотреблением, недолговечностью и не самой высокой надежностью. Неудивительно, что поиск новых подходов к вычислениям и альтернативных носителей информации превращается в одну из главных задач для IT-специалистов.

Идея молекулярных вычислений, кстати, витала в воздухе давно: еще в 1959 году ее озвучил нобелевский лауреат Ричард Фейнман. Позже Винер и Нейман развили эту мысль, предложив хранить информацию на основе молекулярной генетики. Настоящий прорыв случился в 1994-м, когда Леонард Адлман решил знаменитую задачу о гамильтоновом пути с помощью биохимических методов. А всего год спустя Леонард Баум предложил использовать ДНК для построения баз данных. Эти работы, без преувеличения, открыли новую страницу – эру биологических вычислений и хранения данных в ДНК.

Чем же так привлекла ученых дезоксирибонуклеиновая кислота (ДНК)? Своими уникальными свойствами! Она может похвастаться невероятной плотностью записи, способностью хранить информацию десятки тысяч лет и удивительной неприхотливостью в обслуживании. И вот, в 2023 году французская компания Biomemory сделала первый шаг к рынку, представив коммерческую карту памяти на ДНК объемом

в 1 килобайт. Конечно, это только начало, но чем ближе мы подходим к практическому применению, тем острее встает вопрос защиты этих данных: как обеспечить их конфиденциальность, целостность и доступность?

Если классическая криптография опирается на математические «крепости», вроде NP-трудных задач, то ДНК-криптография строит свою защиту на биологических сложностях, которые поджидают на каждом шагу работы с молекулами: от кодирования до синтеза, от хранения до расшифровки. Скажем, без знания верных праймеров не получится воспроизвести нужную последовательность. Измените форму ДНК-оригами – и сборка информации застопорится. А случайная мутация в одной-единственной нуклеотидной паре? Ее вполне можно интерпретировать как скрытый код.

Давайте вспомним, что такое криптография в широком смысле? Это наука о том, как защитить информацию. Она предлагает методы шифрования, делающие данные нечитаемыми для чужих глаз, и методы сокрытия, когда секрет прячется внутри чего-то обыденного. Шифрование бывает симметричным (один ключ на всё, как в AES или DES) и асимметричным (пара ключей – открытый и закрытый, как в RSA или ECC). Есть еще стеганография – искусство встраивать информацию в другие файлы (картинки, музыку, видео) – и цифровые водяные знаки, которые помогают, например, защищать авторские права. Интересно, что и стеганографию, и водяные знаки можно «провернуть» и в биологических системах, включая ДНК.

Когда Адлман показал, что ДНК годится для параллельных вычислений, исследователи задумались: а нельзя ли с помощью биологии взломать классические шифры? Начались эксперименты с DES, RSA, NTRU и другими алгоритмами. Более того, еще в начале 2000-х в ДНК удалось спрятать целую секретную фразу: «6 июня: высадка в Нормандии». Эти опыты и дали старт тому, что мы сегодня называем ДНК-криптографией. Она объединяет и шифрование, и сокрытие информации на молекулярном уровне.

Если заглянуть в «биологическую кухню», ДНК – это последовательность из четырех «букв»-нуклеотидов: аденина (A), гуанина (G), цитозина (C) и тимина (T). Они образуют знаменитую двойную спираль, где A всегда «дружит» с T, а G – с C. Путь генетической информации – от ДНК к РНК, а затем к белку – известен как центральная догма молекулярной биологии. Сначала на матрице ДНК синтезируется РНК (это называется транскрипцией), потом из РНК вырезаются «лишние» куски (это сплайсинг), и только после этого информация «переводится» в последовательность аминокислот. И тут

кроется еще одна хитрость: одна и та же ДНК-последовательность может быть «прочитана» по-разному благодаря альтернативному сплайсингу. Это, конечно, здорово усложняет расшифровку.

Нельзя забывать и о ферментах – настоящих молекулярных «инструментах». Они умеют «резать» и «сшивать» молекулы ДНК. Рестриктазы, лигазы, экзонуклеазы – у каждого свой «участок работы». А уж современные технологии редактирования генома, вроде CRISPR-Cas, порой творят чудеса: они позволяют точечно менять ДНК-последовательности. Это открывает дорогу для внедрения информации в строго определенные места. Особенно любопытен фермент Cas12a: он не только вносит правки, но и может «зачищать» ненужные участки одноцепочечной ДНК.

Гибридизация – еще один ключевой процесс, без которого не обойтись ни в ДНК-вычислениях, ни в методах хранения. Суть проста: одна цепочка ДНК способна найти свою «вторую половинку» – комплементарную ей цепочку – и соединиться с ней. Это свойство используется, например, при создании праймеров для ПЦР (полимеразной цепной реакции) и для «поиска» нужных данных внутри молекулы.

Более того, биологические процессы удалось «перевести на язык» логических операций! Ученые уже разработали правила для сложения, вычитания и даже побитовой операции XOR для ДНК-последовательностей. Фактически, это позволяет обращаться с ДНК как с цифровыми данными, только на биологическом «железе».

А что если скрестить классику и биологию? Так появилась псевдо-ДНК-криптография – симбиоз традиционных методов защиты и биологических «хитростей». Представьте: обычный текст сначала переводят в «генетическую последовательность». Затем эта последовательность проходит через процессы, имитирующие транскрипцию и трансляцию. И только потом получается шифротекст. Такой многоступенчатый подход настолько запутывает структуру данных, что расшифровка без знания особых биологических «ключей» становится почти нереальной задачей.

Так что ДНК-криптография – это не просто экзотический способ обеспечить безопасность. Это целый новый рубеж в развитии информационных технологий, где информатика встречается с биологией. Да, пока есть технические трудности, нет единых стандартов, и с масштабированием не все гладко. Но исследования в этой области не стоят на месте и активно развиваются. И кто знает, возможно, с дальнейшим развитием биотехнологий мы увидим гибридные системы хранения и защиты данных, которые возьмут

лучшее и от цифрового, и от биологического мира.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Лапшин В. С. Криптографическая система, основанная на принципах экспрессии генов / В. С. Лапшин, А. А. Севрюков // Поколение будущего: взгляд молодых ученых – 2018 Сборник научных статей 7-й Международной молодежной научной конференции. — 2018. — № 4(3). — С. 77-80.

2. Сахабутдинова А. Р. Небиологическое применение молекул ДНК / А. В. Чемерис, А. М. Сагитов, А. Р. Сахабутдинова, К. И. Михайленко, М. А. Сагитова, О. Ю. Кирьянова, Р. Р. Гарафутдинов // Биомика. — 2019. — № 3(11). — С. 344-377.

3. Кирьянова О. Ю. GATCGGenerator: новый генератор для создания квазислучайных нуклеотидных последовательностей / О. Ю. Кирьянова, Р. Р. Гарафутдинов, И. М. Губайдуллин, А. В. Чемерис // Advanced Engineering Research (Rostov-on-Don). — 2023. — № 23(3). — С. 296-306.

4. Агафонов В. Б. Теоретико-правовые проблемы обеспечения биологической безопасности Российской Федерации / В. Б. Агафонов, Н. Г. Жаворонкова // Актуальные проблемы российского права — 2020. — № 113(4) — С. 187-194.

5. Жданова С. И. Цифровая трансформация в формировании образовательных траекторий личности / С. И. Жданова // Наукоемкие технологии и инновации (xxv научные чтения) Сборник докладов Международной научно-практической конференции. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. — С. 713-716.

***УДК 629:681.5***

***Радин Е.А.***
***Научный руководитель: Кижук А.С., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## СИСТЕМА УПРАВЛЕНИЯ МОБИЛЬНОЙ ПЛАТФОРМОЙ ДЛЯ ТРАНСПОРТНО-СКЛАДСКИХ ЗАДАЧ

Современные промышленные решения, доступные сегодня, часто представляют собой системы с ограниченной гибкостью, зависящие от закрытых программно-аппаратных комплексов. Кроме того,

автоматизированные транспортные средства, представленные на рынке, отличаются высокой стоимостью. В этой связи разработка доступной мобильной платформы для выполнения задач в области транспортировки и складского хозяйства становится важной задачей. Реализация такого решения принесет ряд значительных преимуществ:

Улучшение безопасности на рабочем месте: автоматизированные системы способны выполнять опасные операции, такие как транспортировка и разгрузка тяжелых грузов, что снижает риск несчастных случаев.

Снижение затрат: роботизированные решения могут функционировать круглосуточно без перерывов и отдыха, что позволяет сократить расходы на оплату труда.

Повышение эффективности работы: роботы могут быстро и точно справляться с рутинными задачами, такими как перемещение и сортировка товаров, превосходя человека по скорости и точности.

Создание подобной бюджетной платформы способно существенно улучшить рабочие процессы, уменьшить издержки и обеспечить более безопасные условия труда.

В рамках исследования поставлена задача проектирования автономной системы управления для роботизированной платформы, предназначенной для логистических операций. Платформа использует светоотражающие полосы для позиционирования и RFID-технологию для навигации объектов. Для этого необходимо решить следующие задачи: спроектировать техническую конфигурацию автономной платформы, создать программные механизмы для управления траекторией перемещения, интегрировать систему позиционирования с использованием RFID-идентификаторов, провести комплексные испытания рабочего прототипа.

Функциональная схема является важным элементом проектирования технических систем. Она позволяет наглядно отразить структуру системы, показать основные элементы и взаимосвязи между ними. Ниже приведена функциональная схема (рис. 1).

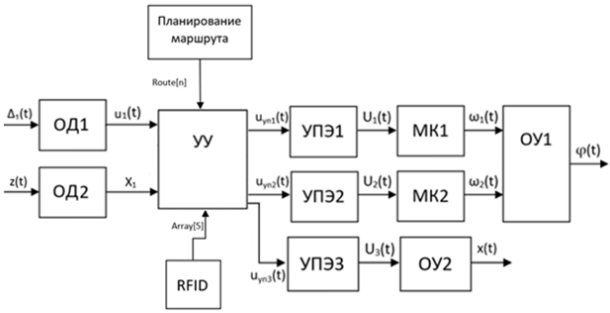



Рис. 1. Функциональная схема мобильной платформы

Траектория движения мобильной платформы регулируется с использованием информации, поступающей от оптического датчика ОД1. Этот датчик определяет смещение $\Delta 1(t)$ между своим центром и центральной линией светоотражающей полосы. Полученные данные преобразуются в электрические сигналы $u1(t)$, которые передаются в управляющее устройство (УУ). Устройство управления обрабатывает эти сигналы и генерирует команды $u_{уп1}(t)$ и $u_{уп2}(t)$, направляемые на усилительно-преобразовательные модули (УПЭ1 и УПЭ2). Модули, в свою очередь, формируют управляющие напряжения $U_1(t)$ и $U_2(t)$, которые подаются на мотор-колеса (МК1 и МК2). Благодаря этому мотор-колеса создают угловые скорости вращения $w_1$ и $w_2$, что позволяет корректировать угол поворота $\varphi(t)$ мобильной платформы (ОУ1).

Активация ленточного механизма осуществляется при обнаружении объектов оптическим датчиком ОД2 рефлекторного типа. Сенсор генерирует цифровой импульс $X_1$, который передаётся в блок управления (УУ) для дальнейшей обработки. В блоке управления сигнал $X_1$ трансформируется в управляющее напряжение $u_{уп3}(t)$, направляемое на усилительно-преобразовательный модуль УПЭ3. Данный модуль выполняет согласование уровней сигнала, формируя выходное напряжение $U_3(t)$, необходимое для регулировки работы приводного двигателя конвейера (ОУ2). В результате изменяется позиция ленты $x(t)$, обеспечивая транспортировку грузов.

Параллельно УУ получает информацию от вышестоящего программного обеспечения о запланированной траектории движения *Route*[*n*]. Массив данных *Array*, содержащий параметры RFID-меток, обновляется при каждом успешном считывании идентификаторов модулем [5]. Это позволяет системе адаптировать работу конвейера в зависимости от текущей задачи.

На рисунке 2 изображена конструкция мобильной платформы, оснащённой дифференциальной ходовой частью. Такая конфигурация обеспечивает высокую манёвренность при движении по сложным траекториям, задаваемым комбинацией оптической и RFID-навигации.

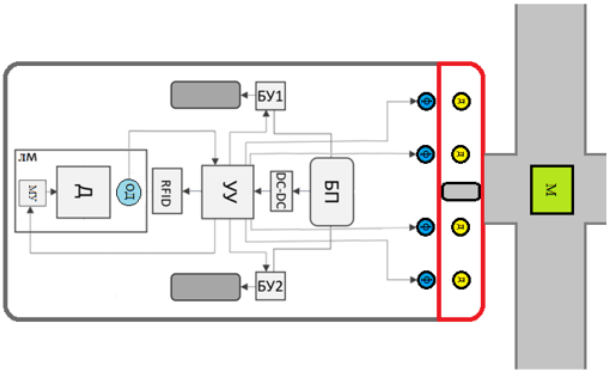



Рис. 2. Структура мобильной платформы

На изображении показаны ключевые элементы, составляющие структуру мобильной платформы: УУ – устройство управления, БП – блок питания мобильной платформы, Ф, Д – фоторезисторы и светодиоды – компоненты оптического аналогового датчика, RFID – считыватель RFID-RC522, М – метка типа MIFARE Classic, БУ – блоки управления мотор-колесами с БДПТ, DC-DC – согласующая плата, преобразующая питание для логической части, ЛМ – система ленточного механизма, Д – двигатель постоянного тока DC80ZYT, МУ – модуль управления (драйвер).

Для того, чтобы иметь чёткое представление о согласовании напряжений и понимать как компоненты системы будут взаимодействовать между собой необходимо спроектировать принципиальную схему подключения компонентов (рис. 3). На схеме отображены ключевые элементы системы: ленточный конвейер, сенсорные модули и линии передачи сигналов. Рефлекторный датчик генерирует импульсный сигнал при обнаружении объектов, который направляется в центральный блок управления (УУ). Микроконтроллер анализирует входящие данные и формирует управляющий импульс для драйвера приводного двигателя, активируя процесс разгрузки или транспортировки грузов.

Работа конвейера синхронизируется с RFID-навигацией: при идентификации метки блок управления (УУ) генерирует команды, корректирующие режим работы механизма. Это обеспечивает привязку технологических операций (старт/стоп, изменение скорости) к конкретным зонам маршрута.

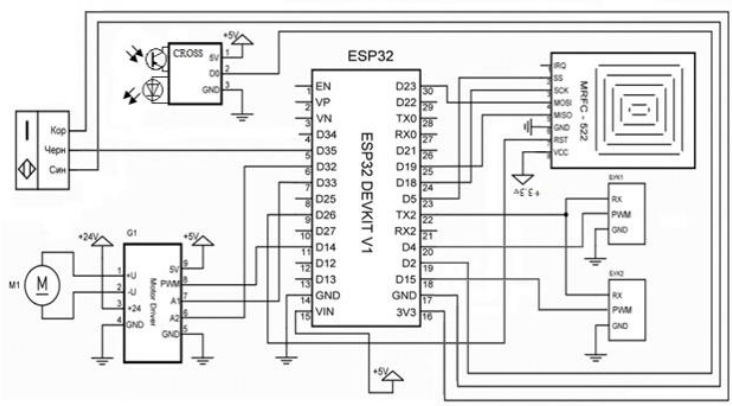



Рис. 3. Принципиальная схема мобильной платформы

Микроконтроллер ESP32 считывает аналоговые данные с оптического сенсора, которые обрабатываются согласно заданному алгоритму управления. На основе этих данных формируются ШИМ-импульсы, регулирующие частоту вращения бесколлекторного DC-двигателя. Сгенерированные сигналы передаются в блок управления (БУ) для дальнейшего исполнения.

Контроллер отслеживает угловое положение ротора через датчики Холла (ДХ) и анализирует текущий режим работы двигателя. В зависимости от этих параметров осуществляется динамическое переключение ключей в Н-мостовой схеме, обеспечивая точное управление направлением и скоростью вращения.

Рассмотренная система управления мобильной платформы для транспортно-складских задач демонстрирует эффективное сочетание доступности, функциональности и безопасности. Использование светоотражающих полос и RFID-навигации позволяет реализовать точное позиционирование и адаптивное управление траекторией движения, что критически важно для выполнения логистических операций в условиях ограниченного пространства складского помещения.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кижук А.С., Гольцов Ю.А. Анализ технических средств в структуре систем управления и их выбор при проектировании: учебное пособие. – Белгород: Изд-во БГТУ, 2016. – 242с.
2. Рубанов В.Г., Бушуев Д.А., Бажанов А.Г., Ващенко Р.А. Проектирование робототехнических систем и комплексов. Белгород: Изд-во БГТУ, 2020. – 190 с.
3. Влияние IT-сферы на отрасли промышленности [Электронный ресурс] URL: https://servernews.ru (дата обращения: 11.05.2025)
4. Access conditions [Электронный ресурс] URL: https://hotdogger.blot.im (дата обращения: 11.05.2025)
5. Порхало В.А., Рубанов В.Г., Бажанов А.Г., Луценко О.В. Автоматизированное проектирование системы управления роботизированной платформы с применением Adams и Matlab // Известия Юго-Западного государственного университета, 2020. Т. 24. № 4. С. 217-229.



***УДК 004.853***



***Романов А.О.***
***Научный руководитель: Васильев Н.С., асс.***
*Чувашский государственный университет*
*им. И.Н. Ульянова, г. Чебоксары, Россия*


## CURIOSITY-DRIVEN LEARNING: КАК ИИ ИССЛЕДУЕТ МИР БЕЗ НАГРАД

В традиционных подходах к обучению с подкреплением агент базируется на внешних вознаграждениях. Однако в ряде случаев такие награды оказываются редкими или задержанными, например, в простейших компьютерных играх, где награда за выполнение уровня реализуется только после его завершения, а предшествующие действия не сопровождаются немедленной обратной связью.

В таких ситуациях на роль внутренней мотивации выступает концепция «любопытства». Механизм можно сравнить с поведением ребёнка, исследующего окружающий мир без конкретных указаний и наград – мотивацией является исключительно интерес к окружению. Аналогично работают curiosity-алгоритмы. Они создают внутреннюю систему мотивации, побуждая агента исследовать новое и избегать повторяющихся действий.

Данный подход особенно полезен в трех случаях:

1. Когда награды в среде очень редкие (как в тех же компьютерных играх);

2. Когда окружение постоянно меняется (например, для роботов в реальном мире);

3. Когда нужно избегать «застревания» в одних и тех же действиях.

Это подводит к ключевому вопросу — как именно формализовать эту «мотивацию», как алгоритмы реализуют этот концепт на практике, и почему это работает даже лучше явных наград в сложных средах.

Основная математическая идея curiosity-подходов выражается через формулу (1) внутренней награды:

$$r_t^{\text{int}} = \eta \cdot \frac{1}{2} \left\| \phi(s_{t+1}) - \hat{\phi}(s_{t+1}) \right\| \quad (1)$$

где:

η — коэффициент масштабирования (обычно 0.01-0.1);

φ($s_{t+1}$) — реальное представление следующего состояния;

φ̂($s_{t+1}$) — предсказанное представление состояния;

||...||² — квадрат евклидова расстояния (мера ошибки).

На практике, в подходе есть три основные фазы:

1. **Фаза кодирования:** энкодер преобразует сырые данные (пиксели экрана, сенсорные показания) в компактный вектор признаков**.**

2. **Фаза предсказания:** модель пытается предугадать следующее состояние.

3. **Расчёт награды:** система сравнивает предсказание с реальностью.

```
class CuriosityWrapper(nn.Module):
    def __init__(self, state_dim):
        super().__init__()
        self.encoder = nn.Linear(state_dim, 64) # Фаза сжатия
        self.predictor = nn.Linear(64 + action_dim, 64)  # Фаза
предсказания

    def forward(self, state, action, next_state):
        encoded = self.encoder(state)
        predicted = self.predictor(torch.cat([encoded, action],
dim=1))
        intrinsic_reward = 0.05 * torch.norm(predicted - self.e
ncoder(next_state))**2 # Фаза сравнения
        return intrinsic_reward
```

Алгоритм постоянно оценивает, насколько хорошо он понимает последствия своих действий. Когда агент попадает в новую ситуацию,

его модель ошибается в предсказаниях — и эта ошибка становится внутренней наградой. По мере изучения среды предсказания становятся точнее, и агент естественным образом переключается на поиск новых «белых пятен».

В качестве тестовой среды выбрана игра «Змейка", представляющая собой минималистичную модель с дискретным пространством действий (повороты) и редкими наградами (поедание яблок). Простота игровой механики в сочетании с нетривиальностью задачи оптимального награждения делает данную среду идеальным полигоном для апробации curiosity-подходов.

Например:

— Первый поворот за угол → большая ошибка предсказания → высокая награда;

— Десятый одинаковый поворот → ошибка минимальна → награда почти нулевая;

— Встреча с новым препятствием → ошибка снова резко растёт.

Данный механизм гарантирует, что агент не застрянет в циклических действиях, автоматически исследует всю карту и адаптируется без ручной настройки наград.

Curiosity-подход демонстрирует особую эффективность в игровых средах, где традиционные методы обучения с подкреплением часто сталкиваются с проблемой редких наград. Давайте рассмотрим, как это работает на практике.

В начальный этап изучения среды агент осуществляется с высокой степенью случайности, что сопровождается получением значительных внутренних наград за любые новые действия. По мере накопления опыта и расширения знаний о среде происходит формирование более точного представления о ее характеристиках. В отличие от традиционных методов обучения с подкреплением, модель основанная на любопытстве продолжает стимулировать поиск новых стратегий и после достижения рабочей решения, что предотвращает застревание в локальных оптимумах.

**Пример из практики.** Игра «Змейка». Обычный RL-агент часто зацикливается на простых паттернах движения, особенно если награда дается только за сбор еды. С curiosity-модулем наблюдается иная картину:

— В первые 1000 итераций агент активно исследует всю карту;

— К 5000 итераций вырабатывается систематический подход к исследованию;

— На 10000 итерации начинается осознанное поведение - змейка не только собирает еду, но и оптимально обходит препятствия.

Для достижения таких результатов важно правильно настроить систему:

— Коэффициент curiosity (η): 0.03-0.1 (меньше для сложных сред);

— Размер энкодированного представления: 64-256 нейронов;

— Продолжительность обучения: 1-5 миллионов шагов;

— Частота обновления: каждые 10000 шагов.

Главное достоинство метода – его автономность. Нет необходимости вручную проектировать сложную систему наград или прописывать правила исследования. Агент самостоятельно находит баланс между исследованием новых территорий, эксплуатацией известных успешных стратегий и адаптацией к изменяющимся условиям.

При этом система остается достаточно универсальной, чтобы работать в разных игровых жанрах - от простых аркад до сложных 3D-миров.

На практике важно учитывать, что для визуальных сред обязательна предварительная обработка кадров, а обучение требует в 2–3 раза больше вычислительных ресурсов по сравнению с обычным обучением с подкреплением.

Curiosity-подход — не единственный способ решения проблемы редких наград. Существуют так же:

1. Эпсилон-жадная стратегия (**ε-greedy**):

Случайные действия с вероятностью ε. Простейший способ исследования. Способ имеет ряд проблем: в нем нет направленного исследования, бесполезен в сложных средах и требует ручной настройки расписания ε. Поэтому подходит только для простых сред с дискретным действиями.

```
action = random_action if np.random.rand() < epsilon else best_
action
```

2. Noisy Networks:

Подход добавляет шум непосредственно к весам нейронной сети, создавая естественную стохастичность в действиях агента. В отличие от ε-greedy, исследование становится более направленным, так как зависит от текущего состояния. Однако метод может приводить к нестабильности обучения, особенно в задачах с длинными эпизодами, где согласованность действий критически важна.

```
self.fc = NoisyLinear(in_dim, out_dim)  # Слой с шумящими весам
и
```

3. Count-Based Exploration:

Метод основан на подсчёте посещённых состояний и награждении за исследование редких областей. Он особенно эффективен в дискретных пространствах с небольшим количеством возможных

состояний. Однако в непрерывных или высокоразмерных пространствах метод плохо масштабируется из-за проблемы разреженности данных и вычислительной сложности хранения статистики. Сравнение подходов представлена в таблице ниже.

Таблица – Критерии подходов

| Критерий | Curiosity | ε-greedy | Noisy Nets | Count-Based |
|---|---|---|---|---|
| Направленность | Высокая | Низкая | Средняя | Средняя |
| Масштабируемость | Высокая | Низкая | Высокая | Низкая |
| Стабильность | Средняя | Высокая | Средняя | Высокая |
| Универсальность | Высокая | Низкая | Высокая | Низкая |

Ключевое преимущество Curiosity заключается в способности автоматически генерировать осмысленные внутренние награды, что особенно ценно в сложных средах с визуальным входом. Метод демонстрирует хороший баланс между исследованием новых областей и эксплуатацией известных стратегий.

Основной недостаток — повышенные вычислительные затраты, связанные с необходимостью обучения дополнительных моделей. Это делает подход менее экономичным по сравнению с более простыми альтернативами в задачах, где достаточно базового исследования.

Для быстрого тестирования разных подходов используется следующий код на python:

```
from stable_baselines3 import DQN
model = DQN('Mlp', env, exploration_fraction=0.1) # ε-greedy
model = DQN('Mlp', env, exploration_noise=0.1) # Noisy Networks
```

Curiosity-driven методы представляют собой перспективное направление в reinforcement learning, предлагая эффективное решение проблемы редких наград в сложных средах. Проведенный анализ демонстрирует их преимущества перед традиционными подходами, такими как ε-greedy и count-based методы, особенно в задачах с высокоразмерными пространствами состояний.

Основные результаты исследования позволяют понять, что Curiosity-подходы обеспечивают более направленное и осмысленное исследование среды за счет внутренней системы мотивации. Метод демонстрирует хорошую масштабируемость для различных типов задач - от игровых сред до робототехники. Однако ключевым ограничением остается высокая вычислительная сложность, связанная с необходимостью обучения дополнительных моделей

Перспективными направлениями дальнейших исследований являются:

— Разработка более эффективных архитектур энкодеров;

— Оптимизация вычислительных затрат;

— Исследование гибридных подходов, сочетающих curiosity с другими методами exploration.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Arthur Juliani Решение задач с разреженным вознаграждением с помощью Curiosity / ARTHUR JULIANI [Электронный ресурс] // unity : [сайт]. — URL: https://unity.com (Дата обращения 5.5.25)

2. Alex Irpan Что не так с обучением с подкреплением (Reinforcement Learning)? / Alex Irpan [Электронный ресурс] // alexirpan : [сайт]. — URL: https://www.alexirpan.com (Дата обращения 5.5.25)

3. Васильев, Н. С. Обучение с подкреплением для реализации игрового искусственного интеллекта / н. с. васильев [текст] // электронные системы и технологии. — Минск: Научное электронное издание, 2023.

***УДК 004.89***

***Руденький А.О.***
*Московский государственный технический университет им. Н.Э. Баумана, г. Москва, Россия*

## СИСТЕМА АУДИОВИЗУАЛЬНОЙ НАВИГАЦИИ ДЛЯ ЛЮДЕЙ С НАРУШЕНИЯМИ ЗРЕНИЯ

Согласно данным, в России проживает более 450 000 человек с нарушениями зрения, которые сталкиваются с трудностями при ориентации в пространстве [1]. Существующие решения, такие как трости, собаки-поводыри или специализированные навигационные устройства, часто либо дороги, либо ограничены в функциональности. Разработанная система аудиовизуальной навигации, основанная на искусственном интеллекте (ИИ), предлагает доступное и эффективное решение, способное работать в реальном времени и адаптироваться к различным условиям. Целью работы является создание прототипа (MVP), который обеспечивает описание окружающей среды для незрячих пользователей с использованием открытых технологий и масштабируемой архитектуры.

**Архитектура системы**

Система состоит из клиентского приложения на базе Android и серверной части, где выполняются основные вычисления. Основные

компоненты включают:

1. **Клиентское приложение**: использует камеру смартфона для захвата изображений.
2. **Серверная часть**: включает модель обработки изображений (визуальный кодировщик), языковую модель Gemma для генерации текстового описания и модель VITS для преобразования текста в речь (Text-to-Speech, TTS).
3. **Инфраструктура**: поддерживает горизонтальное и вертикальное масштабирование, работает в контейнеризированной среде Kubernetes или без неё, использует OpenSource-продукты.

Обобщённая схема взаимодействия компонентов представлена на Рис. 1.

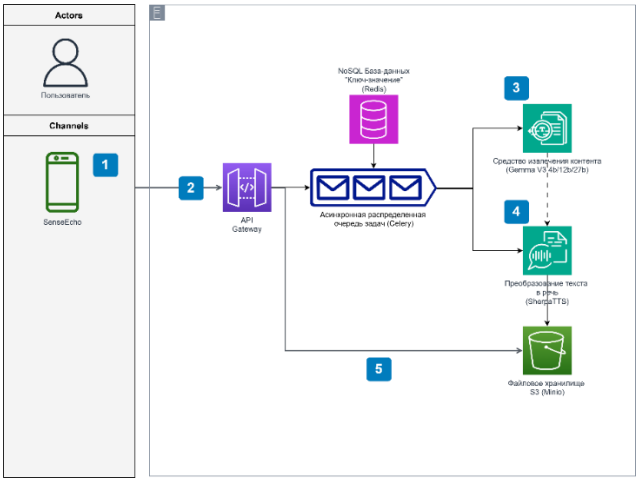



Рис. 1 Архитектура системы: визуальный кодировщик, модель Gemma и TTS-модуль VITS.

Процесс обработки запроса включает следующие этапы:

1. Захват изображения камерой смартфона.
2. Передача данных на сервер, где композиция моделей описывает сцену.
3. Преобразование описания в аудио и передача пользователю.

Модель VITS[2], используемая для TTS, представляет собой условный вариационный автоэнкодер с антагонистическим обучением. Её структура включает нормализующий поток, текстовый кодировщик и предсказатель стохастической длительности.

Производительность системы зависит от скорости обработки

запросов. Среднее время обработки одного изображения на видеокарте Nvidia RTX 2070 (8 ГБ VRAM) составляет 15 секунд. Для описания сцены используется композиция моделей, где визуальный кодировщик преобразует изображение в вектор признаков $V$, который затем обрабатывается языковой моделью для генерации текста $T$:

$$T = Gemma(V), V = Encoder(I) \quad (1)$$

где $I$ — входное изображение, $V$ — вектор признаков, $T$ — текстовое описание. TTS-модель преобразует текст в аудио $A$:

$$A = VITS(T) \quad (2)$$

Эффективность обработки определяется задержкой $\tau$:

$$\tau = \tau_{enc} + \tau_{Gemma} + \tau_{VITS} \quad (3)$$

где $\tau_{enc}, \tau_{Gemma}, \tau_{VITS}$ — время работы визуального кодировщика, модели Gemma [3] и VITS соответственно (1).

**Результаты тестирования**

Система была протестирована на различных сценариях, включая городские улицы, торговые центры и парковки. Примеры описаний:

- **Сцена 1 (городской перекрёсток)**: «На фотографии изображен городской перекресток. На переднем плане – желто-белая полоса пешеходного перехода, на асфальте которой есть следы от проезжающих машин. За переходом видна широкая улица с несколькими машинами. На заднем плане – многоэтажные здания и дорожный знак» (Табл. 1).
- **Сцена 2 (супермаркет)**: «На изображении видна полка в супермаркете. На полке выложены фрукты и овощи в пластиковых контейнерах. Слева – авокадо, рядом – красный лук и морковь. Цены: 43, 209, 179, 389, 109».

Таблица – Примеры описаний сцен

| Сцена | Описание | Время обработки, с |
|---|---|---|
| Перекрёсток | Желто-белая полоса пешеходного перехода, улица с машинами, многоэтажные здания | 14.8 |
| Супермаркет | Полка с фруктами и овощами, цены на наклейках | 15.2 |
| Парковка | Плиточная парковка, два автомобиля, оранжевый почтовый ящик | 15.0 |

Тестирование показало, что система способна генерировать точные и информативные описания, обеспечивая ориентацию в пространстве. Среднее время обработки варьируется от 14.8 до 15.2

секунд на Nvidia RTX 2070.

**Социальный эффект**

Система направлена на улучшение качества жизни людей с нарушениями зрения, обеспечивая:

- Доступ к городской инфраструктуре и транспорту.
- Инклюзивную цифровую среду.
- Упрощение повседневных задач, таких как навигация в магазинах или на улицах.

Разработанная система аудиовизуальной навигации представляет собой уникальное сочетание технологий ИИ и социальной миссии. Готовый прототип демонстрирует высокую точность описания сцен и потенциал для масштабирования. Сотрудничество с НКО и государственными платформами обеспечит широкое внедрение системы, улучшая качество жизни людей с нарушениями зрения.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кузнецова А.В. Назвала число незрячих граждан, проживающих в России / А.В. Кузнецова // Российская газета. — 2024. — № 11. — С. 1–2. — URL: https://rg.ru (дата обращения: 03.06.2025).

2. Kim J., Lee J. VITS: Conditional Variational Autoencoder with Adversarial Learning for End-to-End Text-to-Speech / J. Kim, J. Lee // arXiv. — 2021. — № 2106.06103. — С. 1–12. — URL: https://arxiv.org (дата обращения: 03.06.2025).

3. Gemma Team. Gemma 3 Technical Report / A. Kamath, J. Ferret, S. Pathak et al. // arXiv. — 2025. — № 2503.19786. — С. 1–30. — URL: https://arxiv.org (дата обращения: 03.06.2025).

***УДК 004.891.2***

***Рыбакова А.В.***
***Научный руководитель: Николаева Д.Р., канд. техн. наук, доц.***
*Тюменский индустриальный университет,*
*г. Тюмень, Россия.*

## РАЗРАБОТКА АЛГОРИТМА КЛАСТЕРИЗАЦИИ БИНАРНЫХ ДАННЫХ ДЛЯ ОПТИМИЗАЦИИ МАРШРУТОВ ОБЩЕСТВЕННОГО ТРАНСПОРТА

В статье предложен алгоритм кластеризации пользователей общественного транспорта на основе расстояния Хэмминга для анализа бинарных данных. Метод позволяет выявлять группы пассажиров со

схожими поведенческими паттернами и формировать персонализированные рекомендации по оптимизации маршрутов. Приведены примеры расчетов и практическое применение алгоритма.

Предлагаемый алгоритм кластеризации, основанный на расстоянии Хэмминга, особенно эффективен при анализе данных, где профиль пользователя представлен в виде бинарного вектора. Такой подход позволяет отразить наличие или отсутствие конкретных характеристик, таких как использование определенного маршрута, предпочтение определенного вида транспорта или время поездки.

Расстояние Хэмминга между двумя бинарными векторами (1) определяется как количество позиций, в которых эти векторы отличаются.

$$d_{ij} = \sum_{k=1}^{p} |x_{ik} - x_{jk}|, \quad (1)$$

где, $d_{ij}$ – расстояние Хэмминга между векторами i и j, $p$ – количество элементов (размерность) в каждом векторе, $x_{ik}$ – $k$-й элемент вектора i, $x_{jk}$ – $k$-й элемент вектора j, $|x_{ik} - x_{jk}|$ – абсолютное значение разности между k-ми элементами векторов i и j.

Расстояние Хэмминга хорошо подходит для задач, где признаки представлены в бинарном виде, что позволяет эффективно сравнивать профили пользователей, основанные на использовании определенных маршрутов, предпочтениях по видам транспорта и времени поездок. В отличие от метрик, основанных на непрерывных значениях (например, евклидово расстояние), расстояние Хэмминга непосредственно отражает различия в наборе дискретных характеристик, что упрощает интерпретацию результатов кластеризации.

Алгоритм кластеризации состоит из следующих шагов:

1. Формирование бинарных векторов профилей пользователей. Каждый пользователь представляется в виде бинарного вектора, где каждая позиция соответствует определенной характеристике (например, использование маршрута № 1, предпочтение автобусов, время поездки в утренний час пик). Значение 1 означает наличие характеристики, а 0 – ее отсутствие.

2. Выбор центров кластеров. Изначально выбирается k случайных пользователей, которые становятся центрами кластеров. В качестве альтернативы можно использовать другие методы для выбора начальных центров, например метод k-means++.

3. Распределение пользователей по кластерам. Для каждого пользователя вычисляется расстояние Хэмминга до каждого центра кластера (2). Пользователь относится к тому кластеру, до центра

которого расстояние минимально.

$$C(U) = argmin_c d(u, c), \quad (2)$$

где, C(u) – кластер, к которому относится пользователь u, c – центр кластера.

4. Пересчет центров кластеров. После того, как все пользователи распределены по кластерам, центры кластеров пересчитываются. Новый центр кластера (3) вычисляется как медианный вектор для всех пользователей, принадлежащих данному кластеру. Медианный вектор определяется как вектор, в котором каждая позиция имеет значение, наиболее часто встречающееся среди пользователей кластера.

$$c_i = mode(u_i), \quad (3)$$

где, $c_i$ – значение i-й позиции в центре кластера, $u_i$ – значения i-й позиции для всех пользователей кластера, mode – функция, возвращающая наиболее часто встречающееся значение.

5. Шаги 3 и 4 повторяются до тех пор, пока не будет достигнута сходимость, то есть пока центры кластеров не перестанут меняться или пока количество перераспределений пользователей между кластерами не станет меньше заданного порога.

Рассмотрим задачу группировки 5 пользователей общественного транспорта по 4 бинарным признакам:

- использует маршрут №1 (1 – да, 0 – нет);
- предпочитает автобусы (1 – да, 0 – нет);
- поездки в утренний час пик (1 – да, 0 – нет);
- частота поездок >3 раз в неделю (1 – да, 0 – нет).

Таблица 1 содержит бинарные векторы, представляющие профили пяти пользователей, сформированные на основе четырех признаков, характеризующих их использование общественного транспорта.

Таблица 1 – Исходные данные

| Пользователь | Маршрут №1 | Автобус | Утро | Частота >3 |
|---|---|---|---|---|
| A | 1 | 0 | 1 | 0 |
| B | 0 | 1 | 0 | 1 |
| C | 1 | 0 | 1 | 1 |
| D | 0 | 1 | 0 | 0 |
| E | 1 | 1 | 0 | 1 |

1. Выбираем число кластеров и начальные центры.

Пусть k = 2. Случайно выберем центры кластеров:

- кластер 1 ($C_1$): пользователь A = [1, 0, 1, 0];
- кластер 2 ($C_2$): пользователь B = [0, 1, 0, 1].

2. Распределяем пользователей по кластерам.

Для каждого пользователя вычисляем расстояние Хэмминга до $C_1$ и $C_2$ (количество несовпадающих позиций).

Пользователь A:

– расстояние до $c_1$: |1-1| + |0-0| + |1-1| + |0-0| = 0;
– расстояние до $c_2$: |1-0| + |0-1| + |1-0| + |0-1| = 1 + 1 + 1 + 1 = 4.

Относим к кластеру 1.

Пользователь B:

– расстояние до $C_1$: |0-1| + |1-0| + |0-1| + |1-0| = 1 + 1 + 1 + 1 = 4;
– расстояние до $C_2$: |0-0| + |1-1| + |0-0| + |1-1| = 0.

Относим к кластеру 2.

Пользователь C:

– расстояние до $C_1$: |1-1| + |0-0| + |1-1| + |1-0| = 0 + 0 + 0 + 1 = 1;
– расстояние до $C_2$: |1-0| + |0-1| + |1-0| + |1-1| = 1 + 1 + 1 + 0 = 3.

Относим к кластеру 1.

Пользователь D:

– расстояние до $C_1$: |0-1| + |1-0| + |0-1| + |0-0| = 1 + 1 + 1 + 0 = 3;
– расстояние до $C_2$: |0-0| + |1-1| + |0-0| + |0-1| = 0 + 0 + 0 + 1 = 1.

Относим к кластеру 2.

Пользователь E:

– расстояние до $C_1$: |1-1| + |1-0| + |0-1| + |1-0| = 0 + 1 + 1 + 1 = 3;
– расстояние до $C_2$: |1-0| + |1-1| + |0-0| + |1-1| = 1 + 0 + 0 + 0 = 1.

Относим к кластеру 2.

Итоговое распределение:

– кластер 1: A, C;
– кластер 2: B, D, E.

3. Пересчитываем центры кластеров.

Новый центр кластера – медианный вектор (наиболее часто встречающееся значение в каждой позиции).

1. Кластер 1 (A, C):

– маршрут №1: [1, 1] → mode = 1;
– автобус: [0, 0] → mode = 0;
– утро: [1, 1] → mode = 1;
– частота >3: [0, 1] → mode = 0.

Новый центр $C_1$: [1, 0, 1, 0] (не изменился).

2. Кластер 2 (B, D, E):

– маршрут №1: [0, 0, 1] → mode = 0;
– автобус: [1, 1, 1] → mode = 1;
– утро: [0, 0, 0] → mode = 0;
– частота >3: [1, 0, 1] → mode = 1.

Новый центр $C_2$: [0, 1, 0, 1] (не изменился).

Алгоритм сошелся (центры не поменялись).

Кластер 1: пользователи A и C – те, кто ездит по маршруту №1 утром, но редко (≤3 раз в неделю). Кластер 2: пользователи B, D, E – предпочитают автобусы, не ездят утром, но часто (кроме D).

Для кластера 1 можно предложить утренние абонементы. Для кластера 2 – рекламировать дневные рейсы автобусов.

Представленный в статье алгоритм кластеризации на основе расстояния Хэмминга доказал свою эффективность для задач сегментации пользователей общественного транспорта. Он позволяет выявлять логичные группы даже на небольших данных, а его результаты легко интерпретировать для практического применения.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванова, Л. Н. Методы оптимизации и алгоритм маршрутизации в транспортной логистике / Л. Н. Иванова, С. Е. Иванов. — Текст: электронный // ЭПИ. — 2024. — № 4. — URL: https://cyberleninka.ru (дата обращения: 01.05.2025).

2. Кугаевских, А. В. Классические методы машинного обучения / А. В. Кугаевских, Д. И. Муромцев, О. В. Кирсанова. — Текст: непосредственный. — СПб. : Университет ИТМО, 2022. — 53 с.

3. Кузнецов, А. А. Применение искусственного интеллекта для решения проблемы переполненности и продолжительности ожидания в общественном транспорте / А. А. Кузнецов. — Текст: непосредственный // Научный аспект. — 2024. — Т. 44, № 6. — С. 5504–5508.

4. Рябичев, В. Д. Теория и практика развития искусственного интеллекта на рынке технологий / В. Д. Рябичев, Г. И. Нечаев, Л. Г. Косоногова. — Текст: непосредственный // Вестник Луганского национального университета имени Владимира Даля. — 2020. — № 7 (37). — С. 7–18.

*УДК 004.9*

***Рыбочкин М.Р.***
***Научный руководитель: Кабалянц П.С. канд. техн. наук., доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ОБЗОР СИСТЕМ ОПТИМИЗАЦИИ ТРЕНИРОВОЧНОГО ПРОЦЕССА СПОРТСМЕНОВ С ИСПОЛЬЗОВАНИЕМ VR ТЕХНОЛОГИЙ

Современный этап развития спорта характеризуется активным внедрением цифровых и интеллектуальных технологий в процессы подготовки, оценки и реабилитации спортсменов. Одним из наиболее перспективных направлений является использование технологий виртуальной реальности (VR) в тренировочном процессе. Благодаря высокой степени погружения, возможности имитации игровых ситуаций и интерактивному взаимодействию, VR становится эффективным инструментом моделирования и анализа спортивных навыков, особенно в когнитивно-нагруженных игровых видах спорта, таких как футбол, баскетбол и хоккей. Актуальность данной темы обусловлена сразу несколькими факторами:

1. необходимостью объективной оценки индивидуальной и командной подготовки спортсменов;
2. растущими требованиями к точности аналитики и обратной связи для тренерского штаба;
3. ограничениями традиционного тренировочного процесса, связанными с ресурсами, безопасностью и логистикой;
4. растущим спросом на решения, поддерживающие восстановление спортсменов после травм и доступность спортивной подготовки для лиц с ограниченными возможностями.

Использование VR-технологий в сочетании с алгоритмами системного анализа и обработки информации позволяет реализовать интеллектуальные системы поддержки принятия решений в спорте, ориентированные на адаптивное управление тренировочным процессом, прогнозирование эффективности действий спортсмена, формирование персонализированных тренировочных планов.

Цель настоящей работы — провести обзор существующих решений, реализующих оптимизацию тренировочного процесса спортсменов с применением VR, а также сравнить используемые в них подходы с научной точки зрения. Особое внимание уделяется встроенным аналитическим механизмам, математическим моделям,

способам сбора и обработки данных. В статье рассматриваются наиболее значимые решения — Rezzil, Be Your Best, NeuroTrainer, а также даётся анализ их применимости в различных спортивных сценариях. Кроме того, проводится систематизация подходов к формализации тренировочного процесса, с акцентом на методы многокритериальной оптимизации, машинного обучения и нейросетевого моделирования.

Виртуальная реальность (VR) как инструмент спортивной подготовки представляет собой синтез технологий 3D-моделирования, трекинга движений и обработки сенсорных данных в реальном времени. В контексте спорта VR предоставляет возможность имитировать игровые ситуации с высокой степенью реализма, позволяя тренировать и оценивать не только физические, но и когнитивные способности спортсменов. Современные VR-системы оснащаются датчиками движения (IMU, гироскопы, акселерометры), системами захвата взгляда (eye tracking), а также средствами биометрического мониторинга, что делает их мощным источником данных для построения интеллектуальных моделей оптимизации. Применение VR позволяет многократно отрабатывать сценарии без риска травм и зависимости от погодных или временных условий, получать мгновенную обратную связь о действиях игрока, использовать тренажёры в академиях, реабилитационных центрах, детско-юношеских школах и даже в домашних условиях.

С точки зрения системного анализа, VR-тренировка представляет собой сложную многокомпонентную систему, в которой сочетаются управляющие воздействия (заданные тренером или системой), сенсорные реакции спортсмена, итеративные адаптивные изменения в тренировочном сценарии, аналитические и диагностические модули. На стыке VR и информационных технологий формируются интеллектуальные системы управления тренировочным процессом, в которых применяется обработка временных и пространственных данных, оптимизация поведения на основе обратной связи, прогнозирование и адаптация под индивидуальные особенности спортсмена. VR-технологии не только средство визуализации. Они становятся платформой для сбора информации, её анализа и принятия обоснованных решений, направленных на повышение эффективности подготовки.

Современные VR-системы для спортивной подготовки можно классифицировать по различным признакам: целевая аудитория, типы тренируемых навыков, способы сбора данных, наличие аналитики и математических моделей, а также адаптивность к индивидуальным

параметрам пользователя. Рассмотрим наиболее заметные решения на рынке — Rezzil, Be Your Best и NeuroTrainer. Rezzil - платформа разработана в Великобритании и используется ведущими клубами английской Премьер-лиги. Основной акцент делается на развитие когнитивных навыков: пространственное мышление, внимание, принятие решений. Система позволяет моделировать игровые ситуации в режиме высокого давления, использовать трекинг движений, а также формировать отчёты по точности, реакции и осведомлённости игрока. Используются базовые алгоритмы оценки времени реакции, плотности ошибок и шаблонов движения. Be Your Best - Норвежская разработка, ориентированная преимущественно на индивидуальные тренировки. Предоставляет функции сканирования поля, тренировок принятия решений, симуляции матчевых ситуаций. Алгоритмы строятся на основе данных о реакции и направлении взгляда. Включает в себя систему оценки «visual scan performance» — скорость и частота переключения внимания, а также точность выбора направлений паса и позиции. NeuroTrainer — система, изначально разрабатываемая для широкой аудитории (спортсмены, образовательные учреждения, корпоративный сектор), ориентирована на развитие когнитивных функций: скорость обработки информации, концентрация, рабочая память. Особенность NeuroTrainer — ориентация на абстрактные когнитивные задачи без явной привязки к игровым ситуациям. Применяются методы нейропсихологической диагностики.

Упомянутые системы не реализуют полный цикл оптимизации, включающий трекинг тела, когнитивную и тактическую аналитику, и, что важно, не ориентированы на Российский рынок. Это открывает пространство для разработки решений, сочетающих в себе VR, машинное обучение и принципы системного анализа.

Большинство VR-систем применяют рефлексные модели, основанные на анализе простейших сенсомоторных реакций: точности, времени ответа, скорости перемещения. Однако в более сложных конфигурациях возможен переход к моделям с обратной связью, включающим контроль за выполнением предписанных траекторий (ошибка траектории, overshoot), адаптацию под индивидуальные особенности: вес, инерция, скорость реакции, прогноз реакции в условиях внешних ограничений. Оптимизация тренировочного процесса требует воспроизведения ситуаций, близких к реальной игровой среде. Здесь находит применение агентно-ориентированное моделирование, где игрок моделируется как агент с набором правил поведения, виртуальные соперники и мяч действуют в рамках вероятностной модели и используются алгоритмы оценки «стоимости»

принятого решения (например, через минимизацию временных потерь или риска потери владения). Обработка тренировочных данных требует автоматизации анализа. В VR-среде это достигается с помощью для классификации действий, оценки успешности упражнений и выявления аномалий. Рекуррентные нейронные сети (RNN, LSTM) применяются для анализа временных зависимостей в действиях спортсмена. Особое внимание уделяется фиче-инжинирингу — извлечению осмысленных признаков из данных трекеров и VR-интерфейсов: частота сканирования, реакция на визуальные раздражители, смещения центра тяжести, микропаузы в реакции и прочие параметры. Для адаптации тренировочных программ применяются многокритериальные модели оптимизации, где учитываются реакция, точность, утомляемость, когнитивная нагрузка, также алгоритмы типа NSGA-II, Pareto-оптимизация, позволяющие находить сбалансированные тренировочные сценарии.

Несмотря на прогресс, в большинстве коммерческих решений используются статичные сценарии и простые модели без построения индивидуальных моделей игрока, отсутствует адаптивность — тренировочный процесс не реагирует на поведение в реальном времени, а модели чёрного ящика (например, DNN) часто не интерпретируемы тренером. Преодоление этих проблем требует более сложных моделей предсказания поведения и внедрения принципов системного анализа в архитектуру VR-решений.

На основе проведённого обзора и анализа применяемых методов оптимизации, целесообразно выполнить сравнительную оценку (Табл. 1) наиболее известных VR-систем с научной точки зрения. Для этого выделим ключевые параметры, отражающие не только функциональные характеристики, но и уровень математической формализации, степень адаптивности и интеллектуальности систем.

Таблица 1 – Сравнительная оценка VR-систем

| Система | Модель | Модели и ИИ | Обратная связь | Трекинг |
|---|---|---|---|---|
| Rezzil | Игровая, когнитивная | Простые пороговые модели | Умеренная | Голова, ноги |
| Be Your Best | Когнитивная, матчевая | Алгоритмы сканирования поля | Да, визуальные метрики | Голова, взгляд |
| NeuroTrainer | Абстрактная, когнитивная | Нейропсихологические тесты | Высокая | Нет |

Из приведённых данных видно, что большинство коммерчески доступных VR-систем имеют выраженный когнитивный уклон, при этом используемые математические модели носят ограниченно адаптивный характер. Модели часто непрозрачны, плохо масштабируются и не обладают механизмами оптимизации в рамках системного анализа. Особенно остро стоит проблема интерпретируемости результатов и отсутствия реактивной адаптации сценариев: системы фиксируют данные, но не формируют стратегий изменений тренировочного процесса.

Анализ существующих систем показал, что несмотря на технологическую зрелость отдельных решений, большинство из них ограничены в научной и аналитической глубине. Применяемые модели в основном фиксируют параметры реакции и внимания, однако не обладают полноценной адаптивностью, системной интеграцией и не включают методы формального многокритериального анализа. С точки зрения информационных технологий и системного анализа, основными ограничениями являются низкий уровень интерпретируемости аналитических моделей для тренеров и спортсменов, отсутствие сквозной интеграции трекинга тела, взгляда и когнитивной аналитики, а также использование преимущественно эмпирических сценариев, не поддержанных формализованными моделями.

Таким образом, существует научно обоснованная необходимость в разработке интеллектуальных VR-систем нового поколения, опирающихся на методы многокритериальной оптимизации, агентно-ориентированное и имитационное моделирование, алгоритмы предсказательной аналитики и адаптивного управления и полную интеграцию сенсорных данных с когнитивными метриками.

Перспективным направлением является создание отечественных решений, учитывающих особенности методик подготовки, локализацию и доступность, а также ориентированных на широкое внедрение в практику. Такие системы могут выступать как инструмент для построения цифровых двойников спортсменов, что открывает новые горизонты в индивидуализации подготовки и повышении результативности.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баландин Владимир Артемович, Илюшин Олег Владимирович Особенности использования технологии виртуальной реальности в подготовке спортсменов // StudNet. 2022. №5.

2. Леонов Сергей Владимирович, Поликанова Ирина Сергеевна, Булаева Наталья Игоревна, Клименко Виктор Александрович Особенности использования виртуальной реальности в спортивной практике // Национальный психологический журнал. 2020. №1 (37).

3. Степанов Алексей Владимирович Математическое моделирование при профессиональном ориентировании футболиста и прогрессе развития навыков в достижении топ-уровня // Ученые записки университета Лесгафта. 2019. №8 (174).

4. Костина Анастасия Алексеевна, Махов Станислав Юрьевич Инновационные технологии в профессиональном спорте // Наука-2020. 2017. №1 (12).

5. S. Zuev and P. Kabalyants, "Predicting Analysis of the Multi-Sensor Signals in Terms of Time Series," 2024 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 2024, pp. 697-702, doi: 10.1109/SmartIndustryCon61328.2024.10515457

6. Jessica Sharon Putranto, Jonathan Heriyanto, Kenny, Said Achmad, Aditya Kurniawan, Implementation of virtual reality technology for sports education and training: Systematic literature review, Procedia Computer Science, Volume 216, 2023, Pages 293-300, ISSN 1877-0509

7. Rezzil [Электронный ресурс] /. - Электрон. текстовые дан. - Режим доступа: https://www.rezzil.com, свободный. (Дата обращения 5.5.25)

8. Be Your Best [Электронный ресурс] /. - Электрон. текстовые дан. - Режим доступа: https://www.beyourbest.com, свободный. (Дата обращения 5.5.25)

9. NeuroTrainer [Электронный ресурс] /. - Электрон. текстовые дан. - Режим доступа: https://www.neurotrainer.com, свободный. (Дата обращения 5.5.25)

10. Pico 4 Pro [Электронный ресурс] /. - Электрон. текстовые дан. - Режим доступа: https://www.pico4pro.com, свободный. (Дата обращения 5.5.25)

*УДК 004.383.3*

***Рякин И.В.***
***Научный руководитель: Николаева Д.Р., канд. техн. наук, доц.***
*Тюменский индустриальный университет, г. Тюмень, Россия*

# ЦИФРОВОЙ АЛГОРИТМ ОБРАБОТКИ БИОХИМИЧЕСКИХ ДАННЫХ НА ОСНОВЕ ИНФРАКРАСНОЙ СПЕКТРОСКОПИИ

В статье рассматриваются два типа шумов в сигналах — постоянный и случайный (выбросы) — а также сравниваются наиболее популярные методы и фильтры, для их подавления. Рассматриваются такие методы фильтрации как: среднее арифметическое, бегущее среднее, медианный фильтр и фильтр Калмана. Приведены рекомендации по выбору метода в зависимости от типа сигнала, его скорости обработки, а также от требуемой точности.

Шум можно условно разделить на два типа: постоянный шум датчика с одинаковым отклонением (Рис. 1) и случайный шум, возникающий при различных случайных (обычно внешних) обстоятельствах (Рис. 2).

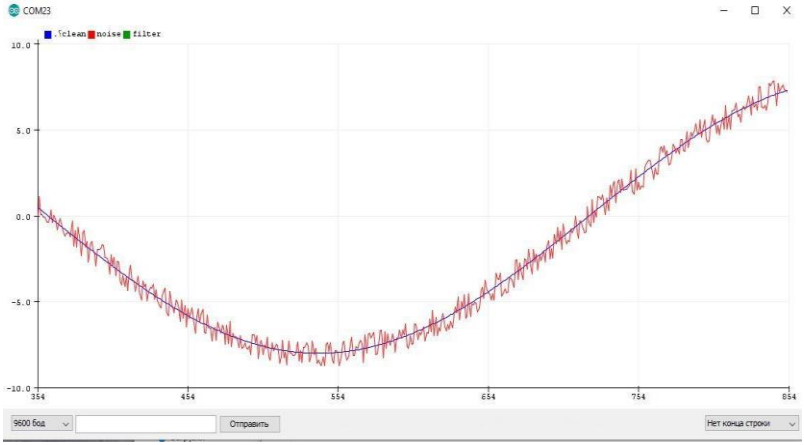



Рис. 1 Сигнал с постоянным шумом

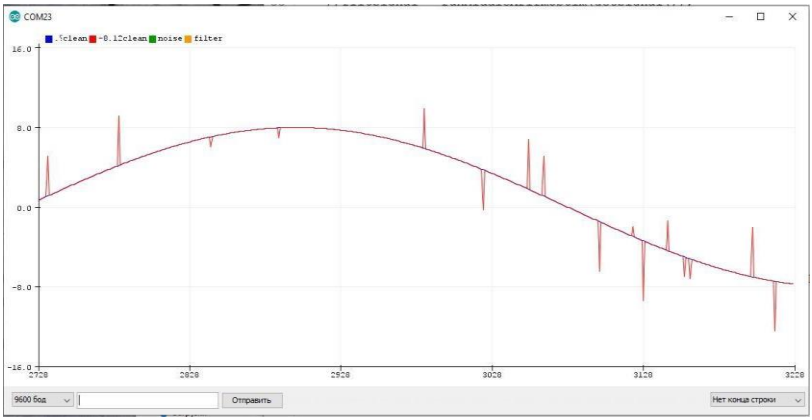


Рис. 2 Сигнал со случайными выбросами

Для обработки данных и устранения выбросов и шумов применяются программные фильтры, которые эффективно справляются с различными типами шума [1]. В числе распространённых методов фильтрации можно выделить следующие:

– среднее арифметическое с однократной выборкой;
– среднее арифметическое с растянутой выборкой;
– бегущее среднее арифметическое;
– медианный фильтр;
– фильтр Калмана.

Среднее арифметическое с однократной выборкой вычисляется как сумма всех значений, делённая на их количество. Этот метод работает следующим образом: в процессе вычислений значения поочередно суммируются, и в конце результат делится на количество элементов, что даёт среднее значение.

Среднее арифметическое с растянутой выборкой отличается тем, что перед расчётом среднего несколько значений накапливаются в буфере. В этом случае хранятся только последние измерения, и с каждым новым значением самое старое удаляется. После обновления буфера вычисляется среднее арифметическое последних данных [2].

Бегущее среднее - один из самых простых и эффективных фильтров. Его действие аналогично предыдущему, но реализация является более оптимальной, где фильтрованное значение получается с помощью вычисления разницы между новым и ранее фильтрованным значением, умноженное на коэффициент.

Для обработки сигналов с быстрыми изменениями может использоваться адаптивный коэффициент. В случае значительных

различий между текущим и фильтрованным значением коэффициент увеличивается, что ускоряет адаптацию. В условиях малых изменений коэффициент уменьшается, что способствует более эффективному подавлению шума. Такой подход позволяет повысить гибкость фильтра и адаптировать его к различным характеристикам сигналов [3].

Медианный фильтр, в отличие от предыдущих методов, не вычисляет среднее значение через математические операции, а выбирает его из набора значений, определяя медиану. Его основным преимуществом является высокая скорость работы, поскольку этот метод основывается на сравнении чисел, а не на сложных вычислениях.

Фильтр Калмана. В фильтре настраивается:

– разброс измерения (ожидаемый уровень шума);

– разброс оценки (есть возможность совпадения с разбросом измерений);

– скорость изменения значений (рекомендуется подбирать вручную, обычно в диапазоне 0,001–1).

Выбор оптимального фильтра зависит от характеристик обрабатываемого сигнала, а также от требований к скорости обработки данных сигналов. Метод среднего арифметического с однократной выборкой наиболее эффективен в тех случаях, когда фильтрация происходит редко и когда каждое измерение имеет минимальное время обработки. В большинстве практических приложений наилучшие результаты демонстрирует метод бегущего среднего, который сочетает высокую скорость обработки и эффективное сглаживание при правильной настройке [4]. Медианный фильтр третьего порядка обладает высокой скоростью работы, однако его применение ограничено только устранением выбросов без значительного сглаживания сигнала. Увеличение порядка медианного фильтра способствует улучшению качества обработки, но это повышает вычислительную сложность алгоритма. Наиболее эффективные результаты часто достигаются при сочетании медианного фильтра третьего порядка с методом бегущего среднего, что позволяет получить сигнал, очищенный от выбросов и одновременно плавный. Фильтр Калмана может демонстрировать сопоставимые результаты по подавлению шума, но требует тщательной настройки параметров и обладает более сложной вычислительной реализацией.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. XL-MaxSonar-WR|WC Datasheet. / [Электронный ресурс] // Maxbotix : [сайт]. — URL: https://www.maxbotix.com (дата обращения:

02.03.2025).
2. Jonathan Y. Stein Digital Signal Processing A Computer Science Perspective / Jonathan Y. Stein [Электронный ресурс] // Википедия: [сайт]. — URL: https://en.wikipedia.org (дата обращения: 06.03.2025).
3. Median filter / [Электронный ресурс] // Википедия: [сайт]. — URL: https://en.wikipedia.org (дата обращения: 04.03.2025).
4. Moving average filters. / [Электронный ресурс] // Аналог: [сайт]. — URL: https://www.analog.com (дата обращения: 06.03.2025).

***УДК 004.6***

***Сабанова Т.А., Галанкин Р.А.***
***Научный руководитель: Савинова Л.А., канд. экон. наук, доц.***
*Чувашский государственный университет*
*им. И.Н. Ульянова, г. Чебоксары, Россия*

## ПРИМЕНЕНИЕ BIG DATA В БИЗНЕСЕ

В настоящее время количество информации стремительно растет с каждой секундой. Компаниям необходимо поддерживать свою конкурентоспособность на рынке, что требует от них оперативной реакции на изменения рынка и повышения эффективности своей деятельности. Для достижения этой цели компаниям необходимо постоянно получать, обрабатывать и анализировать огромный массив данных, зачастую различных форматов и неструктурированных.

Для эффективной работы с такими объемами данных была поставлена задача модернизации инструментов для работы с большими данными. Так, появился термин «Big Data», призванный решить данную проблему. Если раньше этот термин представлял интерес исключительно для узкого круга специалистов, то в настоящее время он стремительно набирает популярность и является одним из самых перспективных направлений в IT. Крупные компании, включая российские, активно инвестируют в развитие Big Data.

В то время как традиционные методы обработки и анализа больших потоков информации малоэффективны, новые технологии способны работать с большим потоком информации, что помогает компаниям в прогнозировании и планировании. Благодаря Big Data компании могут сократить издержки в производстве, разработке или логистике, повысить эффективность своей работы и своевременно выявлять изменения на рынке. Это может послужить причиной увеличения прибыли компаний, поэтому бизнес заинтересован в развитии Big Data.

Понятие «Big Data» относится не только к огромным массивам данных, исчисляемых терабайтами, петабайтами, а иногда и эксабайтами, но и к специализированным методам их обработки и анализа. Причем эти технологии превосходят традиционные решения, предлагая значительные преимущества в скорости анализа, точности выводов и экономической эффективности.

Big Data определяется пятью основными признаками, известные как «5V»:

1. Volume (Объем). Данные представляют собой огромный объем информации, исчисляемый до эксабайтов. Такие масштабы не позволяют хранить и управлять данными в классических СУБД, поэтому требуются специализированные решения, например, распределенные системы хранения (Hadoop, облачные платформы, NoSQL-базы).

2. Velocity (Скорость). Данные постоянно генерируются и изменяются с высокой скоростью, и, чтобы получать актуальную информацию, появляется необходимость обрабатывать данные со скоростью, близкой к реальному времени, или осуществлять потоковую обработку. Для этого используются такие технологии, как Apache Spark и Apache Kafka.

3. Variety (Разнообразие). Данные отличаются неоднородностью, выражающиеся как строго формализованные структуры (таблицы и JSON), так и полностью свободные форматы (мультимедиа). Для эффективной работы требуется инструменты, поддерживающие все типы данных (MongoDB, Cassandra).

4. Veracity (Достоверность). Данные часто содержат ошибки, шумы или противоречия, особенно если информация поступает из неизвестных источников или социальных сетей. Для бизнеса важно отличать достоверную информацию от недостоверной, поэтому современные инструменты включают алгоритмы очистки данных и методы валидации.

5. Value (Ценность). Объем данных не имеет смысла, если из них нельзя извлечь практическую пользу, поэтому ключевой задачей является преобразование данных в бизнес-решение. Это достигается за счет технологий Data Mining для выявления скрытых закономерностей, за счет машинного обучения для прогнозирования и за счет расширенной аналитики для стратегического планирования.

Для любой крупной компании в сфере информационных технологий необходимым условием развития является внедрение Big Data. Благодаря новым технологиям у компаний появляется возможность получить анализ поведения клиентов и прогнозировать

будущие изменения на рынке, и тем самым поддерживать свою конкурентоспособность. Для достижения этого компании используют различные инструменты для хранения и обработки, аналитики и визуализации.

Традиционные реляционные базы данных могут быть неэффективны для работы с большими данными, поэтому требуются специализированные системы хранения, таковой является кластерная файловая система. Малоэффективность традиционных реляционных баз данных связана с несколькими причинами. Одна из них заключается в том, что реляционные базы данных в основном ориентируются на вертикальное масштабирование, что означает повышение производительности посредством добавления новых компонентов (процессоров, оперативной памяти, жесткого диска) к существующему оборудованию, в то время как кластерные – на горизонтальное, то есть посредством добавления новых узлов (серверов). Ещё одним важным преимуществом кластерной файловой системы является хранение сразу на нескольких узлах, где данные автоматически реплицируются на несколько узлов. Одной из первых таких технологий была HDFS в составе Hadoop, обеспечивающая надежное хранение информации. Ещё один способ хранения больших данных – NoSQL-базы данных. К ним относятся, например, MongoDB и Cassandra. А также используются облачные сервисы (к примеру, Amazon S3 и Google BigQuery). Стоит отметить, что перед хранением данные проходят очистку (Data Cleaning) с помощью специальных алгоритмов.

Если говорить про недостаток обработки больших данных традиционными методами, то им является малая эффективность или неэффективность при работе с данными, не являющими структурированными. Одной из первых технологий принявшейся решить эту проблему стала Hadoop, а именно MapReduce и YARN. Однако в настоящее время чаще для работы используется Apache Spark, так как она значительно быстрее за счет использования оперативной памяти. Также для задач, требующих потоковую обработку, используется Apache Kafka.

Следующий этапом работы с данными является анализ обработанной информации. Часто для этой цели используются скрипты и программы, написанные на Python (библиотеки Pandas, NumPy, SciPy). Также популярно для анализа использование машинного обучения и искусственного интеллекта (например, в Python библиотеки PyTorch и TensorFlow). Помимо вышеперечисленных способов анализа используются как классические СУБД (MySQL, PostgreSQL), так и

оптимизированный SQL для Big Data (Apache Spark SQL, Google BigQuery).

Стоит выделить инструменты визуализации данных. Лидерами в этой области являются Tableau и Power BI. Данные платформы способны не только визуализировать данные, но и с помощью встроенных функций проводить их анализ. Можно считать результаты их работы завершающим этапом работы с данными, делающим результаты доступными для восприятия.

Big Data имеет широкое применение в бизнесе. Одной из отраслей, где большие данные смогли трансформировать бизнес является розничная торговля. Один из крупнейших мировых ритейлеров, Amazon, активно использует алгоритмы рекомендации на основе анализа истории просмотра и покупок. Эти алгоритмы используются и в российском бизнесе. Например, на главной странице маркетплейса Ozon можно увидеть раздел «Рекомендуем для вас», в котором собраны товары, способные заинтересовать пользователя. Благодаря этим механизмам Ozon может не только привлекать новых клиентов, но и удерживать существующих, а также повышать частоту повторных покупок. Для доказательства этого обратимся к отчету Ozon за 4 квартал и весь 2024 год [10]. Так, в источнике указывается, что в среднем один пользователь совершает 26 заказов в год, что превышает прошлогодние показатели на 24%. Это прямой индикатор повторных покупок. Также отмечается увеличение активных покупателей на 10 миллионов, и к 31 декабря 2024 года их составило 57 миллионов. Помимо этого, заметен рост валовой стоимости товаров на 64% и количества заказов на 52% по сравнению с прошлым годом. Как итог, выручка от маркетинговых и информационных услуг выросла на 95% по сравнению с 2023.

Также финансовые организации часто используют Big Data для снижения рисков, а точнее антифрод-системы. Например, банки используют системы на основе машинного обучения для противодействия мошенничеству. Эта работа представляет следующее. Система анализирует поведение клиентов: к этому относится время и сумма переводов, геолокация и устройства, с которых совершаются транзакции. Затем система в случае совершения нетипичных для пользователя операций блокирует ее. Такие ML-алгоритмы и ИИ использует, например, Т-Банк. Как отмечалось в «финансовых результатах по МСФО за IV квартал и 2024 год» [12], «с помощью ИИ-технологий мы каждый день защищаем миллионы клиентов Т и триллионы их денег от мошенников». В отчете акцент делается на искусственном интеллекте, но для его функционирования необходимы технологии Big Data для сбора и обработки информации.

Это одни из немногих способов применения технологий работы с большими данными в бизнесе, но они уже показывают ряд преимуществ для интеграции в бизнес. Во-первых, это персонализация услуг. Для пользователя это индивидуализация предложений, например, подборка фильмов и сериалов на Netflix или Кинопоиске, или подборка товаров на маркетплейсах. А для бизнеса это может послужить причиной увеличения количества клиентов и продаж. Во-вторых, прогнозирование трендов. Например, ритейлеры на основе анализа продуктовой корзины покупателей могут корректировать ассортимент, тем самым сокращая затраты на товары с низким спросом.

Можно выделить и несколько недостатков Big Data. Один из них - высокая стоимость внедрения, если речь идет о переходе к Big Data. Стоит отметить, что некоторые крупные компании предлагают в аренду платформы для работы с Big Data, например, Google BigQuery, что делает возможным для малого и среднего бизнеса тоже работать с большими данными. Еще важной проблемой является нехватка квалифицированных специалистов. Это может тормозить развитие Big Data. Также существует этическая дилемма об использовании информационного следа для увеличения прибыли компаний.

Big Data кардинально изменили подходы к ведению бизнеса, позволив компаниям принимать решения по дальнейшим действиям, основанные на анализе множества параметров. Это помогает компаниям привлекать новых клиентов и удерживать старых, а также прогнозировать спрос и изменения на рынке, увеличивать продажи, например, за счет рекомендательных алгоритмов.

Однако внедрение больших данных сталкивается с рядом проблем: нехватка квалифицированных специалистов, высокая стоимость внедрения, риски, связанные с безопасностью и этикой использования данных. Успешные компании преодолевают это благодаря поэтапному внедрению новых технологий, инвестиций в качество данных и строгого соблюдения регуляторных требований.

Очевидно, в будущем влияние Big Data будет только расти. Также новые технологии, такие как искусственный интеллект, откроют новые возможности для бизнеса. Организации, уже грамотно выстраивающие работу с данными, получают конкурентное преимущество.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Орлов, Г.А. Применение Big Data при анализе больших данных в компьютерных сетях / Г.А. Орлов, А.В. Красов, А.М. Гельфанд // Наукоемкие технологии в космических исследованиях Земли. — 2020.

— Т. 12, № 4. — С. 76–84. — DOI: 10.36724/2409-5419-2020-12-4-76-84. — URL: https://www.elibrary.ru (дата обращения: 21.05.2025).

2. Атырова, Р.С. Информационно-аналитические системы для обработки больших данных (Big Data) / Р.С. Атырова, А.Э. Жуманова // Известия Национальной академии наук Кыргызской Республики. — 2022. — № S5. — С. 121–126. — URL: https://www.elibrary.ru (дата обращения: 21.05.2025).

3. Нгуен, Т.Т. Big Data: применение больших данных на практике / Т.Т. Нгуен, Р.С. Зарипова, Ф.Х. Нгуен // Научно-технический вестник Поволжья. — 2023. — № 9. — С. 120–122. — URL: https://www.elibrary.ru (дата обращения: 21.05.2025).

4. Васильев, С.А. Банки, финансовые платформы и Big Data: тенденции развития и направления регулирования / С.А. Васильев, И.А. Никонова, О.С. Мирошниченко // Финансовый журнал. — 2022. — Т. 14, № 5. — С. 105–119. — DOI: 10.31107/2075-1990-2022-5-105-119. — URL: https://www.elibrary.ru (дата обращения: 21.05.2025).

5. Моисеенко, Н.А. Большие данные и некоторые возможности их применения / Н.А. Моисеенко, М.М. Цуев, Э.Х. Саратова // Вестник ГГНТУ. Технические науки. — 2023. — Т. 19, № 3 (33). — С. 15–23. — DOI: 10.26200/GSTOU.2023.65.74.002. — URL: https://www.elibrary.ru (дата обращения: 21.05.2025).

6. Абдирахимов, И.Э. Проблемы и решение в Big data / И.Э. Абдирахимов // Sanoatda raqamli texnologiyalar / Цифровые технологии в промышленности. - 2023. - №1. – С. 158-164. - URL: https://cyberleninka.ru (дата обращения: 21.05.2025).

7. Савзиханова, С.Э. Big data – выигрышная инновация для прогнозирования будущих тенденций / С.Э. Савзиханова // УЭПС: управление, экономика, политика, социология. - 2023. - №2. – С. 69-75. - URL: https://cyberleninka.ru (дата обращения: 21.05.2025).

8. Хаиретдинов, А.Н. Влияние облачных решений на масштабируемость и эффективность технологий Big data / А.Н. Хаиретдинов // Академическая наука. - 2025. - №2. – С. 174-178. - URL: https://cyberleninka.ru (дата обращения: 21.05.2025).

9. Макшанов, А. В. Большие данные. Big Data / А. В. Макшанов, А. Е. Журавлев, Л. Н. Тындыкарь. — 4-е изд., стер. — Санкт-Петербург: Лань, 2024. — 188 с. — ISBN 978-5-507-47346-5. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com (дата обращения: 21.05.2025). — Режим доступа: для авториз. пользователей.

10. Интернет-ресурсы корпорации Ozon: [официальный сайт]. — URL: https://ir.ozon.com (дата обращения: 21.05.2025).

11. Tinkoff запустил Tinkoff Defense — комплексную платформу безопасности экосистемы: [электронный ресурс] // Официальный сайт Т-Банка. — 02.06.2021. — URL: https://www.tbank.ru (дата обращения: 21.05.2025).

12. T-Technologies: [официальный сайт]. — URL: https://t-technologies.ru (дата обращения: 22.05.2025).

***УДК 004.056***

***Седых А.А.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КАК УСТРОЕНЫ АТАКИ ТИПА “ОТКАЗ В ОБСЛУЖИВАНИИ” (DDOS) И КТО ОТ НИХ СТРАДАЕТ

Знаете, есть такая напасть в интернете, называется DDoS-атака. Звучит мудрено, но суть проста, как три копейки: это когда куча народу (вернее, компьютеров) одновременно ломится на какой-нибудь сайт или сервис, и он от такой дикой нагрузки просто "ложится". Представьте, что вы пытаетесь зайти в свой любимый интернет-магазин, а там – как на вокзале в час пик, только еще хуже: сайт либо вообще не открывается, либо тормозит так, что проще плюнуть и уйти. Вот это оно и есть. Хакеры, или кто там за этим стоит, специально заваливают ресурс бессмысленными запросами, пока у него не кончатся все силы – и интернет-канал не выдержит, и процессор "закипит", и память вся забьется. В итоге, для нас с вами, обычных пользователей, сайт становится недоступен.

А кто же эти "нападающие"? Чаще всего это целая армия "зомбированных" компьютеров и всяких умных гаджетов – от камер видеонаблюдения и роутеров до умных холодильников. Да-да, ваш безобидный чайник тоже может участвовать в таком безобразии, если его кто-то взломал! Злодеи, которых называют ботмастерами, заражают эти устройства вирусами, и те начинают слушаться их команд. Собирается такая вот "бот-сеть", иногда из миллионов устройств, и по команде "фас!" вся эта орава начинает долбить одну цель. Особенно легко сейчас насобирать такую армию из всяких IoT-штуковин, потому что производители часто не парятся с безопасностью: пароли ставят смешные, типа "admin/admin", или дыры в программах годами не закрывают. Был такой известный ботнет, Mirai назывался, так он как раз из таких вот "умных" вещей и состоял.

Сами атаки бывают разные, как по силе, так и по хитрости. Самый лобовой вариант – это когда просто пытаются забить интернет-канал жертвы мусорным трафиком. Это как если бы вам в почтовый ящик начали тоннами сыпать рекламные листовки, так что для настоящих писем места бы не осталось. Мощность таких атак измеряют в гигабитах, а то и терабитах в секунду – это очень много! Сюда входит, например, UDP-флуд: на сервер сыплются пакеты данных, которые ему вроде как и не нужны, но он честно пытается их обработать и тратит на это силы. Или пинг-флуд – это когда сервер заваливают запросами "ты тут?", и он вынужден на каждый отвечать. А есть еще атаки с "усилением". Это когда хакер хитрит: он шлет маленькие запросы на какие-нибудь левые серверы (например, старые DNS-серверы, которые всем отвечают), но делает это как бы от имени жертвы. А те серверы в ответ шлют жертве уже гораздо большие объемы данных. Получается, что атакующий малыми силами создает огромную волну трафика.

Бывают атаки похитрее, когда бьют не по ширине канала, а по "мозгам" сервера или сетевого оборудования – всяких там файрволов и балансировщиков. Пытаются исчерпать их ресурсы, используя слабые места в протоколах, по которым общаются компьютеры в сети. Классика жанра – SYN-флуд. Представьте, что кто-то постоянно звонит вам в дверь и убегает, не дожидаясь, пока вы откроете. Вот и сервер так же: ему шлют запрос на соединение, он готовится, ждет, а в ответ – тишина. И таких "пустых" звонков могут быть тысячи, пока сервер просто не перестанет реагировать на нормальные запросы. Раньше была популярна атака "Пинг смерти", когда один криво сделанный пакет мог "уронить" систему, но сейчас от нее вроде как научились защищаться. Но идея использовать дыры в протоколах жива.

Ну и самый такой "интеллигентный" вид атак – это атаки на уровне приложений. Их сложнее всего заметить, потому что они могут выглядеть как обычная активность пользователей. Хакеры не просто заваливают сервер мусором, а заставляют его выполнять какие-то сложные, ресурсоемкие задачи. Например, шлют тысячи запросов на поиск по сайту или просят сгенерировать какую-нибудь сложную страницу. Или, как в атаке Slowloris, подключаются к серверу и очень-очень медленно что-то ему отправляют или от него получают. Сервер терпеливо ждет, держит соединение открытым, а таких хитрых "медленных" клиентов может быть много, и в итоге серверу просто не хватает "рук" на всех. В последнее время модно стало атаковать API – это такие специальные "двери" для программ, через которые они общаются с сервисом. Если найти там уязвимое место, можно заставить сервер выполнять очень тяжелую работу.

А кто же от всего этого страдает? Да практически все, кто так или иначе связан с интернетом. Первыми на ум приходят банки, платежные системы, всякие криптовалютные биржи. Их атакуют, чтобы денег вымогать ("заплати, или не включим"), или чтобы конкурентам насолить, или просто панику посеять. Интернет-магазины и вообще любой онлайн-бизнес – для них каждая минута простоя это потерянные деньги и клиенты, особенно перед праздниками или в дни распродаж. Геймеры тоже часто страдают: игровые серверы – излюбленная мишень для обиженных игроков или нечестных конкурентов.

Государственные сайты, порталы госуслуг – тоже под ударом. Тут мотивы могут быть политическими: кто-то хочет выразить протест, кто-то – помешать работе правительства, а кто-то и вовсе использует DDoS как прикрытие, чтобы незаметно украсть важную информацию. Школы и университеты могут атаковать во время экзаменов или приемной кампании. Новостные сайты, особенно те, что публикуют острые материалы, тоже часто "глушат", чтобы заткнуть им рот. А самое страшное, когда атакуют объекты критической инфраструктуры – энергетические компании, связь, транспорт. Тут уже последствия могут быть куда серьезнее, чем просто недоступный сайт.

Но дело не только в тех, на кого нападают напрямую. Мы с вами, обычные пользователи, тоже страдаем: не можем зайти на нужный сайт, воспользоваться сервисом, теряем время, а иногда и деньги. Интернет-провайдеры и хостинги тоже попадают под раздачу: их оборудование перегружается, страдают другие клиенты, которые вообще ни при чем. Ну и, конечно, те бедолаги, чьи компьютеры или умные утюги стали частью этой "зомби-армии", – у них и интернет тормозит, и техника работает хуже, да еще и могут обвинить в пособничестве хакерам.

Последствия у таких атак – хуже не придумаешь. Это и прямые убытки от того, что сервис не работает, и траты на то, чтобы все починить и как-то защититься на будущее. Это и удар по репутации: кто захочет пользоваться услугами компании, которая постоянно "лежит"? Это и срыв всех рабочих процессов внутри компании. А иногда, как я уже говорил, DDoS – это просто отвлекающий маневр, пока воры потихоньку выносят ценные данные. В общем, приятного мало, и если компанию постоянно так "кошмарят", она может и вовсе уйти с рынка.

Бороться с этим злом – та еще задачка. Хакеры постоянно придумывают что-то новенькое, их инструменты становятся все доступнее – можно даже заказать DDoS-атаку в интернете, как пиццу. А попробуй потом найди, кто за этим стоит, – они же прячутся за кучей прокси-серверов и поддельных адресов.

Так что, как видите, DDoS – это не просто какая-то техническая проблема. Это серьезная угроза, которая касается всех нас. И чтобы с ней справиться, нужны усилия со всех сторон: и чтобы техника была умнее и защищеннее, и чтобы люди были грамотнее, и чтобы полиция разных стран вместе ловила этих кибер-бандитов. Если мы не поймем, как это работает, и кто от этого страдает, так и будем сидеть у разбитого интернет-корыта.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Иванов, И. В. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра / И. В. Иванов, С. И. Жданова // Материалы конференций ГНИИ "НАЦРАЗВИТИЕ". Июнь 2017 : Сборник избранных статей, Санкт-Петербург, 26–30 июня 2017 года / Выпускающий редактор Ю.Ф. Эльзессер Ответственный за выпуск Л.А. Павлов. – Санкт-Петербург: ГНИИ «НАЦРАЗВИТИЕ», 2017. – С. 116-119. – EDN ZDLMQH.

2. Жданова, С. И. Перспективы применения технологии блокчейн в образовании / С. И. Жданова // Содействие профессиональному становлению личности и трудоустройству молодых специалистов в современных условиях : сборник материалов VIII международной научно-практической конференции, посвященной 10-летию Регионального научно-методического центра профессиональной адаптации и трудоустройства специалистов: в 2 частях, Белгород, 18 ноября 2016 года / Белгородский государственный технологический университет им. В.Г. Шухова. Том Часть 1. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2016. – С. 189-193. – EDN ZAWFED.

3. Сачков, И. К. DDoS атаки: технологии, тенденции, реагирование и оформление доказательств / И. К. Сачков // Защита информации. Инсайд. – 2010. – № 6(36). – С. 59-63. – EDN TMLXPT.

4. Терновой, О. С. Раннее обнаружение DDOS атак на основе статистического анализа / О. С. Терновой // Перспективы развития информационных технологий. – 2011. – № 6. – С. 212-215. – EDN RPDHNT.

5. Яремчук, А. В. Борьба с DDoS: защита и оптимальные подходы к развертыванию / А. В. Яремчук // Тенденции развития науки и образования. – 2024. – № 108-12. – С. 183-186. – DOI 10.18411/trnio-04-2024-688. – EDN XCCGCM.

6. Назаров, А. Ш. DDoS-атаки и средства защиты от них / А. Ш. Назаров, И. Т. Ли // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. – 2023. – № 1(61). – С. 42-45. – EDN VZKHKQ.

7. Хохлов, Р. В. Противодействие DDOS - атакам с помощью анти-DDOS / Р. В. Хохлов, С. А. Мишин, Р. А. Солодуха // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2017. – № 1. – С. 151-156. – EDN ZGSRMB.

***УДК 69.003.12***

***Серова А.С., Смирнов Д.С.***
***Научный руководитель: Смирнов Д.С., канд. экон. наук, доц.***
*Национальный ядерный университет, г. Москва, Россия*

# ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В ЗАДАЧЕ КЛАССИФИКАЦИИ СТРОИТЕЛЬНО-МОНТАЖНЫХ РАБОТ

Строительно-монтажные работы (СМР) и их наименования определяются на этапе проектирования объекта капитального строительства. Этот процесс начинается с формирования проектной документации, где закладываются основные параметры будущих работ. Они должны соответствовать содержанию разделов документации и быть однозначно понятными для всех участников строительства. Для этого, наименования и классификация СМР определяется нормативными положениями [1]. Дальнейшая детализация происходит в процессе разработки рабочей документации, которая является основой для проведения конкретных СМР.

Классификацию строительно-монтажных работ проводят в первую очередь для систематизации и упрощения управления строительным процессом. Однако, как только начинаются первые реальные операции на стройплощадке, особенно при внесении изменений в проект или обнаружении неучтённых факторов, в процессе строительства возникает ситуация, когда появляется разница между проектными и фактическими наименованиями, классификация работ также может изменится.

Сроки и точность внесения изменений не регламентируются и определяются внутри организации условиями договора между участниками строительства [2]. Каждый проект строительства обладает уникальным набором технологических процессов, в связи с чем универсальные строительные классификаторы могут быть не применимы [3]. Тем самым эксперты строительной отрасли ограничены локальными классификаторами, работа с которыми требует

значительных ресурсов и экспертизы для проведения точной классификации СМР только по их фактическому наименованию.

Для оперативной поддержки принятия решений в строительном процессе и реализации структурирования строительной информации о СМР требуется автоматизированный инструмент. В большинстве исследований классификация строительно-монтажных работ по наименованиям проводится для задач автоматизации планирования, управления ресурсами, контроля качества и интеграции с цифровыми системами. Часто используются методы системного анализа и группировки на основе ранее разработанных классификаторов [4]. В некоторых научных работах используются статистические и математические инструменты, а также современные цифровые технологии [5]. Активно исследуются подходы на основе машинного обучения для автоматизации распознавания и классификации фактических наименований СМР в строительной документации [6]. Особенно такие средства применимы для автоматизации анализа больших массивов проектной информации и стандартизации данных [7]. Однако, в известных исследованиях процесс обработки наименований строительных работ не описан подробно, так как классификация является инструментом решения более прикладных и узконаправленных задач, а не самим предметом исследования.

В данной работе проведен анализ наименований строительно-монтажных работ, собранных из открытых источников. Работы были классифицированы вручную, использовалась классификация, представленная в открытых базах знаний. Тем самым был сформирован набор данных, в котором содержатся 10 тысяч наименований СМР, разбитых на 65 классов. Для проверки данных был выбран анализ сопряжённости и оценка статистической значимости связей между категориями, сформирована матрица сопряженности.

Критерий хи-квадрат позволяет проверить гипотезу о независимости двух категориальных переменных. При этом рассчитывается сумма квадратов разностей между наблюдаемыми и ожидаемыми частотами для каждой ячейки таблицы сопряжённости, что даёт количественную оценку различий между фактическим и теоретическим распределениями [8].

Коэффициент Крамера V дополняет результаты теста хи-квадрат, нормализуя значение статистики с учётом размера выборки и размеров таблицы сопряжённости. Это позволяет получить универсальную меру силы связи между переменными в диапазоне от 0 до 1, что особенно важно при сравнении таблиц разного размера и структуры [9].

В исследовании для анализа связи между типами и

наименованиями строительно-монтажных работ был также применён коэффициент контингенции Пирсона, вычисляемый на основе статистики хи-квадрат и нормируемый с учётом максимально возможного значения для данной таблицы.

Использование сингулярного разложения матрицы позволило корректно рассчитать максимальное значение коэффициента для таблиц произвольного размера. Это позволило оценить не только силу связи, но и сравнить её с теоретическим максимумом [8].

Таблица 1 – Результаты анализа наименований СМР статистическими методами

| **Название аналитики** | **Полученные результаты** |
|---|---|
| $\chi^2$ статистика | 624971,83 |
| p-value | 1,00 |
| Степени свободы | 630080 |
| Коэффициент контингенции (C) | 0,9921 |
| Максимально возможный коэффициент ($C_{max}$) | 0,9923 |
| Нормированный коэффициент ($C/C_{max}$) | 0,9999 |

В ходе анализа таблицы сопряжённости между типами и названиями строительно-монтажных работ были получены противоречивые результаты. Формально высокая сила связи сочетается с отсутствием статистической значимости. Данное противоречие обусловлено разреженностью матрицы и большим числом уникальных названий, что делает стандартные статистические тесты ненадёжными.

Проведен анализ ассоциации между классами и наименованиями строительно-монтажных работ для выявления устойчивых связей. Показатель разнообразия вычислялся как отношение числа уникальных названий к общему количеству записей в типе, а также определялась доля каждого класса в общем объёме данных. Полученные результаты для всех классов свидетельствует о полной уникальности наименований работ в рамках каждой категории, что делает невозможным статистический анализ ассоциаций между типами и названиями работ традиционными методами.

В дополнение к статистическому анализу для выявления естественной структуры и определения количества видов строительно-монтажных работ применен кластерный анализ [10]. Для выявления скрытой структуры и определения оптимального числа групп в массиве наименований строительно-монтажных работ использован алгоритм K-Means. Векторизация текстовых данных осуществлялась с помощью TF-IDF, каждое наименование представлено в виде числового вектора, отражающего его лексическую специфику. При расчете проводился

перебор числа кластеров в установленном диапазоне. Критерием качества разбиения выступал средний силуэтный коэффициент, отражающий степень различимости и компактности полученных кластеров. На рисунке ниже представлена зависимость среднего силуэтного коэффициента от числа кластеров.

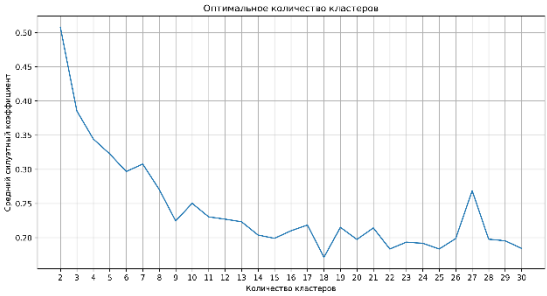



Рис. 5 Зависимость среднего силуэтного коэффициента от количества кластеров наименований СМР

Использование только внутренней метрики, такой как силуэтный коэффициент, для определения оптимального числа кластеров не позволяет объективно оценить соответствие кластеризации реальной предметной структуре. Максимальное значение силуэтного коэффициента при двух кластерах отражает лишь высокую компактность и разделимость на этом уровне агрегации, но не учитывает многообразие и специфику классов, актуальных для строительной отрасли, где количество классов существенно больше в зависимости от применяемых на производстве классификаторов.

В ходе исследования проведён комплексный анализ наименований строительно-монтажных работ и выявлены ограничения традиционных статистических методов классификации из-за высокой разреженности и уникальности текстовых данных. Проведенный анализ подтвердил гипотезу, что подходы к поиску классов работ по их наименованиям на основе простых статистических методов или строгих правил классификации неустойчивы. Для решения задачи автоматической классификации СМР по их наименованиям действительно требуются методы машинного обучения, способные учитывать семантические и контекстуальные особенности текста.

Метод опорных векторов (SVM) применим к высокоразмерным данным, такими как текстовые векторы. Он устойчив к переобучению и способен работать с большим числом признаков, что важно при разреженных текстовых данных. Градиентный бустинг способен

учитывать сложные нелинейные зависимости и взаимодействия признаков, что полезно при неоднородных наименованиях СМР. Логистическая регрессия работает с векторизованными текстами, однако, требуется использовать регуляризацию для предотвращения переобучение.

Большие языковые модели на базе трансформеров демонстрируют высокую эффективность в обработке разреженных и неоднородных текстовых данных, обеспечивая качественное выделение признаков и адаптацию к специфике строительной терминологии. Малые языковые модели представляют собой оптимальный компромисс между производительностью и ресурсными затратами, что позволяет использовать их в практических приложениях для классификации строительной информации.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. "Национальный стандарт российской федерации система проектной документации для строительства основные требования к проектной и рабочей документации" от 03.06.2020 ГОСТ Р 21.101-2020 // Официальный интернет-портал правовой информации. - 01.01.2021

2. Постановление Правительства РФ "О составе разделов проектной документации и требованиях к их содержанию" от 28.12.2024 № 87 // Официальный интернет-портал правовой информации. - 01.01.2025

3. Kereshmeh A.M. Eastman C. A Comparison of Construction Classification Systems Used for Classifying Building Product Models // 52nd ASC Annual International Conference Proceedings. - 2016

4. Каракозова И.В. Исследование универсальной последовательности строительных работ // Вестник МГСУ. 2020. Т. 15. Вып. 9. С. 1321–1333.

5. Киевский И. Л., Аргунов С. В., Жаров Я. В., Юргайтис А. Ю. Алгоритмизация систем планирования, управления и обработки информации в строительстве // Промышленное и гражданское строительство. 2022. № 11. С. 14-24.

6. Moon S., Lee G.., Chi S. и др. Automated Construction Specification Review with Named Entity Recognition Using Natural Language Processing // Journal of Construction Engineering and Management. - 2021. - №1.

7. Коньков В. В., Широков В.И., Жабицкий М.Г. Прогнозирование срывов сроков строительства с использованием машинного обучения на основе исторических данных о фактической продолжительности завершенных проектов // International Journal of

Open Information Technologies. - 2024. - №8. - С. 35-46.

8. Автоматическая обработка текстов на естественном языке и анализ данных: учеб. пособие / Большакова Е.И., Воронцов К.В., Ефремова Н.Э., Клышинский Э.С., Лукашевич Н.В., Сапин А.С. — М.: Изд-во НИУ ВШЭ, 2017. — 269 с.

9. Кузьмина Е. С., Горюнов Д. А. Методы анализа текстовых данных с использованием машинного обучения // Экономика и социум. 2024. №7 (122)

10. Отраднов К.К., Жуков Д.О., Новикова О.А. Модель кластеризации слабоструктурированных текстовых данных // Современные информационные технологии и ИТ-образование. - 2017. - №3. - С. 100-115.

***УДК 625.9***

***Сиденко И.Э.***
***Научный руководитель: Дуганова Е.В., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ

Идея интеграции физических объектов и устройств с сетевым пространством находит ключевое выражение в подходах «Интернета вещей» (IoT), который способствует существенным преобразованиям в технических и организационных аспектах многих промышленных комплексов. Уже сегодня создание “умных” транспортных экосистем, основанных на IoT, предоставляет возможность не только детализировано отслеживать перемещение транспортных средств, но и осуществлять прогнозирование их путей следования, собирая и анализируя данные о потенциальных транспортных потоках и пробках.

На первоначальном этапе термин «Интернет вещей» был введён для подчеркивания единой системы идентификации объектов, связанных посредством радиочастотной идентификации RFID, однако со временем концепция охватила гораздо более широкий спектр интеграции цифровых и физических компонентов — включая работу с многочисленными видами сенсоров, исполнительными механизмами, GPS-технологиями и мобильными устройствами. Современная трактовка IoT подразумевает гибкую, постоянно эволюционирующую инфраструктуру мирового масштаба, обладающую потенциалом самонастройки, поддержкой принятых коммуникационных протоколов, и способную обеспечивать уникальную идентификацию как реальных,

так и виртуальных вещей, которые взаимодействуют через интеллектуальные интерфейсы и органично включаются в единую цифровую коммуникационную ткань.

Базовыми компонентами для такой взаимосвязанной среды выступают координация датчиков, RFID-меток и коммуникационных платформ — это обеспечивает возможность создания единого информационного поля, где окружающие нас предметы получают возможность как обмениваться сведениями между собой, так и синхронизировать свои действия, образуя функционально взаимозависимые системы, служащие для эффективного достижения поставленных задач.

В последние годы растущий интерес к интеграции IoT-технологий наблюдается во множестве сфер промышленной деятельности. Реальные кейсы внедрения концепций промышленного «Интернета вещей» представлены в различных секторах, включая мониторинг состояния окружающей среды, современные решения для сельскохозяйственного производства, пищевую промышленность, системы видеонаблюдения и прочие области. Одновременно с этим складывается стремительная тенденция к увеличению количества научных трудов, посвящённых тематике «Интернета вещей». С целью системного осмысления современного состояния и исследовательских перспектив индустриального IoT специалисты осуществили обобщённый библиометрический анализ профильных публикаций, опираясь на материалы пяти авторитетных электронных научных ресурсов: IEEE Xplore, Web of Knowledge, ACM Digital Library, INSPEC и ScienceDirect.

Теоретические основы и направления современных исследований IoT демонстрируют расширение горизонтов понимания гетерогенных сетей, в которых множество устройств интегрируются в единую инфраструктуру на основе сенсорных, коммуникационных и информационных технологий. Ключевая технологическая составляющая IoT-контекстов — RFID — базируется на применении микросхем для передачи идентификационных данных считывающим устройствам посредством беспроводных каналов. Идентификация и отслеживание объектов, оборудованных RFID-метками, осуществляется автоматически, благодаря чему упрощается мониторинг потоков и управление активами в различных областях деятельности. С момента широкого внедрения в 1980-х годах, RFID-технологии стали неотъемлемой частью логистических систем, сферы фармацевтики, управления цепями поставок и розничной торговли.

Помимо RFID, необходимо отметить настойчивое развитие

беспроводных сенсорных сетей (WSN), которые представляют собой распределённые системы, состоящие из кооперативно функционирующих интеллектуальных сенсоров, способных к коллективному сбору и обработке информации. Эти решения нашли широкое применение для реализации задач по контролю производственных процессов, медицинскому мониторингу, управлению дорожным трафиком, а также сбору экологических данных.

Значимую роль в становлении концепции «Интернета вещей» сыграли современные достижения в области RFID и WSN, однако широкое распространение IoT также обусловлено интеграцией разнообразных решений: от традиционных штрихкодов и облачных вычислений до социальных платформ и смарт-устройств, которые на практике формируют разветвлённую инфраструктуру поддержки IoT-среды. Активное внедрение беспроводной связи, инновационных сенсоров и мобильных телефонов становится движущей силой вовлечения всё большего числа интеллектуальных объектов в экосистему IoT, что отражается на смежных секторах новых информационных и коммуникационных технологий, а также на корпоративных ИТ-системах.

В наши дни заметный всплеск интереса к технологиям «Интернета вещей» фиксируется в транспортно-логистических процессах, торговых сетях, промышленности и даже в сфере фармацевтики. Расширение сетей взаимосвязанных устройств предполагает необходимость формирования строгого набора технических правил, спецификаций и нормативов, определяющих алгоритмы взаимодействия, обработки и обмена данными, чтобы гарантировать пользователям надёжный уровень сервиса. Безусловным условием успеха глобального внедрения IoT становится стандартизация, направленная на достижение совместимости, функциональной устойчивости, беспрепятственной интеграции и надежной работы, открывающих путь к масштабируемому применению технологий по всему миру.

Экономический потенциал подобных инициатив привёл к тому, что крупнейшие мировые и национальные институты – такие, как Международный телекоммуникационный союз, Международная электротехническая комиссия, Международная организация по стандартизации, Институт инженеров электротехники и электроники, Европейский Комитет по электротехнической стандартизации, Китайский институт по электронным стандартам и Американский национальный институт стандартов – активно занимаются разработкой и синхронизацией стандартов для IoT, уделяя особое внимание консолидации региональных и нацональных норм в международном

контексте. Принятие единых стандартов создаёт перспективы для устойчивого повышения масштабов потребления и разработки IoT-приложений при оптимизации издержек эксплуатации и поддержки на длительный срок, одновременно ускоряя цикл массового внедрения новых интеллектуальных технологий.

Направление IoT Развертывание инфраструктуры «Интернета вещей» предполагается осуществлять последовательно, осуществляя модернизацию и интеграцию имеющихся идентификационных решений, к примеру, RFID. Однако для преодоления возникающих сложностей требуется комплексный подход с акцентом на глобальное взаимодействие, а также на обеспечение широкого межгосударственного партнерства и стратегического видения системных процессов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Андреев Ю.С, Третьяков С.Д Промышленный Интернет Вещей. Санкт-Петербург: Изд-во университет ИТОМ, 2019. 54с.

2. Дуганова Е.В., Загородний Н.А., Кравченко А.А., Щетинин Н.А. Производственно-техническая инфраструктура предприятий автомобильного транспорта. Белгород: Изд-во БГТУ им. В.Г. Шухова, 2023. 123 с.

3. Макаров С.Л Arduino Uno и Raspberry Pi 3: схемотехники интернету вещей. М.: ДМК Пресс, 2018. 204с.

4. “СИБУР” Что такое промышленный интернет вещей и зачем он нужен на производствах [Электронный ресурс]. Систем.требования: ЯндексБраузер. URL:https://www.techinsider.ru (Дата обращения 11.5.25)

5. Кранц Мачей, Интернет вещей: новая технологическая революция. Москва: Эксмо, 2018. 336с.

*УДК 004.658*

***Синев Д.А., Чеботков М.С.***
***Научный руководитель: Измайлов А.М., канд. экон. наук, доц.***
*Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия*

# РОЛЬ БИЗНЕС-АНАЛИТИКИ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА

Актуальность данного исследования обусловлена повсеместным внедрением цифровых технологий в бизнес-практику. В современных рыночных условиях это стало обязательным требованием для сохранения конкурентоспособности хозяйствующих субъектов. При этом цифровизация внедряется как в производственные процессы, так и в аналитическую работу, так как отсутствие эффективных систем анализа данных неизбежно приводит к отставанию от более технологически оснащенных конкурентов.

Современные экономические условия диктуют необходимость цифровой трансформации для всех участников рынка: государства, производителя, продавца, потребителя. Основным участником и инициатором цифровой трансформации являются государство и коммерческие организации. Успешными государственными цифровыми проектами стали Госуслуги и личный кабинет налогоплательщика ФНС РФ [1].

Коммерческие структуры выбирают путь цифровой трансформации с целью сохранения конкурентных преимуществ, увеличения доли рынка. В условиях стремительного развития цифровой экономики предприятия, не адаптирующиеся к новым технологическим реалиям, постепенно будут терять конкурентные преимущества [2]. Особенно это касается крупного и среднего бизнеса, в то время как малое предпринимательство не так сильно зависит от цифровизации всех процессов своей деятельности. Для коммерческого сектора этот процесс предполагает глубокую интеграцию цифровых технологий во все сферы деятельности организации, что приводит к кардинальному изменению как внутренних операционных процессов, так и внешних взаимодействий.

Следует подчеркнуть, что цифровая трансформация представляет собой не просто техническую модернизацию, а комплексное преобразование всех аспектов деятельности компании, включая:

- реорганизацию бизнес-процессов;
- изменение корпоративной культуры;

– трансформацию моделей взаимодействия с потребителями [3].

Цифровая трансформация в коммерческой организации направлена на следующие важные аспекты деятельности хозяйствующего субъекта (представлены на рисунке 1).

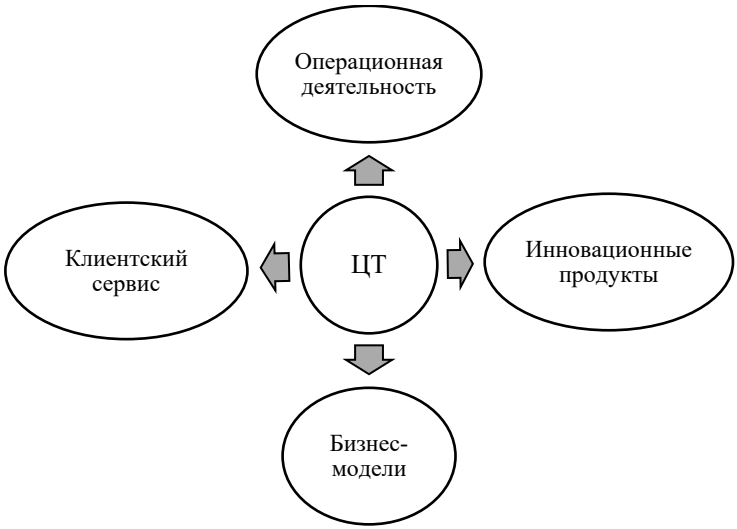



Рис.1 Направления цифровизация в деятельности предприятия

Рассмотрим каждый из аспектов.

Совершенствование операционной деятельности возможно через автоматизацию процессов, внедрение ERP-систем и использование аналитических инструментов. Это позволит повысить производительность, равномерно распределить обязанности между сотрудниками, повысить уровень аналитических исследований.

Повышение качества клиентского сервиса может быть реализовано путем персонализации предложений клиентам, внедрения CRM-систем и анализа потребительского поведения.

Применение цифровых технологий позволяет создавать инновационные продукты и услуги [4].

Переход на платформенные решения и сервисные модели позволяет обеспечивать модернизацию бизнес-моделей.

Однако следует иметь в виду, что цифровая трансформация требует от организаций определенных затрат, а также организационных изменений, которые касаются в первую очередь структуры производственных процессов и нового инструментария для их

реализации и оценки. Особое значение при этом занимает бизнес-аналитика.

Бизнес-аналитику можно определить как систему методов и инструментов, предназначенных для обработки корпоративных данных, извлечения из них полезной информации и поддержки принятия управленческих решений. Ее основная функция заключается в обеспечении рационального выбора стратегических и тактических решений на основе достоверных данных, что позволяет эффективно управлять организационными изменениями [5].

Функциональные возможности бизнес-аналитики в процессе цифровой трансформации проявляются в следующих аспектах:

– выявление слабых мест в текущих процессах и исходя из этого определение возможностей для улучшения;

– разработка стратегических планов преобразований с определением KPI;

– анализ потребительского поведения для повышения лояльности уже имеющихся клиентов и привлечения новых потребителей;

– обеспечение достоверной информационной базой для принятия управленческих решений;

– повышение адаптивности компании к рыночным изменениям [6].

Практическая реализация цифровой трансформации требует применения различных аналитических инструментов, среди которых популярными являются следующие:

– BI-системы (Power BI, Tableau) для визуализации данных;

– Методы Data Mining для выявления скрытых закономерностей;

– Predictive Analytics для прогнозирования тенденций;

– Big Data технологии для обработки больших массивов информации;

– Process Mining для анализа бизнес-процессов;

– CRM-системы для управления клиентскими отношениями.

Ярким примером успешной реализации является опыт Альфа-Банка, где внедрение автоматизированной системы кредитования на основе технологий искусственного интеллекта позволило:

– сократить время обработки заявок с нескольких месяцев до 90 секунд;

– увеличить долю автоматизированных кредитных решений до 24%;

– охватить 63% клиентской базы персонализированными предложениями;

– существенно снизить отток клиентов [7].

Этот пример наглядно демонстрирует, как грамотное применение бизнес-аналитики позволяет не только улучшить клиентский опыт, но и значительно повысить операционную эффективность бизнеса [8]. Таким образом, бизнес-аналитика является ключевым элементом успешной цифровой трансформации, обеспечивая обоснованность управленческих решений, оптимизацию бизнес-процессов, повышение качества клиентского сервиса, создание инновационных продуктов. Компании, эффективно использующие инструменты бизнес-аналитики, получают существенные конкурентные преимущества в условиях цифровой экономики.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Портал государственных услуг Российской Федерации // Госуслуги. – URL: https://www.gosuslugi.ru (дата обращения: 15.05.2025).

2. Гранкина, С. В. Воздействие цифровых решений на устойчивый экономический рост промышленного предприятия / С. В. Гранкина, С. А. Серегин // Экономика и предпринимательство. – 2023. – № 9 (158). – С. 905–908.

3. Измайлов, А. М. Механизм управления информационно-знаниевыми ресурсами / А. М. Измайлов, С. И. Ашмарина // Вестник Воронежского государственного университета инженерных технологий. – 2016. – № 1 (67). – С. 261–266.

4. Джулай, Д. В. Основные направления инновационной деятельности в Самарской области / Д. В. Джулай, А. М. Измайлов // Тенденции развития современного общества: экономико-правовой аспект: сб. науч. тр. междунар. науч.-практ. конф. (Пенза, 14–15 ноября 2016 г.). – Пенза: Пензенский гос. технол. ун-т, 2016. – С. 26–28.

5. Что такое бизнес-аналитика? // SAP. – URL: https://www.sap.com (дата обращения: 15.05.2025).

6. Полковникова, В. Д. Современные системы бизнес-аналитики в управлении организацией / В. Д. Полковникова, А. М. Измайлов, А. Ю. Киндаев // Современные информационные технологии. – 2023. – № 38 (38). – С. 77–80.

7. Кейс Альфа-Банка на Премию FINNEXT: кредитование по онлайн-триггерам // Future Banking. – URL: https://futurebanking.ru (дата обращения: 15.05.2025).

8. Ashmarina S. I. Gaps in the system of higher education in Russia in terms of digitalization / S. I. Ashmarina, E. A. Kandrashina, A. M. Izmailov,

N. G. Mirzayev // Advances in Intelligent Systems and Computing. — 2020. — Vol. 908. — P. 437—443. — DOI: 10.1007/978-3-030-11367-4_43.

***УДК 681.518.25***

***Скуридина Д.И., Кобзева Н.Р., Гольцова М.Ю.***
***Научный руководитель: Гольцов Ю.А., канд. техн. наук, доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ИСПОЛЬЗОВАНИЕ ПРЕДИКАТИВНОЙ АНАЛИТИКИ В СИСТЕМАХ МОНИТОРИНГА ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ

Современные производственные предприятия в условиях жесткой конкуренции и стремительного развития технологий сталкиваются с рядом проблем, связанных с эффективностью эксплуатации технологического оборудования. Способность автоматизированной системы своевременно реагировать на изменения в работе оборудования и предсказывать потенциальные неисправности является важнейшим фактором для поддержания высоких производственных показателей и снижения затрат.

В металлообрабатывающей промышленности большим спросом пользуются токарные станки, которые подвержены различным видам износа и поломок, что может привести к значительным экономическим потерям и снижению качества продукции. Однако стандартные методы профилактического технического обслуживания, такие как регулярная проверка инженерами или работа до отказа, являются трудоемким и неэффективным. Это подчеркивает необходимость замены человеческого труда удаленным мониторингом неисправностей оборудования, который повышает точность диагностики и позволяет избежать долгосрочного простоя, за счет внедрение в производственные процессы систем, способных предсказывать возможные отказы заранее. По данным исследований, незапланированные простои оборудования могут составлять до 25-30% экономических затрат в машиностроении, а своевременное выявление отказов позволяет сократить эти потери на 15-40% [3].

Одним из перспективных подходов для достижения этих целей является разработка автоматизированной системы мониторинга технологического оборудования, основанной на методах предикативной аналитики. Использование предикативной аналитики, как одной из направлений анализа данных, позволяет не только

отслеживать состояние оборудования в режиме реального времени, но и прогнозировать их возникновение на основе исторических данных и алгоритмов машинного обучения [2].

В отличие от нынешних методов исследования применяется подход, предполагающий использование моделей, которые не требуют глубокого понимания внутренних механизмов их работы, но эффективно обрабатывают входные данные для получения прогнозов. Использование этого метода снижает требования к знаниям и навыкам технического персонала, что упрощает процесс внедрения системы в существующие производственные процессы и делает ее доступной для более широкого круга пользователей. В контексте мониторинга токарных станков это означает возможность анализировать данные от различных датчиков (температуры, скорости вращения, крутящего момента) без необходимости детального понимания физических процессов, происходящих внутри оборудования [1].

Традиционные методы мониторинга, такие как линейная регрессия или пороговые алгоритмы, ограничены в способности учитывать нелинейные взаимодействия параметров и часто не справляются с выявлением предшествующих сбоям. Применение метода машинного обучения, основанного на использовании искусственных нейронных сетей, открывает возможности для обнаружения предаварийных состояний [5-6].

Основа структуры любой нейронной сети формируется, как система взаимосвязанных между собой узлов, организованных в слои, напоминающие подобие человеческому мозгу. В искусственных интеллектуальных системах нейроны представлены простыми процессорами, объединенными в единую сеть, способную обрабатывать сложные задачи. Особенность нейронных сетей по сравнению с другими алгоритмами машинного обучения заключается в способности к самообучению. Это объясняется наличием у каждого нейрона индивидуального весового коэффициента, определяющего его влияние на взаимодействие с другими элементами сети [6].

В рамках разработки автоматизированной системы мониторинга технологического оборудования будет использоваться полно связная нейронная сеть типа MLP (Multilayer Perceptron). Архитектура такой сети включает входной, скрытые и выходные слои, что обеспечивает эффективное моделирование сложных взаимосвязей между исходными данными и целевыми переменными. MLP становится мощным инструментом для прогнозирования состояния оборудования и своевременного обнаружения возможных сбоев, благодаря своей способности к обучению на накопленных данных [7-8].

Обучение нейронной сети базируется на подборе оптимальных весовых коэффициентов с применением метода обратного распространения ошибки, что повышает точность прогнозов.

Для решения задачи мониторинга технологического оборудования с использованием предиктивной аналитики был разработан программный код на языке Python, который реализует систему предсказания отказов технологического оборудования на основе полно связной нейронной сети MLP.

На начальном этапе необходимо собрать данные о работе оборудования, его состоянии и возможных сбоях, включая такие параметры, как температура воздуха и процесса, скорость вращения, крутящий момент, износ инструмента, бинарные индикаторы типов отказов, а также провести первичный анализ для выявления закономерностей и аномалий. Здесь важно установить целевую переменную (например, состояние оборудования: «нормально», «предаварийное», «аварийное») [4]. Одним из инструментов анализа данных, предшествующий обучению моделей, является тепловая корреляционная матрица, которая показывает взаимосвязь переменных и факторы их влияния на прогнозирование. Тепловая карта корреляции помогает понять физические взаимосвязи в работе станка (рис.1).

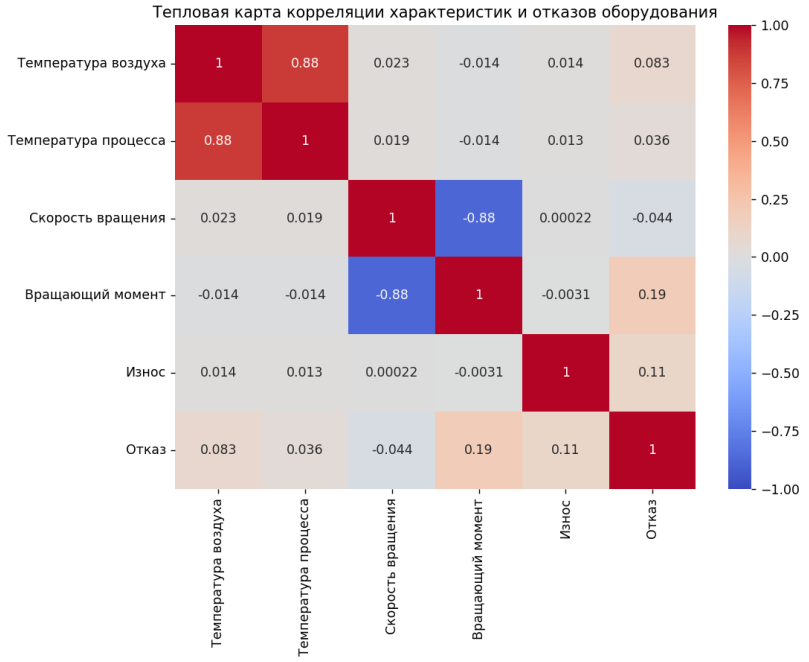



Рис. 1. Тепловая карта корреляции

Например, высокая отрицательная корреляция между скоростью вращения и износом инструмента может указывать на то, что увеличение скорости ускоряет износ. Для последующей оценки качества моделей данные делятся на обучающую (70%) и тестовую (30%) выборки.

Далее осуществляется выбор и обучение модели. Определяем какие алгоритмы машинного обучения лучше всего подходят для решения этой задачи с учетом структуры данных и требований к точности (например, случайные леса, градиентный бустинг, дерево решений). Комбинирование статистических методов и алгоритмов машинного обучения с использованием специализированных инструментов предиктивной аналитики позволяет не только предсказывать, но и визуализировать данные. Для обоснования эффективности системы проводится сравнительный анализ производительности нейросети MLP с классическими методами машинного обучения [6].

Затем проводится оценка модели на тестовой выборке с

использованием метрик, таких как точность, точность предсказаний, полнота, F1-мера и средняя оценка кросс-валидации. Также для оценки качества модели классификации используется матрица ошибок, которая показывает соответствие между фактическими и предсказанными значениями целевой переменной.

Нейронная сеть демонстрирует сопоставимую или превосходящую производительность при достаточном объеме данных, а её способность к обучению на сложных данных делает её более адаптивной к реальным условиям эксплуатации.

На заключительном этапе создаётся пользовательский интерфейс через SCADA-систему для отображения результатов в виде статусов и рекомендаций о состоянии оборудования при обнаружении предаварийных или аварийных состояний [4].

Реализация предложенной автоматизированной системы мониторинга позволит значительно улучшить эксплуатационные характеристики промышленного оборудования, снизить количество аварийных ситуаций и минимизировать количество незапланированных простои, что в конечном итоге приведет к повышению общей производительности и экономической эффективности предприятия. Результаты работы могут быть полезны для широкого круга пользователей в различных отраслях, где используется технологическое оборудование, что делает её актуальной и востребованной.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Белов Д. В., Кузнецов А. П. Машинное обучение в задачах мониторинга и диагностики оборудования. Москва: Издательство МГТУ им. Н. Э. Баумана, 2020. 256 с.

2. Голубев, А. А. Предиктивная аналитика в промышленности: методы и приложения / А. А. Голубев, А. П. Кузнецов. – Москва: Изд-во МГТУ им. Н. Э. Баумана, 2019. – 320 с.

3. Иванов, А. А. Интеллектуальные системы в промышленности: предикативное обслуживание и цифровизация. Вестник машиностроения. 2021. № 5. с. 45–52.

4. Кижук А.С., Гольцов Ю.А. Анализ технических средств в структуре систем управления и их выбор при проектировании: учебное пособие. – Белгород: Изд-во БГТУ, 2016. – 242с.

5. Корнилов, В. В. Машинное обучение для решения задач классификации и регрессии / В. В. Корнилов, А. В. Смирнов. – Санкт-Петербург: Изд-во СПбГУ, 2020. – 192 с.

6. Сидоров, Д. В. Нейронные сети в задачах прогнозирования

технического состояния машин // Автоматизация и управление в технических системах. – 2022. – № 3. – С. 12 – 19.

7. Типы нейронных сетей. Принцип их работы и сфера применения. [Электронный ресурс]. URL: https://otus.ru (дата обращения: 19.04.2025)

8. Zhusubaliyev Zh.T., Sopuev U.A., Abdirasulov A.Z., Kolomiets E.A., Gol'tsov Yu.A., Tsykanov D. Yu. Border collisions and merging phenomena in the unipolar pulse-width modulated control system // International Scientific Conference on Mechanics, "10th Polyakhov's Reading", September 23 – 27, 2024, St. Petersburg State University. P. 606 – 609.

***УДК 004.94***

***Суслов Д.О.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ЦИФРОВЫЕ ДВОЙНИКИ В СИСТЕМАХ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ

Развитие технологий Интернета вещей, искусственного интеллекта и больших данных способствует цифровизации производства и появлению новых подходов к управлению производственными процессами. Одним из ключевых инструментов цифровой трансформации выступает технология **цифрового двойника** — виртуального представления физического объекта, процесса или системы, синхронизированного с его реальным аналогом в реальном времени.

Цифровые двойники позволяют моделировать, анализировать и оптимизировать производственные процессы, прогнозировать поведение оборудования, минимизировать риски и снижать издержки. Это делает их важным компонентом концепции Индустрии 4.0.

***Понятие цифрового двойника***

**Цифровой двойник** — это программная модель физического объекта, которая получает данные от датчиков, установленных на реальном объекте, и отражает его текущее состояние и поведение. Цифровой двойник может быть построен для отдельного станка, производственной линии, логистического процесса или целого предприятия.

Цифровые двойники могут включать в себя:

- **Геометрическую модель** объекта;
- **Физико-математические модели** поведения;
- **Исторические и текущие данные** от сенсоров;
- **Алгоритмы анализа и прогнозирования** (на основе AI/ML).

***Архитектура цифрового двойника***

Стандартная архитектура цифрового двойника включает следующие компоненты:

1. **Физический объект** — станок, линия, установка.
2. **Система сбора данных** — сенсоры, SCADA, IoT-устройства.
3. **Связь и передача данных** — протоколы OPC UA, MQTT и др.
4. **Цифровая модель** — 3D-модель, симулятор, алгоритмы.
5. **Система анализа** — машинное обучение, цифровая аналитика.
6. **Интерфейс пользователя** — визуализация, управление, отчётность.

***Применение цифровых двойников в производстве***

1. Мониторинг состояния оборудования
Цифровые двойники позволяют отслеживать в реальном времени параметры оборудования, выявлять отклонения и предсказывать потенциальные отказы (predictive maintenance).

2. Оптимизация производственных процессов
Виртуальное моделирование технологических операций помогает находить узкие места, снижать время цикла и повышать производительность.

3. Планирование и диспетчеризация
Цифровые двойники позволяют моделировать сценарии планирования, оценивать последствия изменений и выбирать оптимальные стратегии управления.

4. Поддержка принятия решений
На основе анализа цифрового двойника можно вырабатывать рекомендации для операторов и руководителей, включая автоматизированные решения.

5. Обучение персонала и AR/VR
Использование цифровых двойников в симуляторах позволяет готовить персонал к работе с реальными системами без риска повреждений оборудования.

***Примеры реализации***

Siemens использует цифровые двойники в своей промышленной облачной платформе MindSphere, которая обеспечивает подключение и анализ данных от оборудования в реальном времени. С помощью этой системы можно моделировать работу производственных линий, отслеживать ключевые показатели эффективности (KPI),

прогнозировать неисправности и проводить виртуальное тестирование новых конфигураций производственных процессов без остановки оборудования.

General Electric (GE) активно применяет цифровые двойники в энергетическом и авиационном секторах. Один из примеров — создание цифровых двойников для газовых турбин и авиационных двигателей. Эти модели позволяют проводить прогнозно-предупредительное обслуживание (predictive maintenance): на основе анализа данных о температуре, вибрации и других параметрах система предсказывает возможные неисправности и рекомендует меры по их устранению, что существенно сокращает время простоев и затраты на ремонт.

Bosch реализовала цифровые двойники в логистических процессах на своих производственных площадках. Благодаря цифровому моделированию и интеграции с системами отслеживания грузов и поставок, компания добилась повышения точности поставок, оптимизации маршрутов доставки и более гибкого управления складскими запасами. Это также позволило повысить прозрачность логистических процессов и снизить издержки на хранение и транспортировку.

***Преимущества и вызовы***

Преимущества:

- Увеличение эффективности производства: Цифровые двойники позволяют оптимизировать производственные процессы, выявлять узкие места, моделировать альтернативные сценарии и повышать производительность оборудования.
- Повышение надежности и безопасности: За счёт постоянного мониторинга состояния объектов и прогнозирования отказов снижается риск аварийных ситуаций, обеспечивается безопасная эксплуатация оборудования.
- Уменьшение затрат на обслуживание и ремонт: Переход от реактивного к превентивному обслуживанию позволяет экономить ресурсы и продлевать срок службы оборудования.
- Поддержка устойчивого развития: Более точное управление ресурсами, снижение энергопотребления и отходов способствуют достижению целей устойчивого развития (ESG, зеленое производство).

Вызовы:

- Высокая стоимость внедрения: Разработка цифрового двойника требует инвестиций в оборудование, программное обеспечение, инфраструктуру и обучение персонала.

- Требования к качеству и объему данных: Для построения и корректного функционирования модели необходимы точные и непрерывные данные от сенсоров, что требует надежной системы сбора и хранения данных.
- Интеграция с устаревшими системами (legacy systems): На многих предприятиях до сих пор используются системы автоматизации предыдущих поколений, не поддерживающие современные протоколы связи и стандарты данных.
- Вопросы безопасности и защиты информации: Передача и обработка производственных данных в реальном времени требует высокого уровня кибербезопасности и защиты от внешних угроз.

Цифровые двойники представляют собой один из наиболее перспективных инструментов цифровизации производственной сферы. Их способность объединять физическую и виртуальную реальности обеспечивает принципиально новый уровень управления — более гибкий, точный и предсказуемый. Благодаря цифровым двойникам производственные предприятия могут не только повысить эффективность текущих операций, но и заложить фундамент для внедрения интеллектуальных производств будущего, основанных на принципах Индустрии 4.0. Тем не менее, успешное внедрение требует комплексного подхода: от оценки экономической целесообразности и подготовки инфраструктуры до формирования компетенций персонала и обеспечения безопасности данных. В дальнейшем развитие технологий искусственного интеллекта, машинного обучения и облачных вычислений будет способствовать ещё более широкой и доступной интеграции цифровых двойников в производственные процессы, открывая путь к полностью автономным и самообучающимся системам управления.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.Сорокин А.А. В сборнике: Информационные технологии и технологии коммуникаций. Современные достижения Материалы Четвёртой Международной научной конференции, посвящённой 90-летию со дня основания Астраханского государственного технического университета. Астрахань, 2020. С.78

2. Дворянкин. О. А Osint. perents и нетсталкинг -информационные технологии Интернета / О. А. Дворянкин // Национальная Ассоциация Ученых. – 2022. - №84-2. – С. 6-13.

3. Бочкарёв А.В., Лебедев С.И. "Технологии цифровых двойников в проектировании и эксплуатации производственных систем". Журнал "Техническая кибернетика", 2021, №7. С. 19-25.

4. Коломыцева, Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS

***УДК 004.85. 005.591***

***Суслов Д.О.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ В ПРЕДИКТИВНОЙ АНАЛИТИКЕ НА ПРОИЗВОДСТВЕ

Современное производство сталкивается с необходимостью повышения конкурентоспособности, что требует внедрения интеллектуальных систем анализа данных. Предиктивная аналитика позволяет прогнозировать будущие события и состояния на основе исторических данных. В качестве эффективного инструмента анализа больших объемов данных все чаще применяются искусственные нейронные сети (ИНС), обладающие способностью к обучению и выявлению скрытых закономерностей.

***Предиктивная аналитика и нейросети: теоретические основы***

Предиктивная аналитика представляет собой совокупность методов статистики, машинного обучения и обработки данных, направленных на предсказание вероятных исходов. Нейронные сети — это вычислительные модели, имитирующие работу человеческого мозга, состоящие из взаимосвязанных узлов (нейронов), способных обрабатывать и обучаться на больших массивах данных.

Основные типы нейросетей, применяемых в промышленной аналитике:

- Полносвязные нейронные сети (FNN)
- Сверточные нейронные сети (CNN) — для анализа изображений и сигналов

- Рекуррентные нейронные сети (RNN, LSTM) — для временных рядов
- Автокодировщики и GAN — для аномалий и синтеза данных

***Области применения нейросетей в производстве***

**Предиктивное техническое обслуживание (Predictive Maintenance)**

С помощью нейросетей можно выявлять закономерности в работе оборудования и прогнозировать возможные отказы. Используются временные ряды с датчиков (температура, вибрации, давление и др.), обучается модель LSTM, которая определяет отклонения от нормального поведения.

*Пример:*

На автомобильном заводе внедрена система на базе нейросети, которая предсказывает выход из строя конвейерных двигателей за 7–10 дней до поломки, что снизило время простоя на 25%.

**Контроль качества продукции**

Сверточные нейронные сети применяются для анализа изображений изделий, выявления дефектов и отклонений от стандартов. Это особенно актуально в отраслях с высокой точностью производства: микроэлектроника, фармацевтика, пищевая промышленность.

*Пример:*

На линии по производству пластиковых компонентов нейросеть с точностью 98% определяет микротрещины, которые не обнаруживаются человеком.

**Оптимизация производственных процессов**

Нейросети могут использоваться для построения моделей технологических процессов и прогнозирования выхода продукции в зависимости от входных параметров. Это позволяет оптимизировать режимы работы оборудования и снизить потребление ресурсов.

*Пример:*

В металлургии используется нейросетевая модель, прогнозирующая химический состав сплава на основе температуры, давления и состава исходных материалов, что позволяет уменьшить количество некондиционного продукта.

***Преимущества и ограничения нейросетей***

Преимущества:

- Высокая точность прогнозов
- Возможность работы с неструктурированными данными
- Автоматическое обучение на новых данных

Ограничения:

- Необходимость большого объема обучающих данных
- Сложность интерпретации результатов ("чёрный ящик")
- Высокие вычислительные затраты

***Направления дальнейших исследований***

- Разработка объяснимых моделей (Explainable AI)
- Интеграция нейросетей с системами управления производством (MES, SCADA)
- Создание гибридных моделей с учетом экспертных знаний
- Адаптивные модели, обучающиеся в реальном времени

***Заключение***

Применение нейросетей в предиктивной аналитике на производстве позволяет существенно повысить эффективность работы оборудования, улучшить контроль качества и оптимизировать процессы. Такие технологии помогают снижать издержки, предотвращать поломки и повышать общий уровень автоматизации.

Несмотря на вызовы — необходимость больших объёмов данных, сложность интерпретации моделей и высокие вычислительные затраты — нейросети уже доказали свою практическую ценность и активно внедряются в производственные ИТ-системы.

Перспективы дальнейшего развития включают создание объяснимых моделей, адаптацию под реальное время и интеграцию с существующими цифровыми платформами. Нейросети становятся важной частью цифровой трансформации и играют ключевую роль в переходе к Индустрии 4.0 и 5.0.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева, Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS.

2. Сорокин А.А. В сборнике: Информационные технологии и технологии коммуникаций. Современные достижения Материалы Четвёртой Международной научной конференции, посвящённой 90-летию со дня основания Астраханского государственного технического университета. Астрахань, 2020. С.

3. Шведенко В.Н., Щекочихин О.В., Синкевич Е.А. Научно-техническая информация. Серия 2: Информационные процессы и системы. 2020. №9. С.7-14

4. Иванова А.В., Смирнова Л.Г. "Применение виртуальной и дополненной реальности в профессиональном обучении." Журнал "Педагогика и образование", 2021, №5. С. 45-51.

***УДК 004.8***

***Третьяков Д.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ГЕНЕРАТИВНЫЕ AI В АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ

Искусственный интеллект давно перестал быть фантастической идеей и всё увереннее входит в нашу повседневную жизнь, особенно в сферу бизнеса. Сегодня решения на основе генеративных моделей, таких как ChatGPT, Stable Diffusion и им подобные, выступают не просто инструментами, а полноценными участниками рабочих процессов. Они освобождают людей от рутинных операций, ускоряют создание текстов и изображений, а также помогают в программировании — задачи, на которые раньше требовались часы и даже дни.

Для компании внедрение таких систем означает не только экономию времени и ресурсов, но и повышение качества услуг, а также возможность глубже персонализировать предложения для клиентов. В данной статье рассмотрим, как именно генеративный ИИ находит применение в бизнесе, какие задачи он решает и с какими трудностями можно столкнуться при его интеграции.

**Технологии генеративного AI**

Генеративные модели строятся на нейросетевых архитектурах и большом объёме данных: за счёт анализа примеров они учатся выявлять закономерности и порождать новый контент. Наиболее востребованные области их применения:

- НЛП и обработка текста. Модели вроде ChatGPT, Gemini и других способны генерировать тексты, резюмировать данные, проводить семантический анализ и поддерживать осмысленные диалоги.

- Генерация изображений. Инструменты Stable Diffusion, MidJourney, DALL·E переводят текстовые подсказки в визуальный контент, что особенно актуально для маркетинга и дизайна.
- Автоматизация программирования. Сервисы на базе Codex и GitHub Copilot пишут код, исправляют ошибки и предлагают оптимизации, снижая нагрузку на разработчиков.

Со временем модели становятся точнее и надёжнее, а их потенциал — всё шире.

**Примеры использования в бизнесе**

- Автоматическое создание контента: генеративные системы умеют быстро формировать рекламные объявления, SEO-статьи, публикации для социальных сетей и даже сценарии видеороликов, минимизируя согласование и снижая временные затраты.
- Интеллектуальные чат-боты и виртуальные ассистенты: такие решения обрабатывают входящие запросы круглосуточно, отвечают на популярные вопросы, проводят первичную диагностику проблем и перенаправляют сложные кейсы специализированным сотрудникам.
- Аналитика и прогнозирование: благодаря способности обрабатывать терабайты данных, ИИ-модели выявляют скрытые закономерности, строят прогнозы спроса, оптимизируют запасы и помогают планировать маркетинговые активности на основе реальных тенденций.
- Автоматизация документооборота: на основе шаблонов и правил ИИ создаёт проекты договоров, отчётов и актов, проверяет их на соответствие нормативам и стандартам, существенно ускоряя юридические и административные процедуры.

**Преимущества и вызовы**

Преимущества:

1. Скорость и эффективность. ИИ выполняет рутинные операции за доли времени, которые людям требовались бы часы и даже дни.
2. Снижение затрат. Автоматизация уменьшает расходы на выполнение однотипных задач и нагрузку на персонал.
3. Шкала и гибкость. Модели легко масштабируются под возрастающие объёмы данных и запросов, а также адаптируются к новым задачам.
4. Глубокий анализ. Генеративный ИИ выявляет скрытые паттерны в больших массивах информации, что помогает принимать более обоснованные решения.
5. Персонализация. Благодаря учёту характеристик клиентов ИИ создаёт более релевантные и таргетированные предложения.

Вызовы:

1. Вероятность ошибок. Модель может генерировать неточные или противоречивые данные, если столкнётся с недостаточной или неполной информацией.

2. Нужда в контроле. Для обеспечения корректности результатов необходим надзор специалистов и регулярная проверка выданного контента.

3. Правовые вопросы. Вопросы авторских прав и распределения ответственности за созданный ИИ контент остаются предметом дискуссий.

4. Зависимость от инфраструктуры. Высокие требования к качеству данных, вычислительным ресурсам и стабильности систем могут стать барьером для внедрения.

5. Поставщик и переносимость. Привязка к конкретному вендору ИИ решения усложняет миграцию на альтернативные платформы.

**Преобразование взаимодействия людей и бизнеса**

Генеративный ИИ меняет не только внутренние процессы компаний, но и их коммуникацию с клиентами и сотрудниками.

1. Сервис 24/7. Благодаря чат-ботам и автоматизированным системам компании отвечают на запросы круглосуточно, повышая удовлетворённость клиентов.

2. Оптимизация внутренних коммуникаций. ИИ помогает анализировать рабочие процессы, измерять вовлечённость сотрудников и предлагать способы повышения эффективности.

3. Инструмент для креатива. Генеративные модели поддерживают творчество маркетологов и дизайнеров, подсказывая идеи и создавая первые прототипы рекламных концепций.

**Заключение**

Генеративные модели искусственного интеллекта продолжают активно проникать в бизнес, автоматизируя задачи от рутинного ввода данных до сложного творческого процесса. Они позволяют компаниям работать быстрее, более гибко и экономичнее. Вместе с тем внедрение ИИ требует осознанного подхода: необходимо учитывать юридические и этические аспекты, а также поддерживать контроль качества создаваемого контента.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коршак, К. С. Инновации в области искусственного интеллекта: влияние на автоматизацию производственных процессов / К. С. Коршак, Д. Д. Отрешко, Д. А. Давыдов // Междисциплинарный дискурс. Диалог

поколений. – Уфа : Общество с ограниченной ответственностью "Аэтерна", 2024. – С. 50-52. – EDN ODHAZD.

2. Городнова Н. В. Применение искусственного интеллекта в бизнес-сфере: современное состояние и перспективы / Н. В. Городнова // Вопросы инновационной экономики. 2021. № 4. С. 73–93. – EDN MGHEPK.

3. Архипова Л. И. Большие данные и искусственный интеллект в бизнесе: развитие и регулирование / Л. И. Архипова // Big Data and Advanced Analytics. — 2020. — № 6-3. — С. 122-127. – EDN OASXQI.

***УДК 004.056.5***

***Третьяков Д.С.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ

В эпоху цифровизации, когда кибератаки становятся всё более сложными и масштабными, традиционные методы управления рисками информационной безопасности (ИБ) уже не справляются с вызовами времени. Всё больше организаций обращаются к технологиям машинного обучения (ML) как к мощному инструменту выявления, оценки и минимизации угроз. В этой статье рассмотрим, как машинное обучение трансформирует подходы к управлению рисками ИБ.

**Что такое управление рисками информационной безопасности?**

Управление рисками ИБ — это процесс идентификации, анализа, оценки и минимизации рисков, связанных с нарушением конфиденциальности, целостности и доступности информации. Этот процесс включает в себя:

- Оценку уязвимостей систем.
- Мониторинг угроз и инцидентов.
- Прогнозирование потенциального ущерба.
- Выбор и реализацию мер защиты.

**Подготовка данных для ML-моделей**

Перед обучением моделей необходимо:

1. Сбор и агрегация журналов событий, сетевого трафика, данных об уязвимостях.
2. Очистка и нормализация: удаление шумовых записей,

приведение метрик к единым шкалам.

3. Формирование признаков (feature engineering): создание транзакционных, поведенческих и контекстных признаков.

4. Разметка данных: метки классов (нормальное / аномальное поведение, типы инцидентов).

**Роль машинного обучения в управлении рисками**

Машинное обучение позволяет автоматизировать и интеллектуализировать процессы анализа данных, обнаружения аномалий и предсказания инцидентов. Это особенно актуально в условиях огромного объёма данных, поступающих в системы мониторинга безопасности.

1. Обнаружение аномалий

ML-модели могут обучаться на исторических данных нормального поведения системы и выявлять отклонения, которые могут свидетельствовать о кибератаках, внутренних нарушениях или сбоях.

*Пример:* Алгоритмы кластеризации и нейронные сети могут обнаруживать нетипичную активность пользователей или нестандартный трафик, свидетельствующий о вторжении.

2. Предиктивный анализ угроз

Машинное обучение способно предсказывать вероятность возникновения инцидентов на основе поведения пользователей, системных журналов и внешних факторов.

*Пример:* ML может анализировать поведение инсайдеров, чтобы прогнозировать вероятность утечки информации.

3. Классификация инцидентов

ML-классификаторы (например, решающие деревья, случайный лес, SVM) помогают автоматически классифицировать типы инцидентов безопасности и приоритизировать их обработку.

4. Управление уязвимостями

Системы на основе ML могут автоматически оценивать критичность уязвимостей, учитывая контекст инфраструктуры и исторические данные об эксплуатации аналогичных уязвимостей в прошлом.

**Практические примеры**

- Защита периметра сети: платформа на базе автоэнкодера обнаруживает DDoS-потоки, реагируя в реальном времени.
- Внутренний контроль: ML-система предсказывает риск утечки данных инсайдерами, анализируя активность сотрудников.
- Автоматизация SOC: классификатор приоритизирует инциденты по степени критичности, сокращая время реагирования на 30%.

**Основные этапы внедрения**

- Оценка зрелости данных и инфраструктуры.
- Выбор алгоритма и среды разработки (TensorFlow, PyTorch, Scikit-learn).
- Интеграция моделей в SIEM/EDR-системы.
- Тестирование в режиме песочницы и оценка точности.
- Обучение персонала и оформление процедур реагирования.

**Преимущества использования ML в управлении рисками**

- Автоматизация рутинных процессов.
- Повышение точности обнаружения угроз.
- Снижение времени реагирования на инциденты.
- Адаптивность к новым видам атак.

**Ограничения и вызовы**

- Несмотря на перспективность, использование машинного обучения в ИБ сталкивается с рядом вызовов:
- Необходимость большого объёма качественных данных.
- Риск ложных срабатываний (false positives).
- Угрозы для самих ML-моделей (например, adversarial attacks).
- Необходимость интерпретируемости решений.

**Заключение**

Машинное обучение открывает новые горизонты в управлении рисками информационной безопасности, обеспечивая проактивную защиту, высокую адаптивность и автоматизацию процессов. Однако для эффективного использования ML необходимо учитывать как технические, так и организационные аспекты, включая подготовку данных, настройку моделей и интеграцию с существующими системами безопасности.

Будущее кибербезопасности — за интеллектуальными системами, способными учиться, адаптироваться и защищать данные быстрее, чем развиваются угрозы.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS.

2. Комплексная защита информации в организации / М. М. Тараскин, А. Г. Захарова, Ю. И. Коваленко, Г. И. Москвитин. – Москва : Русайнс, 2017. – 354 с. – EDN YJYWMX.

3. Машинное обучение в информационной безопасности. — Текст : электронный // kaspersky : [сайт]. — URL: https://www.kaspersky.ru (дата обращения: 20.05.2025).

***УДК 621.039.58:004.8***

***Трибелев А.А.***
*Национальный исследовательский ядерный университет,*
*г. Москва, Россия*

## РЕЗУЛЬТАТЫ ВЕРИФИКАЦИИ ПРИМЕНИМОСТИ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРЕМЕНЕНИЯ В РАСЧЕТАХ ВЕРОЯТНОСТНОГО АНАЛИЗА БЕЗОПАСНОСТИ АЭС 3 УРОВНЯ

Современное обоснование безопасности АЭС строится на вероятностном подходе, описанном в [1]. Этот подход включает в себя построение вероятностных моделей функционирования систем, вероятностей отказов, моделей безопасностей для оценки рисков и их последствий. При этом обоснование безопасности с применением вероятностного подхода включает в себя верификацию и валидацию моделей, а также построение вероятностных границ безопасности, что обеспечивает достоверность и обоснованность принимаемых решений [2].

ВАБ является основной методологией вероятностного подхода к обоснованию безопасности АЭС [3]. Реализация методологии ВАБ для АЭС сталкивается с рядом ограничений, такими как консерватизм традиционных подходов, недостаточная полнота данных по редким аварийным событиям, ресурсные ограничения, в частности отмеченные в [4, 5, 6], что ограничивает реализованные модели. При этом

Применение методов AI может помочь преодолеть эти ограничения, улучшая качество анализа данных и моделирования сложных зависимостей, что, в свою очередь, повышает достоверность оценки безопасности АЭС. В исследовательской работе проводится верификация модели, основанной на гипотезе, описанной в [6] о применении технологии AI для работы в области ВАБ в части расчета ВАБ 3 уровня.

**Методы исследования**

Любое применение программных средств в области атомной

энергетики должно пройти процедуру верификации. Исследование основывается на определении подходов к верификации и непосредственно проверки работоспособности моделей AI. Проверки гипотезы осуществляться проведением серии расчетов с кросс-верификацией.

**Модель ВАБ**

Модель определена на основе [7]. Модель содержит 4 уровня. Уровень 0 определен на основе [3, 7]. Уровень 1 определен на основе [3, 8]. Уровень [3, 9] определен на основе [3, 9]. Проверяемые граничные условия определены на основе [8, 9].

На текущем уровне абстракции требуется проверка работоспособности модели для ВАБ уровня 3. Были определены следующие ограничения: базовой конфигурации АЭС ВАБ уровня 0 принималась как статичная. Моделирование расчетов сценариев не будет проводиться в явном виде, а будут использованы готовые расчёты ВАБ 1 уровня, ВАБ 2 уровня Курской АЭС-2. Проверка будет производиться только для одного сценария, который определён как наиболее консервативный для данного типа реакторов.

**Модель AI**

Определение модели AI производится на основании систематического обзора [6]. На основании проведённого анализа, сформулированы предположения о перспективах использования генеративно-состязательных сетей (GAN) для моделирования редких событий, скрытых марковских моделей (HMM) для учета динамического поведения систем, методов объяснимого искусственного интеллекта (XAI) для повышения прозрачности моделей и Knowledge-Based Modeling (KBM) для интеграции экспертных знаний, что может значительно повысить точность и надежность анализа безопасности АЭС. Дополнительно определим для работы с технической документаций технологии, основанная на LLM. [10]. Для определения вероятности распределения погодных условий были использованы данные из [11, 12].

В качестве упрощённой модели архитектуры определим следующую конфигурацию, приведённой на рисунке 1 и 2.

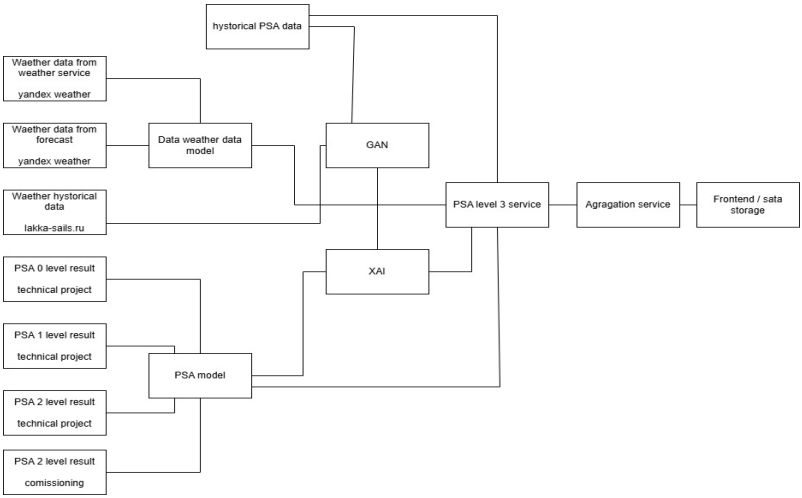



Рис. 1 – функциональная архитектура

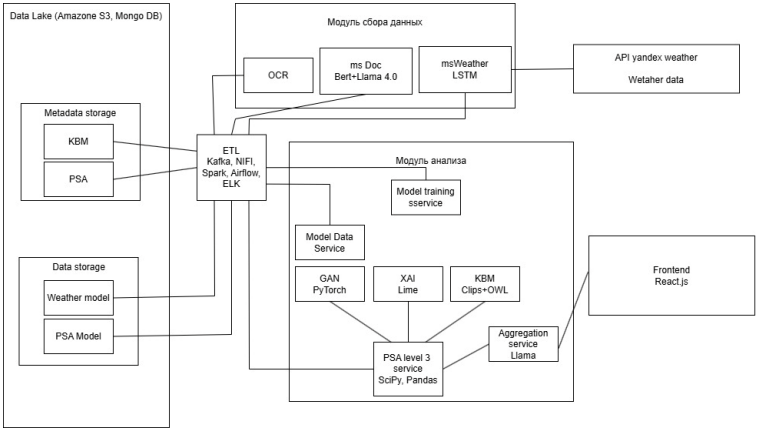



Рис. 2 – Техническая архитектура

Верификация гипотезы осуществляется путем сравнения конечных результатов. В качестве данных для верификации были взяты результаты [12]. Результаты сравнения приведены на рисунке 3. В качестве данных для работы моделей AI были взяты данные для Курской АЭС. Аварийный режим – потеря внешнего энергоснабжения. Расчет проводился для исторических данных для 2015 года.

Как видно из результатов, у расчетов демонстрируется приемлемый уровень сходимости с референсными расчетами. Средняя

относительная погрешность вычислений – 0,1628.

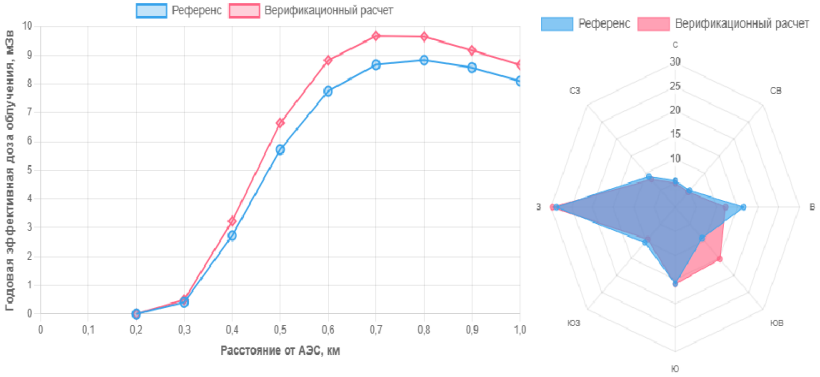



Рис. 3 - Результаты верификационного расчета

В данной работе исследовалась верификация применения методов AI для проведения ВАБ на АЭС. Были разработаны две модели, результаты расчетов которых показали приемлемую сходимость с референсными данными. Однако обе модели имеют ограничения и упрощения. Дальнейшие исследования должны сосредоточиться на улучшении точности моделей, снижении консерватизма в расчетах, оптимизации ресурсов и повышении доверия к результатам через взаимодействие с экспертами.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, IAEA, Vienna (2011).

2. International Atomic Energy Agency. Safety Recommendations: Assessment and Management of Risks for Nuclear Installations. NS-G-1.2. IAEA, Vienna (2002)

3. Федеральные нормы и правила в области использования атомной энергии “Основные требования к вероятностному анализу безопасности блока атомной станции»: НП-095-15 : утв. Приказом Федеральной службы по экологическому, технологическому и атомному надзору от 12 авг. 2015 г. № 311

4. Комаров Ю. А. Проблемы риск-ориентированных подходов для использования в атомной энергетике // Безопасность в техносфере. 2014. №. 1. С. 24-31

5. Калабурдин А. В. Проблемы традиционных методов анализа

безопасности атомных электрических станций / А. В. Калабурдин, Р. В. Радченко // Энерго- и ресурсосбережение. Энергообеспечение. Нетрадиционные и возобновляемые источники энергии. Атомная энергетика: материалы Международной научно-практической конференции студентов, аспирантов и молодых ученых, посвященной памяти профессора Данилова Н. И. (1945–2015) – Даниловских чтений (Екатеринбург, 10–14 декабря 2018 г.). — Екатеринбург : УрФУ, 2018. — С. 831-836.

6. Трибелев А.А. Совершенствование риск-ориентированной модели безопасности АЭС на основе технологии искусственного интеллекта: систематический обзор // Цифровые системы и модели: теория и практика проектирования, разработки и использования: материалы Международной научно-практической конференции, Казань, 10-11 апреля 2025 г. Под общ. ред. И.Г. Ахметовой. Казань: Казан. гос. энерг. ун-т, 2025. С. 1908-1913

7. Машиностроение. Энциклопедия / Ред. Совет: КюВю Фролов (ред) и др. М: Машиностроение. Машиностроение ядерной энергетики. Т.IV-25, В 2-х кн. Кн.1 Е.О. Адамов, Ю.Г. Драгунов, В.В. Орлов и др. Под общ ред. Е.О Адамова. 2005 – 960 с., ил.

8. Федеральные нормы и правила в области использования атомной энергии “Общие положения обеспечения безопасности атомных станций” (ОПБ АС-2015) : НП-001-15 : утв. приказом Федеральной службы по экологическому, технологическому и атомному надзору от 17 дек. 2015 г. № 522

9. Нормы радиационной безопасности : НРБ-99 : СП 2.6.1.758-99 : [утв. Главным государственным санитарным врачом Российской Федерации 2 июля 1999 г.]. - Москва : Минздрав России, 1999.

10. Коньков В.В., Серова А.С., Трибелев А.А. Анализ ссылочных конструкций в текстах нормативной документации атомной отрасли с использованием методик распознавания именованных сущностей и больших языковых моделей // Будущее атомной энергетики – AtomFuture 2024: XIX Международная научно-практическая конференция: Тезисы докладов. Обнинск, 05-06 декабря 2024 г. Обнинск: ИАТЭ НИЯУ МИФИ, 2024. С. 175-177.САЙТ

11. Берберова М.А. Оценка показателей риска для вторых очередей Смоленской и Курской АЭС: дис. на соискание учёной степени кандидата технических наук. Москва, 2015. Автономная некоммерческая организация Международный центр по ядерной безопасности

*УДК 51-74*

***Уточкина Е.С.***
***Научный руководитель: Демкин В.И., канд. техн. наук, доц.***
*Национальный исследовательский университет г. Зеленоград, Россия*

# СОЗДАНИЕ ФИЛЬТРА КАЛМАНА НА PYTHON ДЛЯ ПОИСКА ПОЛОЖЕНИЯ И СКОРОСТИ ПАДАЮЩЕГО ОБЪЕКТА

В современной инженерии присутствует необходимость в точной оценке состояния динамических систем в условиях скрытых состояний и зашумленных данных, так как устройства измерений имеют ограниченную точность, а также подвержены шумам и каким-либо задержкам. Фильтр Калмана является оптимальным методом для решения данной проблемы: у него высокая точность в обработке шума, он учитывает динамику системы, возможна модификация и комбинация с другими методами. Создание фильтра Калмана для поиска положения и скорости падающего объекта является актуальной задачей. Если знать положение падающего объекта и его скорость, то возможен прогноз момента падения и координаты объекта в этот момент. Моделирование падение снарядов, ступеней ракет и спускаемых аппаратов особенно важно в военной и космической промышленности.

Проблема оценки параметров падающих объектов активно изучается в современных исследованиях по фильтрации [1-3].

Целью данного исследования является оценка положения и скорости падающего объекта с минимальной погрешностью в условиях зашумленных измерений с помощью разработанного алгоритма фильтра Калмана на Python. Для достижения цели необходимо выполнить следующие задачи:

1. Провести анализ модели движения и определить параметры системы.
2. Построить математическую модель объекта в пространстве состояний.
3. Написать код алгоритма фильтра Калмана на Python и визуализировать полученный алгоритм с помощью графиков.
4. Провести моделирование с различными параметрами дисперсии для ковариационных матриц.
5. Проанализировать эффективность фильтра (сравнить с истинной траекторией объекта).

В данной работе выдвинуты две гипотезы. Первой гипотезой является предположение, что реализованный алгоритм позволит увеличить точность радара на 80 процентов. Согласно второй гипотезе,

матрица состояния модели оказывает существенное влияние на погрешность, чем матрица ошибок модели.

*Модель падения объекта*

Падение объекта происходит в условиях свободного падения с высоты 40000 метров. Вертикальная скорость объекта 300 м/с, горизонтальная скорость 400 м/с. Сопротивление воздуха не учитывается, на объект действует только гравитация. Радар измеряет расстояние до цели с точностью 100 метров, производя 10 измерений в секунду в течение 30 секунд.

Измерение расстояния (1):

$$z_k = \sqrt{x_k^2 + y_k^2} + v_k, \quad (1)$$

где $z_k$ - измерение в текущий момент времени, $x_k$,$y_k$ – позиция в текущий момент времени, $v_k$ – шум измерений.

Матрица преобразования (2):

$$H = \begin{bmatrix} \frac{x}{\sqrt{x^2+y^2}} & \frac{y}{\sqrt{x^2+y^2}} & 0 & 0 \end{bmatrix}, \quad (2)$$

где x,y – значения позиции на этапе прогнозирования.

Ковариационные матрицы и их параметры (3-5):

Матрица ошибок измерений (R):

$$R = [\sigma_r^2] = [1111.11], \sigma_r = \frac{100}{3} = 33.33, \quad (3)$$

где $\sigma_r$ – дисперсия, найденная по правилу трех сигм (100 м – отклонение радара).

Матрица ошибок модели (Q):

$$Q = BB^T\sigma_a^2, \sigma_a^2 \in \left[\frac{0.01}{3}, \frac{100}{3}\right], \quad (4)$$

где B – матрица управления, $\sigma_a^2$ – дисперсия.

Матрица состояния модели (P):

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sigma_p^2, \sigma_p^2 \in \left[\frac{0.01}{3}, \frac{100}{3}\right], \quad (5)$$

где $\sigma_p^2$ – дисперсия.

*Реализация алгоритма:*

Алгоритм фильтра реализован на Python с шагом дискретизации $\Delta t = 0.1$ с. Для анализа устойчивости были использованы различные параметры $\sigma_p$ (матрица P) и $\sigma_a$ (матрица Q).

Результаты:

Фильтр показал высокую точность оценки положения и скорости (Рис. 1).

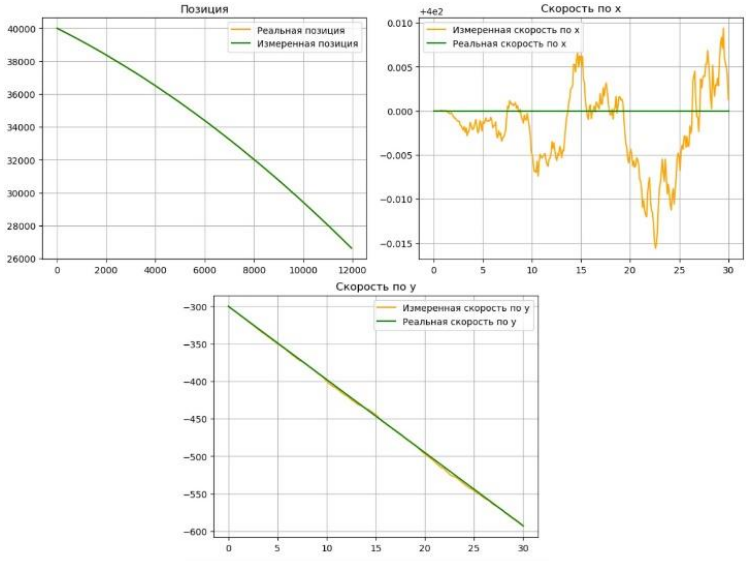



Рис. 1 Графики (реальные и оцененные с помощью фильтра)

Отклонения при изменении параметров составили:

– максимальная ошибка положения возросла в 22 раза ($\sigma_p$), в 3,3 раза ($\sigma_a$). Средняя ошибка возросла в 10 раз ($\sigma_p$), в 1,7 раза ($\sigma_a$).

– максимальная ошибка и средняя ошибка скорости по x: выросли в более чем в 10 $^7$раз ($\sigma_p$), уменьшились в более чем 200 раз ($\sigma_a$).

– максимальная ошибка скорости по y возросла в 6,5 раз ($\sigma_p$), в 16 раз ($\sigma_a$). Средняя ошибка возросла в 2 раза ($\sigma_p$), в 9 раз ($\sigma_a$).

*Гистограммы отклонений при различных значениях $\sigma$:*

Распределение ошибок показало, что большинство отклонений сосредоточено вблизи нуля. При увеличении $\sigma_p$ и $\sigma_a$ хвосты распределений утяжелялись, что указывает на рост редких, но значительных ошибок.

*Выводы:*

В ходе исследования была успешно реализована модель фильтра Калмана на Python для оценки положения и скорости падающего объекта. Данный фильтр значительно улучшает точность радарных данных. Гипотеза о точности подтвердилась при оптимальных параметрах ковариационных матриц. Матрица P оказывает большее влияние, чем матрица Q, так как все значения менялись более значительно при изменении $\sigma_p$. Оптимальные параметры зависят от

задачи: если важнее поиск скорости по x, необходимо увеличить $\sigma_a$, если важна равномерная точность, то следует регулировать параметры. Практическая значимость работы заключается в возможности применения алгоритма в военной и аэрокосмической отраслях для прогнозирования траекторий объектов. В качестве направлений для дальнейших исследований можно выбрать интеграцию с нейросетевыми методами и адаптацию данного алгоритма к реальным системам. В дальнейшем также следует учесть влияние сопротивление воздуха и другие нелинейные эффекты.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алексеева, Ю. А. Алгоритмы фильтрации для обработки данных в космической отрасли / Ю. А. Алексеева, Е. Д. Агафонов // Актуальные проблемы авиации и космонавтики : Сборник материалов VII Международной научно-практической конференции, посвященной Дню космонавтики: в 3 томах, Красноярск, 12–16 апреля 2021 года / Под общей редакцией Ю. Ю. Логинова. Том 2. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева", 2021. – С. 95-97.

2. Тележкин, В. Ф. Обработка информации с использованием фильтра Калмана в Matlab Simulink / В. Ф. Тележкин, Б. Б. Саидов // Системы анализа и обработки данных. – 2021. – № 4(84). – С. 49-62.

3. Товстик, Т. М. Линейный фильтр Калмана - Бьюси с векторными авторегрессионными сигналом и шумом / Т. М. Товстик // Вестник Санкт-Петербургского университета. Математика. Механика. Астрономия. – 2021. – Т. 8, № 1. – С. 111-122.

***УДК 004.94***

***Фальков Г.А.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## АДАПТИВНОЕ ОКОННОЕ ПРЕОБРАЗОВАНИЯ ФУРЬЕ ДЛЯ АНАЛИЗА КАЧЕСТВА ЭЛЕКТРОЭНЕРГИИ ВЫСОКОВОЛЬТНОЙ СЕТИ

Качество электроэнергии высоковольтной сети напрямую влияет на надежность и безопасность работы оборудования. Его отклонение может выражаться в виде гармонических искажений, провалов и

перенапряжений.

Для анализа искажений широко применяется оконное преобразование Фурье, позволяющее получить спектр сигнала, зависящий от времени. Эффективность окна зависит от [2, 3]:

- типа окна (например, Кайзера, Чебышева);
- формы окна (ширина основного лепестка и максимальный уровень боковых лепестков амплитудно-частотной характеристики).

Неправильно подобранные параметры могут привести к искажению спектра, плохому временно-частотному разрешению, а также к чрезмерным вычислительным затратам [4].

Разработанный графический программный комплекс на языке C# реализует метод адаптивного оконного преобразования Фурье (рис. 1) с возможностью изменения параметров оконной функции (тип, длина), что позволит улучшить разрешение спектра и уменьшить вычислительную нагрузку.

Схема алгоритма анализа сигнала с помощью адаптивного оконного преобразования Фурье заключается в следующем:

- сигнал поступает в программу в виде загруженного файла, содержащего временное значение и измеренное значение параметра (напряжения или тока);
- выполняется настройка параметров оконного преобразования Фурье;
- происходит разбиение сигнала на окна;
- осуществляется применение выбранной оконной функции;
- вычисляется амплитудный спектр;
- вывод результатов.

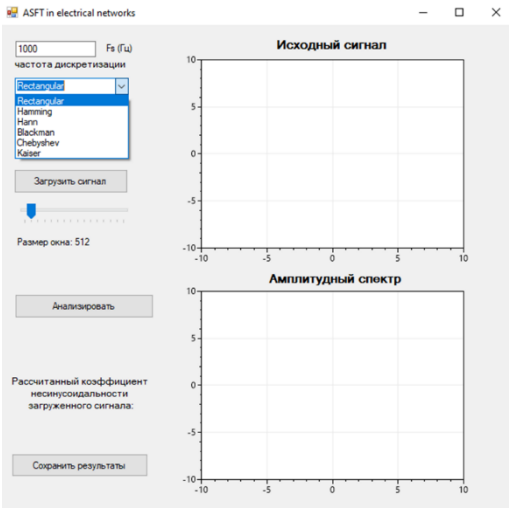



Рис. 1. Скриншот окна программы

В рамках эксперимента был загружен сигнал, содержащий временной ряд значений напряжения в высоковольтной сети (рис. 2). Сигнал представляет собой выборку с равномерной частотой дискретизации, составляющей 1000 Гц, общая длительность составила 1 секунду.

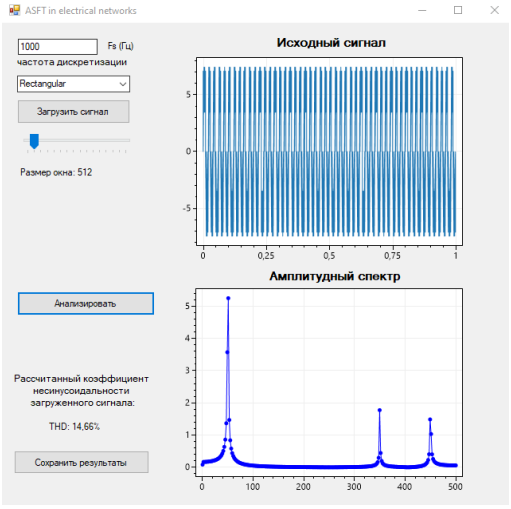



Рис. 2. Скриншот окна результата работы программы

В результате анализа был построен амплитудный спектр сигнала, а также выполнен расчет коэффициента несинусоидальности, который по результатам работы программы указывает на превышение нормативного значения, указанного в ГОСТ 32144-2013 [1].

Таким образом, разработанный программный комплекс на C# для анализа качества электроэнергии на основе адаптивного оконного преобразования Фурье с подбором параметров окна позволил достичь высокой точности и оперативности анализа. Комплекс может быть интегрирован в системы мониторинга или использован в качестве обучающего инструмента.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ 32144-2013 [Электронный ресурс]. – URL: https://electromontaj-proekt.ru (дата обращения: 19.05.2025).

2. Бобро Д.П. Повышение энергоэффективности систем электроснабжения рудодобывающих предприятий с мощными нелинейными электроприемниками/ Д.П. Бобро, Д.А. Прасол // Энергетика и энергосбережение: теория и практика: Сборник материалов vii международной научно-практической конференции, Кемерово, 07–09 декабря 2022 года. – Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. – С. 452-457.

3. Чан Х.Н. Сравнительный анализ методов обнаружения и определения типа модуляции сложных сигналов на основе Фурье-преобразования / Х. Н. Чан, Ч. Н. Нгуен // Новые горизонты: сборник докладов IX научно-практической конференции с международным участием, Брянск, 07 апреля 2022 года. – Брянск: Брянский государственный технический университет, 2022. – С. 344-347.

4. Чижма С.Н. Метод спектрального анализа интергармоник в электроэнергетических системах // Промышленная энергетика. – 2014.– С. 43-47.

*УДК 004.8*

***Фонова А.Ю.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# УГРОЗЫ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЕНЕРАТИВНОГО ИИ: РИСКИ, СЦЕНАРИИ АТАК И ПОДХОДЫ К ЗАЩИТЕ

Стремительное развитие генеративного искусственного интеллекта (GenAI) открыло новую главу в технологическом прогрессе, предлагая беспрецедентные возможности для создания контента, научных изысканий, разработки ПО и персонализации услуг. Модели вроде GPT, DALL-E и Midjourney демонстрируют впечатляющую способность генерировать текст, изображения, аудио и программный код, часто неотличимые от результатов человеческого труда. Однако, как и любая мощная технология двойного назначения, GenAI несет существенные риски, особенно в сфере кибербезопасности. Способность ИИ к обучению, адаптации и автономному созданию сложного контента предоставляет злоумышленникам новые векторы атак, увеличивая их эффективность и масштаб.

Данная статья систематизирует и анализирует ключевые угрозы и вызовы для кибербезопасности, порождаемые распространением генеративного ИИ. Мы рассмотрим основные риски, детализируем потенциальные сценарии атак и предложим комплексные подходы к разработке стратегий защиты.

**Новые риски кибератак с применением генеративного ИИ.** Появление GenAI значительно расширяет арсенал киберпреступников, снижая порог входа для реализации изощренных атак и наращивая их потенциальный ущерб.

Изощренная социальная инженерия:

Автоматизированный и персонализированный фишинг: GenAI позволяет массово генерировать убедительные фишинговые письма и сообщения, лишенные типичных ошибок и адаптированные под конкретную жертву, что резко повышает их результативность.

Создание дипфейков (Deepfakes): Технологии генерации реалистичных аудио- и видеоматериалов открывают дорогу для мошенничества от имени руководства (CEO-fraud), шантажа с использованием компрометирующих видео или распространения дезинформации для манипуляции общественным мнением.

Автоматизация создания и распространения вредоносного ПО:

Генерация полиморфного кода: GenAI может использоваться для создания вредоносов, меняющих свою структуру при каждом заражении, что усложняет их обнаружение традиционными антивирусами.

Помощь в написании эксплойтов: ИИ способен анализировать информацию об уязвимостях (CVE) и содействовать атакующим в разработке или модификации кода эксплойтов.

Усиление атак на системы и инфраструктуру:

Интеллектуальная разведка уязвимостей: GenAI может применяться для более быстрого и эффективного поиска уязвимых систем и слабых мест в защите.

Адаптивные DDoS-атаки: ИИ-управляемые ботнеты способны динамически менять тактику, эффективнее обходя защитные механизмы.

Атаки на сами ИИ-системы:

Отравление данных (Data Poisoning): Внедрение вредоносных образцов в обучающие наборы ИИ-моделей, применяемых в кибербезопасности, может привести к их некорректной работе или пропуску реальных угроз.

Состязательные атаки (Adversarial Attacks): Незначительные, невидимые человеку модификации входных данных способны обмануть ИИ-систему, заставив ее неверно классифицировать угрозу.\

**Примеры сценариев атак с использованием GenAI.** Рассмотрим несколько реалистичных сценариев, иллюстрирующих потенциал GenAI в руках злоумышленников.

Сценарий 1: Масштабный спиэрфишинг с аудио-дипфейками. Атакующие собирают информацию о сотрудниках компании из открытых источников. Затем GenAI, обученный на голосе CEO, генерирует персонализированные аудиосообщения с указанием срочно перевести средства. Убедительность подделки значительно повышает шансы на успех.

Сценарий 2: Автоматизированное создание полиморфного шифровальщика. Кибергруппа использует GenAI для разработки базового шифровальщика, а затем ИИ генерирует множество его уникальных вариантов, изменяя код и методы обфускации, что позволяет обходить антивирусные сигнатуры.

Сценарий 3: Дезинформационная кампания с синтезированными новостями и видео. В преддверии важных событий GenAI генерирует фейковые новости, имитирующие стиль авторитетных СМИ, и дипфейк-видео с политиками. Массовое распространение такого

контента подрывает доверие и вызывает общественный резонанс.

Сценарий 4: Атака на ИИ-систему обнаружения вторжений через отравление данных. Злоумышленники внедряют в данные для обучения IDS/IPS специально подготовленные образцы трафика, помеченные как легитимные, но содержащие скрытые признаки атаки. В итоге обученная модель становится "слепой" к определенным угрозам.

**Комплексные подходы к защите и противодействию.** Противостояние угрозам от генеративного ИИ требует многоуровневой стратегии, объединяющей технологические, организационные и регуляторные меры.

Технологические контрмеры:

ИИ для защиты (AI for Defense): Разработка ИИ-систем кибербезопасности для обнаружения аномалий, паттернов атак (включая созданные другим ИИ) и автоматического реагирования. Сюда входят продвинутые детекторы фишинга, системы анализа поведения (UEBA) и выявления дипфейков [1].

Повышение устойчивости ИИ-моделей: Применение техник вроде состязательного обучения (adversarial training) для защиты собственных ИИ-систем.

Объяснимый ИИ (XAI): Разработка ИИ-моделей, способных пояснять свои решения, что помогает в анализе инцидентов.

Цифровые водяные знаки и проверка происхождения контента: Внедрение технологий маркировки ИИ-контента и верификации его подлинности.

Усиленная аутентификация: Применение многофакторной аутентификации (MFA) и разработка биометрии, устойчивой к дипфейкам [2].

Архитектура "Нулевого доверия" (Zero Trust): Строгая проверка каждого пользователя и устройства перед доступом к ресурсам.

Организационные и процедурные меры:

Обучение персонала: Регулярные тренинги по кибербезопасности с акцентом на новые GenAI-угрозы.

Планы реагирования на инциденты: Адаптация планов с учетом специфики ИИ-атак.

Red Teaming с использованием ИИ: Проведение учений с имитацией атак на базе GenAI для проверки защиты [2].

Обмен информацией об угрозах (Threat Intelligence Sharing): Активное участие в платформах для своевременного получения данных о новых тактиках.

Регуляторные и этические аспекты:

Разработка стандартов и законодательства: Создание нормативной

базы, регулирующей GenAI, включая безопасность и ответственность.

Этические принципы разработки ИИ: Продвижение кодексов, минимизирующих вредоносное использование ИИ.

Международное сотрудничество: Координация усилий для борьбы с киберпреступностью, использующей ИИ.

Эпоха генеративного ИИ обостряет извечную "гонку вооружений" в кибербезопасности. ИИ предоставляет мощные инструменты как злоумышленникам, так и защитникам. Ключевой вызов – скорость развития GenAI, опережающая разработку адекватных защитных механизмов. Существует риск неготовности общества к масштабированию ИИ-управляемых атак. Вопросы этики, ответственности за действия ИИ и его потенциальной предвзятости требуют глубокого осмысления [4].

Генеративный ИИ – революционная технология, но её интеграция несет серьезные угрозы кибербезопасности: от изощренного фишинга и неотличимых дипфейков до автоматизированной разработки вредоносов и атак на сами ИИ-системы. Эффективное противодействие требует не только технологических инноваций, но и повышения осведомленности пользователей, адаптации организационных процессов, развития нормативно-правовой базы и международного сотрудничества. Только совместные усилия позволят обеспечить ответственное развитие GenAI, минимизируя риски и сохраняя его преимущества для общества. Будущие исследования должны фокусироваться на проактивных методах обнаружения и атрибуции атак с GenAI, а также на создании надежных систем детекции синтетического контента.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство : Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Фонова, А. Ю. Искусственный интеллект в области биометрии и идентификации: новые методы аутентификации и безопасности / А. Ю. Фонова // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов Международной научно-технической конференции молодых ученых

БГТУ им. В.Г. Шухова, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 398-402. – EDN VKTSBE.

3. Королев, О. Л. Анализ угроз информационной безопасности с использованием технологии искусственного интеллекта / О. Л. Королев, С. В. Белик // Проблемы информационной безопасности социально-экономических систем : Труды X Международной Юбилейной научно-практической конференции, Симферополь ¾ Гурзуф, 15–17 февраля 2024 года. – Симферополь: ИП Зуева Т.В., 2024. – С. 167-168. – EDN ANOEDH.

4. Разработка программного обеспечения для нахождения брешей в информационной безопасности на основе искусственного интеллекта / Т. Г. Абрамова, А. В. Неустроева, Н. С. Николаев, Д. Н. Иванова // DIGITAL EDU. Цифровые компетенции в образовании : сборник материалов Всероссийского научного форума с международным участием, Якутск, 13 февраля 2024 года. – Киров: Межрегиональный центр инновационных технологий в образовании, 2024. – С. 338-341. – EDN CFZYAV.

***УДК 004.8***

***Фонова А.Ю.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## УГРОЗЫ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЕНЕРАТИВНОГО ИИ: РИСКИ, СЦЕНАРИИ АТАК И ПОДХОДЫ К ЗАЩИТЕ

Стремительное развитие генеративного искусственного интеллекта (GenAI) открыло новую главу в технологическом прогрессе, предлагая беспрецедентные возможности для создания контента, научных изысканий, разработки ПО и персонализации услуг. Модели вроде GPT, DALL-E и Midjourney демонстрируют впечатляющую способность генерировать текст, изображения, аудио и программный код, часто неотличимые от результатов человеческого труда. Однако, как и любая мощная технология двойного назначения, GenAI несет существенные риски, особенно в сфере кибербезопасности. Способность ИИ к обучению, адаптации и автономному созданию сложного контента предоставляет злоумышленникам новые векторы атак, увеличивая их эффективность и масштаб.

Данная статья систематизирует и анализирует ключевые угрозы и вызовы для кибербезопасности, порождаемые распространением генеративного ИИ. Мы рассмотрим основные риски, детализируем потенциальные сценарии атак и предложим комплексные подходы к разработке стратегий защиты.

**Новые риски кибератак с применением генеративного ИИ.** Появление GenAI значительно расширяет арсенал киберпреступников, снижая порог входа для реализации изощренных атак и наращивая их потенциальный ущерб.

Изощренная социальная инженерия:

Автоматизированный и персонализированный фишинг: GenAI позволяет массово генерировать убедительные фишинговые письма и сообщения, лишенные типичных ошибок и адаптированные под конкретную жертву, что резко повышает их результативность.

Создание дипфейков (Deepfakes): Технологии генерации реалистичных аудио- и видеоматериалов открывают дорогу для мошенничества от имени руководства (CEO-fraud), шантажа с использованием компрометирующих видео или распространения дезинформации для манипуляции общественным мнением.

Автоматизация создания и распространения вредоносного ПО:

Генерация полиморфного кода: GenAI может использоваться для создания вредоносов, меняющих свою структуру при каждом заражении, что усложняет их обнаружение традиционными антивирусами.

Помощь в написании эксплойтов: ИИ способен анализировать информацию об уязвимостях (CVE) и содействовать атакующим в разработке или модификации кода эксплойтов.

Усиление атак на системы и инфраструктуру:

Интеллектуальная разведка уязвимостей: GenAI может применяться для более быстрого и эффективного поиска уязвимых систем и слабых мест в защите.

Адаптивные DDoS-атаки: ИИ-управляемые ботнеты способны динамически менять тактику, эффективнее обходя защитные механизмы.

Атаки на сами ИИ-системы:

Отравление данных (Data Poisoning): Внедрение вредоносных образцов в обучающие наборы ИИ-моделей, применяемых в кибербезопасности, может привести к их некорректной работе или пропуску реальных угроз.

Состязательные атаки (Adversarial Attacks): Незначительные, невидимые человеку модификации входных данных способны

обмануть ИИ-систему, заставив ее неверно классифицировать угрозу.\

**Примеры сценариев атак с использованием GenAI.** Рассмотрим несколько реалистичных сценариев, иллюстрирующих потенциал GenAI в руках злоумышленников.

Сценарий 1: Масштабный спиэрфишинг с аудио-дипфейками. Атакующие собирают информацию о сотрудниках компании из открытых источников. Затем GenAI, обученный на голосе CEO, генерирует персонализированные аудиосообщения с указанием срочно перевести средства. Убедительность подделки значительно повышает шансы на успех.

Сценарий 2: Автоматизированное создание полиморфного шифровальщика. Кибергруппа использует GenAI для разработки базового шифровальщика, а затем ИИ генерирует множество его уникальных вариантов, изменяя код и методы обфускации, что позволяет обходить антивирусные сигнатуры.

Сценарий 3: Дезинформационная кампания с синтезированными новостями и видео. В преддверии важных событий GenAI генерирует фейковые новости, имитирующие стиль авторитетных СМИ, и дипфейк-видео с политиками. Массовое распространение такого контента подрывает доверие и вызывает общественный резонанс.

Сценарий 4: Атака на ИИ-систему обнаружения вторжений через отравление данных. Злоумышленники внедряют в данные для обучения IDS/IPS специально подготовленные образцы трафика, помеченные как легитимные, но содержащие скрытые признаки атаки. В итоге обученная модель становится "слепой" к определенным угрозам.

**Комплексные подходы к защите и противодействию.** Противостояние угрозам от генеративного ИИ требует многоуровневой стратегии, объединяющей технологические, организационные и регуляторные меры.

Технологические контрмеры:

ИИ для защиты (AI for Defense): Разработка ИИ-систем кибербезопасности для обнаружения аномалий, паттернов атак (включая созданные другим ИИ) и автоматического реагирования. Сюда входят продвинутые детекторы фишинга, системы анализа поведения (UEBA) и выявления дипфейков [1].

Повышение устойчивости ИИ-моделей: Применение техник вроде состязательного обучения (adversarial training) для защиты собственных ИИ-систем.

Объяснимый ИИ (XAI): Разработка ИИ-моделей, способных пояснять свои решения, что помогает в анализе инцидентов.

Цифровые водяные знаки и проверка происхождения контента:

Внедрение технологий маркировки ИИ-контента и верификации его подлинности.

Усиленная аутентификация: Применение многофакторной аутентификации (MFA) и разработка биометрии, устойчивой к дипфейкам [2].

Архитектура "Нулевого доверия" (Zero Trust): Строгая проверка каждого пользователя и устройства перед доступом к ресурсам.

Организационные и процедурные меры:

Обучение персонала: Регулярные тренинги по кибербезопасности с акцентом на новые GenAI-угрозы.

Планы реагирования на инциденты: Адаптация планов с учетом специфики ИИ-атак.

Red Teaming с использованием ИИ: Проведение учений с имитацией атак на базе GenAI для проверки защиты [2].

Обмен информацией об угрозах (Threat Intelligence Sharing): Активное участие в платформах для своевременного получения данных о новых тактиках.

Регуляторные и этические аспекты:

Разработка стандартов и законодательства: Создание нормативной базы, регулирующей GenAI, включая безопасность и ответственность.

Этические принципы разработки ИИ: Продвижение кодексов, минимизирующих вредоносное использование ИИ.

Международное сотрудничество: Координация усилий для борьбы с киберпреступностью, использующей ИИ.

Эпоха генеративного ИИ обостряет извечную "гонку вооружений" в кибербезопасности. ИИ предоставляет мощные инструменты как злоумышленникам, так и защитникам. Ключевой вызов – скорость развития GenAI, опережающая разработку адекватных защитных механизмов. Существует риск неготовности общества к масштабированию ИИ-управляемых атак. Вопросы этики, ответственности за действия ИИ и его потенциальной предвзятости требуют глубокого осмысления [4].

Генеративный ИИ – революционная технология, но её интеграция несет серьезные угрозы кибербезопасности: от изощренного фишинга и неотличимых дипфейков до автоматизированной разработки вредоносов и атак на сами ИИ-системы. Эффективное противодействие требует не только технологических инноваций, но и повышения осведомленности пользователей, адаптации организационных процессов, развития нормативно-правовой базы и международного сотрудничества. Только совместные усилия позволят обеспечить ответственное развитие GenAI, минимизируя риски и сохраняя его

преимущества для общества. Будущие исследования должны фокусироваться на проактивных методах обнаружения и атрибуции атак с GenAI, а также на создании надежных систем детекции синтетического контента.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство : Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Фонова, А. Ю. Искусственный интеллект в области биометрии и идентификации: новые методы аутентификации и безопасности / А. Ю. Фонова // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов Международной научно-технической конференции молодых ученых БГТУ им. В.Г. Шухова, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 398-402. – EDN VKTSBE.

3. Королев, О. Л. Анализ угроз информационной безопасности с использованием технологии искусственного интеллекта / О. Л. Королев, С. В. Белик // Проблемы информационной безопасности социально-экономических систем : Труды X Международной Юбилейной научно-практической конференции, Симферополь ¾ Гурзуф, 15–17 февраля 2024 года. – Симферополь: ИП Зуева Т.В., 2024. – С. 167-168. – EDN ANOEDH.

4. Разработка программного обеспечения для нахождения брешей в информационной безопасности на основе искусственного интеллекта / Т. Г. Абрамова, А. В. Неустроева, Н. С. Николаев, Д. Н. Иванова // DIGITAL EDU. Цифровые компетенции в образовании : сборник материалов Всероссийского научного форума с международным участием, Якутск, 13 февраля 2024 года. – Киров: Межрегиональный центр инновационных технологий в образовании, 2024. – С. 338-341. – EDN CFZYAV.

*УДК 004.8*

***Фонова А.Ю.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ЭКОЛОГИЧЕСКИЙ СЛЕД ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СКРЫТЫЕ ИЗДЕРЖКИ РАЗВИТИЯ ТЕХНОЛОГИЙ ИИ

Технологии искусственного интеллекта (ИИ) переживают настоящий бум, проникая во все уголки нашей жизни и обещая революционные перемены. Однако за впечатляющими прорывами ИИ, такими как мощные большие языковые модели (LLM) и сложные системы распознавания образов, кроется значительная экологическая "цена". Энергоемкость обучения и эксплуатации ИИ-моделей, а также растущая армия прожорливых дата-центров, создают ощутимую нагрузку на окружающую среду. Эта проблема требует пристального внимания научного сообщества, разработчиков и политиков.

В этой статье мы всесторонне проанализируем экологический след искусственного интеллекта, выявим главные источники его негативного влияния на природу и рассмотрим возможные пути к устойчивому развитию ИИ-технологий.

**Энергетический "аппетит" ИИ: масштаб проблемы.** Одна из главных экологических болевых точек, связанных с ИИ, – его колоссальное энергопотребление, особенно на этапе "вскармливания" сложных моделей глубокого обучения.

Обучение гигантских моделей: Современные флагманские ИИ-модели, вроде GPT-4 от OpenAI или разработок Google DeepMind (например, AlphaFold), требуют для своего обучения невероятных вычислительных мощностей и, как следствие, огромного количества электроэнергии. Процесс обучения может длиться недели, а то и месяцы, загружая тысячи специализированных графических (GPU) или тензорных (TPU) процессоров. К примеру, по оценкам, обучение модели GPT-3 "съело" около 1287 МВт·ч электроэнергии, что по выбросам углекислого газа сопоставимо с несколькими сотнями трансатлантических перелетов [2]. Последующие, еще более крупные модели, вероятно, потребляют значительно больше.

Инференс (работа моделей): Хотя затраты энергии на один запрос к уже обученной модели (инференс) заметно ниже, чем на ее создание, суммарное энергопотребление на этапе эксплуатации может быть очень

высоким. Миллионы пользователей ежедневно обращаются к ИИ-приложениям: чат-ботам, рекомендательным системам, поисковикам с элементами ИИ – все они постоянно "дергают" модели, требуя непрерывной работы серверов.

"Железо" для ИИ: Специализированное оборудование, особенно GPU, само по себе энергоемко. Рост сложности моделей подстегивает разработку все более мощных, но и более "прожорливых" чипов.

Компании-гиганты, такие как OpenAI, Google, Microsoft, Meta, лидирующие в разработке ИИ, не всегда раскрывают полные данные об энергопотреблении своих детищ и дата-центров, что затрудняет точную оценку глобального воздействия [3]. Однако доступные исследования и косвенные оценки указывают на стремительный рост вклада ИИ в мировое потребление электроэнергии.

**Дата-центры и жизненный цикл ИИ: многогранное влияние на природу.** Дата-центры – "мозг" и "сердце" современных ИИ-технологий – оказывают комплексное воздействие на окружающую среду.

Углеродный след: Значительная часть электроэнергии для дата-центров все еще вырабатывается из ископаемого топлива, что ведет к выбросам парниковых газов. Даже при использовании возобновляемых источников, строительство и обслуживание самих дата-центров, а также производство оборудования, имеют свой углеродный след.

Потребление воды: Дата-центры нуждаются в больших объемах воды для охлаждения. Это может создавать нагрузку на местные водные ресурсы, особенно в засушливых регионах.

Электронный мусор (e-waste): Быстрый технологический прогресс в ИИ и "железе" ведет к частой смене серверного оборудования. Утилизация устаревших серверов, GPU и других компонентов – серьезная экологическая проблема из-за содержания в них токсичных материалов.

Редкоземельные металлы: Производство высокопроизводительных чипов для ИИ требует редкоземельных металлов, добыча которых часто наносит вред экологии и связана с социальными проблемами..

**На пути к устойчивому ИИ: "зеленые" вычисления в действии.** Осознание экологических проблем, порождаемых ИИ, стимулирует поиск решений для минимизации его вредного влияния. Концепция "устойчивого ИИ" (Sustainable AI) или "зеленого ИИ" (Green AI) включает различные подходы:

Энергоэффективные алгоритмы и модели:

- Оптимизация архитектур: Создание более компактных и

менее ресурсоемких моделей без серьезной потери качества (например, дистилляция моделей, квантование, прунинг).

- Эффективные методы обучения: Разработка алгоритмов, требующих меньше данных или вычислительных итераций.
- Трансферное обучение и дообучение (fine-tuning): Вместо обучения огромных моделей с нуля, адаптация уже существующих предобученных моделей для конкретных задач, что резко снижает энергозатраты.

Энергоэффективное "железо":

- Специализированные ИИ-чипы (ASICs, FPGAs): Разработка ускорителей, заточенных под конкретные ИИ-задачи и обладающих лучшим соотношением производительность/ватт.
- Новые вычислительные парадигмы: Исследование альтернатив, таких как нейроморфные или квантовые вычисления, которые в перспективе могут быть эффективнее для определенных ИИ-задач [5].

"Зеленые" дата-центры:

- Возобновляемые источники энергии: Перевод дата-центров на солнце, ветер или гидроэнергию.
- Повышение энергоэффективности (PUE): Оптимизация систем охлаждения, использование более эффективного оборудования.

Прозрачность и отчетность:

- Метрики экологического следа ИИ: Создание стандартизированных методик для измерения энергопотребления и углеродного следа ИИ-систем.
- Открытость разработчиков: Стимулирование компаний к раскрытию информации об экологическом воздействии их технологий.
- Ответственное использование оборудования: Продление жизненного цикла серверов и их экологически безопасная переработка.

**Вызовы на пути к "зеленому" ИИ.** Несмотря на существующие инициативы, достижение полной экологической устойчивости ИИ сталкивается с серьезными преградами.

"Гонка вооружений" в ИИ: Стремление создавать все более мощные модели часто отодвигает энергоэффективность на второй план.

Отсутствие стандартов: Без единых метрик и отчетности сложно объективно сравнивать экологический след разных ИИ-решений.

Экономический фактор: Внедрение "зеленых" технологий может требовать значительных первоначальных вложений.

Недостаточная осведомленность: Многие разработчики и пользователи ИИ не до конца осознают масштаб проблемы.

Искусственный интеллект способен решить многие глобальные проблемы, но его собственное развитие не должно усугублять экологический кризис [3]. Огромное энергопотребление при обучении и работе ИИ-моделей, а также экологический след дата-центров, требуют немедленных и скоординированных действий.

Переход к устойчивому ИИ возможен лишь через комплексный подход: энергоэффективные алгоритмы и "железо", "зеленые" дата-центры, прозрачность и стандарты отчетности. Необходимо стимулировать исследования в области "зеленых" вычислений и повышать осведомленность о скрытых издержках ИИ [1].

Ответственное развитие искусственного интеллекта – это не только этика и социальные аспекты [4], но и его экологическая состоятельность. Только найдя баланс между технологическим прогрессом и сохранением планеты, мы сможем в полной мере реализовать позитивный потенциал ИИ для будущего.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство: Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Экологические издержки ИИ: растущий углеродный след вызывает опасения [Электронный ресурс] // VC.ru: [сайт]. – URL: https://vc.ru (дата обращения: 23.04.2025).

3. Воздействие ИИ на окружающую среду [Электронный ресурс] //Хабр: [сайт]. – URL: https://habr.com (дата обращения: 23.04.2025).

4. Права человека в эпоху Искусственного Интеллекта: Европа как созидатель международных стандартов в области искусственного интеллекта // Бюллетень Европейского Суда по правам человека. – 2021. – № 2(224). – С. 142-144. – EDN WJVQBD.

5. Стариков, Е. Н. Сильный искусственный интеллект как интегратор отдельных технологий искусственного интеллекта в систему технологий / Е. Н. Стариков, А. И. Тютюнник // Тенденции развития науки и образования. – 2024. – № 112-7. – С. 31-36. – DOI 10.18411/trnio-08-2024-330. – EDN GQFWBA.

*УДК 004.8*

***Фонова А.Ю.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАБОЧИЕ ПРОЦЕССЫ СОТРУДНИКОВ IT-КОМПАНИЙ: АНАЛИЗ ВЛИЯНИЯ НА ПРОИЗВОДИТЕЛЬНОСТЬ И ЭФФЕКТИВНОСТЬ

Стремительный взлет и распространение технологий искусственного интеллекта (ИИ) кардинально меняют облик всех отраслей экономики, и IT-сектор здесь не просто не исключение – он в авангарде этих перемен. IT-компании зачастую не только создают ИИ-решения, но и активно внедряют их в собственные рабочие будни. Инструменты, основанные на машинном обучении, обработке естественного языка и компьютерном зрении, открывают новые горизонты для автоматизации рутины, оптимизации сложных операций и общего роста производительности.

Эта статья посвящена анализу того, как интеграция ИИ влияет на рабочие процессы сотрудников IT-компаний. Мы оценим его воздействие на продуктивность в различных сферах IT-деятельности – от DevOps и разработки до тестирования и аналитики, а также определим ключевые сдвиги в наборе необходимых компетенций. Понимание этих аспектов жизненно важно для стратегий развития как отдельных компаний, так и всей IT-индустрии [3].

ИИ в ключевых IT-процессах: от кода до операций. Искусственный интеллект находит свое место на всех этапах жизненного цикла разработки программного обеспечения и поддержки IT-инфраструктуры [4].

DevOps и AIOps (ИИ для IT-операций): Умная эксплуатация

В методологии DevOps, где разработчики и эксплуатационники работают в тесной связке, ИИ играет все более заметную роль. Концепция AIOps использует машинное обучение и анализ больших данных для автоматизации и улучшения IT-операций. Алгоритмы ИИ здесь помогают:

Проактивно мониторить и предсказывать проблемы: Обнаруживать аномалии в системах, предвидеть сбои и "узкие места" еще до того, как они станут критическими.

Автоматизировать реакцию на инциденты: ИИ может

анализировать логи, выявлять коренные причины проблем и даже запускать сценарии их автоматического устранения.

Оптимизировать CI/CD-конвейеры: анализировать данные о сборках и развертываниях, чтобы находить неэффективные этапы и предлагать улучшения.

Управлять ресурсами: динамически распределять вычислительные мощности и хранилища, опираясь на прогнозируемую нагрузку.

Разработка ПО: ИИ как напарник программиста

Современные ИИ-инструменты, такие как GitHub Copilot, Tabnine или Amazon CodeWhisperer, меняют сам подход к написанию кода:

Автодополнение и генерация кода: ИИ предлагает варианты кода на основе контекста, комментариев или описаний, заметно ускоряя создание шаблонных или рутинных участков.

Обнаружение ошибок и уязвимостей: Статический анализ кода с помощью ИИ выявляет потенциальные баги, проблемы производительности и "дыры" в безопасности на ранних стадиях.

Рефакторинг и оптимизация: ИИ может предлагать улучшения структуры кода, делая его чище и эффективнее.

Автогенерация документации и комментариев: Упрощение документирования кода, что важно для командной работы и дальнейшей поддержки.

Тестирование ПО: Гарантия качества с ИИ-поддержкой

Автоматизация тестирования с помощью ИИ помогает повысить качество продукта и сократить время его вывода на рынок:

Генерация тестовых случаев: ИИ-системы анализируют требования, код или пользовательские сценарии для автоматического создания релевантных наборов тестов.

Оптимизация выполнения тестов: Приоритизация тестов на основе анализа изменений в коде или оценки риска, сокращение избыточных проверок.

Визуальное тестирование: ИИ-алгоритмы (например, на базе компьютерного зрения) автоматически проверяют корректность отображения интерфейсов на разных устройствах.

Предиктивное тестирование: Анализ истории дефектов и изменений кода помогает предсказывать наиболее проблемные области и концентрировать на них усилия тестировщиков.

Аналитика данных и Business Intelligence: ИИ извлекает знания [2]

В аналитике ИИ становится незаменимым помощником для извлечения ценных инсайтов из огромных массивов данных:

Автоматический поиск паттернов: ИИ-алгоритмы выявляют скрытые закономерности, корреляции и тренды, которые человек мог

бы упустить.

Предиктивная аналитика: Построение моделей для прогнозирования будущих событий, поведения пользователей, спроса на продукты.

Обработка естественного языка (NLP): Извлечение информации из отзывов клиентов, технической документации, отчетов для принятия взвешенных решений.

Автоматизация отчетности: Ускорение подготовки аналитических отчетов и визуализации данных.

Как ИИ влияет на производительность IT-команд? Внедрение ИИ в рабочие процессы IT-компаний многогранно сказывается на их продуктивности и эффективности.

Рост производительности труда:

Автоматизация рутины: Освобождение специалистов от монотонной работы (написание шаблонного кода, ручное тестирование, сбор данных) позволяет им сосредоточиться на более сложных, творческих и стратегических задачах.

Ускорение циклов разработки: Автоматизация на этапах CI/CD, тестирования и развертывания значительно сокращает путь от идеи до релиза.

Меньше ошибок, выше качество: ИИ-инструменты для анализа кода и предиктивного тестирования помогают выявлять дефекты на ранних стадиях, снижая затраты на их исправление.

Повышение общей эффективности:

Оптимизация ресурсов: AIOps позволяет эффективнее управлять IT-инфраструктурой, сокращая издержки.

Более обоснованные решения: Аналитика на основе ИИ дает глубокие инсайты, способствуя принятию верных стратегических решений.

Улучшенный пользовательский опыт: ИИ помогает персонализировать продукты и услуги, а также обеспечивать более быструю и качественную поддержку.

Снижение рисков: Предиктивный анализ помогает выявлять потенциальные угрозы безопасности и операционные риски.

Трансформация навыков IT-специалиста в эпоху ИИ. Активное внедрение ИИ неизбежно меняет ландшафт востребованных компетенций. Речь идет не о замене людей машинами, а о необходимости адаптироваться и осваивать новые навыки.

Технические "харды":

Понимание ИИ и машинного обучения: Базовые знания в ML/AI нужны для эффективного взаимодействия с ИИ-инструментами.

Data Literacy (грамотность в работе с данными): Умение собирать, обрабатывать, анализировать данные и принимать решения на их основе становится ключевым.

Промпт-инжиниринг: Искусство правильно формулировать запросы к генеративным ИИ-моделям для получения лучших результатов.

Навыки интеграции ИИ-решений: Способность встраивать ИИ-компоненты в существующие системы.

"Мягкие" навыки (Soft Skills):

Критическое мышление: Способность анализировать информацию от ИИ, видеть ее ограничения и использовать для решения сложных задач, которые ИИ пока не по зубам.

Адаптивность и жажда знаний: Технологии ИИ быстро развиваются, требуя постоянного обучения.

Креативность и инновационность: ИИ берет на себя рутину, освобождая время для творческого поиска.

Коммуникация и сотрудничество: Эффективное взаимодействие в командах, где есть и люди, и ИИ.

Этическое понимание ИИ: Осознание последствий использования ИИ, вопросов предвзятости и ответственности.

**Вызовы и перспективы на пути к "умному" IT.** Несмотря на очевидные плюсы, интеграция ИИ в IT-компаниях сопряжена с рядом вызовов: от высокой стоимости некоторых решений и необходимости переобучения персонала до проблем с качеством данных и этических дилемм. Существует и риск чрезмерной зависимости от ИИ.

Однако перспективы связаны с дальнейшим углублением этой интеграции, разработкой более совершенных инструментов и созданием синергии между человеческим интеллектом и возможностями ИИ. Компании, которые смогут эффективно использовать ИИ для усиления своих команд, получат неоспоримое конкурентное преимущество.

Внедрение искусственного интеллекта в рабочие процессы IT-компаний – мощный катализатор роста производительности и эффективности. ИИ-инструменты преображают DevOps, разработку, тестирование и аналитику, автоматизируя рутину и открывая двери для инноваций. Однако для полной реализации этого потенциала нужны не только технологии, но и серьезная трансформация компетенций IT-специалистов. Акцент смещается на навыки работы с данными, понимание ИИ, критическое мышление и готовность учиться всю жизнь.

Успешная адаптация к новой реальности требует от IT-компаний

стратегического подхода к внедрению ИИ, инвестиций в людей и создания культуры, открытой инновациям. Преодолев существующие вызовы, IT-индустрия выйдет на новый уровень эффективности и продолжит свое технологическое лидерство.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство : Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Мелихова, Д. А. Искусственный интеллект для работы с данными / Д. А. Мелихова, О. А. Денисова // Актуальные проблемы технических, естественных и гуманитарных наук : Материалы Международной научно-технической конференции. Памяти В.Х. Хамаева, Уфа, 11–18 ноября 2024 года. – Уфа: УГНТУ, 2024. – С. 366-369. – EDN QWLYOY.

3. Чискидов, С. В. Актуальные вопросы автоматизации бизнес-процессов в it-компании с применением технологий искусственного интеллекта / С. В. Чискидов, Е. М. Тарусин // Открытая наука 2024 : Сборник статей III Всероссийской научной конференции с международным участием, Москва, 01 марта – 30 2024 года. – Москва: Интеллект-Центр, 2024. – С. 265-268. – EDN PWSENM.

4. Ахмедова, М. Р. Специфика использования технологий искусственного интеллекта в IT-отрасли / М. Р. Ахмедова, А. Е. Перова // Журнал прикладных исследований. – 2021. – № 5-1. – С. 17-22. – DOI 10.47576/2712-7516_2021_5_1_17. – EDN JBIZIO.

*УДК 004.8*

***Фонова А.Ю.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ: АНАЛИЗ РИСКОВ УТЕЧКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ С ИИ-СИСТЕМАМИ

Стремительное развитие и глубокая интеграция искусственного интеллекта (ИИ) во все уголки нашей жизни – от повседневного общения с чат-ботами до сложнейших промышленных и медицинских систем – порождают лавину данных. В этом потоке информации проблема конфиденциальности личных сведений встает особенно остро. Взаимодействуя с ИИ-системами, мы часто доверяем им чувствительную информацию, не всегда до конца понимая, как она будет использована, сохранена и защищена. Последствия утечек персональных данных могут быть весьма плачевными: от финансового мошенничества и кражи личности до удара по репутации и дискриминации [1].

Эта статья призвана комплексно проанализировать риски утечки личной информации при работе с ИИ, исследовать, как разработчики обращаются с данными, определить зоны ответственности, а также рассмотреть существующие законы и этические нормы в этой области.

Путь данных в ИИ-системах: где кроются риски утечки**?** Когда мы взаимодействуем с ИИ – будь то генеративная нейросеть типа ChatGPT, голосовой помощник или система распознавания лиц – наши данные проходят несколько этапов, и на каждом из них подстерегают угрозы конфиденциальности:

Сбор данных (наш запрос): Текстовые сообщения, голосовые команды, изображения – все это отправляется на серверы ИИ. Запросы могут содержать как явную (имена, адреса, финансы), так и неявную (предпочтения, привычки, эмоциональное состояние, улавливаемое из контекста) личную информацию.

Риски: Перехват при передаче по незащищенным каналам, сбор избыточных сведений, неосознанное раскрытие нами же чувствительной информации.

Обработка нейросетью: ИИ-модель анализирует полученное для генерации ответа. На этом этапе данные могут временно храниться в

оперативной памяти или кэшироваться.

Риски: Уязвимости в самой ИИ-системе, открывающие доступ к обрабатываемым данным; атаки на модели, позволяющие восстановить часть обучающих данных.

Хранение данных: Разработчики ИИ часто сохраняют наши запросы и ответы. Цели могут быть разными: улучшение моделей, персонализация сервиса, анализ трендов, а иногда и таргетированная реклама.

Риски: Несанкционированный доступ к базам данных (внешние атаки, инсайдеры), ненадлежащие условия хранения (без шифрования, со слабыми паролями), слишком долгое хранение.

Использование для обучения моделей: Наши данные, часто в обезличенном виде, могут пойти на дальнейшее обучение ИИ.

Риски: Деанонимизация (возможность сопоставить "анонимные" данные с конкретным человеком), утечка фрагментов обучающих данных через ответы модели, непреднамеренное "запоминание" моделью конфиденциальной информации.

Политики компаний: что они говорят (и о чем умалчивают) об ответственности за наши данные? Политики конфиденциальности разработчиков ИИ – ключевой документ, информирующий нас о судьбе наших данных. Однако они часто объемны, написаны сложным юридическим языком и не всегда прозрачно отражают все нюансы.

Куда уходят наши запросы? Обычно на удаленные серверы компании-разработчика или облачных провайдеров. География этих серверов может влиять на то, какие законы о защите данных будут применяться.

Что компании делают с данными? Кроме непосредственной обработки запроса, данные могут использоваться для:

Улучшения и тренировки ИИ-моделей.

Персонализации нашего опыта.

Проведения исследований и анализа.

Передачи третьим сторонам (партнерам, рекламодателям) – с нашего согласия или на иных законных основаниях.

Кто в ответе? Как правило, ответственность за утечку или неправомерное использование личных данных несет оператор – компания, определяющая цели и средства их обработки. Но в сложных цепочках (например, при использовании сторонних API) найти ответственного бывает непросто. Ответственность может быть и разделенной [2].

Законы на страже данных: опыт России и мира. Для защиты персональных данных, в том числе при использовании ИИ, существуют

различные нормативные акты.

Европейский Союз (GDPR): Общий регламент по защите данных – один из самых строгих в мире. Он устанавливает жесткие требования к согласию на обработку, правам субъектов данных (доступ, исправление, удаление), принципам "privacy by design" (приватность по умолчанию) и предусматривает серьезные штрафы. GDPR касается всех компаний, обрабатывающих данные граждан ЕС, где бы они ни находились.

Российская Федерация (ФЗ-152): Закон "О персональных данных" регулирует их обработку. Он требует согласия на обработку (за рядом исключений) и обязывает операторов обеспечивать безопасность данных. В последние годы законодательство ужесточается в части локализации данных россиян и ответственности за утечки.

США: Единого федерального закона, подобного GDPR, в США нет. Регулирование носит секторальный (HIPAA для медицины, COPPA для детей) и штатный характер (CCPA/CPRA в Калифорнии). Это создает некоторую фрагментарность.

Другие страны: Многие государства принимают собственные законы о защите данных, часто ориентируясь на принципы GDPR.

Несмотря на наличие законов, их применение к стремительно развивающимся ИИ-технологиям часто наталкивается на трудности: трансграничный характер данных, сложность определения виновных и необходимость адаптировать старые нормы к новым реалиям.

Этика и "черный ящик" ИИ: не только о законах. Помимо права, использование ИИ в контексте личных данных поднимает серьезные этические вопросы:

Прозрачность и объяснимость: Многие ИИ-модели, особенно глубокие нейросети, остаются "черными ящиками" – их решения сложно понять [3]. Это мешает аудиту систем на предвзятость или неправомерное использование данных. Как мы можем доверять тому, чего не понимаем?

Предвзятость (Bias): ИИ, обученный на предвзятых данных, может воспроизводить и усиливать социальные стереотипы. Допустимо ли это при обработке личной информации?

Автономность и контроль: По мере роста "самостоятельности" ИИ-систем, не теряем ли мы контроль над обработкой наших данных и решениями, влияющими на наши права?

Цифровое согласие: Насколько осознанно и добровольно мы даем согласие на обработку наших данных сложной ИИ-системой [4], принципы работы которой нам не до конца ясны?

Как минимизировать риски и повысить защищенность? Снизить

риски утечки личной информации при взаимодействии с ИИ можно только комплексными мерами:

Технические барьеры:

- Шифрование данных при передаче и хранении.
- Анонимизация и псевдонимизация.
- Технологии повышения приватности (PETs): гомоморфное шифрование, дифференциальная приватность, федеративное обучение.
- Регулярный аудит безопасности ИИ-систем.
- Инструменты для обнаружения и предотвращения утечек, специфичные для ИИ.

Организационные шаги:

- Четкие политики конфиденциальности и процедуры обработки данных.
- Обучение сотрудников кибербезопасности и правилам работы с персональными данными.
- Принципы "privacy by design" и "privacy by default" на всех этапах разработки ИИ.
- Ограничение доступа к данным.
- Установление четких сроков хранения и процедур безопасного уничтожения.

Регуляторные и этические инициативы:

- Совершенствование законодательства с учетом специфики ИИ.
- Отраслевые стандарты и сертификации для ИИ-систем.
- Повышение прозрачности работы ИИ и развитие методов объяснимого ИИ (XAI).
- Повышение цифровой грамотности пользователей.

Искусственный интеллект открывает перед нами захватывающие возможности, но его повсеместное внедрение бросает серьезный вызов конфиденциальности наших личных данных. Риски утечки подстерегают на каждом шагу взаимодействия с ИИ – от ввода запроса до хранения и использования данных для обучения моделей. Ответственность за безопасность лежит на разработчиках, но требует активного участия и нас самих, и регуляторов.

Существующие законы, такие как GDPR и ФЗ-152, закладывают фундамент защиты, но нуждаются в постоянной адаптации к технологическим изменениям. Этические вопросы прозрачности, предвзятости и контроля требуют глубокого осмысления.

Минимизировать риски можно лишь комплексным подходом, сочетающим передовые технологии, строгие организационные

процедуры, адекватные законы и высокий уровень цифровой грамотности. Только так мы сможем построить доверие к ИИ-системам и реализовать потенциал этой технологии, не жертвуя фундаментальным правом на неприкосновенность частной жизни.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство: Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Шушаков, А. И. Сохранность конфиденциальности данных в банковской сфере при использовании искусственного интеллекта / А. И. Шушаков, А. Ф. Савдерова // Финансово-кредитный механизм регулирования социально-экономического развития в условиях демографической и структурной трансформации: сборник материалов Всероссийской научно-практической конференции, Чебоксары, 20–21 ноября 2024 года. – Чебоксары: Общество с ограниченной ответственностью «Издательский дом «Среда», 2024. – С. 203-205. – EDN BGGHYB.

3. Бомбин, А. Ю. Конфиденциальность в цифровом мире: цифровой след и роль искусственного интеллекта в защите личных данных / А. Ю. Бомбин // Коммуникации в условиях цифровых изменений : сборник материалов VII Международной научно-практической конференции, Санкт-Петербург, 28–29 ноября 2023 года. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2023. – С. 55-57. – EDN ISYDBF.

4. Милкова, Э. Г. Социальная цена искусственного интеллекта: этика, конфиденциальность данных и другие издержки / Э. Г. Милкова // Теория и практика современной науки. – 2021. – № 5(71). – С. 149-154. – DOI 10.46566/2412-9682_2021_71_149. – EDN AWIRWA.

*УДК 004.8*

***Фонова А.Ю.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ЦИФРОВЫЕ АВАТАРЫ И МЕТАВСЕЛЕННАЯ: КАК ТЕХНОЛОГИИ ИИ МЕНЯЮТ КОММУНИКАЦИЮ И ЦИФРОВУЮ ИДЕНТИЧНОСТЬ

Идея метавселенной – совокупности взаимосвязанных трехмерных виртуальных миров, где мы можем общаться и взаимодействовать через своих аватаров – все сильнее будоражит умы исследователей, разработчиков и широкой публики. Центральным элементом этого нарождающегося цифрового пространства становится наш цифровой аватар – персонифицированное воплощение в виртуальности. Технологии искусственного интеллекта (ИИ), виртуальной (VR) и дополненной (AR) реальности выступают главными двигателями эволюции аватаров: из статичных картинок они превращаются в сложные, динамичные и интерактивные сущности. Это коренным образом меняет то, как мы общаемся, представляем себя и формируем свою цифровую идентичность.

Эта статья призвана проанализировать, как ИИ и иммерсивные технологии трансформируют практики общения и само понятие цифровой идентичности в контексте метавселенных. Мы уделим особое внимание возможностям ИИ в создании персонализированных цифровых двойников, а также сопутствующим рискам, таким как потеря аутентичности и уязвимость перед социальной инженерией [1].

Метавселенные и цифровые аватары: новая реальность взаимодействия. Метавселенная обещает стать следующим поколением интернета, предлагая гораздо более глубокий и интерактивный опыт. В отличие от привычных веб-страниц или соцсетей, метавселенные стремятся создать ощущение настоящего присутствия и совместного переживания. Цифровые аватары – наши главные "представители" и инструменты взаимодействия в этих пространствах. Они не просто картинки, а активные агенты, через которых мы выражаем себя, взаимодействуем с окружением и другими людьми. Технологии VR и AR усиливают эффект погружения, позволяя нам буквально "войти" в цифровой мир и общаться с ним более естественно – жестами, движениями тела, голосом. Эволюция аватаров движется в сторону большей реалистичности, гибкой настройки и интерактивности, что

открывает новые горизонты для общения, обучения, работы и развлечений.

ИИ: "оживляя" цифровых аватаров. Искусственный интеллект играет ключевую роль в переходе к аватарам нового поколения, делая их более личными и правдоподобными.

Создание аватаров: Алгоритмы ИИ способны генерировать уникальные аватары на основе самых разных данных: от фотографий и 3D-сканов до текстовых описаний или даже анализа нашего поведения в сети. Процедурная генерация и глубокое обучение позволяют создавать аватары в любом стиле – от фотореалистичных до мультяшных.

Анимация и поведение: ИИ используется для создания естественной анимации аватаров, включая мимику, жесты и язык тела. Системы могут отслеживать наши движения и выражения лица в реальном времени и переносить их на аватар (как, например, Apple Memoji или NVIDIA Maxine). Более того, ИИ может наделять аватары автономным поведением, позволяя им реагировать на окружение и общаться с другими пользователями или ИИ-персонажами даже без нашего прямого управления.

Персональные цифровые двойники: Одно из самых захватывающих направлений – создание персональных цифровых двойников. Это высокоточные виртуальные копии людей, которые не только похожи внешне, но и способны имитировать манеру речи, поведение, знания и даже процесс принятия решений своего прототипа [2]. Такие двойники могут пригодиться для персонализированного обучения, виртуальной помощи, сохранения цифрового наследия или даже для продолжения социального присутствия после ухода человека. Их создание требует анализа огромных объемов личных данных и сложных моделей машинного обучения.

Общение в метавселенных: трансформация привычного. Интеграция ИИ, VR/AR и продвинутых аватаров качественно меняет то, как мы общаемся:

Иммерсивное и воплощенное взаимодействие: Общение в метавселенной становится более "телесным" (embodied). Мы не просто обмениваемся текстом или видим друг друга на экране, а ощущаем совместное присутствие в общем виртуальном пространстве. Это усиливает невербальные сигналы: пространственный звук помогает определить направление голоса, а выразительные аватары передают эмоции через мимику и жесты, делая общение богаче и естественнее.

Преодоление барьеров: ИИ может помочь стереть языковые барьеры благодаря синхронному переводу речи аватаров. Также

возможно создание инклюзивных сред, где аватары адаптированы для людей с особыми потребностями.

Новые формы самовыражения: Метавселенные дают нам свободу экспериментировать со своей внешностью и идентичностью через аватаров, выходя за физические рамки [3]. Это может способствовать самореализации, но и нести определенные психологические вызовы.

ИИ как посредник в общении: ИИ может быть не только инструментом создания аватаров, но и активным участником или модератором общения, например, управляя неигровыми персонажами (NPC) или предлагая нам варианты ответов.

Вызовы цифровой идентичности: между подлинностью и **обманом**Несмотря на впечатляющие возможности, широкое распространение реалистичных ИИ-аватаров в метавселенных несет серьезные риски для нашей цифровой идентичности и безопасности.

Потеря аутентичности и разрыв с реальностью: Возможность создавать идеализированные или вымышленные аватары может привести к разрыву между физической и цифровой личностью. Это ставит вопросы об аутентичности самопрезентации и может влиять на самооценку (например, через Протей-эффект, когда наше поведение меняется в зависимости от аватара) [2].

Дипфейк-аватары и дезинформация: Технологии ИИ, особенно генеративно-состязательные сети (GAN), позволяют создавать крайне реалистичные дипфейк-аватары для имитации реальных людей без их согласия. Это открывает простор для мошенничества, дезинформации, шантажа и атак на репутацию. В метавселенной отличить поддельный аватар от настоящего будет очень сложно.

Социальная инженерия и манипуляции: Убедительные аватары, управляемые ИИ или злоумышленниками, могут использоваться для изощренных атак социальной инженерии. Они способны втираться в доверие, выманивать конфиденциальную информацию, манипулировать мнениями. Иммерсивность метавселенных лишь усилит психологическое воздействие таких атак.

Кража цифровой идентичности: Цифровые аватары, особенно сложные цифровые двойники, становятся ценной мишенью. Их кража или компрометация чреваты серьезными последствиями, включая финансовые потери и репутационный ущерб [4].

Анонимность и ответственность: Псевдонимность или анонимность, частые в виртуальных мирах, затрудняют проверку личности и привлечение к ответственности за противоправные действия, совершаемые через аватаров.

Этические и регуляторные вопросы: навигация в новом

пространстве. Перед обществом и регуляторами встают непростые этические и правовые вопросы. Нужны этические кодексы для разработчиков ИИ и метавселенных, касающиеся создания и использования аватаров [1]. Важны прозрачность (мы должны понимать, общаемся ли с человеком или ИИ), право на цифровую идентичность, защита персональных данных, используемых для "оживления" аватаров, и механизмы борьбы со злоупотреблениями. Требуется обсудить, кому принадлежат цифровые аватары и двойники, и кто несет ответственность за их действия.

Технологии ИИ, VR и AR коренным образом меняют ландшафт цифрового общения и наше понимание цифровой идентичности через эволюцию аватаров в метавселенных. Они открывают захватывающие перспективы для более глубокого, выразительного и персонализированного взаимодействия. Создание реалистичных цифровых двойников с помощью ИИ расширяет границы нашего присутствия в цифровом мире.

Однако эти достижения неотделимы от значительных рисков: от потери аутентичности и возможности создания неотличимых дипфейк-аватаров до новых угроз для безопасности цифровой идентичности. Для гармоничного развития метавселенных и минимизации негативных последствий нужен комплексный подход: разработка этических стандартов, совершенствование законов, создание надежных механизмов верификации и защиты, а также повышение цифровой грамотности пользователей. Дальнейшие междисциплинарные исследования должны помочь нам глубже понять психологические, социальные и технологические аспекты этой нарождающейся цифровой эры.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство: Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Феклушин, А. В. Цифровой аватар: продолжение личности или «кривое зеркало»? / А. В. Феклушин // Тенденции развития науки и образования. – 2025. – № 117-1. – С. 178-180. – DOI 10.18411/trnio-01-2025-48. – EDN RRPLZW.

3. Павлова, К. А. Цифровая идентичность сквозь призму цифровой памяти / К. А. Павлова // Современная идентичность в условиях глобальных вызовов: Сборник материалов международной научно-практической конференции, Санкт-Петербург, 29 ноября – 01 2023 года. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2024. – С. 152-158. – EDN QLLTDI.

4. Артамонов, Д. С. Цифровая идентичность в контексте цифровой памяти / Д. С. Артамонов // Цифровой ученый: лаборатория философа. – 2023. – Т. 6, № 1. – С. 16-23. – DOI 10.32326/2618-9267-2023-6-1-16-23. – EDN THGFIS.

***УДК 004.8***

***Фонова А.Ю.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИНТЕГРАЦИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС СТУДЕНТОВ ВУЗОВ: ВОЗМОЖНОСТИ, ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Стремительное развитие информационных технологий, особенно нейросетей и искусственного интеллекта (ИИ), меняет наш мир. Проникая во все сферы, ИИ преобразует и систему образования, открывая новые горизонты и одновременно ставя перед ней непростые задачи. Генеративные ИИ-модели, такие как ChatGPT для работы с текстом, MidJourney для создания изображений и Copilot для помощи в программировании, все активнее входят в арсенал студентов. Это ставит на повестку дня вопрос системной интеграции этих технологий в образовательный процесс вузов, а также требует глубокого анализа сопутствующих возможностей, вызовов и долгосрочных перспектив.

В этой статье мы комплексно рассмотрим потенциал и проблемы внедрения нейросетевых технологий в образовательную среду высших учебных заведений.

Как нейросети могут трансформировать учебный процесс? Внедрение нейросетевых технологий (ННТ) в учебный процесс вузов сулит значительные выгоды, способствуя повышению его эффективности и качества.

Персонализация обучения: Инструменты на базе нейросетей, в частности чат-боты на основе больших языковых моделей (LLM) вроде ChatGPT, могут подстраиваться под индивидуальный темп и стиль

обучения каждого студента. Они способны стать персонализированными тьюторами: объяснять сложные темы, отвечать на вопросы 24/7, генерировать дополнительные учебные материалы и тесты разной сложности. Это помогает студентам глубже осваивать материал и закрывать пробелы в знаниях в удобное им время [2].

Поддержка исследовательской деятельности: ChatGPT и аналогичные системы – ценные помощники в исследованиях. Они могут содействовать в формулировании исследовательских вопросов и гипотез, участвовать в обзоре литературы, помогать структурировать научную работу и анализировать большие объемы данных. Это позволяет студентам сэкономить время на рутине и сосредоточиться на творческой и аналитической составляющих исследования.

Развитие ИТ-компетенций: Такие инструменты, как GitHub Copilot, интегрируемые в среды разработки, предлагают контекстно-зависимые подсказки, автодополнение кода и даже генерацию целых функций по описанию. Это не только ускоряет написание кода, но и служит эффективным образовательным ресурсом, позволяя студентам наглядно осваивать лучшие практики и новые подходы в программировании.

Визуализация и креатив: Нейросети для генерации изображений (например, MidJourney, DALL-E) открывают новые горизонты для визуализации абстрактных концепций, создания иллюстраций к проектам, презентациям и научным статьям. Это улучшает понимание материала и развивает креативное мышление, особенно в дизайне, архитектуре, маркетинге и искусстве.

Автоматизация рутины и обратная связь: ННТ способны взять на себя автоматическую проверку некоторых типов заданий (тестов, простых программ), обеспечивая быструю обратную связь. Это разгружает преподавателей, давая им больше времени для индивидуальной работы со студентами и более глубокого погружения в сложные аспекты преподавания.

Какие вызовы и риски несет «переход на ИИ» в образовании? Однако, несмотря на очевидные плюсы, повсеместное внедрение ННТ несет и серьезные риски, требующие вдумчивого подхода.

Академическая добросовестность и плагиат: Легкость, с которой генеративные ИИ создают тексты, код или изображения, вызывает серьезные опасения по поводу плагиата и самостоятельности выполнения работ. Существующие антиплагиат-системы не всегда справляются с выявлением ИИ-сгенерированного контента, что требует разработки новых подходов к оценке знаний [3].

Угроза критическому мышлению: Чрезмерная опора на ИИ как на

источник готовых ответов рискует ослабить у студентов навыки самостоятельного анализа информации, поиска решений и развития критического мышления. Появляется риск "поверхностного" усвоения материала, когда ответ получен без понимания глубинных принципов.

Достоверность ИИ-контента: Несмотря на прогресс, нейросети могут выдавать неточную, предвзятую или даже ложную информацию (так называемые "галлюцинации" ИИ). Студентам необходим высокий уровень медиаграмотности и критического мышления для оценки достоверности данных, полученных от ИИ.

Новая роль преподавателя и потребность в переподготовке: Интеграция ИИ требует от педагогов новых навыков: умения встраивать ИИ-инструменты в учебные программы, разрабатывать задания, стимулирующие критическое мышление в условиях доступности ИИ. Преподаватель все больше становится наставником и фасилитатором, а не просто транслятором знаний. Это диктует необходимость масштабных программ повышения квалификации.

Этические дилеммы: Применение ИИ в образовании ставит этические вопросы, связанные с конфиденциальностью студенческих данных, возможной предвзятостью алгоритмов (bias) и ответственностью за решения, принятые на основе рекомендаций ИИ [1].

Как образовательной системе адаптироваться: перспективы и стратегии. Чтобы успешно и эффективно интегрировать нейросетевые технологии в высшее образование, нужны комплексные стратегии адаптации.

Развитие ИИ-грамотности: Важно включать в учебные программы модули, формирующие у студентов и преподавателей понимание принципов работы ННТ, их возможностей, ограничений и этических аспектов использования.

Новые подходы к оценке: Акцент следует сместить с проверки запоминания фактов на оценку умения критически мыслить, решать нестандартные задачи, применять знания на практике и эффективно взаимодействовать с ИИ-инструментами. Решением может стать внедрение проектной деятельности, устных экзаменов, заданий, требующих рефлексии и анализа процесса работы с ИИ.

Этические ориентиры и руководства: Вузам стоит разработать четкие правила и рекомендации по использованию ННТ в учебном процессе, определяющие границы допустимого применения ИИ и меры ответственности за нарушения академической этики.

ИИ как помощник, а не замена: ННТ стоит рассматривать как вспомогательные инструменты, расширяющие возможности

преподавателя и студента, а не как полную замену традиционным методам или человеческому взаимодействию. Крайне важно сохранить ценность личного общения, дискуссий и наставничества.

Поддержка исследований в области ИИ в образовании: Необходимо активно поддерживать научные изыскания, направленные на изучение эффективности различных моделей интеграции ИИ, разработку новых педагогических подходов и инструментов для безопасного и продуктивного использования ННТ [4].

Внедрение нейросетей вроде ChatGPT, MidJourney и Copilot в образовательный процесс вузов действительно открывает впечатляющие возможности для персонализации обучения, повышения его эффективности и развития компетенций, востребованных в XXI веке. Однако этот путь сопряжен с серьезными вызовами, включая риски для академической честности, необходимость развития критического мышления в новых условиях и трансформацию роли преподавателя.

Будущий успех образования с ИИ во многом зависит от готовности образовательной системы проактивно адаптироваться к изменениям. Это означает разработку новых педагогических подходов, этических норм и стратегий обучения, которые позволят максимально использовать потенциал нейросетей, минимизируя сопутствующие риски. Ключевой момент – формирование культуры ответственного и осознанного использования ИИ, где технология служит инструментом для углубления знаний и развития человеческого потенциала, а не его подмены.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е.П., Фонова, А. Ю. Этические аспекты искусственного интеллекта в сфере информационных технологий / А. Ю. Фонова, Е. П. Коломыцева // Образование. Наука. Производство: Сборник докладов XV Международного молодежного форума, Белгород, 23–24 октября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 374-378. – EDN AORBSY.

2. Борисова, И. В. Образование 2.0: как искусственный интеллект меняет правила игры в образовании? / И. В. Борисова // Наука молодых: вызовы гуманитарной науки: материалы Всероссийской научной школы с международным участием для молодых исследователей, Абакан, 19–21 сентября 2024 года. – Абакан: Федеральное государственное бюджетное образовательное учреждение высшего

профессионального образования "Хакасский государственный университет им. Н.Ф. Катанова", 2024. – С. 24-28. – EDN VXGLKR.

3. Доненко, О. Л. Искусственный интеллект в образовании как фактор, повышающий качество образования / О. Л. Доненко, И. Л. Доненко, Е. М. Байбагышов // Наука и творчество: вклад молодежи : Сборник материалов IV всероссийской молодежной научно-практической конференции студентов, аспирантов и молодых ученых, Махачкала, 08–09 ноября 2023 года. – Махачкала: Типография ФОРМАТ, 2023. – С. 22-24. – EDN FICBES.

4. Сизов, Л. А. Инновационный прорыв применения искусственного интеллекта в профессиональном образовании в рамках цифровизации образования / Л. А. Сизов // Вестник МПА ВПА (сборник научных трудов). – 2024. – № 2(6). – С. 34-36. – EDN PUXQVA.

***УДК 004.896***

***Фролов О.С.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УПРАВЛЕНИИ ИНТЕЛЛЕКТУАЛЬНЫМИ СИСТЕМАМИ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Всем известно, что искусственный интеллект (ИИ) находит все большее применение в различных отраслях промышленности. Искусственный интеллект играет важную роль в управлении сложными системами, такими как системы автоматизированного проектирования (САПР) и автоматические системы управления (АСУ). Эти системы обеспечивают значительные преимущества в скорости, эффективности и точности и становятся неотъемлемой частью современного производственного процесса. Интеллектуальные САПР и АСУ позволяют автоматизировать сложные процессы проектирования и управления, сократить время разработки изделий и повысить надежность производства.

ИИ привносит в эти системы самообучение и адаптивность, значительно повышая их возможности и позволяя решать задачи, которые раньше требовали значительных человеческих ресурсов. В данной статье рассматривается применение ИИ в САПР, АСУ и робототехнике, описываются преимущества и недостатки этих систем,

примеры их использования на практике и потенциал для дальнейшего развития.

Системы автоматизированного проектирования (САПР) давно стали важным инструментом для инженеров и дизайнеров, поскольку они позволяют автоматизировать рутинные задачи, такие как создание чертежей и 3D-моделей. Однако традиционные САПР требуют значительного вмешательства человека на каждом этапе процесса, что повышает риск ошибок и замедляет процесс. Внедрение искусственного интеллекта в САПР позволило создать интеллектуальные системы, которые могут самостоятельно анализировать данные, выявлять закономерности и оптимизировать процесс проектирования. Это позволило создать интеллектуальные системы, способные самостоятельно анализировать данные, выявлять закономерности и оптимизировать процесс проектирования. (Рис. 1)

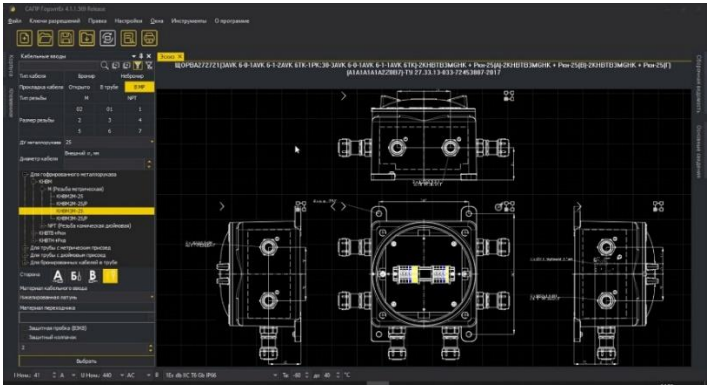


Рис. 1: Технология создания моделей в САПР.

Интеллектуальные системы автоматизированного проектирования с искусственным интеллектом обладают рядом важных преимуществ

Самообучение и адаптация: используя методы машинного обучения, такие системы могут обучаться на основе предыдущих проектов, предлагая оптимальные решения и сокращая количество ошибок. Например, система может автоматически корректировать чертежи и схемы, если в аналогичных проектах были обнаружены ошибки.

Анализ данных: интеллектуальные системы автоматизированного проектирования могут анализировать большие объемы данных, включая результаты предыдущих проектов, параметры материалов и информацию о производственных мощностях. Такой анализ позволяет

системе генерировать улучшенные решения и находить новые подходы к проектированию.

Оптимизация ресурсов: одно из главных преимуществ ИИ в САПР - возможность оптимизировать использование материальных и производственных ресурсов. Программа может предложить наиболее эффективные методы производства и материалы, помогая снизить производственные затраты и уменьшить количество отходов.

Автоматические системы управления (АСУ) играют важную роль в современном производстве, контролируя работу технологического оборудования и процессы. Традиционные системы автоматического управления основаны на жестко закодированных алгоритмах, которые являются негибкими и не всегда способны реагировать на изменение условий производства. Интеграция искусственного интеллекта в автоматические системы управления может повысить их адаптивность, надежность и эффективность. ИИ в системах автоматического управления позволяет системам не только отслеживать параметры оборудования, но и прогнозировать возможные сбои, оптимизировать работу машин и адаптироваться к изменяющимся условиям. Например, методы глубокого обучения могут использоваться для анализа огромных объемов данных, собранных с датчиков, и на основе этого анализа предсказывать отказы оборудования задолго до их возникновения. (Рис 2)

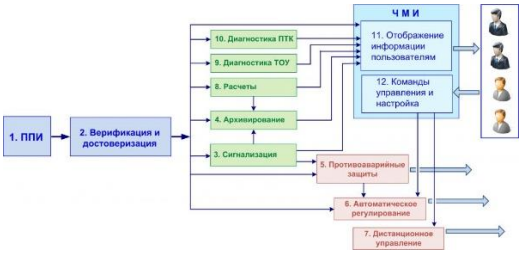



Рис. 2 Концептуальная схема АСУ с искусственным интеллектом.

Основные функции АСУ с искусственным интеллектом:

Прогнозирование неисправностей и отказов: анализируя данные о состоянии оборудования, ИИ может выявлять отклонения от нормы и предотвращать аварии. Это особенно важно для дорогостоящего оборудования, простой которого может привести к значительным убыткам.

Оптимизация работы оборудования: системы управления с поддержкой ИИ могут анализировать состояние оборудования в режиме реального времени и предлагать изменения в режимах работы для

повышения эффективности. Например, скорость машины можно регулировать в зависимости от нагрузки или условий окружающей среды.

Адаптация к изменениям: условия производства часто меняются, поэтому АСУ должны быть гибкими; системы ИИ могут адаптироваться к этим изменениям и настраивать оборудование без вмешательства человека.

Примером использования ИИ в АСУ является интеграция систем управления на предприятиях по производству электроники. Там важно поддерживать стабильные условия работы с высокой точностью и требованиями к качеству; ИИ может помочь оптимизировать процессы пайки, сборки и контроля изделий, снизить риск ошибок и повысить производительность (рис. 2).

Робототехника - одна из самых быстроразвивающихся областей, где ИИ играет важную роль. Современные промышленные роботы могут выполнять широкий спектр задач, от сборки и сварки до упаковки и контроля качества. Однако традиционные роботы ограничены жесткими алгоритмами, которые не могут адаптироваться к изменениям в рабочей среде. ИИ открывает новые возможности в робототехнике, позволяя создавать роботов, которые могут обучаться и адаптироваться в режиме реального времени.

Примеры применения ИИ в робототехнике включают:

1. Обучение роботов новым навыкам: с помощью технологий глубокого обучения и машинного зрения роботы могут обучаться новым задачам без необходимости перепрограммирования. Это особенно полезно на производственных линиях, где задачи часто меняются.

2. Работа с людьми: интеллектуальные роботы могут работать с людьми, анализируя их поведение и адаптируя свои движения для совместной работы с оператором. Это повышает безопасность и снижает нагрузку на оператора.

Будущий потенциал использования ИИ в САПР и АСУ очень велик. В ближайшем будущем ИИ будет все глубже интегрироваться в производственные процессы, что приведет к созданию полностью автономных систем, способных управлять производством без вмешательства человека. Эти системы будут не только следить за работой оборудования, но и предлагать решения для повышения качества продукции, оптимизации производственных процессов и снижения затрат.

В то же время одной из главных проблем, стоящих перед разработчиками таких систем, является безопасность и надежность ИИ. Поскольку системы становятся все более автономными, важно

обеспечить их защиту от сбоев и внешних угроз. Также основной проблемой является отсутствие продвинутого интеллектуального обеспечения для формирования проекта АСУ. Основные проблемы, возникающие при создании такой САПР. К их числу относятся: раз работка реляционных баз данных проектной информации, дополнительный предметный сервис к графическому ядру САПР, ИТ технологии генерации отчетных форм с использованием баз данных, разработка управляющей про Современные технологии. Системный анализ.

Использование искусственного интеллекта в системах автоматизированного проектирования и управления - важный шаг на пути к совершенствованию производственных процессов. Интеллектуальные САПР, АСУ и робототехника открывают новые возможности для оптимизации производства, повышения эффективности и снижения затрат. Ожидается, что в будущем эти технологии будут еще более востребованы и сыграют важную роль в развитии промышленности.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стативко Р. У., Пентюк С. И., Тетюхин А. О. Подходы к разработке модуля генераторов тестовых заданий и модуля адаптивного тестирования для поддержки учебного процесса в режиме онлайн // Информатизация образования и науки. 2021, № 4. С. 178-185

2. Боровский А. В., Сачков Д. И. Методы и алгоритмы разработки САПР для проектирования автоматизированных систем управления технологическими процессами // Современные технологии. Системный анализ. Моделирование № 3 (51) 2016, С. 119-126

3. Стативко Р. У., Коломыцева Е. П. Разработка алгоритмов определения необходимости использования типовых моделей датчиков // Известия Юго-Западного государственного университета. 2018, № 6. С. 118-126

*УДК 004.514.4*

***Фролов О.С.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ВСПЛЫВАЮЩЕЕ МЕНЮ И НИСПАДАЮЩЕЕ МЕНЮ В ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСАХ

В современной разработке программного обеспечения ключевым аспектом является создание удобных и интуитивных пользовательских интерфейсов. Пользовательский интерфейс — это все, что помогает людям управлять устройствами и программами с помощью голоса, нажатий, жестов и через командную строку. К пользовательскому интерфейсу относится «Меню». Меню – набор опций, отображаемых на экране, где пользователи могут выбирать и выполнять действия, тем самым, производя изменения в состоянии интерфейса. Достоинство меню в том, что пользователи не должны помнить на звание элемента или действия, которое они хотят выполнить, а должны только распознать его среди пунктов меню. Таким образом, меню может использовать даже неопытный пользователь. Однако проект меню должен быть тщательно продуман – чтобы меню было эффективным, названия пунктов меню должны быть очевидными. Меню может занимать много экранного места, но есть решение для этой проблемы – использование всплывающего или ниспадающего меню. При нажатии на иконку, строку меню или другой объект вызывается всплывающее или ниспадающее меню. Элементы интерфейса, такие как всплывающие и ниспадающие меню, играют важную роль в человеко-машинном взаимодействии (ЧМВ), улучшая навигацию и повышая эффективность взаимодействия пользователя с системой. Эти меню позволяют структурировать и скрывать информацию до тех пор, пока она не понадобится пользователю, что особенно важно в условиях ограниченного пространства экрана. В данной статье обсуждаются различия между всплывающими и ниспадающими меню, их преимущества, недостатки и особенности проектирования.

Всплывающее меню — это элемент интерфейса, который появляется по запросу пользователя, обычно при нажатии правой кнопки мыши или длительном нажатии на сенсорных устройствах. Оно предоставляет контекстно-зависимые действия, которые применимы к текущему объекту или операции, что помогает пользователю быстрее ориентироваться в функционале системы. (Рис. 1)

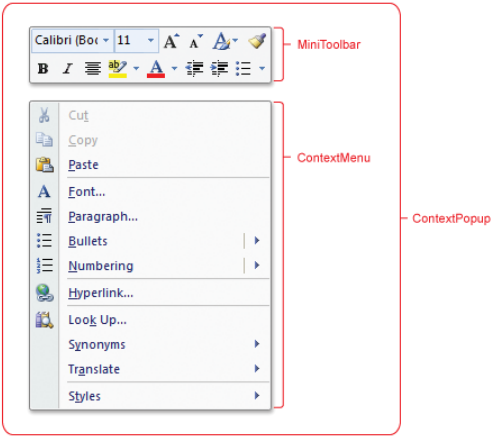



Рис. 1 Всплывающее меню

Всплывающие меню активно используются в различных системах, от операционных систем до специализированных приложений. Например, в текстовых редакторах всплывающее меню позволяет быстро получить доступ к функциям копирования, вставки, форматирования и редактирования текста. Это существенно сокращает количество необходимых шагов для выполнения задачи.

Кроме того, всплывающие меню широко применяются в графических редакторах, таких как Adobe Photoshop и GIMP, где они дают возможность мгновенно выбирать инструменты или изменять параметры, не переходя к основному меню программы. Подобные решения повышают продуктивность работы, позволяя сосредоточиться на выполнении основной задачи без необходимости отвлекаться на поиск функций в основном интерфейсе.

Одним из главных преимуществ всплывающего меню является его контекстная зависимость. Оно отображает только те опции, которые необходимы в текущий момент, что сокращает информационную нагрузку на пользователя. Пользователь может быстро найти нужную функцию, не отвлекаясь на ненужные опции, что делает интерфейс более интуитивным.

Однако у всплывающих меню есть и недостатки. Например, если их неправильно спроектировать, они могут быть слишком перегруженными или не интуитивными, что затруднит работу. Правильное проектирование всплывающего меню требует минимализма и логичности. Каждая опция должна быть связана с

конкретным действием пользователя, а количество элементов должно быть минимальным, чтобы не перегружать интерфейс. Например, для контекстного меню текстового редактора целесообразно включить только те функции, которые непосредственно касаются работы с текстом — копирование, вставка, изменение шрифта, и т.д. Исследования также показали, что всплывающие меню должны появляться мгновенно, без задержек, и иметь четкую визуальную структуру. Это помогает пользователям быстро находить нужные опции.

Ниспадающее меню представляет собой элемент интерфейса, который раскрывается при взаимодействии с главным элементом, таким как кнопка или строка меню. В отличие от всплывающего, ниспадающее меню открывается сверху вниз и позволяет пользователю выбрать одну из заранее скрытых опций. (Рис. 2)

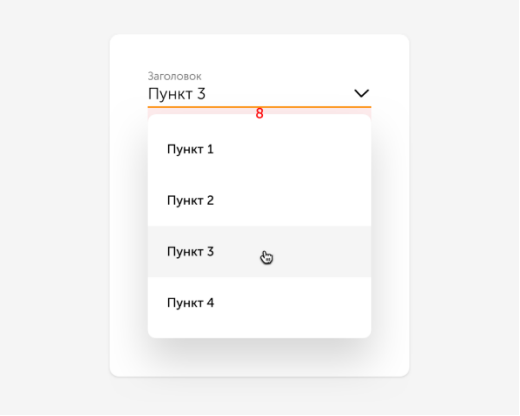



Рис. 2 Ниспадающее меню

Ниспадающие меню находят широкое применение в веб-дизайне и мобильных приложениях. Например, на сайтах оно используется для организации навигации, скрывая менее важные ссылки и отображая их только тогда, когда пользователь взаимодействует с соответствующим разделом. Это позволяет сохранить чистоту интерфейса и избежать перегруженности, что особенно важно при работе с небольшими экранами мобильных устройств.

Примером может служить меню на сайтах электронной коммерции, где пользователь может выбирать категории товаров, а затем более детализированные подкатегории, которые раскрываются по мере необходимости. Это улучшает пользовательский опыт, предоставляя доступ к большому количеству информации без лишней сложности.

Ниспадающее меню позволяет значительно экономить пространство в интерфейсе, что является важным преимуществом, особенно для мобильных устройств и адаптивных веб-сайтов. Оно скрывает большое количество опций, пока пользователь не инициирует его раскрытие, что делает интерфейс более упорядоченным и менее нагруженным.

Однако одно из главных ограничений ниспадающего меню заключается в том, что его содержание не всегда очевидно для пользователя до момента раскрытия. Как отмечает Иванов (2021), если меню слишком глубокое или сложное, пользователь может потеряться и потратить больше времени на поиск нужной опции.

Проектирование ниспадающего меню требует особого внимания к деталям. Одной из главных задач является обеспечение плавности его раскрытия и закрытия, чтобы пользователи не испытывали дискомфорта при работе с интерфейсом. Важно также обеспечить доступность всех элементов меню для пользователей с различными устройствами, включая тех, кто использует клавиатуру или сенсорные экраны.

Исследования показали, что хорошо спроектированное ниспадающее меню должно открываться мгновенно и содержать логически сгруппированные элементы. Это уменьшает когнитивную нагрузку на пользователя и улучшает восприятие интерфейса в целом.

Оба типа меню — всплывающее и ниспадающее — играют важную роль в улучшении пользовательского опыта. Всплывающее меню предоставляет более контекстуально зависимые функции, что ускоряет доступ к нужным инструментам. Ниспадающее меню, напротив, помогает сохранить чистоту интерфейса, скрывая менее важные элементы до момента их необходимости.

Элементы интерфейса, такие как всплывающие и ниспадающие меню, играют важную роль в создании удобных и эффективных человеко-машинных интерфейсов. Их грамотная реализация позволяет улучшить эргономику системы и повысить удовлетворённость пользователей. Будущие разработки в области ЧМВ должны учитывать изменения в потребностях пользователей и возможности современных технологий, что позволит создавать более интуитивные и адаптивные интерфейсы.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Батенькина О.В. Дизайн пользовательского интерфейса информационных систем // Минобрнауки, ОмГТУ. – Омск: Изд-во ОмГТУ, 2014. С. 35-36

2. Анастасия Свеженцева Что такое пользовательский интерфейс // UxJournal
3. Меню и контекстные меню // Microsoft Learn

***УДК 004***

***Худяков М.В.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## CI/CD И МОНИТОРИНГ: АВТОМАТИЗАЦИЯ ЦИФРОВЫХ ЭКОСИСТЕМ

Мир цифровых технологий меняется стремительно, предъявляя новые вызовы к тому, как мы создаем и поддерживаем программное обеспечение. Эпоха громоздких монолитных приложений с их долгими циклами выпуска постепенно уходит в прошлое. На смену приходят распределенные системы, микросервисная архитектура, облачные платформы и необходимость частых обновлений. В таких условиях классические подходы к управлению жизненным циклом ПО (SDLC) теряют свою актуальность. Возникает острая потребность в методологиях и практиках, которые позволили бы не только ускорить доставку ценности конечному пользователю, но и одновременно повысить надежность и стабильность работающих систем.

Именно для решения этих задач и возникла философия DevOps. В ее основе лежит идея тесного сотрудничества между командами разработки (Dev) и эксплуатации (Ops), а также повсеместное внедрение автоматизации на всех этапах жизненного цикла ПО. Практическим воплощением принципов DevOps стали такие подходы, как непрерывная интеграция (Continuous Integration, CI), непрерывное развертывание или доставка (Continuous Delivery/Deployment, CD) и всесторонний мониторинг. Эти практики призваны устранять "бутылочные горлышки", снижать риски, связанные с внедрением изменений, и обеспечивать ясное понимание состояния всей цифровой экосистемы.

В данной работе мы рассмотрим, как взаимосвязаны CI/CD и мониторинг, какой синергетический эффект дает их совместное внедрение, и почему автоматизация является ключевым фактором успеха при эксплуатации современных цифровых систем.

Непрерывная интеграция (CI) – это подход к разработке, при котором программисты регулярно, порой несколько раз в сутки,

вливают результаты своей работы в общий кодовый репозиторий. Каждое такое изменение немедленно и автоматически проверяется: запускается сборка проекта и прогоняется набор тестов. Главная цель CI – обнаруживать и устранять проблемы интеграции как можно раньше и чаще. Это позволяет избежать так называемого "интеграционного ада" и снизить риски, связанные со слиянием больших объемов кода от разных разработчиков.

Для успешной реализации CI-процесса необходимы несколько ключевых компонентов. Во-первых, это система контроля версий (VCS), где Git стал фактически стандартом, предоставляя возможности для параллельной работы и удобного слияния изменений. Во-вторых, важна автоматизированная сборка – процесс компиляции кода и формирования артефактов (например, Docker-образов, JAR-файлов), который запускается автоматически при каждом коммите или создании пулл-реквеста. Третьим неотъемлемым элементом является автоматизированное тестирование, включающее модульные и интеграционные тесты, а также статический анализ кода с помощью линтеров и анализаторов безопасности. Эти тесты должны выполняться быстро и автоматически после каждой успешной сборки. Наконец, всем этим оркестрирует сервер CI – специализированное программное обеспечение (например, Jenkins, GitLab CI, GitHub Actions, CircleCI), которое отслеживает изменения в VCS, запускает сборку и тесты, а также уведомляет команду о результатах.

Польза от внедрения CI несомненна: ошибки обнаруживаются на ранних стадиях, качество кода улучшается, время на отладку сокращается, а разработчики чувствуют большую уверенность в своем коде и его готовности к развертыванию. Таким образом, CI подготавливает почву для следующего важного шага – непрерывного развертывания.

Идеи CI находят свое логическое продолжение в непрерывной доставке (Continuous Delivery). В этом случае каждое изменение, успешно прошедшее все автоматизированные тесты в рамках CI, считается готовым к развертыванию в производственную среду. Однако сам момент развертывания может потребовать ручного одобрения со стороны ответственного лица. Следующим уровнем автоматизации является непрерывное развертывание (Continuous Deployment). Здесь каждое изменение, прошедшее все этапы конвейера (включая автоматизированные тесты на промежуточных средах), автоматически попадает в производственную среду без какого-либо ручного вмешательства. Такой подход требует очень высокого уровня автоматизации и глубокого доверия ко всему выстроенному процессу.

Типичный конвейер CD обычно строится из последовательности этапов. Все начинается с получения готового артефакта из CI-системы. Затем следует автоматизированное развертывание на тестовые или staging-среды. После этого выполняются более длительные и комплексные тесты, такие как нагрузочные, приемочные или сквозные. В случае Continuous Deployment далее происходит автоматизированное развертывание в производственную среду. Важными поддерживающими процессами являются управление конфигурацией инфраструктуры и приложений (с помощью инструментов вроде Ansible, Chef, Puppet, Terraform) и управление средами выполнения (например, Kubernetes для контейнеризированных приложений).

Главный выигрыш от CD заключается в скорости и надежности поставки новых функций и исправлений. Сокращение времени от написания кода до его появления у конечных пользователей позволяет быстрее реагировать на потребности бизнеса и получать обратную связь. Автоматизация самого процесса развертывания также значительно снижает вероятность ошибок, связанных с человеческим фактором.

Когда изменения внедряются так часто, как это происходит при использовании CI/CD, особенно остро встает вопрос непрерывного отслеживания состояния работающей системы. Именно мониторинг дает возможность видеть и понимать, что происходит с приложением и инфраструктурой в реальном времени. Он становится неотъемлемой частью процесса эксплуатации и формирует важнейший канал обратной связи для всего цикла CI/CD.

Объектами наблюдения при мониторинге служат различные аспекты системы. Это и метрики производительности приложений, такие как время отклика, пропускная способность, количество ошибок, использование ресурсов (CPU, память), а также показатели работы баз данных. Не менее важны метрики инфраструктуры, отражающие состояние серверов, сетевого оборудования, облачных сервисов и систем хранения данных. Огромный пласт информации содержат логи – системные журналы, журналы приложений и безопасности, фиксирующие события и ошибки. Наконец, для оценки эффективности важны бизнес-метрики и показатели пользовательского опыта, например, число активных пользователей, конверсия, время загрузки страниц и доступность ключевых функций.

Современные системы мониторинга (например, Prometheus с Grafana, ELK Stack, Zabbix, Nagios, а также коммерческие решения вроде Datadog или New Relic) собирают, хранят и визуализируют эти данные, а также генерируют оповещения о проблемах. Благодаря

мониторингу удается оперативно обнаруживать проблемы и сбои, оценивать влияние изменений, внесенных через CI/CD, на производительность и стабильность. Он также помогает планировать ресурсы, анализируя тренды их использования, лучше понимать поведение пользователей и эффективность бизнес-процессов, и, что крайне важно, формировать обратную связь для команд разработки о необходимости оптимизации или исправления ошибок.

Весь потенциал CI/CD и мониторинга проявляется тогда, когда они интегрированы и образуют единый, автоматизированный цикл обратной связи. Мониторинг не просто пассивно "наблюдает" за системой, развернутой через CD; он активно участвует в процессах разработки и эксплуатации.

Влияние мониторинга на CI/CD многогранно. Во-первых, это раннее обнаружение проблем в production: если мониторинг выявляет снижение производительности или сбои после развертывания, это немедленно становится сигналом для команд разработки, инициируя создание новых задач, которые затем проходят через CI/CD конвейер. Во-вторых, в продвинутых CD-конвейерах данные мониторинга могут запускать автоматический откат к предыдущей стабильной версии при значительном ухудшении показателей. Кроме того, мониторинг абсолютно необходим при канареечных релизах и A/B-тестировании, позволяя оценить стабильность и эффективность новой версии на небольшой группе пользователей. Наконец, информация о нагрузке и "узких местах", полученная из систем мониторинга, помогает командам разработки оптимизировать код и архитектуру, а эти улучшения снова проходят через CI/CD.

В свою очередь, CI/CD также способствует эффективному мониторингу. Автоматизированное внедрение средств мониторинга, таких как агенты, экспортеры метрик и конфигурации логирования, может стать частью CD-конвейера. Применение инфраструктуры как кода (IaC) позволяет включать настройку систем мониторинга непосредственно в скрипты развертывания. Версионирование конфигураций мониторинга через системы контроля версий обеспечивает согласованность и аудит. Более того, в рамках пайплайна CI/CD можно даже проводить тестирование самого мониторинга, проверяя корректность сбора метрик или генерации оповещений.

Такое тесное взаимодействие CI/CD и мониторинга формирует мощную петлю обратной связи. Разработка и эксплуатация получают немедленную информацию о влиянии своих действий на "живую" систему, что позволяет быстро адаптироваться, исправлять проблемы и непрерывно улучшать как сам продукт, так и процессы его создания.

Красной нитью через все практики CI/CD и мониторинга проходит идея автоматизации. Без нее реализация этих подходов в масштабах современных сложных систем была бы попросту невозможна. В CI автоматизируются сборка, тестирование и анализ кода, сокращая время обратной связи для разработчика до минут. В CD автоматизация охватывает развертывание, управление конфигурацией и оркестрацию сред, что позволяет выполнять развертывания часто и надежно. В сфере мониторинга автоматизируются сбор метрик, агрегация логов, анализ данных, генерация оповещений и даже автоматическое реагирование, обеспечивая непрерывную видимость без ручного вмешательства.

Беря на себя рутинные, повторяющиеся и подверженные ошибкам задачи, автоматизация высвобождает время инженеров для решения более сложных и творческих проблем, связанных с архитектурой, оптимизацией и внедрением инноваций. Она делает процессы предсказуемыми, воспроизводимыми и масштабируемыми.

Путь внедрения CI/CD и мониторинга не всегда гладок. Основные трудности включают культурные изменения, необходимые для перехода к DevOps, и сложность самого инструментария, требующего усилий для настройки и поддержки. Вопросы безопасности также стоят остро, так как конвейер CI/CD может стать вектором атаки, что диктует необходимость его защиты и внедрения практик DevSecOps. Кроме того, распределенные системы генерируют огромные объемы данных мониторинга, требующие мощных систем для их обработки.

Взгляд в будущее показывает, что развитие этих областей будет идти по пути дальнейшей автоматизации и активного применения технологий искусственного интеллекта и машинного обучения (AIOps). AIOps призваны анализировать данные мониторинга, предсказывать проблемы, автоматически выявлять аномалии и даже самостоятельно принимать решения. Также набирает силу концепция "наблюдаемости" (Observability), которая фокусируется не только на заранее определенных метриках, но и на возможности глубоко исследовать систему в ответ на любой возникающий вопрос.

Можно с уверенностью сказать, что CI/CD и мониторинг – это фундаментальные элементы современных подходов к разработке и эксплуатации цифровых систем. Непрерывная интеграция и развертывание обеспечивают скорость, гибкость и надежность поставки изменений. В то же время мониторинг предоставляет необходимую прозрачность для понимания состояния системы, оценки влияния этих изменений и оперативного реагирования на возникающие проблемы. При этом автоматизация служит тем стержнем, который делает все эти процессы масштабируемыми и по-настоящему эффективными.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Веретенников, О. В. Модули для Opencart: цели использования, распространенность, экономическая выгода / О. В. Веретенников, К. Ю. Станиславская // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 21-24. – EDN XBIKYO.

2. Ампилогов, Н. С. Типовая структура API социальных сетей / Н. С. Ампилогов // Альманах научных работ молодых ученых Университета ИТМО : Материалы XLVI научной и учебно-методической конференции, Санкт-Петербург, 31 января – 03 2017 года. Том 4. – Санкт-Петербург: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2017. – С. 4-6. – EDN LXXIMH.

3. Прохоров, П. В. Современные подходы в backend разработке на примере онлайн-магазина / П. В. Прохоров, Н. В. Разговоров // Прикладная математика и фундаментальная информатика. – 2020. – Т. 7, № 2. – С. 23-28. – DOI 10.25206/2311-4908-2020-7-2-24-29. – EDN HUGGWY.

4. Зотова, Ю. А. Разработка архитектуры rest api для взаимодействия с сервисами приложения / Ю. А. Зотова, И. Д. Котилевец // Информационные технологии и математическое моделирование систем 2018 : труды международной научно-технической конференции, Одинцово, 19–21 ноября 2018 года. – Одинцово: Федеральное государственное бюджетное учреждение науки Центр информационных технологий в проектировании Российской академии наук, 2018. – С. 61-65. – EDN PLVMYQ.

5. Savant R. V. Cloud-Native CDN Monitoring Using CI/CD / R. V. Savant, S. N. Sunder, S. Seshadri, N. Panda, S. M. Rajagopal // 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) : Conference proceedings. Kamand, India. — 2024. — P. 1–9. DOI: 10.1109/ICCCNT61001.2024.10724159.

*УДК 004*

***Худяков М.В.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# ВЕБ-САЙТ ЦИФРОВЫХ ЭКОСИСТЕМ И БОТ TELEGRAM КАК ИНСТРУМЕНТЫ РАЗВИТИЯ БИЗНЕСА

За последние годы цифровая трансформация из модного тренда превратилась в насущную необходимость для обеспечения устойчивого роста и конкурентоспособности компаний. Современные технологии все активнее используются предприятиями для оптимизации взаимодействия с клиентами, автоматизации бизнес-процессов и расширения каналов продаж. Среди множества доступных решений особое место занимают два элемента: веб-сайт как сердце цифровой инфраструктуры и Telegram-бот как эффективный инструмент прямой коммуникации. Их грамотное объединение позволяет создать гибкую и целостную систему, отвечающую запросам современного динамичного рынка.

Понятие "цифровая экосистема" описывает сложную сеть взаимосвязанных элементов – пользователей, платформ, сервисов и данных. Эта система обеспечивает бесперебойный обмен информацией, позволяет автоматизировать операции и предоставлять клиентам персонализированные услуги. Хорошо известным примером является платформа Alibaba, где покупатели, продавцы, службы логистики и платежные системы функционируют в рамках единого цифрового пространства. В центре такой экосистемы, как правило, находится веб-сайт, выполняющий роль основного входа, главного канала общения и ключевой коммерческой площадки.

Функционал сайта сегодня выходит далеко за рамки простой "визитки". Он служит инструментом для привлечения клиентов, осуществления продаж, сбора аналитических данных и организации технической поддержки. Возможность интеграции с CRM-системами, ERP-платформами, мессенджерами и прочими инструментами превращает его в центральный узел цифровой инфраструктуры компании. К примеру, крупные онлайн-ритейлеры используют свои сайты не только для демонстрации ассортимента, но и для контроля запасов, обработки заказов и сбора детальной обратной связи. Такой комплексный подход повышает прозрачность и скорость выполнения ключевых бизнес-операций.

Однако в условиях жесткой конкуренции и постоянно растущих ожиданий потребителей одной лишь веб-платформы часто оказывается недостаточно. Пользователи стремятся к максимально быстрому и удобному способу взаимодействия, что делает актуальным использование мессенджеров. Telegram, в частности, завоевал популярность в бизнес-среде благодаря своей открытой архитектуре API и широким возможностям для разработки. Создавая собственных ботов, компании могут автоматизировать клиентский сервис, предоставлять необходимую информацию мгновенно и упрощать процедуру оформления заказа.

Telegram-боты представляют собой специализированные программы, имитирующие диалоговое общение с пользователем. Спектр задач, которые они способны решать, весьма широк – от ответов на типовые вопросы до осуществления платежей. Например, банк "Открытие" успешно внедрил Telegram-бота для оперативного уведомления клиентов о транзакциях и состоянии счетов. Это решение не только снизило нагрузку на их контакт-центр, но и повысило уровень удовлетворенности клиентов. Другой распространенный пример – использование чат-ботов в службах доставки еды, где они помогают отслеживать заказы и информируют об актуальных акциях.

Объединение функционала веб-сайта и Telegram-бота открывает перед бизнесом новые перспективы. Сайт может мягко перенаправлять посетителей в мессенджер для более детального взаимодействия или получения оперативной информации, в то время как бот, наоборот, способен отправлять пользователю ссылки на конкретные страницы сайта или предлагать перейти в веб-интерфейс для завершения покупки или иной целевой операции. Такая двусторонняя связь позволяет сохранять полный контекст общения и опираться на единую базу данных о клиенте. Представьте: пользователь начал искать товар на сайте, а затем продолжил консультацию с ботом в Telegram, при этом вся история его запросов и просмотренных товаров сохраняется.

Техническая реализация подобного взаимодействия обычно включает использование API (интерфейсов программирования приложений), вебхуков и облачных сервисов. Разработчики могут применять различные технологии, такие как Node.js или Python, а также платформы типа Firebase или специализированные конструкторы ботов вроде Botpress и ManyChat. Эти инструменты обеспечивают необходимую гибкость при создании интерактивных интерфейсов и позволяют легко масштабировать решение при росте нагрузки. Крайне важно также уделять пристальное внимание вопросам безопасности передачи данных и неукоснительному соблюдению законодательных

норм, например, требований GDPR.

Оценить эффективность внедрения таких комплексных решений можно по ряду показателей: времени реакции на обращения клиентов, коэффициенту конверсии, числу повторных покупок и общей степени удовлетворенности пользователей. Согласно исследованию, проведенному Statista, применение чат-ботов способно сократить затраты на клиентскую поддержку до 30%, а также значительно увеличить скорость выполнения ряда стандартных операций.

Особую ценность синергия веб-сайта и Telegram-бота представляет для малого и среднего бизнеса, где ограниченные ресурсы требуют максимальной эффективности от каждого внедряемого инструмента. Создание единого цифрового пространства взаимодействия становится здесь ключевым фактором успеха.

Давайте проиллюстрируем это на конкретном примере. Представьте онлайн-школу. На её сайте пользователи регистрируются, выбирают курс, оплачивают его и получают доступ к учебным материалам. Однако в процессе обучения у них часто возникают типовые вопросы: уточнение расписания, порядок сдачи домашних заданий, поиск дополнительных материалов. Обработка этих запросов требует времени менеджеров или преподавателей, увеличивая их загрузку.

Внедрение Telegram-бота позволяет автоматизировать значительную часть такой коммуникации. После регистрации на сайте ученик получает ссылку на чат-бота, через которого ему приходят уведомления о начале занятий, где он может отправлять выполненные задания, задавать вопросы по материалам и даже проходить небольшие тесты. Более того, бот способен направлять пользователя обратно на сайт для выполнения действий, требующих авторизации или расширенного интерфейса, например, просмотра видеолекций или скачивания методичек.

Подобная интеграция становится возможной благодаря использованию API. Сайт передает боту необходимые данные о пользователе и его прогрессе, которые хранятся, например, в облачной базе данных. Это обеспечивает единую точку доступа к информации и гарантирует её согласованность. Такая модель взаимодействия не только качественно улучшает пользовательский опыт, но и способствует оптимизации операционных расходов.

Еще один показательный пример – компания, занимающаяся доставкой товаров. Клиент оформляет заказ на сайте, а затем получает в Telegram серию полезных уведомлений: подтверждение принятия заказа, расчетное время доставки, номер телефона курьера и даже

ссылку на карту с его текущим местоположением. Такая прозрачность процесса существенно повышает доверие клиента и снижает поток звонков в службу поддержки с типовыми вопросами.

Критически важно отметить, что успех внедрения подобных решений зависит не только от совершенства технической части, но и от качества проработки пользовательского интерфейса бота. Он должен быть интуитивно понятным, предоставлять максимально четкие и полезные ответы, а также уметь распознавать запросы, сформулированные естественным языком. Для этого активно используются технологии обработки естественного языка (NLP).

Исследования, в частности отчет McKinsey, подтверждают экономическую целесообразность такого подхода: использование ИИ в клиентской коммуникации может снизить затраты на поддержку до 30%, одновременно повысив уровень удовлетворенности клиентов примерно на 20%. Таким образом, интеграция ботов становится не просто вопросом удобства, но и эффективным бизнес-решением.

Вместе с тем, необходимо принимать во внимание и ряд потенциальных ограничений. Во-первых, не все сегменты аудитории или пользователи в определенных регионах активно пользуются Telegram. Во-вторых, существует риск зависимости от политики сторонней платформы: изменения в API или даже возможная блокировка сервиса могут создать проблемы. В-третьих, поддержание актуальности и функциональности бота требует регулярных усилий по обновлению и тестированию.

Тем не менее, при условии тщательного планирования и качественной реализации, объединение мощностей веб-сайта и гибкости Telegram-бота становится по-настоящему сильным инструментом в арсенале цифровой стратегии. Особенно это актуально для тех отраслей, где высокая скорость реакции, круглосуточная доступность и максимальное удобство для клиента являются ключевыми конкурентными преимуществами.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Веретенников, О. В. Модули для Opencart: цели использования, распространенность, экономическая выгода / О. В. Веретенников, К. Ю. Станиславская // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 21-24. – EDN XBIKYO..

2. Люлюченко, М. В. Автоматизация бизнес-процессов как условие экономического развития предприятия / М. В. Люлюченко, А. А. Рябов // Наукоемкие технологии и инновации : сборник докладов международной научно-практической конференции, Белгород, 06–07 октября 2016 года / Белгородский государственный технологический университет им. В.Г. Шухова. Том Часть 8. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2016. – С. 64-69. – EDN WBBYYD..

3. Третьякова, Н. В. Автоматизация бизнес-процессов / Н. В. Третьякова, А. И. Солодовников // Теория и практика современной аграрной науки : Сборник V национальной (всероссийской) научной конференции с международным участием, Новосибирск, 28 февраля 2022 года. – Новосибирск: Издательский центр Новосибирского государственного аграрного университета "Золотой колос", 2022. – С. 1717-1720. – EDN RJJHNW.

4. Тимофеев, К. Д. Чат-боты для бизнеса / К. Д. Тимофеев // ВУЗ и реальный бизнес. – 2017. – Т. 1. – С. 32-38. – EDN ZAPCTD.

5. Новиков, Д. А. Механизмы функционирования многоуровневых организационных систем / Д. А. Новиков. – Москва, 1999. – 161 с. – EDN PFGVGV.

***УДК 004***

***Худяков М.В.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## АРХИТЕКТУРА ЦИФРОВОЙ ЭКОСИСТЕМЫ: КАК СВЯЗАТЬ САЙТ, TELEGRAM-БОТА И ОБЩУЮ БАЗУ ДАННЫХ

В условиях сегодняшнего высококонкурентного рынка и стремительного развития технологий компании сталкиваются с насущной необходимостью выстраивать единое цифровое пространство для взаимодействия с клиентами. Простая онлайн-презентация уже не удовлетворяет пользователей – они требуют комплексного подхода, охватывающего все привычные каналы: от веба до мессенджеров и мобильных приложений. Создание по-настоящему слаженной цифровой экосистемы, где ключевые компоненты – веб-сайт, Telegram-бот и центральное хранилище данных – работают как единое целое, становится одним из наиболее действенных ответов на этот вызов. Этот подход существенно повышает эффективность работы с информацией

и, главное, качество обслуживания клиентов.

Что же такое цифровая экосистема? По сути, это комплекс взаимосвязанных элементов, позволяющий бизнесу бесперебойно функционировать в цифровой среде. Обычно она включает клиентские интерфейсы, серверную логику и, конечно, основную базу данных. Самое важное при ее проектировании – заложить принципы единообразия данных, стандартизации процессов и достаточно высокой гибкости архитектуры, чтобы система могла легко адаптироваться к изменениям.

Представьте пользователя: он регистрируется на сайте, делает заказ, получает важные уведомления через Telegram, а затем, возможно, возвращается на сайт в свой личный кабинет для просмотра истории покупок. Чтобы такой пользовательский путь был действительно гладким и бесшовным, критически важно, чтобы все части системы работали с одним и тем же актуальным набором данных и следовали общим правилам их обработки.

Чтобы все эти сервисы функционировали как единое целое, был реализован подход с использованием общего программного интерфейса (API), который предоставляет централизованный бэкенд-сервис. Это решение позволило полностью исключить дублирование бизнес-логики и четко определить роль каждого компонента: сайт – основной канал взаимодействия; Telegram-бот – инструмент для оперативной связи и быстрых уведомлений; база данных – центральный, неоспоримый источник истины обо всех сущностях (клиентах, заказах, товарах и т.п.). Такая архитектура заметно упрощает масштабирование, поддержку и повышает устойчивость к изменениям.

Сердцевина всей системы, безусловно, централизованная база данных. Она служит единым хранилищем всей информации. При выборе конкретной СУБД (системы управления базами данных) ключевыми факторами стали надежность, производительность и возможность легко масштабироваться по мере роста. В результате мы остановились на PostgreSQL – мощной и чрезвычайно гибкой системе, отлично справляющейся со сложными запросами, JSON и даже геоданными.

Особое внимание при проектировании структуры базы уделялось вопросам синхронизации данных между разными точками взаимодействия. Например, предусмотрен механизм связывания пользовательского аккаунта на сайте с его профилем в Telegram, используя специальное поле telegram_id. Это гениально простое решение позволяет системе мгновенно узнавать одного и того же пользователя, независимо от того, через какой канал он к нам пришел,

поддерживая единый контекст общения и гарантируя по-настоящему бесшовный пользовательский опыт.

Сам веб-сайт выступает как главный пользовательский интерфейс, предоставляя полный доступ к каталогу, процессу оформления заказов, управлению личным профилем и отслеживанию статусов. Важно отметить, что его серверная часть (бэкенд) построена как REST API. Это означает, что вся логика и данные доступны через стандартизированный набор вызовов, которым пользуются не только сайт, но и другие элементы экосистемы.

Проектирование API велось строго по принципам RESTful, что обеспечивает его стандартизированность и предсказуемость взаимодействия. Все действия выполняются привычными HTTP-запросами, а ответы приходят в универсальном формате JSON. Такая структура делает API чрезвычайно гибким и позволяет легко подключать к нему не только веб-интерфейс, но и любых других потребителей, например, наш Telegram-бот.

Telegram-бот – незаменимый инструмент для повышения вовлеченности пользователей и обеспечения оперативного отклика. Он активно используется для мгновенной рассылки уведомлений, быстрого приема обращений, проведения опросов или предоставления актуальной информации по запросу. Благодаря своим возможностям и открытости, Telegram давно стал популярной платформой для автоматизации коммуникаций с клиентами.

Ключевой момент – интеграция бота в общую информационционную среду происходит через те же самые API-эндпоинты, что и для сайта. Это решение полностью исключает дублирование бизнес-логики, значительно упрощает техническое сопровождение и делает всю систему в целом надежнее. Как уже упоминалось, здесь тоже реализована функция связывания аккаунтов, что позволяет поддерживать единый контекст взаимодействия и предлагать по-настоящему персонализированный сервис.

Одной из принципиально важных задач было построение единой системы идентификации, позволяющей пользователю абсолютно беспрепятственно переключаться между разными частями экосистемы, не теряя свой профиль и контекст. Зарегистрироваться можно как через сайт, так и прямо через Telegram, где идентификатором выступает уникальный ID мессенджера. Достигается это за счет хитрого, но эффективного решения: в таблице пользователей предусмотрено специальное поле telegram_id, которое связывает аккаунт в нашей системе с Telegram-профилем. Результат? Даже если пользователь не посещает сайт месяцами, он по-прежнему может полноценно

взаимодействовать с системой через мессенджер, получать уведомления и использовать доступные функции.

Безопасность данных – это, без преувеличения, краеугольный камень нашей системы. Учитывая, что мы работаем с личной, а иногда и финансовой информацией, предусмотрена многоуровневая система защиты. Она включает надежную аутентификацию пользователей (с использованием токенов), строгий контроль прав доступа к API, повсеместное шифрование передаваемых данных, тщательную валидацию всех входящих запросов и, конечно, защищенное хранение критически важных ключей и конфигураций. Вся передача данных осуществляется исключительно по защищенным протоколам, а доступ к самым чувствительным операциям жестко регулируется. Весь этот комплекс мер призван максимально снизить риски несанкционированного доступа и укрепить доверие наших пользователей.

Ключевым моментом при развертывании стал подход, ориентированный на максимальную скорость ввода в эксплуатацию и простоту последующего масштабирования. Основные компоненты – бэкенд и веб-сайт – были изначально развернуты на одном сервере (физическом или виртуальном), используя Nginx как обратный прокси для маршрутизации запросов. Сам Telegram-бот работает как совершенно отдельный сервис, что обеспечивает его независимость и отказоустойчивость. Для автоматизации всего жизненного цикла разработки – от коммита кода до продакшена (CI/CD) – мы активно задействовали инструменты типа GitHub Actions. Это позволило не только существенно ускорить процесс выпуска обновлений, но и повысить общую надежность и предсказуемость системы.

Одним из самых заметных преимуществ нашей архитектуры является заложенный в нее потенциал к масштабированию. По мере увеличения нагрузки мы можем без труда добавлять новые серверные мощности, внедрять системы очередей сообщений для эффективной обработки фоновых задач или подключать специализированные платформы для глубокой аналитики данных. Но это не предел! В перспективе экосистема легко может быть дополнена мобильным приложением, интегрирована с устройствами интернета вещей, CRM-системами или любыми другими внешними сервисами. Такой подход позволяет еще глубже встроить цифровые процессы в бизнес и открыть новые горизонты для автоматизации и персонализации взаимодействия.

Таким образом, построение цифровой экосистемы, объединяющей веб-сайт, Telegram-бот и единую базу данных, уже давно перешагнуло рамки чисто технической задачи. Это, по сути, стало одним из

важнейших стратегических шагов для любого бизнеса, стремящегося к успешной цифровой трансформации. Такая система не только заметно улучшает качество обслуживания клиентов и ускоряет реакцию на их запросы, но и помогает оптимизировать операционные расходы. Ключ к успеху здесь – продуманная архитектура, централизация данных, использование унифицированного API и построение бесшовной системы авторизации. Все это вместе создает по-настоящему гибкую, устойчивую и легко масштабируемую платформу, способную оперативно адаптироваться к меняющимся условиям рынка. Особенно ценен такой подход для малого и среднего бизнеса. Он открывает доступ к передовым цифровым инструментам без необходимости строить громоздкую инфраструктуру с нуля, делая инвестиции в цифровое будущее компании вполне оправданными и перспективными.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Веретенников, О. В. Модули для Opencart: цели использования, распространенность, экономическая выгода / О. В. Веретенников, К. Ю. Станиславская // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 21-24. – EDN XBIKYO.

2. Никитин, И. В. Сравнение подходов монолитной архитектуры и микросервисной архитектуры при реализации серверной части веб-приложения / И. В. Никитин, Т. Ю. Гриценко // Дневник науки. – 2020. – № 3(39). – С. 22. – EDN TTOGCE.

3. Бегунов, И. С. Автоматизация онлайн-бизнеса с помощью чат-ботов / И. С. Бегунов, А. В. Ботиенко // Инновации, технологии и бизнес. – 2024. – № 2(16). – С. 11-18. – EDN IWFFVL.

4. Саакян, Р. Р. Разработка интерактивной системы поддержки научных исследований в виде единой информационной платформы / Р. Р. Саакян, И. А. Шпехт // Вестник ИМСИТ. – 2015. – № 2(62). – С. 58-60. – EDN UHGYKH.

*УДК 004*

***Худяков М.В.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# СЕРДЦЕ ЦИФРОВОЙ ЭКОСИСТЕМЫ РАЗРАБОТКА БЭКЕНДА ДЛЯ СЕТИ КОФЕЕН И ВЕНДИНГА

В наш цифровой век, когда без технологий шагу не ступить, идея связать кофейни и вендинговые аппараты в одну общую сеть выглядит вполне себе здравой. Нужен сайт, чтобы клиент мог неспешно полистать меню и сделать выбор. Telegram-бот — для тех, кто вечно спешит и заказывает на лету. И, конечно, админка — чтобы владельцы бизнеса и партнеры-франчайзи могли всем этим хозяйством эффективно управлять. Снаружи эти инструменты могут выглядеть по-разному, но чтобы вся эта конструкция заработала как часы, им необходим единый «мозг» — система, которая будет обрабатывать запросы, надежно хранить данные и реализовывать всю бизнес-логику. Этот «мозг» и есть то, что мы называем бэкендом.

Именно в бэкенде и разворачивается вся невидимая глазу магия: создаются учетные записи, обрабатываются заказы, начисляются баллы по программе лояльности и — что особенно важно для нас — строятся мосты к другим системам. Будь то сами вендинговые автоматы или уже установленные в кофейнях POS-терминалы. А то, что для этой серверной части мы выбрали Java со Spring Boot и старый добрый PostgreSQL, – это не случайность. Такой стек обеспечивает и производительность, и адаптивность, и пространство для маневра на перспективу, для всех наших будущих идей.

Давайте заглянем под капот: из чего же состоит этот бэкенд, который дирижирует всем нашим цифровым оркестром?

Пользователи: кто есть кто и как сделать их счастливыми

Любой сервис, стремящийся наладить контакт с клиентом, первым делом должен позаботиться о грамотном управлении его аккаунтом. Бэкенд берет на себя эту непростую задачу: с момента регистрации нового пользователя и до хранения всех его предпочтений и управления правами доступа.

Клиент регистрируется через сайт или бота — бэкенд тут же подхватывает эти данные, пароль надежно шифрует (хеширует, разумеется, никаких открытых текстов!) — и всё это аккуратно укладывает в базу PostgreSQL. Когда пользователь входит в систему,

бэкенд сверяет предоставленные им данные с хранящимися, и если всё сходится — выдает своего рода «пропуск» (например, JWT-токен). Этот токен потом и сайт, и бот предъявляют бэкенду при каждом обращении, чтобы тот понимал, с кем имеет дело, и не заставлял человека каждый раз вводить логин и пароль.

Но и это еще не всё. Бэкенд — это еще и хранитель всех пользовательских «сокровищ»: контактной информации, истории заказов, любимых напитков и накопленных бонусов. Клиентские приложения могут запрашивать эти данные через API, но вот изменять их или проверять на корректность — это уже сугубо серверная задача. Так мы можем быть уверены, что всё в целости и сохранности. Здесь на сцену выходит Spring Security (часть Spring Boot), который здорово облегчает жизнь, разбираясь с аутентификацией, разграничением прав (кто обычный пользователь, кто администратор, а кто франчайзи) и защитой API.

Заказы: от «хочу кофе» до «заказ готов»

Для клиента главное – чтобы заказ оформлялся легко и без проволочек. И здесь бэкенд – ключевая фигура, он дирижирует всем процессом от А до Я:

Заявка поступает: Клиент выбирает напиток в меню на сайте или в боте, указывает точку получения и желаемое время – вся эта информация улетает на бэкенд через специальный интерфейс API (о котором мы уже упоминали, говоря о его проектировании).

Система проверяет, всё ли в порядке: Бэкенд анализирует: есть ли такая позиция в меню? Существует ли указанная точка выдачи? Реально ли приготовить заказ к этому времени (если это актуально)? Достаточно ли у клиента средств или бонусов?

Расчеты, скидки, бонусы: Если проверка прошла успешно, бэкенд рассчитывает итоговую сумму, учитывая все возможные скидки и бонусы.

Сохранение в базу: Детали заказа со всей подноготной и текущим статусом (например, «Новый») отправляются на хранение в PostgreSQL.

Держим в курсе: Бэкенд может дать команду Telegram-боту, чтобы тот уведомил клиента о принятии заказа. Параллельно информация о новом заказе может уйти на кухню или в административную панель.

Смена статусов – все оповещены: Заказ принят в работу, приготовлен, выдан – при каждом изменении статус на бэкенде обновляется (часто это происходит через админку или кассовый аппарат), и клиент тут же видит эти изменения через API.

Подводный камень здесь – необходимость виртуозно управляться с множеством статусов заказа, корректно обрабатывать отмены и

изменения, и при этом следить, чтобы данные на бэкенде и у клиента всегда (или почти всегда) совпадали. Spring Boot с его способностью обрабатывать HTTP-запросы и Spring Data JPA для взаимодействия с базой данных здесь как нельзя кстати.

Бонусы и плюшки: как превратить клиентов в друзей

В наши дни одними продажами сыт не будешь – нужно выстраивать отношения с покупателями. И программа лояльности – это тот самый инструмент, который помогает укрепить эту связь. И вся эта бонусная механика – целиком и полностью забота бэкенда.

Он точно знает, как начислять бонусы (например, какой процент от суммы чека или сколько баллов за определенное действие). Заказ успешно выполнен – бэкенд немедленно начисляет клиенту его «плюшки» и обновляет баланс в базе данных. Клиент хочет использовать накопленное при новом заказе – бэкенд проверяет, достаточно ли бонусов, и списывает их, прежде чем подтвердить оплату.

Кроме того, бэкенд ведет подробный учет всех бонусных операций – когда начислили, когда списали. Эту историю клиент может просмотреть через API, чтобы видеть все свои накопления. И вот тут критически важно, чтобы все эти операции с бонусами работали как швейцарские часы – без сбоев, чтобы бонусы не начислились или не списались дважды (особенно если связь прервалась в момент оплаты). Без транзакционных возможностей Spring и PostgreSQL здесь не обойтись, чтобы избежать казусов.

Интеграции: женим «цифру» с «железом»

А теперь к самому любопытному (и, не будем скрывать, порой самому заковыристому) – это как подружить наш бэкенд с реальным миром, особенно с такими устройствами, как вендинговые автоматы и уже работающие кассы в кофейнях.

С вендинговыми автоматами: Тут бэкенд может взаимодействовать по-разному, всё зависит от возможностей самих аппаратов. Либо он просто «слушает» их сигналы (как дела, есть ли кофе, сколько продано), либо даже сам отдает им команды (вроде, «приготовь кофе вот этому господину, он уже оплатил через приложение»). Нередко приходится, так сказать, «шаманить» со всякими специфическими протоколами (MDB/ICP, проприетарные API, MQTT – чего только не встретишь), которые бэкенд должен понимать. Его задача – перевести язык автомата на понятный системе (и обратно), а также связать событие у автомата с конкретным пользователем в нашей системе (например, по QR-коду или номеру).

С POS-системами: Если в кофейне уже функционирует своя

кассовая система (POS), бэкенд должен найти с ней общий язык. Например, обмениваться меню и ценами, передавать заказы с сайта или бота на кухню, а также синхронизировать данные о продажах и, что очень важно, информацию по программе лояльности. Если клиент на кассе тратит или накапливает бонусы, POS-система должна сообщить об этом бэкенду, чтобы тот обновил баланс. Обычно это реализуется через API или обмен файлами, для чего на стороне бэкенда приходится разрабатывать специальные «адаптеры».

С платежными системами: С приемом платежей тоже своя история. Клиент оплачивает заказ через сайт или бота, но «за кулисами» бэкенд обращается к платежному шлюзу, ожидает от него ответ (часто через webhook) и только после подтверждения успешной транзакции меняет статус заказа. Это и безопаснее (ключи доступа к платежной системе хранятся на сервере, а не у клиента), и надежнее.

PostgreSQL и Spring Data JPA: наши верные хранители данных

Почему наш выбор пал на PostgreSQL? Все просто: он надежен, отлично справляется со сложными запросами, поддерживает транзакции и готов к масштабированию, когда это потребуется. А Spring Data JPA – это вообще отдельная песня. Разработчику не нужно глубоко погружаться в написание SQL-запросов; он работает с данными почти как с обычными объектами в коде. Это ускоряет разработку и делает код чище. И, само собой, грамотно спроектированная схема базы данных (таблицы для пользователей, заказов, меню, бонусов, кофеен и т.д.) – это фундамент, от которого зависит скорость и гибкость всей системы.

В итоге: мощный двигатель для сложного механизма

Спроектировать бэкенд для такой масштабной системы, как цифровая экосистема для кофеен и вендинга, – это все равно что создать сердце для живого, сложного организма. Ведь именно там сосредоточена вся ключевая бизнес-логика, там хранятся данные о пользователях, заказах, бонусах, и именно бэкенд связывает все компоненты воедино. Использование Java Spring Boot и PostgreSQL дает нам прочную основу не только для текущих задач, но и для будущего роста. От качества реализации этого ядра напрямую зависит, будет ли вся цифровая инфраструктура работать стабильно, будет ли она удобна для пользователей и эффективна для бизнеса. Словом, грамотно выстроенный бэкенд – это и есть тот самый двигатель, без которого вся эта амбициозная цифровая затея попросту не полетит.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Веретенников, О. В. Модули для Opencart: цели использования, распространенность, экономическая выгода / О. В. Веретенников, К. Ю. Станиславская // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 21-24. – EDN XBIKYO.

2. Прохоров, П. В. Современные подходы в backend разработке на примере онлайн-магазина / П. В. Прохоров, Н. В. Разговоров // Прикладная математика и фундаментальная информатика. – 2020. – Т. 7, № 2. – С. 23-28. – DOI 10.25206/2311-4908-2020-7-2-24-29. – EDN HUGGWY.

3. Денисов, А. А. Современные средства разработки сайтов / А. А. Денисов // Вестник Воронежского института высоких технологий. – 2019. – № 2(29). – С. 68-71. – EDN MKPIWE.

4. Готская И. Б., Васильченко А. Д. Анализ клиентских фреймворков для разработки веб-приложений //Инновации. Наука. Образование. — 2022. Режим доступа: https://www. elibrary. ru (дата обращения: 23.04. 24).



***УДК 004***



***Худяков М.В.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ И ИНФРАСТРУКТУРЫ В КОНТЕКСТЕ ЦИФРОВОЙ ЭКОСИСТЕМЫ: ПРИНЦИПЫ И МЕТОДЫ ЗАЩИТЫ

Современная цифровая экосистема представляет собой сложную, постоянно меняющуюся и тесно взаимосвязанную среду. Она объединяет множество участников, разнообразные платформы, многочисленные сервисы и непрерывные потоки данных. В основе жизнедеятельности любой такой экосистемы лежит активный обмен информацией и взаимодействие различных компонентов инфраструктуры. В условиях неуклонно растущих киберугроз, обеспечение надежной защиты данных и критически важных элементов инфраструктуры превращается из чисто технической задачи в

необходимое условие устойчивости, доверия и самой жизнеспособности всей экосистемы. Утечки конфиденциальной информации, сбои в работе сервисов или компрометация инфраструктуры способны нанести непоправимый ущерб репутации, привести к значительным финансовым потерям и нарушению законодательных требований. Данная работа посвящена анализу ключевых принципов и методов обеспечения безопасности в рамках цифровой экосистемы, охватывая такие важные аспекты, как шифрование данных, управление доступом (включая аутентификацию и авторизацию), защита от различных видов кибератак и обеспечение безопасности межсистемных взаимодействий через интерфейсы программирования приложений (API).

Особенности цифровой экосистемы порождают ряд уникальных сложностей в области обеспечения безопасности. Прежде всего, это гетерогенность и распределенность: экосистема часто включает в себя множество различных технологий, платформ, как унаследованных, так и облачных систем, принадлежащих разным организациям или их подразделениям. Такое разнообразие существенно затрудняет применение единых и последовательных политик безопасности. Кроме того, интенсивный обмен данными, когда большие объемы чувствительной информации перемещаются между компонентами экосистемы, значительно увеличивает потенциальную поверхность атаки. Динамичность среды, выражающаяся в постоянном добавлении новых сервисов, участников и интеграций, требует создания гибкой и адаптивной системы безопасности, способной быстро реагировать на изменения. Нельзя забывать и о зависимости от третьих сторон, ведь безопасность всей экосистемы во многом определяется уровнем защищенности ее наименее защищенного участника. Наконец, сложность управления идентификацией и доступом обусловлена необходимостью предоставлять различным участникам и сервисам доступ к определенным ресурсам, что требует внедрения продуманных механизмов аутентификации и авторизации.

Успешное противостояние этим вызовам требует многоуровневого подхода к безопасности, который бы охватывал как защиту самих данных, так и защиту инфраструктуры, через которую эти данные передаются, хранятся и обрабатываются.

Шифрование является фундаментальным инструментом защиты информации, обеспечивающим ее конфиденциальность и, при использовании соответствующих криптографических механизмов, целостность. В контексте цифровой экосистемы шифрование должно применяться на различных уровнях и этапах жизненного цикла данных.

Крайне важно обеспечивать шифрование данных при их хранении (Encryption at Rest). Это касается защиты информации, находящейся на постоянных носителях – в базах данных, файловых хранилищах или облачных контейнерах. Такой подход критически важен для предотвращения несанкционированного доступа в случае физической кражи носителей или компрометации систем хранения. Могут применяться как методы полного шифрования диска (FDE - Full Disk Encryption), так и шифрование на уровне отдельных файлов или баз данных с использованием надежных алгоритмов, таких как AES. При этом управление ключами шифрования (Key Management) становится отдельной и весьма значимой задачей, требующей использования специализированных систем, например, аппаратных модулей безопасности (HSM - Hardware Security Modules) или облачных сервисов управления ключами.

Не менее важным является шифрование данных при их передаче (Encryption in Transit). Это подразумевает защиту информации во время ее перемещения по сетям, в том числе между различными компонентами экосистемы. Основными протоколами для обеспечения безопасности передачи данных служат TLS/SSL (Transport Layer Security / Secure Sockets Layer), которые широко используются для защиты HTTP-трафика (обеспечивая HTTPS), а также других протоколов, таких как FTPS или SMTPS. Внутри частных сетей или при обмене данными между центрами обработки данных могут использоваться виртуальные частные сети (VPN) с шифрованием на сетевом уровне, например, с применением IPsec. Шифрование при передаче эффективно предотвращает перехват и изменение данных злоумышленниками.

Применение сильных, проверенных временем криптографических алгоритмов и протоколов, а также выстраивание надежного процесса управления жизненным циклом ключей шифрования являются обязательными элементами комплексной стратегии безопасности данных в любой цифровой экосистеме.

Контроль доступа к ресурсам и данным внутри экосистемы реализуется посредством механизмов аутентификации и авторизации.

Аутентификация (Authentication) – это процесс проверки и подтверждения подлинности субъекта (будь то пользователь, сервис или устройство), который запрашивает доступ. В условиях распределенной экосистемы применяются разнообразные методы аутентификации. Классическим методом остаются пароли, однако их использование должно быть усилено требованиями к сложности и обязательным применением многофакторной аутентификации (MFA),

особенно для учетных записей с расширенными привилегиями. Широко используются сертификаты на основе инфраструктуры открытых ключей (PKI) для аутентификации как пользователей, так и сервисов, например, при взаимодействии между микросервисами. Для аутентификации и авторизации в распределенных веб-приложениях и API активно применяются токены (например, в рамках протоколов OAuth 2.0 и OpenID Connect), позволяющие делегировать полномочия без необходимости прямой передачи учетных данных. В некоторых случаях, для аутентификации конечных пользователей на клиентских устройствах, может использоваться биометрия. В сложных экосистемах также актуальны решения по единому входу (Single Sign-On, SSO) и федерации идентификации, которые позволяют пользователям или сервисам единожды пройти процедуру аутентификации и получить доступ к множеству ресурсов в рамках экосистемы.

После успешной аутентификации вступает в действие процесс авторизации (Authorization). Он заключается в предоставлении или запрете доступа аутентифицированному субъекту к определенным ресурсам или выполнению конкретных действий, основываясь на его правах и назначенных ролях. Эффективные модели авторизации в экосистеме включают ролевое управление доступом (RBAC - Role-Based Access Control), где права доступа назначаются ролям, а пользователи или сервисы ассоциируются с этими ролями. Более гибкой моделью, особенно для сложных и динамичных сред, является управление доступом на основе атрибутов (ABAC - Attribute-Based Access Control), где решения о доступе принимаются динамически на основе набора атрибутов субъекта, объекта, предполагаемого действия и текущего контекста.

Реализация строгих и детализированных политик авторизации, основанных на принципе минимальных привилегий (Least Privilege), является критически важной задачей. Такой подход позволяет ограничить потенциальный ущерб в случае компрометации какой-либо учетной записи.

Цифровая экосистема находится под постоянной угрозой различных кибератак. Комплексная защита ее инфраструктуры требует применения многослойной системы безопасности. Важным элементом является сетевая безопасность, которая включает использование межсетевых экранов (Firewalls) для контроля входящего и исходящего трафика, систем обнаружения и предотвращения вторжений (IDS/IPS) для выявления и блокирования вредоносной активности, а также сегментацию сети для ограничения возможного горизонтального перемещения злоумышленника в случае проникновения.

Необходимо также обеспечить защиту от DDoS-атак (распределенных атак типа "отказ в обслуживании"), которые способны парализовать работу всей экосистемы. Для этого требуется использование специализированных сервисов и технических решений, направленных на фильтрацию вредоносного трафика и абсорбцию атаки. Управление уязвимостями – еще один критический аспект, предполагающий регулярное сканирование компонентов инфраструктуры на наличие известных уязвимостей, своевременное применение патчей и обновлений, а также управление конфигурациями для минимизации рисков.

Защита конечных точек (End-point security), включающая антивирусное программное обеспечение, средства обнаружения инцидентов на конечных устройствах и реагирования на них (EDR), а также контроль за запускаемыми приложениями, также играет важную роль. Нельзя обойтись без мониторинга и логирования: сбор, корреляция и анализ журналов событий безопасности со всех компонентов экосистемы с помощью систем класса SIEM (Security Information and Event Management) позволяют оперативно выявлять инциденты и реагировать на них. Наконец, разработка и регулярное тестирование планов реагирования на инциденты для различных типов угроз безопасности помогают минимизировать потенциальный ущерб и время простоя системы.

Интерфейсы программирования приложений (API) выступают в роли своеобразного "клея", связывающего воедино различные компоненты цифровой экосистемы. Одновременно с этим они представляют собой значительную поверхность атаки, поскольку предоставляют программный доступ к данным и функциональности системы. Обеспечение безопасности API является критически важной задачей.

Каждый запрос к API должен проходить процедуру аутентификации и авторизации. Для аутентификации могут использоваться токены OAuth 2.0, API-ключи или цифровые сертификаты, после чего запрос должен быть авторизован в соответствии с правами вызывающего субъекта. Валидация ввода, то есть строгая проверка и очистка всех входных данных, необходима для предотвращения атак типа SQL Injection, XSS и других видов инъекций. Для защиты от DDoS-атак и злоупотреблений со стороны клиентов применяется ограничение скорости запросов (Rate Limiting) и установка квот на количество запросов за определенный период.

Эффективным подходом является использование API-шлюзов (API Gateways), которые позволяют централизовать функции

безопасности, такие как аутентификация, авторизация, ограничение скорости, логирование и трансформация запросов/ответов, на едином шлюзе, выступающем единственной точкой входа для внешних запросов к API. Необходимо также применять практики безопасного кодирования и регулярно проводить тестирование на наличие распространенных уязвимостей API, например, из списка OWASP API Security Top 10. Наконец, мониторинг API-трафика для выявления аномалий и потенциально вредоносной активности является неотъемлемой частью обеспечения безопасности.

Безопасность цифровой экосистемы – непрерывный командный марафон. Шифрование, строгий контроль доступа, многослойная защита инфраструктуры и безопасные API – вот столпы надежности. Эффективное их применение не только отражает атаки и утечки, но и строит доверие, помогает соблюдать нормы и открывает путь инновациям. В мире постоянно меняющихся угроз, неустанное улучшение защиты и киберграмотность всех участников – ключ к долгосрочной стабильности и успеху экосистемы.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванов, И. В. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра / И. В. Иванов, С. И. Жданова // Материалы конференций ГНИИ "НАЦРАЗВИТИЕ". Июнь 2017 : Сборник избранных статей, Санкт-Петербург, 26–30 июня 2017 года / Выпускающий редактор Ю.Ф. Эльзессер Ответственный за выпуск Л.А. Павлов. – Санкт-Петербург: ГНИИ «НАЦРАЗВИТИЕ», 2017. – С. 116-119. – EDN ZDLMQH.

2. Тахиева, А. Э. Безопасность информации на web-сайтах и приложениях / А. Э. Тахиева, И. И. Ишмурадова // Качество в производственных и социально-экономических системах: сборник научных статей 10-й Международной научно-технической конференции, Курск, 15 апреля 2022 года / Юго-Западный государственный университет. – Курск: Юго-Западный государственный университет, 2022. – С. 386-390. – EDN PNFRDS.

3. Рузанов, П. А. Защита данных в наиболее популярных системах управления контентом с открытым кодом / П. А. Рузанов, М. С. Чисталев // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей LX Международной научно-практической конференции, Пенза, 15 октября 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 14-17. – EDN NNNAVZ.

4. Дюмин, М. А. Обеспечение безопасности web-сайтов / М. А. Дюмин, Е. А. Кулешова // Современные информационные технологии и информационная безопасность: сборник научных статей 2-й Всероссийской научно-технической конференции, Курск, 28 февраля 2023 года. – Курск: Юго-Западный государственный университет, 2023. – С. 28-31. – EDN OPNAJT.

5. Апатова, Н. В. Проблемы информационной безопасности контента / Н. В. Апатова // Проблемы информационной безопасности социально-экономических систем: Труды IX Международной научно-практической конференции, Гурзуф, 02–04 марта 2023 года / Под редакцией О.В. Бойченко. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2023. – С. 3-5. – EDN UHXQSU.

***УДК 004***

***Худяков М.В.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## API-ДИЗАЙН КАК ОСНОВА БЕСШОВНОЙ ЦИФРОВОЙ ЭКОСИСТЕМЫ ДЛЯ СЕТИ КОФЕЕН И ВЕНДИНГА

Сегодня, когда все мы постоянно онлайн, бизнесу для успеха кровь из носу нужно быть удобным для клиента, где бы тот ни находился. Кофейни, вендинговые аппараты – штуки, казалось бы, чисто офлайновые – тоже все активнее уходят в «цифру». И вот тут-то создание целой цифровой «паутины» из сайта, мобильных приложений, чат-ботов и даже самих «умных» автоматов – это уже не просто фишка, чтобы выделиться, а вопрос выживания.

Чтобы все это – сайт, боты, автоматы – работало как единый организм, нужен «дирижер». Этим дирижером, по сути, и становится грамотно сделанный API (программный интерфейс приложения). Он как раз и позволяет всем частям системы – от сайта, на который зашел клиент, и Telegram-бота до админки и, возможно, каких-то систем учета или самих автоматов – понимать друг друга и обмениваться информацией.

Если говорить о нашем проекте – а мы как раз и строим такую экосистему на Java Spring Boot с PostgreSQL под капотом, с сайтом для клиентов и Telegram-ботом – то тут от API вообще зависит львиная доля успеха. Ведь именно то, насколько толково он спроектирован, решает, легко ли будет, скажем, прикрутить быстрый предзаказ кофе через бота

или сайт, удобно ли франчайзи смогут рулить своими точками через админку. Да и вообще, насколько гибкой вся эта махина окажется для будущих «хотелок» вроде интеграции с платежками или аналитикой. Хороший API – это не просто списочек «ручек»; это целая философия взаимодействия, которая следит за порядком в данных и логике по всей системе.

Когда садишься проектировать API, который должен стать становым хребтом для такой сложной штуки, как цифровая экосистема, есть несколько золотых правил, которых стоит держаться:

REST всему голова (ресурсно-ориентированный подход): Принципы REST делают API понятным на интуитивном уровне. Мыслим сущностями: Пользователь, Заказ, Кофейня, ПозицияВМеню. И работаем с ними через обычные HTTP-штуки: GET – чтобы посмотреть, POST – чтобы создать, PUT/PATCH – чтобы подправить, DELETE – чтобы удалить. Хочешь глянуть заказы пользователя? Пожалуйста: GET /users/{userId}/orders. Такой подход – бальзам на душу для ребят с фронтенда и тех, кто пилит бота, им сразу все ясно.

Все едино и предсказуемо: Тут без вариантов: API должен разговаривать на одном языке. Это значит – одинаковые правила для названий «ручек» (эндпоинтов), форматов запросов-ответов (обычно это JSON, куда ж без него) и того, как система ругается на ошибки. Когда ответ всегда приходит в понятной структуре (типа, всегда есть поля status, message, data) и HTTP-коды не врут – разработка летит, а багов становится в разы меньше.

Версии, версии, версии: Система же не стоит на месте, она будет расти и меняться. Новые поля в данных, переделанная логика, свежие фичи – все это может сломать уже работающий сайт или бота, если API не умеет в версионность. Поэтому номер версии прямо в URL (/v1/users, /v2/users) или в заголовках – это маст-хэв. Так и API обновить можно безболезненно, и старые клиенты не отвалятся.

Документация – наше всё: API без понятной доки – это как пытаться собрать сложный конструктор без инструкции. Инструменты типа Swagger (OpenAPI), которые сами генерят документацию прямо из кода (например, из контроллеров Spring Boot), – это просто спасение. Они гарантируют, что описание всегда будет свежим и соответствовать тому, что есть на самом деле. Хорошая документация – это не трата времени, а инвестиция, которая потом экономит кучу нервов и часов на разработке и поддержке.

«Не навреди» при повторе (идемпотентность): Некоторые операции, вроде оформления заказа или оплаты, важно сделать так, чтобы их можно было безопасно повторять. То есть, если один и тот же

запрос с теми же данными прилетит несколько раз, ничего страшного не случится: деньги дважды не спишутся, заказ не задвоится. Это прямо суперважно для надежности, особенно когда интернет лагает или запросы пытаются пройти снова и снова.

Безопасность превыше всего: API – это, по сути, главные ворота к вашим данным и всей бизнес-логике. Так что без надежной проверки, кто стучится (аутентификация) и что ему можно делать (авторизация), никуда. Стандартные протоколы вроде OAuth2 или JWT (JSON Web Tokens) вместе со Spring Security позволяют гибко настроить, кому и к каким частям API можно давать доступ – будь то обычный пользователь сайта/бота или админ с суперправами.

Давайте набросаем, как это могло бы выглядеть для основных кусков нашей системы:

Разбираемся с пользователями:

POST /v1/auth/register: Заводим нового пользователя.

POST /v1/auth/login: Пускаем в систему, выдаем ключик (токен).

GET /v1/users/{userId}: Показываем профиль.

PUT /v1/users/{userId}: Даем обновить данные.

Без этого никуда: личные кабинеты на сайте, опознание пользователя в боте – все строится на этом.

Меню и где найти кофе:

GET /v1/menu: Весь список того, что можно заказать.

GET /v1/menu/{itemId}: Подробности по конкретной позиции.

GET /v1/locations: Список всех кофеен и автоматов – с адресами, работают/не работают.

GET /v1/locations/{locationId}/menu: Что есть в меню именно в этой точке (а то вдруг отличается).

Это нужно, чтобы на сайте показать карту с точками и их менюшками, а бот мог подсказать, где забрать заказ и что там есть.

Заказы: оформляем и следим:

POST /v1/orders: Создаем новый заказ (что выбрал, где заберет, когда).

GET /v1/users/{userId}/orders: Все заказы этого человека.

GET /v1/orders/{orderId}: Детали по конкретному заказу.

POST /v1/orders/{orderId}/cancel: Если передумал – отменяем.

Именно эта часть API дает ту самую возможность быстро заказать «с собой» или к определенному времени – одна из главных фишек проекта. API должен четко отслеживать, что там с заказом: новый, готовится, ждет, выдан или отменен.

Плюшки для постоянных клиентов (программа лояльности):

GET /v1/users/{userId}/loyalty: Сколько бонусов на счету, может,

история накоплений/списаний.

(Встроено в POST /v1/orders): Когда оформляет заказ, API должен дать возможность потратить бонусы, а когда заказ успешно завершен – начислить новые.

Подружить с вендингом (тут все зависит от глубины проекта):

GET /v1/vending/{vendingId}/status: Как там автомат поживает (есть ли кофе, не сломался ли) – тут, конечно, нужна будет специальная магия на уровне «железа».

POST /v1/vending/{vendingId}/linkUser: Чтобы система знала, что вот этот пользователь что-то сделал у этого автомата (для бонусов, например).

Эта часть самая замороченная с технической стороны, нужны свои протоколы для общения с автоматами. API должен быть готов к тому, что данные могут приходить из очень разных мест.

Для тех, кто всем рулит (админка):

Тут понадобится свой набор «ручек» (что-то вроде /v1/admin/*) с расширенными правами. Чтобы администраторы могли смотреть и менять данные по пользователям, заказам, точкам, меню, ну и, конечно, видеть общую картину – например, через /v1/admin/dashboard/analytics.

И тут Spring Boot – прямо то, что доктор прописал. В нем куча всего удобного для создания таких RESTful-сервисов: аннотации @RestController и @RequestMapping легко связывают HTTP-запросы с нужными методами в коде, Spring Data JPA помогает без головной боли работать с PostgreSQL, а Spring Security позволяет гибко рулить правами доступа. Если делить логику по-умному – на контроллеры (прием запросов), сервисы (мозги) и репозитории (общение с базой) – то получается чистая архитектура. Такой API и поддерживать приятно, и расширять не страшно. А еще DTO (Data Transfer Objects) – классная штука, чтобы API отдавал каждому клиенту ровно то, что ему нужно: админке – побольше деталей, боту – самый минимум.

Один API для всех, но каждому свое. Одна из главных прелестей хорошо сделанного API в том, что он может обслуживать совершенно разных клиентов – от навороченного сайта до простенького Telegram-бота – через один и тот же набор команд. Сайту обычно нужно больше данных, чтобы красиво все показать. Telegram-бот, наоборот, общается короткими командами и кнопками, ему лишняя информация ни к чему. Грамотное использование DTO на стороне API как раз и позволяет отдавать каждому ровно столько данных, сколько нужно, не перегружая никого и не дублируя логику на бэкенде.

Конечно, гладко все бывает только на бумаге. Делать API для такой навороченной системы – это всегда вызовы. Нужно думать, как его

развивать, не ломая то, что уже работает; как защитить данные по максимуму; как грамотно обрабатывать ошибки и постоянно обновлять документацию. Все это требует собранности и дисциплины. Внедрение CI/CD (непрерывной интеграции и доставки) сильно упрощает жизнь, автоматизируя тесты и выкатку обновлений, а системы мониторинга помогают быстро ловить и чинить проблемы.

Запустить цифровую экосистему для кофеен и вендинга – задачка не из легких, и успех тут напрямую зависит от того, насколько крепким будет технический фундамент. Продуманный API, сделанный по уму, с учетом всех современных подходов и особенностей бизнеса (как работают сайт, Telegram-бот, админка), – это та самая основа, которая обеспечит гладкую работу всего и вся, поможет автоматизировать рутину и даст простор для роста в будущем. Вложения в четкую архитектуру и детальное проектирование API на старте – это не траты, а самая что ни на есть разумная инвестиция. Она потом много раз окупится, когда нужно будет что-то интегрировать, добавить новые фичи или просто убедиться, что все работает как часы. Именно API и делает возможным создание такого единого цифрового мира, где все части играют слаженно, а клиенты (и сам бизнес) получают от этого только удовольствие.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Веретенников, О. В. Модули для Opencart: цели использования, распространенность, экономическая выгода / О. В. Веретенников, К. Ю. Станиславская // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 21-24. – EDN XBIKYO.

2. Ампилогов, Н. С. Типовая структура API социальных сетей / Н. С. Ампилогов // Альманах научных работ молодых ученых Университета ИТМО: Материалы XLVI научной и учебно-методической конференции, Санкт-Петербург, 31 января – 03 2017 года. Том 4. – Санкт-Петербург: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2017. – С. 4-6. – EDN LXXIMH.

3. Прохоров, П. В. Современные подходы в backend разработке на примере онлайн-магазина / П. В. Прохоров, Н. В. Разговоров // Прикладная математика и фундаментальная информатика. – 2020. – Т. 7, № 2. – С. 23-28. – DOI 10.25206/2311-4908-2020-7-2-24-29. – EDN

HUGGWY.

4. Зотова, Ю. А. Разработка архитектуры rest api для взаимодействия с сервисами приложения / Ю. А. Зотова, И. Д. Котилевец // Информационные технологии и математическое моделирование систем 2018 : труды международной научно-технической конференции, Одинцово, 19–21 ноября 2018 года. – Одинцово: Федеральное государственное бюджетное учреждение науки Центр информационных технологий в проектировании Российской академии наук, 2018. – С. 61-65. – EDN PLVMYQ.

***УДК 004***

***Худяков М.В.***
***Научный руководитель: Коршак К.С., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ОБЛАЧНАЯ ИНФРАСТРУКТУРА КАК ФУНДАМЕНТ МАСШТАБИРОВАНИЯ ЦИФРОВОЙ ЭКОСИСТЕМЫ: АСПЕКТЫ ВЫБОРА И КОНФИГУРАЦИИ

Разработка комплексной цифровой экосистемы, интегрирующей веб-приложения, Telegram-боты и физические точки обслуживания (кофейни, вендинговые автоматы), детерминирует высокие требования не только к архитектуре бэкенда и гибкости API, но и к надежности и масштабируемости платформы размещения. В современных реалиях доминирующей основой для таких систем выступают облачные платформы. Их преимущества – гибкость, эластичность предоставления вычислительных ресурсов по требованию и обширный инструментарий управляемых сервисов – являются критически важными для проектов, ориентированных на динамичное развитие и потенциальное расширение, включая модели франчайзинга.

Обоснованность выбора облачных решений для систем подобного класса, особенно в контексте роста и масштабирования, обусловлена способностью ведущих провайдеров (например, AWS, Google Cloud Platform (GCP), Microsoft Azure) оперативно предоставлять ресурсы, адаптируясь к флуктуациям нагрузки. В сравнении с поддержкой собственной физической инфраструктуры (on-premises), облачные модели нивелируют значительную часть операционных издержек, связанных с приобретением, конфигурированием, техническим обслуживанием аппаратного обеспечения и обеспечением его физической безопасности. Такой подход позволяет оптимизировать

затраты за счет оплаты фактически потребленных ресурсов, оперативно наращивать вычислительные мощности при увеличении пользовательской активности или объема заказов, и аналогичным образом сокращать их в периоды снижения нагрузки.

В рамках рассматриваемой цифровой экосистемы для индустрии гостеприимства, облачная инфраструктура призвана обеспечить функционирование ряда ключевых компонентов: бэкенд-приложения, реализованного на Spring Boot, базы данных PostgreSQL, а также специфических модулей, таких как обработчики webhook-уведомлений Telegram Bot API или микросервисы для внешних интеграций. Выбор конкретного провайдера облачных услуг (будь то AWS, GCP или Azure) зачастую зависит от преференций разработчиков, их опыта взаимодействия с определенной платформой, ценовой политики и доступности специфических сервисов в целевом регионе. Тем не менее, фундаментальные принципы выбора и конфигурации основных инфраструктурных компонентов остаются в значительной степени унифицированными.

Ключевые компоненты облачной инфраструктуры

При развертывании экосистемы в облачной среде необходимо определить стратегию размещения для каждого ее элемента:

Вычислительные ресурсы (Compute): Локализация бэкенд-логики

Виртуальные машины (VMs): Традиционный и прямолинейный подход. У провайдеров данный сервис представлен как Amazon EC2, Google Compute Engine или Azure Virtual Machines. Арендуется виртуальный сервер с требуемыми характеристиками, на котором разворачивается операционная система, среда исполнения Java, приложение Spring Boot и конфигурируются все зависимости. Этот метод предоставляет полный контроль над окружением, однако требует ручного управления и масштабирования, хотя и существуют механизмы автоматического масштабирования (autoscaling).

Контейнеризация: Более современный и гибкий подход, базирующийся на использовании Docker-контейнеров и систем оркестрации (например, Kubernetes, Docker Swarm). Облачные провайдеры предлагают управляемые сервисы: Amazon ECS/EKS, Google GKE, Azure AKS. Приложение Spring Boot упаковывается в Docker-образ, а облачный сервис автоматически управляет жизненным циклом контейнеров (запуск, остановка, масштабирование) в зависимости от текущей нагрузки. Данный метод демонстрирует высокую эффективность при развертывании, управлении и масштабировании микросервисных архитектур, а также для монолитных приложений.

Бессерверные вычисления (Serverless): Парадигма, исключающая необходимость управления серверной инфраструктурой. Разработчик загружает код (функцию), а провайдер обеспечивает его выполнение в ответ на триггерные события (HTTP-запрос, сообщение в очереди, webhook). Примерами служат AWS Lambda, Google Cloud Functions, Azure Functions. Для рассматриваемой экосистемы это может быть оптимальным решением для обработки входящих webhook-уведомлений от Telegram Bot API. Вместо постоянно активного сервера, прослушивающего запросы, используется легковесная Lambda-функция, активирующаяся только при получении webhook, обрабатывающая его и инициирующая запрос к основному API бэкенда. Такой подход может обеспечить существенную экономию затрат и высокую масштабируемость для специфических, событийно-ориентированных задач.

Система управления базами данных (Database): Размещение PostgreSQL

Управляемые сервисы баз данных (Managed Database Services): Настоятельно рекомендуется использование таких сервисов, как Amazon RDS for PostgreSQL, Google Cloud SQL for PostgreSQL, Azure Database for PostgreSQL. В этом случае провайдер берет на себя все аспекты администрирования СУБД: установку, применение патчей, резервное копирование, восстановление, мониторинг, репликацию и масштабирование. Пользователь выбирает тип инстанса и версию PostgreSQL. Это значительно снижает операционные издержки и повышает общую надежность системы. Управляемые сервисы обеспечивают возможности как вертикального (увеличение мощности инстанса), так и горизонтального (добавление реплик чтения) масштабирования, что критично при росте нагрузки.

Объектное хранилище (Object Storage):

Сервисы типа Amazon S3, Google Cloud Storage, Azure Blob Storage предоставляют надежное и масштабируемое хранилище для произвольных файлов. Они могут использоваться для хранения медиаконтента (изображения продукции, логотипы), резервных копий баз данных, журналов работы приложения.

Сетевая инфраструктура (Networking):

Виртуальные частные облака (VPC в AWS, VPC Network в GCP, VNet в Azure) позволяют создать изолированную сетевую среду в облаке для размещения ресурсов.

Конфигурация правил сетевой безопасности (Security Groups в AWS, Firewall Rules в GCP, Network Security Groups в Azure) обеспечивает контроль трафика к инстансам и от них, разрешая доступ

только по необходимым портам (например, 80/443 для HTTP/HTTPS, 5432 для PostgreSQL с ограничением доступа для бэкенда).

Балансировщики нагрузки (Load Balancers) распределяют входящий трафик между несколькими экземплярами бэкенд-приложения, обеспечивая высокую доступность и горизонтальную масштабируемость.

Процесс выбора и конфигурации инфраструктуры

Выбор между провайдерами и конкретными сервисами должен базироваться на комплексном анализе следующих факторов:

Технические требования проекта: Необходимая производительность, объемы хранения данных, требования к уровню доступности (например, SLA 99.95%).

Бюджетные ограничения: Сравнительный анализ стоимости аналогичных сервисов у различных провайдеров. Управляемые сервисы, как правило, дороже базовых VM, но компенсируют это экономией на администрировании. Бессерверные функции могут быть экономически эффективны при неравномерной нагрузке.

Экспертиза команды: Работа с уже знакомой платформой может ускорить процесс внедрения и снизить риски на начальном этапе.

Наличие специфических сервисов: Определенный провайдер может предлагать уникальный сервис, идеально соответствующий специфическим задачам экосистемы (например, специализированный сервис для IoT, потенциально полезный для интеграции с вендинговыми аппаратами).

После выбора провайдера и сервисов следует этап конфигурации. Здесь крайне рекомендуется применение подхода "Инфраструктура как код" (Infrastructure as Code - IaC) с использованием инструментов, таких как Terraform, AWS CloudFormation, Google Cloud Deployment Manager или Azure Resource Manager. Вместо мануальной настройки через веб-интерфейс провайдера, вся инфраструктура (виртуальные машины, базы данных, сетевые конфигурации, правила безопасности) описывается в декларативных конфигурационных файлах. Это обеспечивает ряд преимуществ:

Автоматизация: Быстрое и автоматизированное развертывание инфраструктуры.

Версионирование: Конфигурационные файлы хранятся в системе контроля версий (например, Git), что позволяет отслеживать изменения и осуществлять откат к предыдущим состояниям.

Воспроизводимость: Легкость создания идентичных окружений (тестовое, staging, production).

Снижение вероятности ошибок: Минимизация ошибок, связанных

с человеческим фактором при ручной настройке.

Процесс настройки включает конфигурацию сети (VPC, подсети, таблицы маршрутизации), определение правил безопасности, развертывание вычислительных ресурсов (например, настройка Auto Scaling Group для серверов Spring Boot для автоматического масштабирования в зависимости от нагрузки), запуск управляемой СУБД с требуемыми параметрами, а также настройку систем мониторинга и логирования (CloudWatch, Google Cloud Monitoring, Azure Monitor).

Механизмы масштабирования в облачной среде

Одним из ключевых преимуществ облачных платформ является их эластичность. При росте числа пользователей и, соответственно, нагрузки на экосистему, облачная инфраструктура предоставляет возможности для адаптации:

Вертикальное масштабирование: Увеличение ресурсов (CPU, RAM) существующих виртуальных машин или инстансов баз данных. Часто требует перезагрузки сервиса.

Горизонтальное масштабирование: Добавление новых экземпляров VM или контейнеров для бэкенд-приложений, а также реплик баз данных. Это предпочтительный метод для веб-приложений, так как он позволяет обрабатывать большее количество запросов параллельно и повышает отказоустойчивость (при отказе одного инстанса остальные продолжают функционировать). Группы автоматического масштабирования (Auto Scaling Groups) динамически управляют количеством инстансов бэкенда на основе предопределенных метрик (например, загрузка CPU). Управляемые сервисы СУБД также предоставляют опции автоматического или полуавтоматического масштабирования.

Масштабирование бессерверных функций: Облачный провайдер автоматически обеспечивает запуск необходимого количества экземпляров функции в ответ на входящие события, полностью абстрагируя разработчика от задач управления масштабированием.

Заключение

Стратегический выбор и корректная конфигурация облачной инфраструктуры являются не просто технической задачей, а фундаментальным решением, определяющим перспективы масштабируемости, уровень надежности и совокупную стоимость владения (TCO) цифровой экосистемой для сети кофеен и вендинговых автоматов. Современные облачные платформы предоставляют широкий спектр управляемых сервисов – от гибких вычислительных мощностей (VM, контейнеры, serverless-архитектуры) и надежных

СУБД как сервис до объектных хранилищ и развитых сетевых инструментов. Применение принципов "Инфраструктуры как кода" для автоматизации настройки и развертывания является передовой практикой, обеспечивающей управляемость и воспроизводимость конфигураций. В конечном счете, тщательно спроектированная облачная архитектура формирует надежный фундамент, на котором цифровая экосистема способна эффективно расти, развиваться и успешно обслуживать увеличивающийся поток пользователей и точек продаж, обеспечивая бесперебойное функционирование ее центрального компонента – бэкенда.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Веретенников, О. В. Модули для Opencart: цели использования, распространенность, экономическая выгода / О. В. Веретенников, К. Ю. Станиславская // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 21-24. – EDN XBIKYO.

2. Прохоров, П. В. Современные подходы в backend разработке на примере онлайн-магазина / П. В. Прохоров, Н. В. Разговоров // Прикладная математика и фундаментальная информатика. – 2020. – Т. 7, № 2. – С. 23-28. – DOI 10.25206/2311-4908-2020-7-2-24-29. – EDN HUGGWY.

3. Денисов, А. А. Современные средства разработки сайтов / А. А. Денисов // Вестник Воронежского института высоких технологий. – 2019. – № 2(29). – С. 68-71. – EDN MKPIWE.

4. Готская И. Б., Васильченко А. Д. Анализ клиентских фреймворков для разработки веб-приложений //Инновации. Наука. Образование—2022. Режим доступа: https://www. elibrary. ru (дата обращения: 23.04. 24).

5. Минаков, В. Ф. Развертывание облачной инфраструктуры в региональном информационном пространстве / В. Ф. Минаков, О. С. Лобанов, А. А. Остроумов // Научное обозрение. – 2014. – № 11-1. – С. 103-106. – EDN TJXMZV.

*УДК 004*

***Худяков М.В.***
***Научный руководитель: Жданова С.И., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

# БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ CMS СИСТЕМ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ DRUPAL, JOOMALA, WORDPRESS И WEBASYST

Сегодня системы управления контентом (CMS) стали неотъемлемой частью создания и поддержания веб-сайтов любого масштаба, будь то скромный личный блог или крупный корпоративный или государственный портал. С учетом растущего числа кибератак, вопросы обеспечения безопасности таких платформ приобретают первостепенное значение. В рамках данного материала мы подробно рассмотрим архитектуру и особенности безопасности четырех распространенных CMS – Drupal, Joomla, WordPress и Webasyst. Наша цель – выявить их сильные стороны и потенциальные уязвимости, а также предложить набор практических рекомендаций для усиления защиты веб-ресурсов, функционирующих на их основе.

Хотя CMS и являются удобным инструментом, их повсеместное распространение часто делает их привлекательной мишенью для злоумышленников. Среди наиболее частых угроз можно выделить:

- SQL-инъекции: Попытки внедрения вредоносных команд в базу данных через поля ввода на сайте.
- XSS (межсайтовое выполнение скриптов): Встраивание злонамеренных скриптов в веб-страницы, которые затем выполняются в браузере пользователя.
- CSRF (межсайтовая подделка запросов): Принуждение пользователя выполнить нежелательные действия на сайте, на который он уже аутентифицирован.
- Уязвимости в сторонних расширениях: Плагины, темы и дополнительные модули, часто разрабатываемые без должного контроля безопасности.
- Использование устаревшего ПО: Несвоевременные обновления ядра CMS и расширений оставляют "двери открытыми" для известных эксплойтов.

Стандартный арсенал средств защиты включает в себя разграничение пользовательских прав, шифрование конфиденциальной информации, использование протокола HTTPS, регулярное обновление

всех компонентов, а также налаженные процессы резервного копирования и мониторинга (аудита) действий.

Drupal пользуется заслуженной популярностью в корпоративном и государственном секторах благодаря своей архитектурной надежности и высокой степени гибкости. Его часто выбирают для создания сложных и масштабных порталов, включая официальные веб-сайты органов власти и образовательных учреждений.

Проектировщики Drupal изначально делали ставку на безопасность. Его модульная структура позволяет каждому элементу системы выполнять конкретную функцию и проходить независимую проверку. Система контроля доступа здесь отличается особой гибкостью: API управления доступом (Access Control API) дает возможность настроить права пользователей с высокой детализацией, вплоть до отдельных элементов контента (узлов).

Существенным плюсом является наличие мощной системы фильтрации входящих данных, эффективно предотвращающей XSS-атаки еще до момента отображения контента на странице. Команда безопасности Drupal ведет непрерывный мониторинг потенциальных угроз, оперативно публикует соответствующие бюллетени и рекомендации по установке обновлений. Зачастую уязвимости устраняются еще до того, как ими смогут широко воспользоваться злоумышленники.

Платформа Joomla широко применяется для создания бизнес-сайтов, интернет-магазинов и новостных ресурсов. Ее можно отнести к CMS средней сложности, предлагающей хороший баланс между богатым функционалом и удобством использования.

Joomla оснащена рядом встроенных защитных механизмов: здесь реализована двухфакторная аутентификация, предусмотрено использование CSRF-токенов, осуществляется фильтрация пользовательского ввода и реализовано разграничение прав доступа. Важным преимуществом является наличие единой панели для отслеживания и установки обновлений как ядра системы, так и всех установленных расширений.

Однако Joomla в значительной степени зависит от сторонних расширений, среди которых, к сожалению, встречаются модули с небезопасным кодом. Нередко источником проблем становятся именно компоненты, разработанные сторонними разработчиками. Кроме того, отсутствие автоматических обновлений ядра может привести к тому, что администраторы используют устаревшие, а следовательно, потенциально уязвимые версии системы длительное время.

Команда безопасности Joomla регулярно публикует информацию

об обнаруженных уязвимостях и дает рекомендации по их устранению, но общий уровень защищенности ресурса во многом определяется квалификацией и внимательностью администратора.

WordPress сегодня является самой распространенной CMS в мире, используемой для создания всего: от личных блогов и портфолио до новостных порталов и крупных интернет-магазинов. Эта универсальность, делающая платформу столь привлекательной, одновременно является и источником ее уязвимости.

Ядро WordPress регулярно обновляется, и система поддерживает автоматические обновления, что существенно снижает риск эксплуатации давно известных уязвимостей. Дополнительно существуют многочисленные плагины безопасности (такие как Wordfence, iThemes Security, Sucuri), предлагающие функции фаервола, сканирования на вирусы, защиты от подбора паролей и ведения подробных логов активности.

Тем не менее, главной "болевой точкой" WordPress остаются плагины и темы: их разработка ведется огромным числом авторов, и качество кода часто не подвергается строгому контролю. Именно расширения чаще всего становятся точкой входа для атак. Некорректная настройка прав доступа также может привести к повышению привилегий атакующего или компрометации всего сайта. Учитывая популярность, WordPress постоянно подвергается атакам автоматизированных сканеров и ботнетов, что диктует необходимость дополнительной защиты на уровне веб-сервера.

Обеспечение надежной безопасности для WordPress возможно, но требует от администратора высокой вовлеченности и постоянного мониторинга состояния системы.

Webasyst – менее известный, но активно используемый в малом и среднем бизнесе продукт, особенно на территории постсоветских стран. Он ориентирован в первую очередь на создание интернет-магазинов и CRM-систем.

С точки зрения архитектуры, Webasyst представляет собой довольно закрытую экосистему. Большая часть функционала поставляется непосредственно от разработчика платформы, что минимизирует риски, связанные с использованием непроверенных сторонних плагинов. Обновления системы централизованы, управление доступом осуществляется на основе ролей. Поддерживаются стандартные меры безопасности, такие как HTTPS, настройка резервного копирования и уведомления о подозрительной активности.

К недостаткам можно отнести относительно небольшое сообщество и, как следствие, менее активный независимый аудит

безопасности по сравнению с гигантами рынка. Из-за меньшей распространенности и закрытости отсутствует такое же масштабное тестирование на уязвимости. Тем не менее, ограниченное количество внешних зависимостей снижает вероятность критических нарушений безопасности, связанных с их кодом.

Таблица 1 – сравнительный анализ

| Параметр | Drupal | Joomala | WordPress | WebAsyst |
|---|---|---|---|---|
| Основная сфера | Корпоративные и гос. сайты | Бизнес-сайты | Блоги, магазины | Малый и средний бизнес |
| Архитектурная безопасность | Высокая | Средняя | Средняя | Средняя |
| Обновления ядра модулей | Надёжные | Частично надёжные | Надёжные | Централизованные |
| Уязвимости расширений | Низкие | Высокие | Очень высокие | Низкие |
| Безопасность «из коробки» | Продвинутая | Базовая | Средняя | Базовая |
| Поддержка сообщества | Высокая | Средняя | Очень высокая | Низкая |

Для повышения уровня защищенности веб-ресурсов на базе любой CMS рекомендуется предпринять следующие действия:

1. Оперативно устанавливать все доступные обновления ядра CMS и всех установленных расширений.
2. Выбирать плагины и темы исключительно из официальных или хорошо зарекомендовавших себя репозиториев.
3. Настраивать права доступа пользователей по принципу наименьших привилегий, строго в соответствии с их ролями.
4. Включать двухфакторную аутентификацию для учетных записей администраторов и других пользователей с расширенными правами.
5. Рассмотреть возможность установки веб-аппликационного брандмауэра (WAF) для фильтрации вредоносного трафика.
6. Регулярно создавать резервные копии сайта и базы данных, а также настроить систему аудита действий администраторов.

Проведенный анализ позволяет заключить, что Drupal выделяется как наиболее защищенная система на уровне архитектуры и является оптимальным выбором для проектов, где требования к безопасности особенно высоки. WordPress, несмотря на свою колоссальную популярность и простоту использования, требует постоянного внимания и активного применения дополнительных мер защиты из-за

обилия сторонних расширений. Joomla представляет собой сбалансированное решение, но, как и WordPress, чувствительна к качеству используемых сторонних компонентов. Webasyst является надежной платформой для небольших бизнес-проектов с несколько ограниченной гибкостью, но приемлемым уровнем встроенной безопасности.

Выбор конкретной CMS для нового проекта должен учитывать не только набор предоставляемых функций, но и потенциальные риски, уровень ответственности разработчиков платформы за безопасность, а также готовность и возможности администратора постоянно поддерживать высокий уровень защиты веб-ресурса.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванов, И. В. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра / И. В. Иванов, С. И. Жданова // Материалы конференций ГНИИ "НАЦРАЗВИТИЕ". Июнь 2017: Сборник избранных статей, Санкт-Петербург, 26–30 июня 2017 года / Выпускающий редактор Ю.Ф. Эльзессер Ответственный за выпуск Л.А. Павлов. – Санкт-Петербург: ГНИИ «НАЦРАЗВИТИЕ», 2017. – С. 116-119. – EDN ZDLMQH.

2. Тахиева, А. Э. Безопасность информации на web-сайтах и приложениях / А. Э. Тахиева, И. И. Ишмурадова // Качество в производственных и социально-экономических системах: сборник научных статей 10-й Международной научно-технической конференции, Курск, 15 апреля 2022 года / Юго-Западный государственный университет. – Курск: Юго-Западный государственный университет, 2022. – С. 386-390. – EDN PNFRDS.

3. Рузанов, П. А. Защита данных в наиболее популярных системах управления контентом с открытым кодом / П. А. Рузанов, М. С. Чисталев // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей LX Международной научно-практической конференции, Пенза, 15 октября 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 14-17. – EDN NNNAVZ.

4. Дюмин, М. А. Обеспечение безопасности web-сайтов / М. А. Дюмин, Е. А. Кулешова // Современные информационные технологии и информационная безопасность: сборник научных статей 2-й Всероссийской научно-технической конференции, Курск, 28 февраля 2023 года. – Курск: Юго-Западный государственный университет, 2023. – С. 28-31. – EDN OPNAJT.

5. Апатова, Н. В. Проблемы информационной безопасности контента / Н. В. Апатова // Проблемы информационной безопасности социально-экономических систем: Труды IX Международной научно-практической конференции, Гурзуф, 02–04 марта 2023 года / Под редакцией О.В. Бойченко. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2023. – С. 3-5. – EDN UHXQSU.

***УДК 004.057.4***

***Чаков И.А., Евтюхов М.С.***
***Научный руководитель: Павловский В.В., преп.***
*Российский государственный университет нефти и газа им. И.М. Губкина, г. Москва, Россия*

## ОСОБЕННОСТИ НАСТРОЙКИ И ПРИМЕНЕНИЯ ПРОТОКОЛА IGMPV2 В ОПЕРАЦИОННОЙ СИСТЕМЕ АЛЬТ

В условиях стремительного роста групповых коммуникаций в современных компьютерных сетях вопросы корректной настройки и управления multicast-трафиком приобретают особую значимость. Групповые рассылки данных являются технологической основой для таких востребованных сервисов, как IP-телевидение (IPTV), видеоконференцсвязь, массовые онлайн-трансляции.

*Актуальность* нашего исследования заключается в эффективной организации multicast-трафика, которая невозможна без правильной реализации протокола IGMP (Internet Group Management Protocol), отвечающего за управление подпиской на групповые рассылки.

*Объектом* данного исследования являются сетевые технологии, связанные с передачей и маршрутизацией группового (мультикаст) трафика в IP-сетях. Особое внимание уделяется средствам управления групповой подпиской на уровне сетевого стека операционной системы.

*Предметом* исследования выступает реализация и настройка протокола IGMPv2 в отечественной операционной системе семейства «Альт». Рассматриваются инструменты и методы настройки IGMPv2 средствами самой ОС, включая системные утилиты и сетевые конфигурационные файлы.

*Цель* нашего исследования заключается в разработке и апробации пошаговой инструкции по настройке IGMPv2 в ОС Альт, демонстрации корректной работы протокола на практике, а также в формировании рекомендаций по использованию мультикаст-технологий в рамках отечественного программного обеспечения.

Проблематика применения протокола IGMPv2 в современных

операционных системах поднималась в ряде исследований. Сергей Калашников в своей статье «Оптимизация передачи multicast-трафика в локальной сети с помощью IGMP snooping» [1], в которой автор приводит примеры практической настройки протокола IGMPv2 с использованием встроенных системных инструментов.

Екатерина Куклева в своей статье «Приручаем multicast» [2] рассматривает реализацию работы протокола IGMPv2 и разрабатывает оптимальную конфигурацию сетевого оборудования.

Использование протокола IGMPv2 в современных операционных системах позволяет оптимизировать multicast-трафик в локальных сетях за счёт эффективного управления групповыми рассылками. Однако его настройка и взаимодействие с сетевым оборудованием требуют дополнительного анализа и адаптации под конкретные условия эксплуатации. Предполагается, что применение оптимальных конфигураций IGMPv2, предложенных в исследовании, может значительно снизить нагрузку на сеть и улучшить производительность multicast-передач.

Данное исследование носит прикладной характер, так как мы на практическом примере показываем пошаговую настройку и тестирование работы протокола IGMPv2 в дистрибутиве ОС Альт.

Для того, чтобы произвести настройку и тестирование работоспособности протокола IGMPv2 в дистрибутиве ОС Альт, нам следует подобрать необходимые пакеты, реализовать топологию эксперимента, используя программы VirtualBox версии 7.1.6.167084 и GNS3 версии 2.2.52 [3]. Также нам необходимо применить технологию IGMP Snooping на виртуальной машине, выступающей в роли коммутатора. Топология эксперимента представлена на рисунке 1.

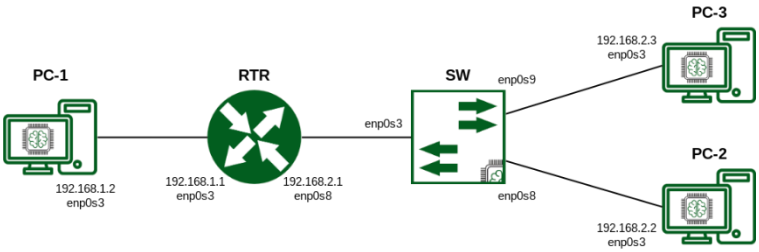



Рис. 1 Топология эксперимента

Таблица – Использование утилит на устройствах

| Утилита | Маршрутизатор | Коммутатор | Компьютеры |
|---|---|---|---|

| | | | |
|---|---|---|---|
| iperf | - | - | + |
| smcroute | + | - | - |
| wireshark | + | + | + |
| openvswitch | - | - | - |
| Linux Bridge | - | + | - |
| iptables | + | + | + |
| iproute2 | + | + | + |
| net-tools | + | + | + |

Выполним базовую настройку протокола IGMPv2 [4]. Будут использованы следующие дистрибутивы: ALT Workstation версии 10.4 и ALT Server версии 10.4. Для начала установим необходимые пакеты из репозитория: smcroute версии 2.4.4, wireshark версии 4.4.5, iperf версии 2.0.12, openvswitch версии 2.17.11. Также будут задействованы пакеты iproute2 версии 5.13.0, iptables версии 1.8.7 и net-tools версии 1.60. Данные утилиты установлены в дистрибутивы ОС Альт по умолчанию.

Настроили адресацию на всех устройствах, кроме коммутатора. Настройка адресации на маршрутизаторе и одном из компьютеров представлена на рисунках 2, 3.

```
[root@RTR ~]# ip addr add 192.168.1.1/24 dev enp0s3
[root@RTR ~]# ip addr add 192.168.2.1/24 dev enp0s8
[root@RTR ~]# ip link set dev enp0s3 up
[root@RTR ~]# ip link set dev enp0s8 up
[root@RTR ~]# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             192.168.1.1/24 fe80::a00:27ff:fe86:c3ca/64
enp0s8           UP             192.168.2.1/24 fe80::a00:27ff:fea6:f8ce/64
```

Рис. 2 Настройка адресации на маршрутизаторе

```
[root@PC1 ~]# ip addr add 192.168.1.2/24 dev enp0s3
[root@PC1 ~]# ip link set dev enp0s3 up
[root@PC1 ~]# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             192.168.1.2/24 fe80::a00:27ff:fe03:141d/64
```

Рис. 3 Настройка адресации на компьютере

На компьютерах описали статические маршруты, использовав шлюз по умолчанию. Пример описания статических маршрутов с использованием шлюза по умолчанию представлен на рисунке 4.

```
[root@PC1 ~]# ip route add default via 192.168.1.1
[root@PC1 ~]# ip r
default via 192.168.1.1 dev enp0s3
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.2
```

Рис. 4 Описания статических маршрутов с помощью шлюза

На маршрутизаторе разрешили переброс пакетов между интерфейсами, установив в файле /etc/net/sysctl.conf параметр net.ipv4.ip_forward равным единице. В этом же файле для всех интерфейсов отключили path filtering и указали версию протокола IGMP, а именно вторую версию. Используя операторы вывода cat и less проверили готовность к маршрутизации. Проверка готовности к маршрутизации представлена на рисунке 5.

```
[root@RTR ~]# less /proc/config.gz | grep '\(MROUTE\|MULTICAST\)'
CONFIG_IP_MULTICAST=y
CONFIG_IP_MROUTE_COMMON=y
CONFIG_IP_MROUTE=y
CONFIG_IP_MROUTE_MULTIPLE_TABLES=y
CONFIG_IPV6_MROUTE=y
CONFIG_IPV6_MROUTE_MULTIPLE_TABLES=y
[root@RTR ~]# cat /proc/sys/net/ipv4/conf/default/forwarding
1
[root@RTR ~]# cat /proc/sys/net/ipv4/conf/enp0s3/rp_filter
0
[root@RTR ~]# cat /proc/sys/net/ipv4/conf/enp0s8/rp_filter
0
[root@RTR ~]# cat /proc/sys/net/ipv4/conf/enp0s3/force_igmp_version
2
[root@RTR ~]# cat /proc/sys/net/ipv4/conf/enp0s8/force_igmp_version
2
```

Рис. 5 Проверка готовности к маршрутизации

Настроили цепочки iptables для работы со специальными multicast-подсетями [5]. Настройка цепочек iptables представлена на рисунке 6.

```
[root@RTR ~]# iptables -I INPUT -d 224.0.0.0/4 -j ACCEPT
[root@RTR ~]# iptables -I FORWARD -d 224.0.0.0/4 -j ACCEPT
```

Рис. 6 Настройка цепочек iptables

Прописали маршрут. Пример прописанного маршрута представлен на рисунке 7.

```
[root@RTR ~]# route add -net 224.0.0.0/4 dev enp0s8
```

Рис. 7 Пример прописанного маршрута

Перешли к настройке статической маршрутизации. Запустили демон smcroute командой smcroute -d. После настроили маршруты по примеру: smcroute -a eth0 10.1.0.18 224.2.2.2 eth1, где

- eth0 — входящий интерфейс для трафика
- 10.1.0.18 — адрес интерфейса-источника трафика
- 224.2.2.2 — MC-группа в сети 224.0.0.0/4
- eth1 — один или несколько внешних интерфейсов

Пример настройки маршрута с использованием демона smcroute представлен на рисунке 8.

```
[root@RTR ~]# smcroute -a enp0s3 192.168.1.2 224.2.2.2 enp0s8
```

Рис. 8 Пример настройки маршрута с помощью smcroute

Технология IGMP Snooping является неотъемлемой частью настройки протокола IGMPv2, так как позволяет эффективно управлять multicast-трафиком, анализируя IGMP-сообщения между маршрутизаторами и хостами. Это предотвращает ненужную рассылку группового трафика на все порты, уменьшая нагрузку на сеть и повышая её производительность. Таким образом, IGMP Snooping оптимизирует работу IGMPv2, обеспечивая точную доставку multicast-пакетов только подписанным получателям.

Выполним подключение технологии IGMP Snooping на коммутаторе. Для начала на устройстве SW-1 создали мост, используя программную реализацию сетевого моста Linux Bridge: добавили виртуальный интерфейс, который будет выступать в роли моста, привязали к нему сетевые интерфейсы, соединяющие коммутатор с маршрутизатором и двумя компьютерами, после чего включили все интерфейсы [10]. Пример настройки моста представлен на рисунке 9.

```
[root@SW ~]# ip link add name br0 type bridge
[root@SW ~]# ip link set dev enp0s3 master br0
[root@SW ~]# ip link set dev enp0s8 master br0
[root@SW ~]# ip link set dev enp0s9 master br0
[root@SW ~]# ip link set dev br0 up
[root@SW ~]# ip link set dev enp0s3 up
[root@SW ~]# ip link set dev enp0s8 up
[root@SW ~]# ip link set dev enp0s9 up
[root@SW ~]# bridge link
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 master br0 state forwarding priority 32 cost 100
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 master br0 state forwarding priority 32 cost 100
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 master br0 state forwarding priority 32 cost 100
```

Рис. 9 Пример настройки моста

В директории /sys/class/net/br0/bridge/ установили параметр multicast_snooping равным единице, чтобы включить технологию IGMP Snooping на коммутаторе. В этой же директории установили параметр multicast_querier равным единице. Данный параметр необходим, чтобы

интерфейс отправлял IGMP-запросы [6]. Пример настройки IGMP Snooping представлен на рисунке 10.

```
[root@SW ~]# ip link set dev br0 type bridge mcast_snooping 1
[root@SW ~]# ip link set dev br0 type bridge mcast_querier 1
[root@SW ~]# cat /sys/class/net/br0/bridge/multicast_snooping
1
[root@SW ~]# cat /sys/class/net/br0/bridge/multicast_querier
1
```

Рис. 10 Пример настройки IGMP Snooping

Для тестирования работоспособности протокола IGMPv2 используем пакет iperf. С помощью данного пакета вошли на устройствах PC2-1 и PC3-1 в режим ожидания входящего трафика, после чего отправили с устройства PC1-1 multicast-трафик в мультикаст группу с адресом 224.2.2.2. Пример использования пакета iperf представлен на рисунках 11, 12.

```
[root@PC2 ~]# iperf -s -u -B 224.2.2.2 -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Binding to local address 224.2.2.2
Joining multicast group  224.2.2.2
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
```

Рис. 11 Вход в режим ожидания входящего трафика

```
[root@PC1 ~]# iperf -c 224.2.2.2 -u -T 5 -t 30 -i 1 -b 1M
------------------------------------------------------------
Client connecting to 224.2.2.2, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
Setting multicast TTL to 5
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 192.168.1.2 port 37659 connected with 224.2.2.2 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   131 KBytes  1.07 Mbits/sec
```

Рис. 12 Отправка multicast-трафика

На всех интерфейсах выполнили захват трафика, использовав пакет Wireshark. Во время multicast-вещания зафиксировали IGMPv2 и UDP пакеты на всех интерфейсах, кроме интерфейса между коммутатором и устройством PC3-1 [7]. На данном интерфейсе отсутствуют UDP пакеты, так как в ходе работы мы вошли в режим ожидания multicast-трафика только на устройстве PC2-1, что наглядно демонстрирует корректную работу технологии IGMP Snooping. Результаты тестирования представлены на рисунках 13, 14.

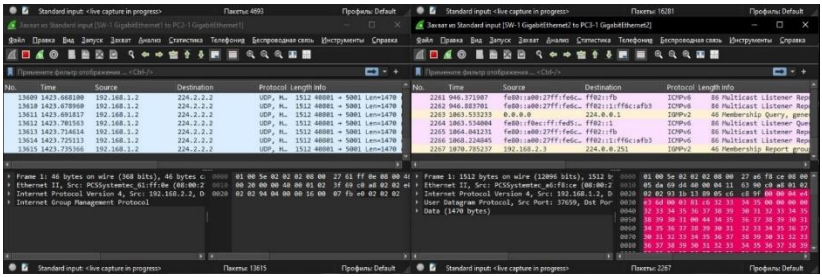


Рис. 13 Захват трафика на всех интерфейсах с помощью Wireshark

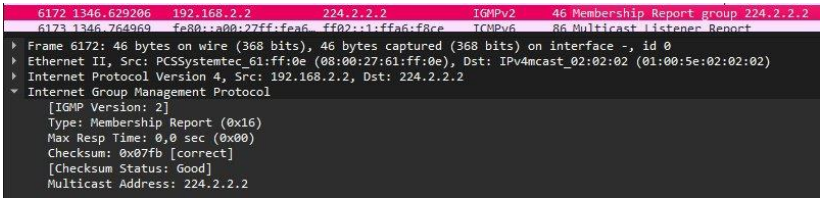



Рис. 14 Подробный анализ пакета IGMPv2 в Wireshark

Нами было обнаружено, что IGMP Snooping не работает, если на коммутаторе при настройке моста использовать пакет OpenvSwitch, т.к. у данного пакета отсутствует поддержка технологии IGMP Snooping. Был сделан вывод, что для настройки и тестирования протокола IGMPv2 лучшим решением является Linux Bridge.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Калашников С. Оптимизация передачи multicast-трафика в локальной сети с помощью IGMP snooping / Калашников С. [Электронный ресурс] // habr [сайт]. — URL: https://habr.com (дата обращения: 21.05.2025).

2. Куклева Е. Приручаем multicast / Куклева Е. [Электронный ресурс] // habr: [сайт]. — URL: https://habr.com (дата обращения: 21.05.2025).

3. Уймин, А. Г. Компьютерные сети. L2-технологии: практикум для СПО / А. Г. Уймин — Саратов: Профобразование, Ай Пи Ар Медиа, 2024 — 190 с.

4. IGMP / [Электронный ресурс] // Википедия : [сайт]. — URL: https://ru.wikipedia.org (дата обращения: 22.05.2025).

5. Static Multicast Routing / [Электронный ресурс] // ALT Linux Wiki: [сайт]. — URL: https://www.altlinux.org (дата обращения:

27.05.2025).

6. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. Учебное пособие для вузов / А. Г. Уймин — Санкт-Петербург: Лань, 2024 — 116 с.

7. Э. Таненбаум, Д. Уэзеролл. Компьютерные сети [Текст] / Э. Таненбаум, Д. Уэзеролл. — 6-е изд. — Санкт-Петербург: Питер, 2023 — 992 с.

***УДК 004.94+004.946***

***Чернобровенко А.Е.***
***Научный руководитель: Островский А.М., канд. соц. наук., доц.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КУАЙНЫ ДЛЯ ПОИСКА ПОДМНОЖЕСТВ ЧИСЕЛ С НУЛЕВОЙ СУММОЙ

Куайны (компьютерные программы, воспроизводящие свой код) выступают удобной моделью для изучения вычислительных характеристик алгоритмов, поскольку их структура требует точной самореференции и оптимальной организации языкового выражения, обеспечивающей воспроизводство без внешних зависимостей. Анализ куайнов позволяет исследовать минимальную сложность, необходимую для самовоспроизведения, и определенные свойства алгоритмической самодостаточности.

Применение куайнов для анализа NP-трудных задач вселяет надежду на нахождение новых подходов к их декомпозиции через изучение взаимосвязи между структурой самовоспроизводящегося кода и сложностью реализуемых вычислительных схем.

В этом контексте классическая проблема о нахождении непустого подмножества множества чисел с суммой, равной нулю (Subset Sum Problem) представляет особый интерес как пример задачи, для которой интеграция алгоритма в структуру куайна позволяет проследить, как рост вычислительной сложности влияет на увеличение объёма и сложности самовоспроизводящегося кода.

Задача формулируется следующим образом: дано множество натуральных чисел; требуется определить, существует ли непустое подмножество, сумма элементов которого равна нулю, и в случае существования — найти одно из таких подмножеств. Для этой задачи не существует известного полиномиального алгоритма решения в общем

случае, а её сложность растёт экспоненциально с увеличением размера входных данных.

Для того, чтобы определить чувствительность структуры куайна к усложнению алгоритма, можно поэтапно модифицировать его код, внедряя всё более затратные по времени решения и отслеживая, как это отражается на размере, читаемости и самодостаточности программы. Это позволяет не только выявить пределы компактности самовоспроизводящегося кода, но и оценить, как внутренние зависимости и рекурсивные элементы влияют на общую вычислительную нагрузку и устойчивость схемы к росту сложности.

В данной работе рассматривается генерация самовоспроизводящихся программ (куайнов) с некоторыми конструктивными мутациями и проводится анализ их поведения. Представляется, что далее можно исследовать как добавление механизмов перебора, мемоизации, жадных и приближённых стратегий влияет на структуру куайна и порог его воспроизводимости. Одним из ключевых аспектов анализа является отслеживание баланса между кодом, отвечающим за логику задачи, и кодом, обеспечивающим самореференцию — при превышении определённой сложности задача начинает «вытеснять» саму способность программы к полной самовоспроизводимости.

Также может рассматриваться возможность использования сжатия и кодогенерации как средств компенсации роста сложности внутри куайна. Например, применение макроподстановок, шаблонных генераторов или even-odd инвариантов может позволить сохранять воспроизводимость даже при увеличении логических ветвлений и объёма состояния. Это особенно важно для задач, в которых количество конфигураций растёт экспоненциально.

Для оценки вычислительных характеристик построенных куайнов предлагается использовать метрики, включающие:

1) Объём самовоспроизводимого кода (в байтах или токенах).

2) Глубину самореференции (уровень вложенности ссылок на собственные структуры).

3) Сложность трассировки воспроизведения (оценку сложности выполнения до восстановления полного исходного текста).

4) Устойчивость к мутациям, определяемая через минимальные изменения, нарушающие воспроизводимость.

В контексте вычислительного эксперимента нами были разработаны серии куайнов, инкапсулирующих различные стратегии решения задачи поиска подмножеств с нулевой суммой. Эти программы не только воспроизводят свой собственный исходный код, но и

выполняют вычисления, направленные на нахождение искомого подмножества в заданном множестве чисел. Такой подход позволяет экспериментально оценить, как включение алгоритмической нагрузки NP-трудного характера влияет на структуру, размер и устойчивость самовоспроизводящегося кода.

Алгоритм 1. Алгоритм перебирает все возможные подмножества заданного списка чисел, рекурсивно выбирая либо включение, либо исключение каждого элемента. В каждом рекурсивном вызове происходит проверка: если достигнут конец списка, а сумма выбранных чисел равна нулю и подмножество непусто, то оно возвращается как результат. Сам алгоритм оформлен в виде куайна — он содержит в себе строку, хранящую собственный исходный код, и выводит его при нахождении решения. Таким образом, происходит не только вычисление, но и самовоспроизведение: программа печатает свой код, подставляя актуальное множество чисел. Такая конструкция позволяет одновременно анализировать поведение алгоритма решения NP-трудной задачи и устойчивость структуры куайна при усложнении логики.

```
numbers = [3, 1, -4, 2]
f = lambda i, s, p: (
    p
    if i == len(numbers) and s == 0 and p
    else i < len(numbers)
    and (
        f(i + 1, s, p)
        or f(
            i + 1,
            s + numbers[i],
            p + [numbers[i]],
        )
    )
)
S = '''numbers = %r
f = lambda i, s, p: (
    p
    if i == len(numbers) and s == 0 and p
    else i < len(numbers)
    and (
        f(i + 1, s, p)
        or f(
            i + 1,
            s + numbers[i],
            p + [numbers[i]],
        )
    )
)
S = %r
if r := f(0, 0, []):
    print(S %% (numbers, S))
    print("#", r)
'''
if r := f(0, 0, []):
    print(S % (numbers, S))
    print("#", r)
```

Рис. 1 Алгоритм 1. Рекурсивный самовоспроизводящийся перебор подмножеств с нулевой суммой

Алгоритм 2. Алгоритм осуществляет поиск подмножества заданного множества чисел, сумма которого равна нулю, с использованием рекурсии и метода ветвей и границ. На каждом шаге он принимает решение — включать или не включать текущий элемент — и отслеживает накопленную сумму. Если сумма на каком-либо этапе становится меньше теоретически возможного минимума, вычисленного как сумма всех отрицательных элементов, соответствующая ветка отсеивается. При достижении конца списка проводится проверка, равна ли накопленная сумма нулю, и если да — возвращается найденное подмножество. Алгоритм встроен в структуру куайна, что позволяет

программе не только решать задачу, но также печатать собственный исходный код вместе с найденным решением.

```
numbers = [3, 1, -4, 2]
total = sum([x for x in numbers if x < 0])

def f(i, s, p):
    # Отсекаем, если суммарно уже не может быть достигнут ноль
    if s < total:
        return None
    if i == len(numbers):
        return p if s == 0 and p else None
    # Ветка без включения numbers[i]
    res = f(i + 1, s, p)
    if res:
        return res
    # Ветка с включением numbers[i]
    return f(i + 1, s + numbers[i], p + [numbers[i]])

S = '''numbers = %r
total = sum([x for x in numbers if x < 0])

def f(i, s, p):
    if s < total:
        return None
    if i == len(numbers):
        return p if s == 0 and p else None
    res = f(i + 1, s, p)
    if res:
        return res
    return f(i + 1, s + numbers[i], p + [numbers[i]])

S = %r
if r := f(0, 0, []):
    print(S %% (numbers, S))
    print("#", r)
'''

if r := f(0, 0, []):
    print(S % (numbers, S))
    print("#", r)
```

Рис. 2 Алгоритм 2. Самовоспроизводящийся поиск подмножества с нулевой суммой и отсечением невозможных ветвей

Таблица — Сравнение самовоспроизводящихся алгоритмов решения задачи Subset Sum по структурным и вычислительным метрикам

| Метрика \ Алгоритм | Алгоритм 1 | Алгоритм 2 |
|---|---|---|
| Объём кода (байт) | 667 | 966 |
| Объём кода (токены) | 102 | 157 |
| Глубина самореференции | 2 | 2 |
| Сложность трассировки воспроизведения | 6 | 14 |
| Устойчивость к мутациям (оценка) | Низкая | Низкая |

Проведённые эксперименты позволяют утверждать, что куайны, инкапсулирующие в себе NP-трудные компоненты, могут служить моделью для оценки вычислительного потенциала, после которого системная самодостаточность рушится. Это, в свою очередь, открывает перспективы для нового взгляда на границы аппроксимируемости, декомпозируемости и возможного автоматического анализа сложности программ через их способность к самовоспроизводству.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Saghiri, A.M., Wang, N. Self-Evolving Programs: A Novel Approach Leveraging LLMs and Quine Programs / A.M. Saghiri, N. Wang. — 2024. — Режим доступа: https://www.wpunj.edu (Дата обращения 5.5.25)

2. Sarkar, A. Quines are the fittest programs: Nesting algorithmic probability converges to constructors / A. Sarkar. — arXiv:2010.09646. — 2020. — Режим доступа: https://arxiv.org (Дата обращения 5.5.25)

3. Moss, L.S. Algebra of Self-Replication / L.S. Moss. — arXiv:2309.09931. — 2023. — Режим доступа: https://arxiv.org (Дата обращения 5.5.25)

4. Островский А.М. О компьютерных технологиях поиска эмпирических закономерностей в базах данных // Социология: 4М. — 2008. — №27. — С.140 — 157

5. Островский А.М. Оптимизация социального управления человеко-компьютерными системами в техническом вузе: Монография.

— Белгород: Изд-во "Белаудит"; БГТУ им. В.Г. Шухова, 2003. — 208 с. — ISBN 5-7414-0083-3.

***УДК 004.056.55***

***Черновский Д.Д.***
***Научный руководитель: Жданова С.И. ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ (GAN) ДЛЯ УЛУЧШЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Системы обнаружения вторжений (IDS) – это, без преувеличения, краеугольный камень современной кибербезопасности. Однако у них есть свои ахиллесовы пяты: им непросто успевать за калейдоскопом хакерских атак, да и ложные тревоги – частый гость. И вот здесь на сцену выходят генеративно-состязательные сети (GAN) – интересный класс моделей глубокого обучения, который, похоже, способен здорово помочь в решении этих проблем. Суть в том, чтобы «научить» GAN работать на благо IDS. Например, они могут генерировать правдоподобные, но синтетические данные об атаках, чтобы лучше натренировать защитные системы. Ещё GAN помогают выявлять необычное, подозрительное поведение в сети или повышать «иммунитет» IDS к хитрым атакам через так называемое адверсариальное обучение. Конечно, у этого подхода есть не только плюсы, но и свои «подводные камни», да и поле для будущих исследований тут огромное – область-то развивается семимильными шагами.

Если копнуть глубже, то традиционные IDS часто пасуют перед лицом всё новых и всё более изощрённых киберугроз. Одни, которые работают по принципу "знаю этого вредителя в лицо" (сигнатурные), слепы к абсолютно новым, "нулевого дня" атакам. Другие, что пытаются отловить всё "не как обычно" (на основе аномалий), то и дело бьют ложную тревогу или, наоборот, пропускают удар. Добавьте сюда вечную нехватку хороших, разнообразных данных по свежим атакам – и картина становится совсем не радужной для обучения и проверки IDS. Но тут на помощь приходят те самые GAN, придуманные Яном Гудфеллоу с коллегами. Это как игра в кошки-мышки между двумя нейросетями: одна (генератор) изо всех сил старается создать данные, неотличимые от настоящих, а вторая (дискриминатор) – пытается их

разоблачить. Именно этот "творческий спор" и открывает новые перспективы для прокачки IDS.

Давайте представим, как это работает. У GAN есть генератор – этакая фабрика, которая из случайного "сырья" (шума) производит, скажем, образцы сетевого трафика или записи из системных журналов, очень похожие на следы реальных атак или, наоборот, на обычную, мирную работу системы. А есть дискриминатор – строгий критик, который смотрит и на настоящие данные, и на "поделки" генератора, вынося вердикт: "верю" или "не верю". В контексте IDS, GAN предлагают несколько любопытных сценариев.

Один из них – это "наштамповать" синтетических данных об атаках. Это просто спасение, когда реальных примеров атак мало или они однотипны. Таким образом можно "разбавить" обучающие наборы, чтобы IDS не была перекошена в сторону обычного трафика, и научить её распознавать больше разных угроз. Более того, так можно даже попытаться смоделировать характеристики атак, которых ещё не было, если обучить GAN на достаточно общих признаках. Да и для стресс-тестов IDS – самое то: проверить, как она справится с чем-то новым. Исследователи, например, уже успешно «скармливали» классификаторам IDS сгенерированные GAN данные о DoS-атаках, и это давало хорошие результаты.

Ещё одно интересное применение – это ловля аномалий. Представьте, мы натренировали GAN на огромном количестве данных о том, как система ведёт себя в обычном, "здоровом" состоянии. Генератор научится идеально воспроизводить эту норму. И вот, если ему подсунуть что-то из ряда вон выходящее – например, признаки начинающейся атаки – он не сможет это так же гладко "перерисовать". Большая ошибка в такой реконструкции или если дискриминатор с сомнением отнесется к этому образцу, как раз и будет сигналом: "Внимание, аномалия!". Этот метод хорош для охоты на "атаки нулевого дня", о которых мы ещё ничего не знаем.

И, наконец, адверсариальное обучение – это как закалка IDS. Хакеры ведь тоже не дремлют и придумывают, как обмануть защитные системы. GAN могут выступить в роли такого "продвинутого хакера", генерируя особенно коварные примеры атак, которые существующая IDS может пропустить. Если затем включить эти "учебные тревоги" в тренировочный процесс IDS, она станет куда более устойчивой и научится распознавать даже самые хитрые уловки.

Преимуществ у такого подхода немало. Это и шанс научиться выявлять те самые "атаки нулевого дня", и способ решить наболевшую проблему нехватки данных по редким атакам. IDS, "закалённые" в боях

с GAN-сгенерированными угрозами, становятся более крепкими орешками для злоумышленников. А если GAN научится лучше моделировать "норму", то и ложных срабатываний, по идее, должно стать меньше.

Но не всё так гладко. Обучение GAN – та ещё задачка. Они капризны, могут "зацикливаться" на производстве однотипных данных или вовсе не сходиться к нужному результату. Плюс, это довольно ресурсоёмкий процесс, требующий мощного "железа" и времени. Как оценить, насколько хороши и полезны сгенерированные атаки – тоже большой вопрос, универсальной линейки тут нет. Да и сами GAN, как и многие их собратья из мира глубокого обучения, зачастую – "чёрный ящик": почему они приняли то или иное решение, понять сложно. И всегда есть риск, что генератор либо создаст слишком "идеальные" атаки, которые легко поймать, либо, наоборот, что-то настолько оторванное от реальности, что обучение на этом будет бессмысленным.

Тем не менее, работа кипит. Учёные ищут способы сделать GAN более стабильными, придумывают, как подружить их с другими методами машинного обучения – например, с обучением с подкреплением. Очень важно научиться "заглядывать внутрь" GAN, чтобы понимать их логику. Стоит задача адаптировать их для работы в реальном времени, где каждая секунда на счету. Не хватает и общих "полигонов" – стандартных наборов данных и тестов – чтобы честно сравнивать разные подходы. Интересное направление – федеративное обучение GAN, когда модели учатся на данных из разных источников, не компрометируя их конфиденциальность.

В общем, генеративно-состязательные сети – это действительно многообещающий инструмент, способный серьёзно усилить наши системы обнаружения вторжений. Возможность создавать реалистичные сценарии атак, выявлять нештатные ситуации и делать IDS более "зубастыми" – всё это открывает новые горизонты в кибербезопасности. Да, есть трудности с обучением и оценкой, но наука не стоит на месте, и с каждым днём появляются всё более совершенные решения. Похоже, именно за технологиями вроде GAN – будущее интеллектуальных систем защиты от киберугроз.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Малахов Ю. А. Анализ и применение генеративно-состязательных сетей для получения изображений высокого качества / Ю. А. Малахов, А. А. Андросов, А. В. Аверченков // Журнал Эргодизайн. — 2020. — № 3(17). — С. 167-176.

2. Айрапетов А. Э. Виды генеративно-состязательных сетей / А. Э. Айрапетов, А. А. Коваленко // Достижения науки и образования ООО «Олимп». — 2019. — № 2(100). — С. 1-7.

3. Цибулис Д. Э. Анализ информационных сигналов с использованием генеративно-состязательных нейронных сетей / Д. Э. Цибулис, А. Н. Рагозин // Безопасность информационного пространства Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург. — 2021. — С. 40-44.

4. Разумов С. Е. Использование генеративно-состязательных нейронных сетей для решения проблемы дефицита медицинских данных / С. Е. Разумов, В. С. Панищев, М. И. Труфанов // Информационные технологии и математическое моделирование систем 2020 Труды международной научно-технической конференции. — 2020. — С. 135-136.

5. Жданова С. И. Безопасное хранение электронных образовательных документов с помощью технологии распределенного реестра / С. И. Жданова, И. В. Иванов // Материалы конференций ГНИИ "Нацразвитие". Сборник избранных статей, 2017. — С. 116-119.

***УДК 004.056.55***

***Черновский Д.Д.***
***Научный руководитель: Коршак К.С. ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## КРИПТОВАЛЮТЫ БЕЗ БЛОКЧЕЙНА: БЕЗОПАСНЫ ЛИ DAG-ПРОТОКОЛЫ (IOTA, HEDERA) ПРОТИВ SYBIL-АТАК

Все мы видим, как криптовалюты развиваются. Блокчейн был первым, но у него есть свои болячки – медленно, дорого, не всегда справляется с кучей пользователей. Поэтому народ начал искать что-то новенькое, и тут на сцену выходят так называемые DAGи – направленные ациклические графы. Представьте себе не линейную цепочку блоков, а такую паутину, где транзакции цепляются друг за дружку. IOTA с ее Tangle и Hedera Hashgraph – как раз из этой оперы, обещают быть быстрее и круче. Но, как и везде, где есть что-то ценное, тут же появляются желающие это "что-то" подпортить. Одна из главных заноз – это Sybil-атака. Грубо говоря, это когда один хитрец создает целую армию фейковых "личностей" или узлов в сети, чтобы получить больше влияния, чем ему положено. Зачем? Да чтобы мутить воду:

мешать транзакциям проходить, отрезать честных пользователей от сети, подтасовывать результаты голосования или вообще положить всю систему. Если такая атака удастся, то можно и деньги дважды потратить, и сеть остановить – в общем, катастрофа. Поэтому для ребят, которые делают DAG-криптовалюты, придумать хорошую защиту от этих "многоликих Янусов" – задача номер один.

Давайте посмотрим на IOTA. У них есть Tangle – та самая паутина транзакций, где каждая новая подтверждает две старые. Раньше, чтобы вся эта конструкция не развалилась от атак, у них был специальный "смотрящий" – Координатор. Он время от времени ставил "контрольные точки", показывая, какая версия паутины правильная. Это, конечно, здорово било по рукам любителям Sybil-атак, потому что Координатор всегда мог сказать: "Нет, ребята, вот тут правильно, а ваши фейки – ерунда". Но такой "центральный начальник" – это не очень-то в духе децентрализации, за которую все так топят. Поэтому IOTA взялась за проект Coordicide – то есть "убийство Координатора", чтобы сеть стала по-настоящему самостоятельной.

Главное оружие IOTA против Sybil-атак в новой версии – это "Mana". Представьте ее как репутацию или "вес" в сети. Зарабатываешь Mana, когда держишь монеты IOTA и активно участвуешь в жизни сети – например, отправляешь транзакции, особенно с реальными деньгами. Mana бывает двух видов: одна (Access Mana) дает тебе "зеленый свет" на отправку транзакций – чем больше у тебя ее, тем быстрее твои транзакции пролетают. Это мешает спамерам с кучей фейковых узлов завалить сеть мусором, ведь у них Mana будет кот наплакал. Другой тип Mana (Consensus Mana) определяет, насколько весом твой голос, когда сеть решает, какие транзакции правильные, а какие – нет, в системе консенсуса под названием FPC (Fast Probabilistic Consensus). Там узлы как бы "голосуют" по спорным вопросам, и чей голос громче – зависит от Consensus Mana. Так что, чтобы серьезно повлиять на решения сети, злоумышленнику нужно накопить очень много этой Mana, а для этого – купить и держать кучу токенов IOTA. Это уже делает атаку дорогой. Плюс, Mana помогает узлам находить себе "хороших соседей" для обмена информацией, отсеивая подозрительных новичков без репутации. Сами узлы, конечно, можно насоздавать сколько угодно (ключи-то бесплатные), но без Mana они будут просто бесполезными пустышками. В теории, Mana – это такой экономический щит. Но, конечно, есть вопросы: а что если монета IOTA сильно подешевеет? Или кто-то найдет хитрый способ накручивать Mana?

Теперь заглянем в Hedera Hashgraph. У них свой тип DAG и свой способ договариваться – через "сплетни о сплетнях" и "виртуальное

голосование". Звучит забавно, но на деле это дает очень серьезные гарантии безопасности, так называемую асинхронную византийскую отказоустойчивость (aBFT). Но главная фишка Hedera в борьбе с Sybil-атаками на уровне консенсуса – это то, что не каждый желающий может стать полноценным узлом, который участвует в принятии решений. Есть Совет Управляющих Hedera – это группа больших, известных компаний и организаций. Только они могут запускать эти ключевые узлы. Представьте, что это такой закрытый клуб, куда абы кого с улицы не пустят. Злоумышленнику просто так не пролезть и не наплодить там своих Sybil-узлов.

Вдобавок, Hedera использует Proof-of-Stake. Вес каждого узла Совета в принятии решений (и его доля пирога от комиссий) зависит от того, сколько монет HBAR (это их криптовалюта) у него на счету. И обычные пользователи могут "одолжить" свои монеты узлам Совета, как бы делегируя им свой голос и усиливая их. Так что, даже если представить невероятное – что злодей как-то пробрался в Совет или взломал одну из компаний – ему все равно пришлось бы заполучить контроль над более чем третью всех монет HBAR в стейкинге, чтобы реально навредить. А это уже баснословные деньги и почти нереальная задача. Да, за создание аккаунта и транзакции берут небольшую плату, что отпугивает совсем уж мелких спамеров, но это так, вишенка на торте, а не основной щит. Конечно, Hedera критикуют за то, что Совет – это все-таки элемент централизации. Но если говорить чисто про защиту от Sybil-атак на уровне консенсуса, то их модель очень крепкая.

Так что же в итоге? И IOTA (с ее будущим без Координатора), и Hedera придумали интересные штуки против Sybil-атак, но пошли разными путями. IOTA хочет быть полностью открытой и децентрализованной, полагаясь на то, что экономика (через Mana) и здравый смысл не дадут мошенникам разгуляться. Насколько это будет работать, сильно зависит от того, как точно настроят Mana, не найдут ли в ней дыр, и сколько будет стоить сама монета IOTA – ведь от этого зависит цена атаки. Есть риск, что если монета дешевая или Mana можно легко "нарисовать", то и защита ослабнет. Hedera же выбрала более осторожный путь: производительность и безопасность прежде всего, даже если это означает, что управлять ключевыми узлами будет ограниченный круг доверенных лиц. Зато от Sybil-атак на "святая святых" – процесс консенсуса – они защищены очень хорошо. Здесь атака потребовала бы каких-то невероятных усилий по взлому членов Совета или скупке гигантского количества монет.

Получается, оба подхода показывают, что и без классического блокчейна можно строить системы, устойчивые к "многоликим" атакам. IOTA ставит на умную экономику и репутацию в открытом поле, а Hedera – на управляемое доверие для максимальной защиты ядра. Выбор между ними – это часто выбор между идеалами полной свободы и практическими соображениями скорости и надежности для бизнеса. Ясно одно: ни одна система не застрахована на 100%, и цель – сделать атаку такой дорогой и сложной, чтобы она просто не имела смысла. А как эти DAG-протоколы покажут себя в реальной жизни, под натиском новых угроз – покажет только время и пытливые умы исследователей безопасности.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Микенин Д. В. Биткойн и блокчейн - криптовалюта, которая меняет мир / Д. В. Микенин, О. Ю. Радько // Вестник научных конференций Издательство: ООО "Консалтинговая компания Юком". — 2016. — № 10-7(14). — С. 345-348.
2. Закоржевский В. В. Криптовалюты - обзор, принцип работы, текущее использование, правовое регулирование / В. В. Закоржевский // Глобальные рынки и финансовый инжиниринг. — 2016. — № 3-4. — С. 281-294.
3. Брюховецкий А. А. Классификация основных типов атак в VANET и методы обеспечения безопасности БТС / А. А. Брюховецкий, Ю. В. Таций // Modern science Издательство: Научно-информационный издательский центр "Институт стратегических исследований". — 2021. — № 2-2. — С. 362-367.
4. Пелых В. Я. Проблемы внедрения технологии блокчейн / В. Я. Пелых // Colloquium-journal — 2019. — № 9(33) — С. 1-3.
5. Коршак К. С. Перспективы объединения технологии блокчейн и интернет вещей / К. С. Коршак, А. Д. Московченко // Наукоемкие технологии и инновации (xxv научные чтения) Сборник докладов Международной научно-практической конференции. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. — С. 725-728.

*УДК 004.421.4*

***Черных А.В.***
***Научный руководитель: Косоногова М.А., канд. техн. наук, доц.***
*Белгородский государственный университет*
*им. В.Г. Шухова, г. Белгород, Россия*

# МЕТОД И СРЕДСТВА ВЫЧИСЛЕНИЯ МЕТОК ПО ТЕХНИЧЕСКИМ ХАРАКТЕРИСТИКАМ КОМПЬЮТЕРНЫХ УСТРОЙСТВ

В условиях растущего разнообразия компьютерных устройств, наличия у них различных технических характеристик и их стремительного обновления, процесс выбора подходящего устройства становится все более сложным. Зачастую конечному пользователю требуется быстро и понятно интерпретировать большое количество данных об устройстве, представленных в виде числовых и текстовых значений, что затрудняет принятие решения, т.е. выбор устройства. С проблемой подбора устройства пользователи сталкиваются как в случае личного использования, так и в рамках корпоративных сценариев использования компьютерной техники.

Одним из эффективных способов упрощения восприятия информации является присвоение устройствам меток, отражающих их ключевые свойства в сжатом и осмысленном виде. Такие метки, как «Производительный», «Лёгкий», «Устаревший», «Защищённый» и другие, позволяют обобщить данные о характеристиках устройства и представить их в виде, удобном для анализа и сравнения.

Цель данной работы заключается в разработке метода вычисления меток на основе анализа технических характеристик компьютерных устройств, а также описании программного средства, которое реализует описанную идею. Предлагаемый метод вычисления объединяет простые логические правила с математически сложными расчетами.

Метки — это текстовые ярлыки, присваиваемые компьютерным устройствам на основе анализа их технических характеристик. Они представляют собой обобщённые выводы, сделанные на основе одного или нескольких параметров устройства. В отличие от сухих спецификаций, метки дают быстрое и более понятное представление об особенностях и преимуществах устройства. Для каждого устройства может быть присвоено как одна, так и несколько меток.

При анализе характеристик компьютерных устройств можно выделить множество меток. В данной статье будут описаны следующие метки:

- «Устаревший» и «Новинка»
- «Производительный»
- «Легкий» и «Тяжелый»
- «Защищенный»

Метки «Устаревший» и «Новинка» используются для классификации устройств по степени их актуальности. Данные метки используются для разделения устройств на те, которые недавно поступили на рынок и те, которые находятся уже на грани морального и\или технического устаревания.

При вычислении данной метки используется год выпуска устройства (указывается в характеристиках устройства) и текущий календарный год. Принцип вычисления выглядит следующим образом:

- Если устройство выпущено менее одного года назад, ему присваивается метка «Новинка».
- Если устройство выпущено четыре года назад или ранее, ему присваивается метка «Устаревший».

Пороговое значение в один год при вычислении метки «Новинка» отражает современные тенденции обновления модельного ряда устройств. Порог в четыре года при вычислении метки «Устаревший» обусловлен на основе анализа средних сроков морального и технического устаревания устройств [3-4].

Метка «Производительный» присваивается устройствам, имеющим потенциально высокую производительность. Для вычисления данной метки используется метод взвешенных суммарных баллов [2], который относится к категории методов мультикритериального принятия решений [1]. Выбор данного метода для вычисления данной метки обусловлен следующими причинами:

- Позволяет учитывать несколько разнородных характеристик. Для вычисления данной метки используются такие характеристики, как: конфигурация ядер процессора, его кэш-память, а также его TDP.
- Позволяет задать индивидуальные веса для каждой характеристики, участвующей в расчете.
- Прост в использовании.

Формула расчета выглядит следующим образом (1):

$$S = \sum_{i=1}^{n} (W_i * X_i), \quad (1)$$

где S – итоговая сумма баллов, n – количество критериев, $W_i$ – вес критерия, $X_i$ – оценка альтернативы по i-му критерию (оценка может быть, например, по шкале от 0 до 1 или от 1 до 10).

Т.к. выбранные для вычисления характеристики разнородны, перед началом вычисления выполняется ряд процедур:

- Поиск минимального и максимального значения.
- Нормализация значений выбранных характеристик.
- Присвоение весов каждой характеристике

Конфигурация ядер процессора описывается как количество ядер определенной группы (например, энергоэффективные) и частота этих ядер. Для того, чтобы правильно учитывать данный параметр в ходе основного расчета, метод взвешенных суммарных баллов совместно с нормализацией применяется и к конфигурации ядер процессора.

Нормализация данных выполняется по следующей формуле (2):

$$x_{\text{норм}} = \frac{x - \min(x)}{\max(x) - \min(x)}, \tag{2}$$

где x – исходное значение, $x_{\text{норм}}$ – нормализованное значение, min(x) и max(x) – минимальное и максимальное значения в наборе данных соответственно.

Полученный результат будет нормирован в диапазоне от 0 до 1 и для более понятной интерпретации конечный результат переводится в нормализацию от 0 до 100.

Вычисление метки «Легкий» или «Тяжелый» выполняется исходя из веса устройства, который также обычно указан в технических характеристиках устройства.

Перед вычислением метки определяется средний вес устройств каждого типа по формуле (3), который затем сравнивается с весом рассматриваемого устройства. Помимо этого, вычисляется стандартное отклонение (4).

$$\mu = \frac{1}{k}\sum_{i=1}^{k} w_i \tag{3}$$

Здесь $\mu$ – средний вес, $k$ – количество устройств определенной категории, $w_i$ – вес i-го устройства.

$$\sigma = \sqrt{\frac{1}{k}\sum_{i=1}^{k}(w_i - \mu)^2} \tag{4}$$

Здесь $\sigma$ – стандартное отклонение, $\mu$ – вычисленный ранее средний вес, $w_i$ – вес i-го устройства, $k$ – количество устройств определенной категории.

После выполнения вычислений по формулам (3)-(4), происходит присвоение меток по следующим правилам:

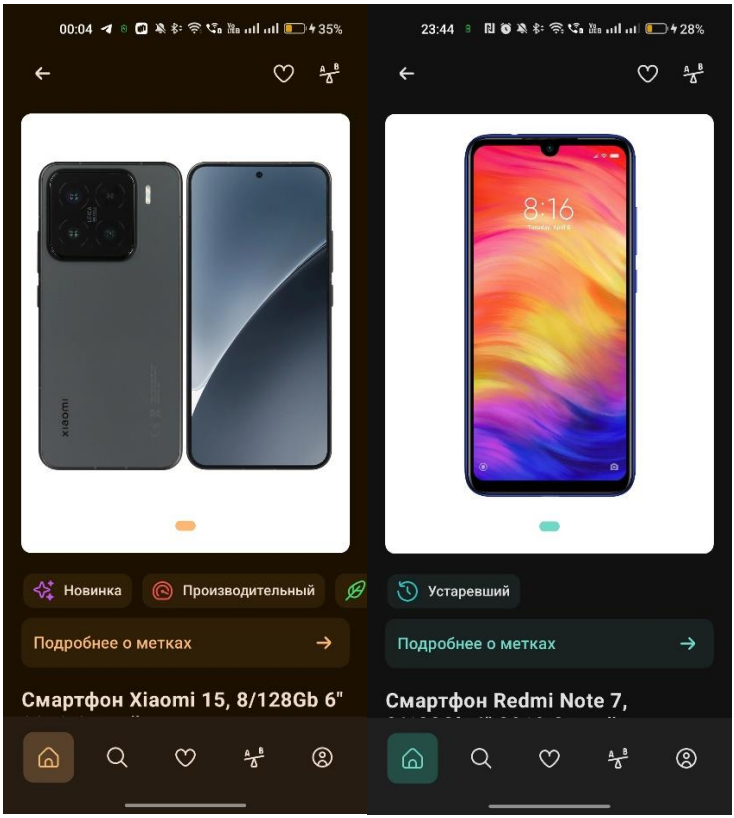
- Устройству присваивается метка «Легкий», если его вес меньше разности среднего значения и стандартного отклонения.
- Устройству присваивается метка «Тяжелый», если его вес больше суммы среднего значения и стандартного отклонения.

Метка «Защищённый» присваивается компьютерным устройствам, которые имеют некоторые программные и аппаратные защитные механизмы. Среди характеристик устройств, для вычисления данной метки используются следующие:

- Степень влагозащиты устройства (IP-рейтинг).
- Наличие сканера отпечатков пальцев.
- Наличие технологии распознавания лица (FaceID).

Метка присваивается на основании наличия в устройстве хотя бы одного из вышеперечисленных параметров.

В качестве средства для вычисления меток, согласно описанному ранее методу, будет выступать разработанное мобильное приложение. На 0 представлены два устройства с вычисленными метками: Xiaomi 15 и Redmi Note 7. Рассмотрим на примере меток «Устаревший» и «Новинка». Redmi Note 7 был выпущен в 2019 году и ему присвоена метка «Устаревший» (метка присваивается, если устройству 4 и более лет). Xiaomi 15 был выпущен в 2025 году и ему присвоена метка «Новинка» (метка присваивается, если устройство выпущено менее года назад). Таким образом, благодаря меткам можно получить понятную информацию об устройстве, не заглядывая в его характеристики.



Метки на Xiaomi 15 и Redmi Note 7

Рассмотренные метки «Устаревший», «Новинка», «Производительный», «Легкий», «Тяжелый» и «Защищенный» способны упростить восприятие сложных параметров, а также сделать выбор устройства более наглядным и интуитивным для пользователя. Вычисление этих меток основано на различных технических характеристиках устройства, некоторые из которых достаточно разнородны. Представленные методики расчета могут быть применены как в обычных пользовательских системах, так и корпоративных решениях.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Черных, А. В. Метод принятия решений на основе баллов. Исследование плюсов и минусов / А. В. Черных // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова : Сборник докладов Международной научно-технической конференции молодых ученых БГТУ им. В.Г. Шухова, Белгород, 20–21 мая 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 443-446. – EDN ALEXKE (дата обращения: 21.05.2025).

2. Черных, А. В. Применение метода взвешенных суммарных баллов для расчета производительности процессора смартфона на основе его характеристик / А. В. Черных // Образование. Наука. Производство: Сборник докладов XVI Международного молодежного форума, Белгород, 30–31 октября 2024 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2024. – С. 258-262. – EDN KEWTNT. (дата обращения: 21.05.2025)

3. Через сколько лет нужно менять смартфон, и какие данные не стоит доверять старому телефону [Электронный ресурс] – Режим доступа: https://overclockers.ru (дата обращения: 21.05.2025)

4. Данные по анализу окончания срока службы устройств [Электронный ресурс] – Режим доступа: https://endoflife.date (дата обращения: 21.05.2025)

5. Лазебная, Е. А. Методы и средства проектирования информационных систем и технологий : Учебное пособие / Е. А. Лазебная. – Белгород : Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. – 127 с. (дата обращения: 21.05.2025)

*УДК 004.023*

***Чжан Ю.***
***Научный руководитель: Спицын В.Г., д-р техн. наук, проф.***
*Национальный исследовательский Томский государственный университет, г. Томск, Россия*

# СОЗДАНИЕ ПАРАЛЛЕЛЬНЫХ КОРПУСОВ ХАРАКТЕРИСТИЧЕСКИХ ПРИЗНАКОВ ДИВАНА НА ОСНОВЕ КИТАЙСКИХ И РОССИЙСКИХ LLM

В настоящее время между Китаем и Россией трансграничная электронная коммерция (Aliexpress, Ozon, Wildberries) и международной торговли развиваются все быстрее, что обуславливает спрос на создание двуязычного контента на платформах электронной коммерции. Однако из-за значительных различий в структуре китайского и русского языков традиционные методы перевода (например, машинный перевод на основе правил или статистический перевод) не могут точно соответствовать межкультурной семантике, а также имеют очевидные недостатки в контроле стиля, локализации продукта и культурной адаптации и в основном полагаются на человеческих переводчиков и команды локализации. В последние годы большие языковые модели (LLM) совершили прорыв в области обработки естественного языка, обладают сложным лингвистическим мышлением и способностью понимать культурные особенности, что открывает новые возможности для автоматического создания кросс-культурных описаний продуктов. В частности, эти модели могут уменьшить зависимость от масштабных наборов данных с ручными метками и обеспечить высококачественное создание кросс-культурного контента с помощью подходов, основанных на обучении «с нуля» и «с нескольких кадров». Цель данного исследования - изучить возможность и эффективность использования передовых больших языковых моделей в качестве интеллектуальных агентов для автоматического создания межкультурной генерации параллельных текстов и характеристических признаков в качестве основы для будущего создания описаний товаров.

Китайская и Российская культуры демонстрируют значительные различия в модели культурных измерений. Hofstede и др. показали, что в китайской культуре больше внимания уделяется коллективизму, маскулинности и долгосрочной ориентации, в то время как в российской культуре выше дистанция власти, фемининность и избегание неопределенности [1]. Эти культурные различия напрямую влияют на достоверность описания товара. Например, Zhang и др.

обнаружили, что потребители в коллективистских культурах с большей вероятностью примут описание продукта, подчеркивающее социальную идентичность и групповую принадлежность, в то время как потребители в индивидуалистических культурах предпочитают описания, подчеркивающие личные интересы и уникальность [2]. Эти культурные различия приводят к тому, что китайцы и русские фокусируются на разных характеристических признаков товаров и описывают их по-разному. Такие различия отражены в крупных языковых моделях, которые разработаны Китаем и Россией. Однако Тао и др. отметили, что магистратура, основанная на обучении по западному корпусу, имеет культурные предубеждения и предубеждения в понимании, когда имеет дело с незападным культурным контентом [3]. Исследование, проведенное Power и соавторами [4], показывает, что даже многоязычная LLM имеет значительные различия в своей работе на разных языках, особенно в понимании выражений, специфичных для культуры, и подразумеваемых культурных знаний. Однако именно эти проявления позволяют нам использовать LLM разных стран для создания корпуса межкультурных характеристических признаков.

Таблица 1 - Система классификации терминологических соответствий

| | Прямые соответствия | Частичные соответствия | Уникальные термины |
|---|---|---|---|
| Определение | Термины с полной семантической эквивалентностью | Частично различающиеся семантические соответствия | Культурно-специфические характеристические признаки |
| Метод обработки данных | Применяется прямой перевод и выравнивание | Фиксация направления различий (CN→RU или RU→CN) Создание адаптационных правил для генерации описаний | Отдельная документация с развернутыми объяснениями Формирование пользовательского интерфейса выбора |

Методология промпт-инженерии (Prompt Engineering):

Теоретическая основа

1. Ролевые игры: модели отвечают как отраслевой эксперт.
2. Семантическое понимание: модели переводят характеристические признаки на основе определения.
3. Сравнительные проверки: получение ответов при различных

обстоятельствах.

4. Многомодульная перекрестная верификация: перекрестная верификация между различными моделями.

5. Процесс итеративной оптимизации

6. Начальная промпт-инженерия: На основе базовых знаний об отрасли, полученных из большой языковой модели, выпущенной в Китае, с использованием перекрестного перевода DeepSeek и YandexGPT.

7. Корректировка промпт-инженерии: Корректировка промпт-инженерии для устранения недостатков результата, полученного в начальной промпт-инженерии.

8. Формулировка вопросов о деталях: Разработка более подробных вопросов или расширенного знания по конкретным аспектам.

9. Перекрёстная проверка: Проверка на согласованность полученных знаний с помощью различных вопросов, и путем многократной перекрестной проверки моделей, опубликованных в Китае и России.

10. Интеграция и подведение итогов: Преобразование полученных параллельных корпусов в определенный формат.

В таблице 2 показаны два значения характеристических признаков материалов дивана и результат, полученный в процессе создания базы данных выравнивания.

Таблица 2 - Результат, полученный в процессе создания базы данных выравнивания

| Значение на китайском рынке - 头层牛皮 | | |
|---|---|---|
| Ситуация | Модель ChatGPT | Модель GigaChat 2 Max |
| Обычный покупатель | Натуральная кожа высокого качества, Натуральная кожа первого слоя | натуральная кожа |
| Профессиональный жаргон | Кожа первого слоя, Лицевая кожа | Кожа первого слоя бычьего происхождения |
| В онлайн-магазинах | Натуральная кожа (первый слой) | натуральная бычья кожа первого слоя |
| Распространенные выражения | Натуральная кожа, Высококачественная натуральная кожа | Настоящая натуральная кожа, Высшего качества кожа |
| Значение на китайском рынке - 磨砂皮 | | |

| | | |
|---|---|---|
| Обычный покупатель | Матовая кожа, Шлифованная кожа | Замша, матовая кожа |
| Профессиональный жаргон | Шлифованная кожа первого/второго слоя, Замшевая поверхность обработанной кожи | Наппа, пескошлифованная кожа |
| В онлайн-магазинах | Натуральная матовая кожа (нубук) | обивка из замши, матовая кожа |
| Распространенные выражения | Матовая кожа, Нубук, Шлифованная кожа | Замша, мелковорсистой кожей |

Для первого значения характеристических признаков, модель ChatGPT и Giga Chat 2 Max выводят подобные результаты: «Кожа первого слоя» и «Лицевая кожа» - специальные термины используются среди производителей мебели и дизайнеров интерьеров; «Натуральная кожа», «Высококачественная натуральная кожа» - распространенные выражения используются в описании товара в онлайн-магазинах и в обычной жизни. На основе полученных результатов, высокая частота использования "натуральная кожа" и подобное выражение (кожа первого слоя) отражают согласованность. ChatGPT склоняется к использованию "высокого качества" для характеристики качества, Giga Chat 2 Max использует "бычья кожа" для характеристики технологии производства.

Второе значение характеристических признаков имеет свои особенности. Главное отличие — китайское название прямо указывает на технологический процесс полировки (шероховатость удаляется и создается гладкий материал), тогда как русские термины делают упор на конечные свойства материала (приятность, красота). На основе полученных результатов, высокая частота использования характеристики "матовая кожа" отражает согласованность. Нубук","Замша" и "Наппа" являются близкими значениями характеристических признаков.

В этом исследовании предлагается метод создания межкультурных параллельных корпусов характеристических признаков дивана на основе китайских и российских LLM. Эта методология содержит трехуровневую систему гармонизации терминов и методологию промпт-инженерии (Prompt Engineering).

Исходя из полученных результатов, мы можем четко видеть, что результаты прямого перевода, основанные на переводчике, не могут удовлетворить созданию межкультурных корпусов характеристических признаков товаров на китайском и русском языках. Метод, предложенный в данной статье, позволяет модели выдавать

высококачественные отраслевые знания и создавать комплексные параллельные корпуса характеристических признаков на основе китайских и российских LLM.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Geert Hofstede. Cultures and organizations: Software of the mind: intercultural cooperation and its importance for survival / Gert Jan Hofstede, Michael Minkov — 1. — New York: McGraw-Hill, 2010 — 576 с..

2. Yanni Zhang. Comparative study of Chinese and American media reports on the COVID-19 and expressions of social responsibility: A critical discourse analysis / Naveed Akhtar, Qamar Farooq, Yiwei Yuan, Irfan Ullah Khan // Journal of Psycholinguistic Research. — 2022-06-01. — № 3. — С. 455-472..

3. Yan Tao. Cultural bias and cultural alignment of large language models / Olga Viberg, Ryan S Baker, René F Kizilcec // PNAS Nexus. — 2024. — № 3. — С. 346-354..

4. Siddhesh Pawar, Junyeong Park, Jiho Jin, Arnav Arora и т.д. Survey of cultural awareness in language models: Text and beyond / Junyeong Park, Jiho Jin, Arnav Arora и т.д. — 1. — 2: , 2024 — 87 с.

***УДК 004.8:338.2***

***Шайдуллина А.Р.***
***Научный руководитель: Уразбахтина Л.Р., канд. экон. наук, доц.***
*Казанский государственный энергетический университет,*
*г. Казань, Россия*

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СТРАТЕГИЧЕСКОМ УПРАВЛЕНИИ РИСКАМИ

Стратегическое управление рисками является основополагающим аспектом стратегии компании. Оно включает в себя выявление и оценку потенциальных рисков, которые могут повлиять на достижение организационных целей и задач.

Стратегическое управление рисками — это непрерывный и проактивный процесс, который позволяет компаниям выявлять уязвимости, смягчать угрозы и извлекать выгоду из возможностей. По мере дальнейшего продвижения в цифровую эпоху будущее стратегического управления рисками будет определяться силой технологий и искусственного интеллекта. Современный мир бизнеса сталкивается с беспрецедентным уровнем неопределенности.

Стратегическое управление рисками, некогда ориентированное на ретроспективный анализ, трансформируется под влиянием технологического прогресса и, в особенности, искусственного интеллекта. Будущее за прогностическим анализом рисков, осуществляемым искусственным интеллектом. Алгоритмы машинного обучения способны обрабатывать огромные массивы данных, выявляя скрытые закономерности и предсказывая потенциальные угрозы задолго до их проявления [1].

Технологии блокчейн обеспечивают прозрачность и безопасность в управлении рисками, минимизируя риски мошенничества и коррупции. Интернет вещей (IoT) предоставляет данные в реальном времени для оперативного реагирования на возникающие риски. Искусственный интеллект автоматизирует процессы оценки рисков, освобождая ресурсы для стратегического планирования и принятия решений. Интеграция этих технологий позволит организациям не только минимизировать потери, но и использовать риски в качестве возможностей для роста и инноваций.

Организации осознают огромный потенциал использования технологий и искусственного интеллекта для улучшения своих методов управления рисками и сохранения лидирующих позиций в сегодняшнем быстро меняющемся бизнес-ландшафте. Одним из ключевых методов, с помощью которых технологии и искусственный интеллект могут коренным образом изменить стратегическое управление рисками, является автоматизация процедур оценки рисков. Ранее процесс оценки рисков требовал значительных временных и ресурсных затрат, зачастую опираясь на ручной сбор и анализ данных.

Однако с появлением передовых инструментов анализа данных и алгоритмов искусственного интеллекта организации теперь могут оптимизировать свои усилия по оценке рисков и получать информацию о потенциальных рисках в режиме реального времени[2]. Еще одна область, в которой технологии и искусственный интеллект могут существенно повлиять на стратегическое управление рисками, — это прогнозирование и предсказание рисков. Используя возможности предиктивной аналитики, организации могут оставаться на шаг впереди потенциальных рисков, что позволяет им принимать упреждающие меры и минимизировать их влияние на бизнес.

Кроме того, технологии и искусственный интеллект могут повысить эффективность стратегий снижения рисков. Например, передовые технологии кибербезопасности на базе искусственного интеллекта могут непрерывно отслеживать сетевой трафик, обнаруживать аномалии и реагировать на потенциальные угрозы

в режиме реального времени. Такой уровень автоматизации и реагирования может значительно улучшить способность организации защищать свои конфиденциальные данные и предотвращать нарушения кибербезопасности. Использование технологий и искусственного интеллекта может способствовать более тесному сотрудничеству и общению между заинтересованными сторонами, вовлеченными в стратегическое управление рисками [3].

Важно отметить, что в России активно развиваются собственные решения в области искусственного интеллекта для управления рисками. Компании внедряют инновационные подходы, адаптированные к специфике отечественного бизнеса и законодательства. Такие решения обеспечивают технологический суверенитет и учитывают особенности российской экономики.

Отечественные разработки в области искусственного интеллекта позволяют российским компаниям эффективно конкурировать на глобальном рынке, обеспечивая высокий уровень защиты от разнообразные угроз, включая санкционные риски и кибератаки. Государственная поддержка таких инициатив в рамках национальных проектов создает прочную основу для дальнейшего развития этого направления.

Стратегическое управление рисками стало незаменимой практикой для организаций, стремящихся к успеху и сохранению конкурентного преимущества. Осознавая значимость качественной оценки рисков, применяя подходящие инструменты, компании способны самостоятельно выявлять и расставлять приоритеты в отношении рисков, разрабатывать целевые стратегии их минимизации и принимать обоснованные решения для обеспечения безопасности своего бизнеса и оптимизации общей стратегии.

В эпоху цифровой трансформации компании, инвестирующие в передовые технологии управления рисками и формирующие культуру осознания рисков на всех уровнях организации, будут наиболее подготовлены к преодолению неопределенностей и использованию возможностей динамичной глобальной экономики.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Artificial Intelligence Techniques for Flood Risk Management in Urban Environments / W. Sayers, D. Savic, Z. Kapelan, R. Kellagher // Procedia Engineering. 2024. Vol. 70. P. 1505-1512.

2. Нагродская В.Б. Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л.А. Новоселовой. М.: Проспект, 2020. 128 с.

3. Карцхия А.А. Цифровые технологические (онлайн) платформы: российский и зарубежный опыт регулирования // Гражданское право. 2021. № 3. С. 25—28.

***УДК 004.056:623.746.-519***

***Шевченко А.С.***
*Национальный исследовательский университет,*
*г. Санкт-Петербург, Россия*

## ОБЗОР ИНФОРМАЦИОННЫХ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

Рынок потребительских и коммерческих беспилотных воздушных судов в последние десятилетия развивается быстро, в том числе и в России [1]. Для работы беспилотных воздушных судов используется различное программное обеспечение, встраиваемые системы и беспроводные каналы связи, которые могут быть уязвимы для злоумышленников.

В этой работе рассматриваются значимые Common Vulnerabilities and Exposures (CVE), выявленные в 2020-2025 годах в программном обеспечения различного оборудования, используемого в сфере беспилотных авиационных систем.

**Платформы с открытым исходным кодом.** Полетные контроллеры, такие как PX4 Autopilot и Ardupilot широко используются в сфере любительских и профессиональных беспилотных воздушных судов. Несколько критических CVE были обнаружены в системах этих контроллеров.

К примеру, до версии 1.14.0-rc1 PX4 содержал ошибку переполнения буфера в куче парсера данных из-за отсутствия проверки индекса, что позволяло злоумышленнику записывать неограниченные данные в память кучи (CVE-2023-46256) [2].

В PX4 1.14.0-rc2 имелась аналогичная уязвимость глобального переполнения буфера в парсере протокола CRSF RC (CrsfParser_TryParseCrsfPacket), которое могло быть вызвано отправкой неправильно сформированного пакета дистанционного управления, что приводило к непредсказуемому поведению беспилотника (CVE-2023-47625) [2]. Подобные ошибки синтаксического анализа обычно

возникают из-за неадекватной проверки входных данных на основе поступающих данных радио или датчиков.

PX4 также подвержен уязвимостям, связанным с геозонами: в версиях до 1.14 отсутствовала надлежащая синхронизация загрузки данных о геозонах (состояние "гонки") (CVE-2024-24254) [2]. Злоумышленник мог воспользоваться этим для загрузки перекрывающихся или несогласованных границ бесполетной зоны. В другом баге PX4 (CVE-2024-30800) логические ошибки позволяли злоумышленникам полностью обойти геозону, позволяющим беспилотнику залететь в запретные зоны [2].

Веб-интерфейс ArduPilot содержал ошибку, связанную с повреждением памяти, в функции HTTP CGI unescape (CVE-2022-28711), в результате чего веб-запрос мог повредить память [2]. Эта критическая ошибка (CVSS 9.8) могла привести к выполнению кода на полетном контроллере.

На других платформах, разрабатываемых сообществом, также имелись различные CVE. Например, при анализе MAVLink были обнаружены уязвимости PX4/AP: CVE-2024-38951 описывает переполнение буфера в PX4 1.12.3, вызванное вредоносным сообщением MAVLink, что привело к отказу в обслуживании [2]. Более старая уязвимость (CVE-2021-34125) в PX4 1.11.3 позволяла злоумышленникам выполнять произвольные команды NuttX в БВС на базе Yuneec/PX4, что приводило к утечке конфиденциальных данных [2]. Таким образом, полетные контроллеры с открытым исходным кодом сталкиваются с классическими программными ошибками (переполнение буфера, условия гонки) в коде полета и инструментах поддержки. Эти проблемы означают необходимость тщательной проверки входных данных и контроля параллелизма в программном обеспечении беспилотных летательных аппаратов в режиме реального времени.

**Проприетарные платформы.** Производители коммерческих БВС также столкнулись с различными CVE. DJI, лидер рынка, имел несколько серьезных недостатков в своих устройствах и SDK. Например, несколько моделей DJI (серия Mavic 3, Matrice 300) содержали уязвимости в «v2sdk_service», работающем на порту 10000. CVE-2023-51454 описывает запись за пределами допустимого диапазона в libv2_sdk DJI, что позволяло повредить память или выполнить код через специально созданную полезную нагрузку TCP [2].

Аналогично, CVE-2023-51452 (Record Future) и CVE-2023-6948 включают неправильные проверки ввода в том же SDK, что приводит

либо к сбоям в работе службы, либо к отказу в обслуживании на перечисленных ранее БВС [2]. Подсистема Wi-Fi DJI также была уязвима: в CVE-2023-6951 говорится о «слабых учетных данных» в сети Wi-Fi QuickTransfer некоторых моделей Mavic и Matrice [2]. Злоумышленник мог получить ключ WPA2 и подключиться к точке доступа БВС, что давало ему несанкционированный доступ и возможность расшифровки пользовательского трафика.

В ПО производителя Parrot также имелись CVE. Например, CVE-2022-46416 (Parrot Bebop 4.7.1) позволял злоумышленнику в сети Wi-Fi БВС исчерпать пул адресов DHCP, что не давало клиентам подключаться [2]. Исчерпание DHCP фактически ведет к отказу в обслуживании в отношении подключения к наземной станции. Как и уязвимость DJI QuickTransfer, она возникает из-за невнимания к ограничениям сетевых служб.

Модуль удаленного распознавания Holy Stone/Drone-Go2 (ASTM F3411 BLE broadcast) имел уязвимость CVE-2024-52876, которая позволяла запускать удаленное отключение питания через интерфейс удаленного распознавания GATT [2]. Неподтвержденная команда BLE на удаленном радиомаяке идентификации могла отключить беспилотное воздушное судно.

Таким образом, проприетарные системы беспилотных воздушных судов также имеют широкий спектр типов CVE: переполнение памяти (DJI SDK), слабость аутентификации (DJI Wi-Fi, Autel BLE) и сбои в обслуживании (Parrot DHCP).

**Уязвимости систем идентификации.** Внедрение Remote ID создало новые категории уязвимостей. Некоторые CVE нацелены на приемники и модули Remote ID. Одним из примеров является серия приемников BlueMark DroneScout (используется службами безопасности и правоохранительными органами). Исследователи обнаружили несколько CVE в прошивке приемника BlueMark DroneScout ds230.

CVE-2023-31191, представляет собой ошибку внедрения информации: отправляя поддельные сообщения Open Drone ID (ODID) по соседним каналам, злоумышленник может заставить приемник сообщать сфабрикованные данные JSON вместо настоящих [2]. CVE-2023-31190 — неправильная аутентификация, которая может допускать произвольные обновления прошивки [2]. CVE-2023-29156 — это аналогичная уязвимость «потеря информации», при которой поддельные сообщения заставляют получателя игнорировать подлинные маяки Remote ID [2]. Другими словами, злоумышленники

могут подделывать или глушить сигналы RID, чтобы скрыть присутствие беспилотного воздушного судна.

**Основные типы уязвимостей.** После проведения обзора известных уязвимостей программного обеспечения беспилотных воздушных судов, можно выделить наиболее распространенные типы:

1. Ошибки доступа к памяти: переполнение буфера и непроверенное копирование буферов. Сюда относятся ранее упомянутые CVE-2023-51454, CVE-2024-23957.

2. Недостатки аутентификации и контроля доступа: слабые или жестко закодированные ключи позволяют получить доступ к сети. К этому типу относятся CVE-2023-6951, CVE-2023-31190.

3. Уязвимости отказа обслуживания: вызываются исчерпанием ресурсов (CVE-2022-46416), использованием условий гонки (CVE-2024-24254), отправкой вредоносных пакетов (CVE-2024-38951).

4. Спуфинг и инъекции: Подмена Remote ID (CVE-2023-31191), утечка учетных данных Wi-Fi (DJI CVE-2023-6951) демонстрируют, как злоумышленники могут выдавать себя за авторизованные источники или прослушивать коммуникации.

**Методы предотвращения.** В качестве методов борьбы с уязвимостями можно перечислить следующие:

1. Усложнение протоколов связи. Внедрение сильной аутентификации и шифрования для всех видов связи.

2. Избегание жестко закодированных учетных данных.

3. Строгая проверка входных данных. Все входящие данные должны обрабатываться как ненадежные. Использование языков с безопасным доступом к памяти или статического анализа может помочь предотвратить подобные ошибки.

4. Важны надежные механизмы обновления и своевременное обновление встроенного ПО.

**Заключение**. Исходя из проведенного обзора можно сделать вывод, что в течение последних пяти лет обнаруживались уязвимости программного обеспечения связанных с беспилотными авиационными системами: от полетных контроллеров с открытым исходным кодом, коммерческих платформ беспилотных воздушных судов, до устройств удаленной идентификации.

Распространенные уязвимости включают в себя неконтролируемые входные данные, плохую аутентификацию, уязвимые реализации протоколов спуфинг и инъекции.

Для обеспечения безопасности беспилотных авиационных систем, эффективными являются следующие меры: совершенствование протоколов связи, использование языков с безопасным доступом к

памяти, использование инструментов статического анализа для проверки кода программного обеспечения полетных контроллеров и иного оборудования, проверка и фильтрация входных данных, избегание жестко закодированных учетных данных.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рынок гражданских беспилотных аппаратов. Объем, динамика и сценарии применения беспилотников в отраслях экономики [Электронный ресурс] // Ростелеком. — URL: https://ai.gov.ru/ (Дата обращения 5.5.25)
2. Vulnerabilities [Электронный ресурс] // National Vulnerability Database. — URL: https://nvd.nist.gov/ (дата обращения: 14.05.2025)
3. Рынок гражданских беспилотных аппаратов. Объем, динамика и сценарии применения беспилотников в отраслях экономики [Электронный ресурс] // Ростелеком. — URL: https://ai.gov.ru/ (Дата обращения 5.5.25)

***УДК 004.056.5***

***Шевченко П.В.***
***Научный руководитель: Коломыцева Е. П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБНАРУЖЕНИИ КИБЕРАТАК И АНОМАЛИЙ

С каждым годом объём информации, с которой мы работаем, становится всё больше. Вместе с этим растёт и число кибератак. Привычные методы защиты уже не справляются так эффективно, как раньше. Современные атаки становятся всё хитрее: злоумышленники используют новые технологии и сложные способы маскировки, из-за чего обнаружить угрозу сразу не всегда получается. В таких условиях особенно важно использовать более продвинутые подходы. Один из них — это применение искусственного интеллекта (ИИ). Благодаря ИИ можно в автоматическом режиме следить за состоянием сети, замечать подозрительную активность и сразу принимать меры. Это помогает быстрее реагировать на угрозы и лучше защищать данные.

***Методы применения ИИ в выявлении аномалий***

ИИ сегодня активно применяется в области безопасности, потому что он умеет находить то, что выходит за рамки обычного поведения в

системе. Это особенно важно, когда речь идёт о потенциальных рисках, которые ещё не успели нанести вред. В отличие от старых методов, где всё работало по заранее заданным правилам, искусственный интеллект использует гибкие алгоритмы. Они могут адаптироваться под новую обстановку и даже учиться распознавать ранее неизвестные атаки.

*Машинное обучение*

Одним из самых полезных инструментов для выявления аномалий является машинное обучение. Оно основано на том, что система анализирует большое количество предыдущих данных и «запоминает», как в норме работает система. Если появляется что-то странное или необычное, алгоритм это замечает и сообщает о возможной угрозе. Например, в банках такие технологии помогают выявлять мошенничество: система отслеживает обычное поведение клиентов и сигнализирует, если происходит что-то подозрительное, например, нестандартная операция по счёту.

*Глубокие нейронные сети*

Глубокие нейросети (ГНС) представляют собой сложные многоуровневые структуры, способные обрабатывать большие объемы данных и обнаруживать скрытые взаимосвязи. Они особенно эффективны при выявлении комплексных атак: целевые фишинговые атаки или вредоносные программы, которые маскируются под легитимные процессы. ГНС используются в системах защиты корпоративных сетей, где они анализируют сетевой трафик и выявляют аномалии, связанные с возможными утечками информации.

*Анализ поведения и аномалий на основе поведенческих моделей*

Метод анализа поведения и аномалий основан на изучении типичных действий пользователей и автоматизированных систем. В случае отклонения от стандартного поведения система может запустить дополнительную проверку. Например, если сотрудник компании неожиданно начинает скачивать большие объемы данных в нерабочее время, это может указывать на взлом его учетной записи.

*Практическое применение*

Один из ярких примеров того, как искусственный интеллект помогает в обеспечении безопасности — это Microsoft Defender. Защита от угроз Microsoft Defender для облачных служб ИИ определяет угрозы для создания приложений искусственного интеллекта в режиме реального времени и помогает реагировать на проблемы безопасности.

Искусственный интеллект постоянно развивается и предлагает всё более полезные способы защиты, которые заметно позволяют сократить риски и улучшить безопасность информационных систем.

***Применение ИИ в предотвращении кибератак***

На сегодняшний день искусственный интеллект используется не только для выявления угроз, но и как активный участник в борьбе с ними. Его основное преимущество — это способность действовать на опережение. То есть ИИ может вмешаться до того, как вред будет нанесён. Рассмотрим, как это реализуется на практике:

• Выявление угроз на ранней стадии

Современные системы, основанные на ИИ, умеют в реальном времени отслеживать сетевой трафик. Благодаря этому они способны замечать подозрительную активность ещё до того, как атака развернётся полностью. Это помогает вовремя отреагировать и предотвратить возможные последствия, такие как утечка данных или сбой в работе систем.

• Автоматическое реагирование на инциденты

Если раньше специалистам приходилось вручную реагировать на каждую потенциальную угрозу, то теперь значительная часть этих задач может выполняться автоматически. Интеллектуальные алгоритмы не только фиксируют подозрительные действия, но и самостоятельно блокируют вредоносные запросы, отключают уязвимые участки сети или ограничивают доступ для подозрительных пользователей. Это ускоряет весь процесс реагирования и снижает нагрузку на специалистов по информационной безопасности.

• Адаптация и обучение систем защиты

Одна из ключевых особенностей ИИ — это способность к самообучению. Алгоритмы анализируют новые типы атак, запоминают их особенности и обновляют свои модели реагирования. Это особенно важно в условиях, когда киберугрозы постоянно меняются и появляются всё более сложные и изощрённые способы взлома. К примеру, решения формата XDR (Extended Detection and Response) объединяют данные из разных источников — почтовых серверов, облачных сервисов, локальных сетей — и на их основе формируют более полную картину происходящего. Это помогает быстрее обнаруживать даже нестандартные атаки и минимизировать ущерб.

ИИ занимает ключевую роль в современной кибербезопасности, предоставляя инструменты для анализа огромных объемов данных, обнаружения аномалий и автоматической адаптации к новым угрозам. Его развитие и внедрение позволяют значительно повысить уровень защиты информационных ресурсов от сложных и эволюционирующих киберугроз. В будущем, благодаря прогрессу в области ИИ, появится возможность создать более умные и автономные системы защиты, обеспечивающие устойчивость информационных инфраструктур.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Коломыцева Е. П. Методы защиты персональных данных в эпоху цифровизации / Е. П. Коломыцева, И. В. Сиротин, К. С. Коршак // Наукоемкие технологии и инновации (XXV научные чтения) : Сборник докладов Международной научно-практической конференции, Белгород, 23 ноября 2023 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. – С. 717-720. – EDN EDSEFS.

2. Кузнецов С. В., Пелехов Д. А., Новлянский В. В. Роль искусственного интеллекта в обнаружении и предотвращении кибератак / С. В. Кузнецов, Д. А. Пелехов, В. В. Новлянский // Наука и реальность. – 2024. – № 3. – С. 52-58. – EDN IRNKNO.

3. Комплексная защита информации в организации / М. М. Тараскин, А. Г. Захарова, Ю. И. Коваленко, Г. И. Москвитин. – Москва : Русайнс, 2017. – 354 с. – EDN YJYWMX.



***УДК 004.33***



***Щукин К.К.***
***Научный руководитель: Коломыцева Е.П., ст. преп.***
*Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия*


# УСТРОЙСТВО И РАЗВИТИЕ РАЗЛИЧНЫХ ХРАНИЛИЩ ДАННЫХ И НАКОПИТЕЛЕЙ

В современных условиях развития общества, экономики, большой импульс в своем развитии получили информационные технологии. Они стремительно развиваются, приобретают новые формы, средства. Данное обстоятельство позволяет обрабатывать большие объёмы данных, хранить их. Если в начале 2000-х годов стандартным объёмом оперативной памяти бытового персонального компьютера считался 64 – 128 МБ, а самым популярным накопителем данных являлся CD-диск объёмом до 700 МБ, то в настоящее время эти объемы кратно увеличились. Однако следует признать, что объемы обрабатываемых данных и данных хранения будут зависеть от их предназначения.

В связи с этим устройства хранения информации можно классифицировать по способу хранения данных на:

- магнитные;
- оптические;
- электронные.

Развитие устройств хранения можно проследить с 2000-х годов. Наиболее распространённым хранилищем данных в это время являлась дискета (англ. Floppy Disk). Внутри пластмассового квадратного корпуса находился тонкий магнитный диск, на которой записывалась информация. Самый первый Флоппи-Диск представила компания IBM в 1971 году с объёмом хранилища в 80 КБ данных. Почти за 2 десятилетия объём данных увеличился лишь до 1,4 МБ на одной дискете, но этого хватало для хранения и передачи текстовых документов и даже Microsoft Word 2.0, презентованный компанией Майкрософт в 1991 году умещался на одной дискете, а компьютерная игра DOOM, выпущенная Id Software в 1993 году распространялась уже на 4 кассетах – по дискете на внутриигровую главу, т.к. приближенная к трёхмерной компьютерная графика требовала больших ресурсов памяти и целиком игра занимала около 3 МБ. Для использования дискет компьютер должен был быть оснащён приводом для дискет (floppy drive), который принимал дискеты размером 3.5 дюйма. Со временем многие компании и пользователи перешли на более удобный формат CD, однако до сих пор флоппи-диски используются в медицинских и военных целях. Так, ВС США лишь в 2019 году отказались от формата 8-дюймовых дискет, которые использовались в системе ядерного вооружения с 1960-х годов.

Несмотря на относительно большой период технологии дискет, жёсткие диски (HDD – Hard Disk Driver) появились значительно раньше. Жесткий диск — это традиционное устройство хранения, использующее вращающиеся магнитные диски для хранения и извлечения данных, работающее через исполнительный механизм с читающей/записывающей головкой. Эти диски популярны для настольных ПК, ноутбуков и серверов, их емкость обычно варьируется от 500 ГБ до 2 ТБ, а скорость измеряется в об./мин, обычно 5,400 или 7,200 об./мин. Их срок службы обычно составляет от 3 до 5 лет, при этом частое использование является распространенной причиной выхода из строя. Прародителем современных HDD был 305 RAMAC (Random Access Method of Accounting and Control), изготовленный корпорацией IBM, который весил 970 кг и имел габариты современных морозильных систем, но метод использования пластин, покрытых ферромагнетиком, дожил до наших дней. Главным новшеством в 1961 стала реализация технологии Air Bearing — между «блинами» и «пишущей головкой» появился зазор 5 микрометров, что позволило повысить надежность и долговечность прибора. Современные жёсткие диски по-прежнему используют вращающийся магнитный диск для хранения данных.

Новинкой в начале 1980-х в сфере носителей информации стал компакт-диск (англ. CD, Compact Disc), т.к. впервые миру было представлено оптическое хранение данных - считывание информации осуществлялось при помощи лазера. Изначально созданный компаниями Sony и Philips для хранения аудиозаписей в цифровом формате, новый формат стал активно использоваться в ПК начала 2000-х годов за его возможность записывать и хранить значительный по тем временам объем – до 700 Мбайт данных. Данные на диск записываются в виде спиральной дорожки из так называемых питов (углублений), которые выдавливаются в поликарбонатной основе, что напоминает работу виниловых пластинок, заменить которые должен был оптический диск. Со временем, появились многочисленные варианты хранилища:

– CD-ROM (Compact Disc Read Only Memory) – диск с возможностью только чтения данных

– CD-R (Compact Disc Recordable) – компакт-диск с возможностью записи на него данных

– CD-RW (Compact Disk Re-Writable) – перезаписываемый компакт-диск

Следующим этапом развития технологии хранения данных на оптических дисках стало появление DVD (Digital Video Disk – цифровой видеодиск), способный вмещать до 4,7 Гбайт информации и до 8,5 Гбайт при возможности записи на двух сторонах диска. У DVD существовали такие же разновидности дисков, как и у CD формата. В 2006 году был представлен Blu-Ray Disc, объёмом в 50 ГБ. Своё название он получил от использования для записи и чтения коротковолнового (405 нм) синего лазера. Однослойный диск Blu-ray (BD) может хранить 25 ГБ, двухслойный диск может вместить 50 ГБ, трёхслойный диск может вместить 100 ГБ, четырёхслойный диск может вместить 128 ГБ.

Несмотря на многообразие оптических накопителей, используемых в настоящее время, их существенным недостатком является физический износ. Царапины и прочие потёртости могут стать причиной потери важных данных. Данное обстоятельство послужило основанием для разработки более надёжного устройства хранения информации. Новым способом записи стала флеш-память (flash memory) - разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти. USB-накопители или же флеш-накопители изначально имели сравнительно небольшой размер памяти – всего лишь 8 МБ, но даже так, они стали заменой флоппи-дисков из-за возможности быстро и неоднократно перезаписывать данные. В 1994 году группа компаний, включая Intel и Microsoft,

разработала стандарт USB – Universal Serial Bus, который обеспечил единообразный и удобный интерфейс для подключения устройств, что упростило использование портативных накопителей. Современные «флешки» могут иметь объём до 1 ТБ данных и высокую скорость чтения/записи файлов, вплоть до 10 Гбит/с.

К флеш-накопителям относят и SD-карты (Security Digital Memory Card), которые встречаются в размерах: SD, MiniSD, MicroSD. Существуют 5 поколений карт памяти данного формата, различием между которыми является объём хранимых данных:

- SD 1.0 – от 8 МБ до 2 ГБ;
- SD 1.1 – до 4 ГБ;
- SDHC – до 32 ГБ;
- SDXC – до 2 ТБ;
- SDUC – до 128 ТБ;

К преимуществам флеш-накопителей можно отнести:

- Универсальность. Практически все современные устройства имеют USB-разъёмы.
- Низкое энергопотребление.
- Компактность.
- Широкий диапазон рабочих температур.

Из недостатков можно выделить:

- Ограниченная пропускная способность USB. Чем ниже версия USB-разъёма, тем более низкие скорости.
- Ограниченное число циклов перезаписи

Сейчас всё чаще используются твердотельные накопители (Solid-State Drive, SSD) – немеханические запоминающие устройства на основе микросхем памяти. В настоящее время твердотельные накопители используются как в ноутбуках и в стационарных компьютерах для производительности. На 2016 год наиболее производительными выступали SSD формата M.2 с интерфейсом NVMe, а к 2025 году их скорость достигла 14900 Мбайт/с.

В современных условиях развития информационных технологий каждый из перечисленных выше накопителей нашёл своё применение в различных сферах жизни и свою сферу использования. Однако, отталкиваясь от исторического экскурса, который представлен в статье, следует отметить, что технический прогресс в полной мере затронул развитие различных хранилищ данных и накопителей цифровой информации. Это обусловлено развитием экономики и технологиями искусственного интеллекта.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Дроботун Е.Б. О сложности безвозвратного удаления данных на SSD-накопителях / Дроботун Е.Б. // перспективы развития информационных технологий. - 2011. - №3-2. - С. 14-16.
2. Минаев А.С., Дидрих В.Е. Защита данных от несанкционированного использования с флэш-накопителей / Минаев А.С., Дидрих В.Е. // математические методы и информационно-технические средства материалы IX Всероссийской научно-практической конференции. - Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Краснодарский университет Министерства внутренних дел Российской Федерации", 2013. - С. 194-195.
3. Коршак К.С., Шапошников К.А. Классификация и объектная модель технических систем / Коршак К.С. // наукоёмкие технологии и инновации (xxv научные чтения) Сборник докладов Международной научно-практической конференции. - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. - С. 757-761.



***УДК 004.738.2***



***Явтуховский Е.Ю., Верещагина Е.А., Ярмонов А.С.***
*Дальневосточный федеральный университет*
*г. Владивосток, Россия*


# НАБЛЮДАЕМОСТЬ НЕКООПЕРАТИВНЫХ СЕТЕЙ

В настоящее время осуществляется бурное развитие сетевых технологий, напрямую связанное с возрастающим количеством передаваемых данных в глобальной сети Интернет.

Согласно исследованию CloudFlare, одной из крупнейших организаций, предоставляющей услуги по управлению веб-ресурсами и их защите, за 2024 год общемировой объем интернет-трафика увеличился на 17,2% [1].

Стремительный рост является следствием активного внедрения и массового применения алгоритмов искусственного интеллекта во всех сферах деятельности человека [2].

Одновременно с этим, неуклонно возрастает количество применяемых устройств, реализующих технологии Интернета вещей [3], что также увеличивает нагрузку на сети передачи данных.

Совместно с ростом количества коммутируемых устройств и

нагрузки на сетевое оборудование осуществляется усложнение схем взаимодействия, как внутри локальных вычислительных сетей, так и между ними [4].

Отдельные информационно-телекоммуникационные системы, через которые транслируется информация, обретают состояние черных ящиков, когда логика обработки данных внутри системы сокрыта от стороннего наблюдателя [5].

Возрастающая неопределенность при передаче информации внутри информационных систем напрямую влияет на предсказуемость их взаимодействия с другими.

При этом, вся цепочка от источника информации до ее получателя, состоящая из описанных информационных систем, не может быть детерминирована и формируется хаотично для каждого отдельного запроса или сеанса связи.

Таким образом, можно сделать вывод о стохастичности процессов передачи данных в современных сетях связи и рассматривать их как марковские сети.

Исходя из предыдущего вывода, сложность обеспечения надежного пути доставки информации возрастает, в силу высокой изменчивости среды.

Совместно с этим, трудность поиска оптимального маршрута для интернет-трафика также повышается, а управляемость всей цепочкой систем уменьшается.

В свою очередь, указанные системы проявляют поведение, аналогичное математической модели некооперативной игры, поскольку они не имеют механизмов административного взаимодействия друг с другом [6].

Вследствие чего, создание и распространение единых политик управления интернет-соединениями для всех участвующих телекоммуникационных систем невозможно.

Каждой отдельной системой осуществляется приоритизация обработки трафика, направленного самой информационной системе и для нее, перед транзитным.

В совокупности, обозначенные проблемы влекут за собой снижение эффективности глобального межсетевого взаимодействия.

Решением данных задач может служить улучшение наблюдаемости [7] внутри информационных систем, путем внедрения специальных метрик, общих для всех участников обмена.

Общепринятые методы определения оптимальных маршрутов не учитывают сложность внутренних маршрутов и связанные с этим временные издержки некооперативных сетей, которые возникают из-за

их изменчивости.

В настоящее время применяются два вида протоколов динамической маршрутизации:

– дистанционно-векторные протоколы – каждый маршрутизатор хранит информацию о соседних устройствах, маршрутах, доступных через них, и дистанции до этих сетей (количество маршрутизаторов, через которые будут транслироваться данные, учитывая их пропускные способности и общую задержку);

– протоколы состояния каналов связи – каждый маршрутизатор хранит информацию обо всех устройствах своей зоны и доступных маршрутах, лучший маршрут определяется с помощью алгоритма Дейкстры (при расчете учитываются пропускные способности маршрутизаторов на всем пути трафика).

Для корректного определения оптимального маршрута предлагается использовать не только общую задержку на передачу предыдущего пакета данных и пропускную способность, но и применить ретроспективный анализ задержек на единицу времени или количества обработанной информации.

Это позволит создать статистическую выборку динамики работы сетевых устройств и прогнозировать их загрузку.

Следующим этапом предлагается осуществлять генерацию вероятностной модели загруженности сети передачи данных и поиск наиболее выгодного маршрута.

На основе полученных данных также могут быть оценено состояние сетевых устройств и информационных систем и определены перегрузки указанных элементов, что свидетельствует о повышение наблюдаемости и общей надежности.

Таким образом, рассмотренная проблемная область является актуальной и требует дополнительного анализа. В первую очередь необходимо определение затрат вычислительных ресурсов для оперативного проведения расчетов, а также размерности статистической выборки для наибольшей корректности и актуальности проводимых расчетов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Belson D. Cloudflare 2024 Year in Review / Belson D. [Электронный ресурс] // Cloudflare.com: [сайт]. — URL: https://blog.cloudflare.com (дата обращения: 24.05.2025).

2. Кузина Л.С., Полякова В.В., Талакаускас Д.С. От фантастики к реальности: ИИ в руках населения / Кузина Л.С., Полякова В.В.,

Талакаускас Д.С. [Электронный ресурс] // Национальный исследовательский университет «Высшая школа экономики»: [сайт]. — URL: https://issek.hse.ru (дата обращения: 24.05.2025).

3. Вишневский К.О., Димов Г.В., Комаров М.М., Приворотская С.Г. Перспективы Интернета вещей / Вишневский К.О., Димов Г.В., Комаров М.М., Приворотская С.Г. [Электронный ресурс] // Национальный исследовательский университет «Высшая школа экономики»: [сайт]. — URL: https://issek.hse.ru (дата обращения: 24.05.2025).

4. Таненбаум, Э.С., Фимстер Н., Уэзеролл Д. Компьютерные сети [Текст] / Э.С. Таненбаум, Н. Фимстер, Д. Уэзеролл — 6-е изд. — СПб: Питер, 2023 — 992 с.

5. Олифер, В.Г., Олифер, Н.В. Компьютерные сети. Принципы, технологии, протоколы [Текст] / В.Г. Олифер, Н.В. Олифер — 6-е изд. — СПб: Питер, 2024 — 1008 с.

6. Маракулин В.М. Элементы теории некооперативных игр [Текст] / Маракулин В.М. — 1-е изд. — Новосибирск: Новосибирский государственный университет, 2024 — 85 с.

*7.* Емельянов, С.В., Коровин, С.К., Ильин, А.В., Фомичев, В.В., Фурсов, А. С. Математические методы теории управления. Проблемы устойчивости, управляемости и наблюдаемости [Текст] / С.В. Емельянов, С.К. Коровин, А.В. Ильин, В.В. Фомичев, А.С. Фурсов — 1-е изд. — Москва: Физматлит, 2014 — 200 с.

***УДК 629.78***

***Якимова К.В.***
***Научный руководитель: Аристов А.А., преп.***
*Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия*

## ИДЕНТИФИКАЦИЯ СПУТНИКА CUBESAT С ПРИМЕНЕНИЕМ МАРКЕРОВ В СИСТЕМЕ ТЕХНИЧЕСКОГО ЗРЕНИЯ

В последние годы космическая индустрия претерпевает значительный рост числа запусков малых космических аппаратов, таких как CubeSat. Эти компактные спутники, размеры которых составляют всего 10x10x11 сантиметров и вес 1,33 кг на единицу объема (U) [1], открывают новые горизонты для научных исследований и технологий. Конфигурации CubeSat позволяют ученым и инженерам реализовывать проекты с минимальными затратами и в короткие сроки [4]. Однако с увеличением числа таких аппаратов возникает необходимость

разработки эффективных систем управления и отслеживания, обеспечивающих их точную ориентацию.

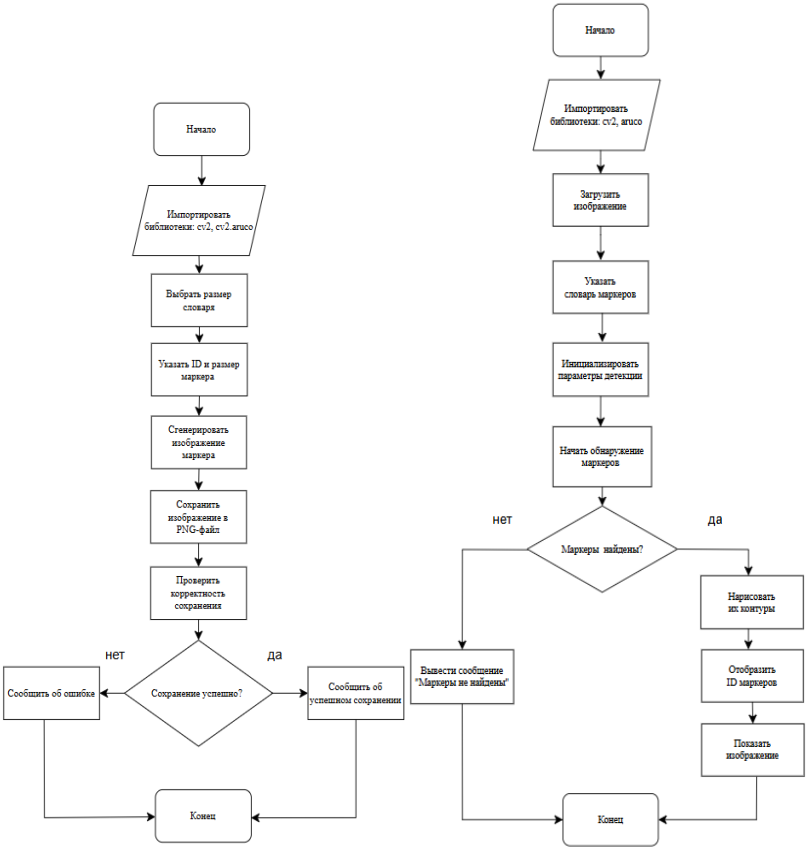
Одной из ключевых задач для обеспечения точной ориентации CubeSat является разработка алгоритмов для их идентификации и отслеживания [3].

В данной работе использованы маркеры ArUco — бинарные квадратные маркеры с уникальными идентификаторами, которые могут быть распознаны с помощью камер. Алгоритмы для работы с маркерами реализованы с использованием библиотеки OpenCV [2]. Эта библиотека поддерживает работу с маркерами ArUco, начиная с версии 3.0.0.

Процесс разработки системы состоит из двух основных этапов:

1. Создание маркеров ArUco (Рис.1 а): на первом этапе генерируются маркеры с использованием словарей маркеров, таких как DICT_4X4_50, и сохраняются для дальнейшего использования. Каждый маркер имеет уникальный идентификатор и фиксированный размер, для его распознавания. (Рис.1 а))

2. Обнаружение маркеров (Рис.1 б): для обнаружения маркеров необходимо импортировать OpenCV, загрузить изображение и указать словарь маркеров. Затем настраиваются параметры детекции для повышения точности, включая пороги и минимальный размер. Если маркер найден, ему присваивается ID, и на изображении рисуются его контуры. Результаты выводятся на экран или сохраняются. Если маркер не найден, выводится сообщение об этом. (рис1б))




а) б)

Рис. -1 Алгоритмы идентификации маркеров

Для проверки эффективности разработанных алгоритмов было проведено экспериментальное исследование на учебном макете CubeSat 1U с использованием широкоугольной камеры. Камера имела разрешение 200 МП и диафрагму f/1.9. Обнаружение маркеров проводилось на различных расстояниях (от 1 до 9 метров с шагом 1 метр) и при разных углах съемки (от 0 до 345 градусов с шагом 15 градусов). Результаты приведены в таблице ниже.

Таблица 1 - Результат обнаружения

| расстояние,м \угол,° | 0 | 15 | 30 | 45 | 60 | 75 | 90 | 105 | 120 | 135 | 150 | 165 | 180 | 195 | 210 | 225 | 240 | 255 | 270 | 285 | 300 | 315 | 330 | 345 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | да | да | да | да | да | да | да | да | да | нет | нет | да | да | да | да | да | да | да | да | да | да | да | да | да |
| 2 | да | да | да | да | да | да | да | да | да | да | да | нет | нет | да | да | да | да | да | да | да | да | да | да | да |
| 3 | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | нет |
| 4 | да | да | да | да | да | да | да | да | да | да | нет | да | да | нет | да | да | да | да | да | да | да | да | нет | да |
| 5 | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да | да |
| 6 | да | да | да | да | да | да | да | да | да | да | да | нет | да | да | да | да | да | да | да | да | да | да | да | да |
| 7 | да | нет | да | нет | да | да | да | да | да | да | да | да | да | нет | да | да | да | да | да | да | да | да | да | да |

Эксперимент показал, что вероятность успешного обнаружения маркеров составляет около 93%, что указывает на высокую эффективность предложенных алгоритмов. Тем не менее, проведенный анализ позволил выявить некоторые аспекты, требующие улучшения.

Во-первых, при определенных углах съемки (в диапазоне 135-195 градусов) было замечено снижение точности обнаружения маркера с ID 43. Это может указывать на недостаточную наработанность алгоритмов для данного маркера, а также на необходимость изучения его формы.

Во-вторых, необнаруженность маркеров на близких расстояниях в некоторых случаях может быть связана с нечеткостью печати. Это подчеркивает необходимость улучшения качества материалов и технологий печати маркеров для повышения их читаемости.

Проведенное исследование подтвердило высокую эффективность алгоритмов для обнаружения и отслеживания малых космических аппаратов на основе маркеров ArUco. Несмотря на выявленные ограничения, связанные с качеством маркеров и угловыми характеристиками, предложенная система может стать основой для разработки процессов управления спутниками. В дальнейшем планируется улучшение алгоритмов и разработка нейронных сетей для повышения точности идентификации CubeSat и их взаимодействия.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Официальная документация OpenCV по ArUco // OpenCV. – URL: https://docs.opencv.org (дата обращения: 25.10.2024).

2. CUBESAT INFORMATION. URL: https://www.cubesat.org /cubesatinfo (дата обращения: 27. 10.2024).

3. Авиакосмическое приборостроение. Современные методы обработки изображений для наноспутников // Авиакосмическое приборостроение. - 2023. - № 5. - С. 34-41.

4. Захаров И.В. Основы проектирования CubeSat: от теории к практике / И.В. Захаров. - Санкт-Петербург: Политехника, 2019. - 215 с. - ISBN 978-5-123-45678-9.

*УДК 629.78*

***[1]Якимова К.В., [2]Кулешов Н.В.***
***Научный руководитель: Аристов А.А., преп.***
*[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия*
*[2]Калининградский Государственный Технический Университет. г. Калининград, Россия*

# АНАЛИЗ ВОЗМОЖНОСТИ РАЗМЕЩЕНИЯ ИИ НА БОРТУ МАЛОГО КОСМИЧЕСКОГО АППАРАТА

Использование нейросетевых алгоритмов на малых космических аппаратах применяется в задачах автономной обработки изображений, получаемых с бортовых камер. В условиях ограниченного объема вычислительных ресурсов и задержек связи с наземной станцией требуется реализация обработки непосредственно на борту. Проведём анализ аппаратных платформ для реализации нейросетевых алгоритмов, рассмотрим особенности использования программируемых логических интегральных схем (ПЛИС) и графических процессоров (GPU), а также методы оптимизации моделей ИИ для работы в условиях космической среды.

ПЛИС позволяют выполнять выделенные вычисления, не задействуя вычислительные мощности бортового компьютера. При этом уменьшается объем передаваемой информации за счёт предварительной обработки и сжатия, например, замены полного изображения на вектор идентифицированных объектов [2]. ПЛИС характеризуются ограниченным энергопотреблением и допускают размещение в условиях ограниченного пространства. При этом следует учитывать чувствительность архитектуры ПЛИС к радиационным воздействиям, ограниченное количество логических элементов и необходимость обеспечения отказоустойчивости [3].

Графические процессоры обладают значительно большей вычислительной мощностью по сравнению с ПЛИС, что позволяет выполнять сложные нейросетевые вычисления с минимальным временем отклика. Однако для космических применений GPU имеют серьёзные недостатки: высокая чувствительность к радиации, приводящая к сбоям и повреждениям; повышенное энергопотребление, требующее мощного питания и охлаждения, что затруднено в условиях космоса из-за отсутствия конвекции; большие размеры современных GPU, затрудняющие их размещение на малых космических аппаратах [5]. Тем не менее, на низких околоземных орбитах возможно

использование специализированных GPU с дополнительными средствами защиты, однако в дальнем космосе подобные решения неприменимы.

Поэтому выбор аппаратной платформы для нейросетевой обработки должен учитывать не только вычислительные характеристики, но и ограничения нахождения в космическом пространстве. В отличие от GPU, ПЛИС имеют значительно меньшее энергопотребление, компактнее по габаритам и менее чувствительны к радиации при соответствующем проектировании. При выборе ПЛИС учитываются количество логических блоков, наличие DSP, объём встроенной памяти, тактовая частота, поддерживаемые интерфейсы и возможность работы в условиях повышенного радиационного фона [3]. Конфигурация модели зависит от архитектурных особенностей. Доступными решениями являются 5400TC015, Virtex-5QV и RTPF500T (табл. 1).

Таблица 1 – Доступные решения ПЛИС и их характеристик

| Характеристика | 5400TC015 | Virtex-5QV | RTPF500T |
|---|---|---|---|
| Логические элементы | 1104 | 131072 | 481000 |
| Встроенная память | — | 8 Мбит | 16 Мбит |
| DSP-блоки | — | 320 | 756 |
| Скоростные трансиверы | нет | нет | 24 |
| Тактовая частота, МГц | До 200 | До 300 | До 400 |
| Энергопотребление, Вт | До 2 | До 12 | До 15 |
| Порты ввода-вывода | 36 | 24 | до 632 |
| Температурный диапазон, °C | -60...+85 | -55...+125 | -55...+100 |
| Особенности | Низкое потребление, компактность | Стойкость к радиации | Высокоскоростная передача данных |

Virtex-5QV оснащена встроенной блочной памятью и цифровыми сигнальными процессорами, что обеспечивает эффективную реализацию свёрточных операций. RTPF500T обладает 24 высокоскоростными трансиверами, позволяющими параллельно передавать данные по нескольким каналам. 5400TC015 отличается компактностью и низким энергопотреблением, что делает её подходящей для систем с ограниченными ресурсами.

Ограниченные ресурсы бортовой аппаратуры требуют адаптации нейросетевых моделей под аппаратные ограничения. Для этого применяются различные методы структурной и числовой оптимизации (Табл. 2). К числу таких методов относится сжатие моделей и уменьшение разрядности, включая квантование весов и активаций с 32-

битного плавающего формата до INT8 или ниже. Применяется также прореживание сети (pruning), при котором удаляются малозначимые параметры, не оказывающие существенного влияния на выход модели. Для уменьшения количества вычислений используется факторизация свёрточных слоёв, позволяющая сократить число умножений. Кроме того, используется обучение компактных моделей на выходах более крупных сетей (knowledge distillation), что позволяет сохранить точность при снижении ресурсоёмкости. Архитектурные упрощения включают уменьшение числа слоёв, замену сложных операций на более простые, объединение отдельных слоёв в один и сокращение размера входных данных. Методы сжатия нейросетей показали значительное снижение ресурсоёмкости [1].

Таблица 2 – Методы оптимизации нейросетей для малых космических аппаратов

| Метод | Описание | Результат | Эффективность |
|---|---|---|---|
| Квантование (Quantization) | Снижение разрядности весов | Уменьшение объёма памяти | Снижение размера модели до 75 % [1] |
| Прореживание (Pruning) | Удаление малозначимых весов и нейронов | Снижение числа операций, сокращение объёма модели | Уменьшение размера модели до 60 % [6] |
| Факторизация свёрток | Разложение свёрток на более простые операции | Ускорение вычислений, снижение нагрузки на аппаратуру | Сокращение количества операций до 50 % [7] |
| Обучение с дистилляцией знаний | Обучение малой модели по выходам большой (teacher-student) | Сохранение точности при снижении ресурсоёмкости | Сохранение точности до 98 % от исходной модели [8] |
| Архитектурные упрощения | Сокращение числа слоёв, замена операций, объединение блоков | Адаптация под конкретные аппаратные ограничения | Снижение вычислений до 50 % [9] |

Так же, для переноса предобученных моделей нейросетей в аппаратную реализацию на ПЛИС необходим единый формат представления вычислений и инструменты автоматизации этого процесса. Нейросети обычно хранятся в формате ONNX — графе вычислений, совместимом с популярными ML-фреймворками. Этот формат поддерживается инструментами HLS4ML, FINN и Vitis AI, которые автоматизируют значительную часть процесса генерации HDL-кода, включая настройку параллелизма, разрядности операций и структуры памяти. Хотя итоговая интеграция требует доработки и адаптации под конкретную платформу, использование таких инструментов значительно ускоряет переход от модели к аппаратной реализации, что упрощает внедрение ИИ в автономные бортовые системы космических аппаратов.

В ходе анализа установлено, что ПЛИС являются предпочтительным решением для размещения ИИ на борту малых космических аппаратов благодаря их энергоэффективности, компактности и радиационной стойкости. Несмотря на ограниченные вычислительные ресурсы, современные подходы к оптимизации моделей позволяют эффективно реализовывать нейросети на ПЛИС. GPU применимы лишь на низких орбитах и требуют сложной защиты. Таким образом, ПЛИС при использовании специализированных инструментов и оптимизаций представляют собой наиболее сбалансированное решение для автономной бортовой обработки изображений.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Tan K., Wang D. Compressing Deep Neural Networks for Efficient Speech Enhancement // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2021. P. 8358–8362.

2. Лебедев М. С., Белецкий П. Н. Реализация искусственных нейронных сетей на ПЛИС с помощью открытых инструментов // Труды Института системного программирования РАН. 2021. Т. 33, № 6. С. 175–192.

3. Nguyen V. H., Chen Y.-H., Kim H. FPGA-based Neural Network Inference Acceleration for Space Applications // IEEE Aerospace Conference Proceedings. 2022. DOI: 10.1109/AERO53065.2022.9843896.

4. Blott M., Umuroglu Y., Fraser N. J., Gambardella G., Leong P., Jahre M. FINN-R: An End-to-End Deep-Learning Framework for Fast Exploration of Quantized Neural Networks on FPGAs // ACM Transactions on Reconfigurable Technology and Systems. 2018. Vol. 11, No. 3. Article

16. DOI: 10.1145/3242897.

5. Xu J., Beaty J., Chen J. Evaluation of GPU Use in Onboard Spacecraft Processing // Journal of Aerospace Information Systems. 2023. Vol. 20, No. 4. P. 200–212. DOI: 10.2514/1.I010949.

6. Anh Tuan. Introduction to Pruning [Электронный ресурс]. URL: https://medium.com (дата обращения: 25.05.2025).

7. Wang M., Liu B., Foroosh H. Factorized Convolutional Neural Networks // ICCV 2017 Workshops [Электронный ресурс]. URL: https://openaccess.thecvf.com (дата обращения: 25.05.2025).

8. Train Smaller Neural Network Using Knowledge Distillation — MathWorks [Электронный ресурс]. URL: https://www.mathworks.com (дата обращения: 25.05.2025).

9. Barrett C. et al. Simplifying Neural Networks Using Formal Verification [Электронный ресурс]. URL: https://theory.stanford.edu (дата обращения: 25.05.2025).

**Оглавление**

Абдусалямова М.В., Якимова А.А., Плеханов Д.В.

ОПТИМИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ ПРОГРАММНЫХ РЕШЕНИЙ..... 3

Акимова Е.А.

КИБЕРБЕЗОПАСНОСТЬ В КОСМИЧЕСКИХ ТЕХНОЛОГИЯХ .... 6

Акимова Е.А.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И ИХ ВЛИЯНИЕ НА КРИПТОГРАФИЮ ..... 10

Акимова Е.А.

ИИ-МОШЕННИЧЕСТВО: КАК НЕЙРОСЕТИ УПРОЩАЮТ ВЗЛОМ ЧЕЛОВЕЧЕСКОГО ДОВЕРИЯ..... 14

Акимова Е.А.

АНОНИМНОСТЬ В DARKNET: МИФЫ И РЕАЛЬНОСТЬ..... 18

Акимова Е.А.

УЯЗВИМОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ В КИБЕРБЕЗОПАСНОСТИ..... 21

Акуппа Ю.А.

ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МЕДИЦИНЕ ..... 25

Акуппа Ю.А.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕМ С ИСПОЛЬЗОВАНИЕМ ДАТЧИКОВ ..... 28

Акуппа Ю.А.

РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ПЛАТФОРМЕ ARDUINO ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 31

Акуппа Ю.А.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ: АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ДАННЫХ ..... 35

Акуппа Ю.А., Чикин Н.А.

ОПТИМИЗАЦИЯ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ С ПОМОЩЬЮ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ..... 38

Акуппа Ю.А., Чикин Н.А.

КИБЕРБЕЗОПАСНОСТЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ СИСТЕМАМИ..... 41

Амиров М.С.

АНАЛИЗ ИСХОДНОГО КОДА ПРИ ТРАНСЛЯЦИИ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ ..... 45

Амиров М.С.

СТРАТЕГИИ СИНТАКСИЧЕСКОГО РАЗБОРА ДЛЯ ФОРМАЛЬНЫХ ГРАММАТИК..... 48

Анджич Дж.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНЖЕНЕРИИ И АРХИТЕКТУРЕ: ОТ ГЕНЕРАТИВНОГО ДИЗАЙНА К АВТОНОМНОМУ ПРОЕКТИРОВАНИЮ..... 50

Булгаков В.Д., Воскобойников И.С.

МЕТОДЫ ШИФРОВАНИЯ И ЗАЩИТЫ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ В ДЕЦЕНТРАЛИЗОВАННЫХ БЛОКЧЕЙН-ХРАНИЛИЩАХ ..... 54

Воскобойников И.С., Булгаков В.Д.

ОБЗОР И СРАВНЕНИЕ МЕТОДОВ ОБРАБОТКИ НЕСТРУКТУРИРОВАННЫХ ТЕКСТОВЫХ ДАННЫХ..... 60

Воскобойников И.С.

ЭПИСТЕМОЛОГИЯ И ФИЛОСОФИЯ НАУКИ В КОНТЕКСТЕ ОБРАБОТКИ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ..... 64

Гарайшин Р.Р., Бабенков Ю.М., Елютин И.П.

ОБУЧЕНИЕ НЕЙРОСЕТИ DARKNET ДЛЯ РАСПОЗНОВАНИЯ ОБЪЕКТОВ..... 67

Гоенко И.О.

РАЗВИТИЕ И ФУНКЦИОНАЛ ИГРОВОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ..... 70

Гоенко И.О.

МЕТОДЫ УПРАВЛЕНИЯ ИГРОВЫМИ ОБЪЕКТАМИ В КОМПЬЮТЕРНЫХ ИГРАХ ..... 75

Гончаренко Е.Д.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ, МОДЕЛИРОВАНИИ И ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ: КАК ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ МЕНЯЮТ КОРПОРАТИВНУЮ КУЛЬТУРУ ..... 79

Гуленко Д.Г.

ДИСКРЕТНАЯ МАТЕМАТИКА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ЗАДАЧИ И ОБЛАСТИ ПРИМЕНЕНИЯ ..... 82

Давыдов Д.А.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ, МОДЕЛИРОВАНИИ И ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ: РЕВОЛЮЦИЯ ЦИФРОВОЙ ЭПОХИ ..... 87

Журавлева Т.В.

ВИРТУАЛЬНАЯ СЕТЕВАЯ ЛАБОРАТОРИЯ EVE-NG ..... 92

Зеновская Д.А.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЛЕЧЕБНО–ПРОФИЛАКТИЧЕСКИМ УЧРЕЖДЕНИЕМ ..... 96

Зубарев М.И., Шевченко А.О.

ХЕШ-ФУНКЦИЯ, ОСНОВАННАЯ НА СТРУКТУРЕ АПЕРИОДИЧЕСКОГО ЗАМОЩЕНИЯ ТИПА ПЕНРОУЗА..... 101

Иванисов Д.С.

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В УПРАВЛЕНИИ ЦЕПЯМИ ПОСТАВОК: ВЫЗОВЫ И ПЕРСПЕКТИВЫ ТРАНСФОРМАЦИИ ЛОГИСТИКИ ..... 105

Иванисов Д.С.

РОЛЬ ИНТЕРФЕЙСОВ ЧЕЛОВЕК–МАШИНА В РАЗВИТИИ ЦИФРОВЫХ СИСТЕМ ..... 107

Иванисов Д.С.

ЭВОЛЮЦИЯ ОПЕРАЦИОННЫХ СИСТЕМ: ОТ МОНОЛИТНЫХ ЯДЕР К РАСПРЕДЕЛЁННЫМ СИСТЕМАМ ..... 110

Иванисов Д.С.

ЦИФРОВОЙ ДВОЙНИК В ПРОИЗВОДСТВЕННОМ МЕНЕДЖМЕНТЕ: ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ НА ОСНОВЕ ИММИТАЦИОННОГО МОДЕЛИРОВАНИЯ ..... 113

Иванисов Д.С.

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ НА ОСНОВЕ АНАЛИЗА ДАННЫХ ..... 116

Иванисов Д.С.

ЭВОЛЮЦИЯ ПРИКЛАДНЫХ ИНТЕРФЕЙСОВ: ОТ НАСТОЛЬНЫХ ПРОГРАММ ДО МУЛЬТИПЛАТФОРМЕННЫХ СРЕД ..... 119

Иванисов Д.С.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ..... 122

Иванисов Д.С.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕДИЦИНЕ: ТРАНСФОРМАЦИЯ ДИАГНОСТИКИ, ЛЕЧЕНИЯ И ПРОГНОЗИРОВАНИЯ ЗАБОЛЕВАНИЙ ..... 125

Иванов К.И.

УМНЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ЖИЛЫМИ КОМПЛЕКСАМИ (SMART PROPERTY MANAGEMENT): ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЖИЛИЩНОЙ ИНФРАСТРУКТУРЫ ..... 129

Иващенко И.А.

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ И ШИФРОВАНИЕ В 3D-ПЕЧАТИ МЕТАЛЛИЧЕСКИХ ДЕТАЛЕЙ ..... 133

Иващенко И.А.

ГОЛОГРАФИЧЕСКИЕ СИМУЛЯКРЫ В СОВРЕМЕННЫХ ВОЕННЫХ ОПЕРАЦИЯХ ..... 136

Иващенко И.А.

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ И УСТОЙЧИВОСТЬ К КВАНТОВЫМ АТАКАМ..... 140

Иващенко И.А.

ВЫБОР КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ С УЧЁТОМ ПРОИЗВОДИТЕЛЬНОСТИ И БЕЗОПАСНОСТИ..... 143

Иващенко И.А.

ФИТНЕС-ТРЕКЕРЫ: КАК НОСИМЫЕ УСТРОЙСТВА ИЗМЕНЯЮТ ПОДХОД К ФИЗИЧЕСКОЙ АКТИВНОСТИ ..... 146

Иващенко И.А.

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ И РАЗВИТИЕ СОВРЕМЕННЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ..... 149

Каликина А.С.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ, МОДЕЛИРОВАНИИ И ЭКОНОМИЧЕСКОГО АНАЛИЗА..... 152

Капицкий Ю.Ю., Плотникова К.А., Чайкина Н.А.

РЕАЛИЗАЦИЯ ОБРАБОТКИ И ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ ..... 156

Карташов М.В.

МОДЕЛИРОВАНИЕ СИСТЕМЫ РЕГУЛИРОВАНИЯ КОНЦЕНТРАЦИИ CO2 В ПОМЕЩЕНИИ ..... 160

Князева Н.А.

РАЗРАБОТКА ОНЛАЙН-ПЛАТФОРМЫ ДЛЯ БАННОГО КОМПЛЕКСА ..... 163

Козиненко Е.А.

ГЕЙМИФИКАЦИЯ В ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМАХ: КАК КВЕСТЫ И ИНТЕРАКТИВНЫЕ ОПРОСЫ ПОВЫШАЮТ КОНВЕРСИЮ ..... 167

Колесников В.Д.

АНАЛИЗ ПРИМЕНЕНИЯ МОДЕЛЕЙ РАСПОЗНАВАНИЯ ОБЪЕКТОВ ДЛЯ ОПРЕДЕЛЕНИЯ ДЕТАЛЕЙ ТЕХНИЧЕСКИХ ЧЕРТЕЖЕЙ ..... 172

Колпакова В.С.

ПРОЕКТИРОВАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ НА ПРИМЕРЕ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ..... 177

Костюкова А.С.

РАЗРАБОТКА ВЕБ-СЕРВИСОВ ДЛЯ ДОМАШНИХ КОНДИТЕРОВ ..... 181

Крутова Д.А.

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ УПРАВЛЕНИЯ ПЕРСОНАЛОМ ..... 186

Кузнецова Д.В.

ОСОБЕННОСТИ УПРАВЛЕНИЯ ИТ-ПРОЕКТАМИ НА ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЕ ..... 189

Курулева У.Е., Крузин К.О., Петров И.С.

СФЕРЫ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ В НАСТОЯЩЕЕ ВРЕМЯ И В БЛИЖАЙШЕМ БУДУЩЕМ ..... 192

Лазарре А.

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ, ПРИМЕНЯЕМЫЕ В ИНФОРМАЦИОННЫХ ТЕРРИТОРИЯХ НА ПРЕДПРИЯТИИ ... 196

Лапко Н.А.

ИНФОРМАЦИОННАЯ СИСТЕМА АНАЛИЗА ЛИЧНЫХ РАСХОДОВ С УЧЁТОМ ЭМОЦИОНАЛЬНОГО ФОНА ПОЛЬЗОВАТЕЛЯ ..... 201

Ляхова О.Р.

РОЛЬ БИЗНЕС-АНАЛИТИКИ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОРГАНИЗАЦИЙ ..... 204

Ляхова О.Р.

ОПАСНОСТЬ OVERSHARING В ЦИФРОВОЙ СРЕДЕ..... 208

Ляхова О.Р.

cОЦИАЛЬНЫЕ АСПЕКТЫ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ: СОПРОТИВЛЕНИЕ ПЕРСОНАЛА И СТРАТЕГИИ АДАПТАЦИИ ..... 211

Ляхова О.Р.

ФИШИНГ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: СОВРЕМЕННЫЕ УГРОЗЫ И ПРОТИВОДЕЙСТВИЯ..... 214

Ляхова О.Р.

BI-СИСТЕМЫ, ДОСТУПНЫЕ В РФ В 2025 ГОДУ: СРАВНЕНИЕ ЯНДЕКС DATALENS, FINEBI И ANALYTICA BY ФОРС..... 217

Манькова Ю.В.

МЕТОДЫ И ПОДХОДЫ К РАЗРАБОТКЕ АДАПТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ НА ОСНОВЕ АНАЛИЗА ДАННЫХ ..... 221

Манькова Ю.В.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМ ПРОЦЕССОМ: РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИЗУЧЕНИИ АЛГОРИТМОВ ..... 225

Матренина Е.Р.

АВТОМАТИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ С ПОСТАВЩИКАМИ И ЛОГИСТИКА В 1С ДЛЯ АВТОСЕРВИСОВ..... 229

Матренина Е.Р.

РИСКИ И ПРОБЛЕМЫ АВТОМАТИЗАЦИИ АВТОСЕРВИСНОГО БИЗНЕСА..... 232

Митюков А.Е.

ИМПУЛЬСНАЯ СИСТЕМА УПРАВЛЕНИЯ БЕСКОЛЛЕКТОРНЫМ ДВИГАТЕЛЕМ ПОСТОЯННОГО ТОКА ..... 236

Московченко А.Д.

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ПОДБОРА КОМПОНЕНТОВ АВТОМОБИЛЬНОЙ АУДИОСИСТЕМЫ..... 242

Мубараков Н.А.

ОБОСНОВАНИЕ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ АКАДЕМИЧЕСКОГО ПЛАНИРОВАНИЯ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ..... 246

Низамов Н.А.

ИННОВАЦИОННЫЕ ЦИФРОВЫЕ ИНСТРУМЕНТЫ ДЛЯ УПРАВЛЕНИЯ ПЕРСОНАЛОМ..... 251

Новосельцев В.Д.

ТЕОРИЯ ЧИСЕЛ В ДИСКРЕТНОЙ МАТЕМАТИКЕ: ПРОСТЫЕ ЧИСЛА И ИХ СВОЙСТВА..... 256

Новосельцев В.Д.

КИБЕРБЕЗОПАСНОСТЬ: СУЩЕСТВУЮЩИЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ ДАННЫХ..... 259

Новосельцев В.Д.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: ПРИНЦИПЫ РАБОТЫ И ПЕРСПЕКТИВЫ..... 262

Павлов Д.А., Бадрисламов Д.И., Маньянов А.Р.

ПРОБЛЕМА ЦИФРОВОГО НЕРАВЕНСТВА ..... 265

Панова А.А.

PROCESS MINING КАК ИНСТРУМЕНТ ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ В ГРАЖДАНСКОЙ АВИАЦИИ ..... 268

Письменный А.Б.

ГИБРИДНЫЕ ЭВРИСТИКИ ДЛЯ РАЗБИЕНИЯ МУЛЬТИМНОЖЕСТВ С РАВНЫМИ СУММАМИ ..... 272

Подлеснова А.В.

СЕРВИСНО-ОРИЕНТИРОВАННАЯ АРХИТЕКТУРА НА ПРЕДПРИЯТИЯХ ГРАЖДАНСКОЙ АВИАЦИИ..... 277

Попов С.А.

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ АНАЛИЗА НЕСИНУСОИДАЛЬНЫХ СИГНАЛОВ В СИСТЕМАХ ЭЛЕКТРОЭНЕРГЕТИКИ ПОСРЕДСТВОМ АДАПТИВНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ..... 282

Попова П.Н.

ПРОГРАММЫЕ КОМПЛЕКСЫ РАСЧЕТА НАДЕЖНОСТИ ..... 286

Путилин Н.И.

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ: СТАНДАРТЫ NIST И ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС ..... 290

Путилин Н.И.

ДНК-КРИПТОГРАФИЯ: НОВЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ БИОЛОГИЧЕСКИХ ДАННЫХ ..... 295

Радин Е.А.

СИСТЕМА УПРАВЛЕНИЯ МОБИЛЬНОЙ ПЛАТФОРМОЙ ДЛЯ ТРАНСПОРТНО-СКЛАДСКИХ ЗАДАЧ ..... 298

Романов А.О.

CURIOSITY-DRIVEN LEARNING: КАК ИИ ИССЛЕДУЕТ МИР БЕЗ НАГРАД ..... 303

Руденький А.О.

СИСТЕМА АУДИОВИЗУАЛЬНОЙ НАВИГАЦИИ ДЛЯ ЛЮДЕЙ С НАРУШЕНИЯМИ ЗРЕНИЯ ..... 308

Рыбакова А.В.

РАЗРАБОТКА АЛГОРИТМА КЛАСТЕРИЗАЦИИ БИНАРНЫХ ДАННЫХ ДЛЯ ОПТИМИЗАЦИИ МАРШРУТОВ ОБЩЕСТВЕННОГО ТРАНСПОРТА ..... 311

Рыбочкин М.Р.

ОБЗОР СИСТЕМ ОПТИМИЗАЦИИ ТРЕНИРОВОЧНОГО ПРОЦЕССА СПОРТСМЕНОВ С ИСПОЛЬЗОВАНИЕМ VR ТЕХНОЛОГИЙ ..... 316

Рякин И.В.

ЦИФРОВОЙ АЛГОРИТМ ОБРАБОТКИ БИОХИМИЧЕСКИХ ДАННЫХ НА ОСНОВЕ ИНФРАКРАСНОЙ СПЕКТРОСКОПИИ ..... 322

Сабанова Т.А., Галанкин Р.А.

ПРИМЕНЕНИЕ BIG DATA В БИЗНЕСЕ ..... 325

Седых А.А.

КАК УСТРОЕНЫ АТАКИ ТИПА “ОТКАЗ В ОБСЛУЖИВАНИИ” (DDOS) И КТО ОТ НИХ СТРАДАЕТ ..... 331

Серова А.С., Смирнов Д.С.

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В ЗАДАЧЕ КЛАССИФИКАЦИИ СТРОИТЕЛЬНО-МОНТАЖНЫХ РАБОТ ..... 335

Сиденко И.Э.

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ..... 340

Синев Д.А., Чеботков М.С.

РОЛЬ БИЗНЕС-АНАЛИТИКИ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА ..... 344

Скуридина Д.И., Кобзева Н.Р., Гольцова М.Ю.

ИСПОЛЬЗОВАНИЕ ПРЕДИКАТИВНОЙ АНАЛИТИКИ В СИСТЕМАХ МОНИТОРИНГА ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ ..... 348

Суслов Д.О.

ЦИФРОВЫЕ ДВОЙНИКИ В СИСТЕМАХ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ ..... 353

Суслов Д.О.

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ В ПРЕДИКТИВНОЙ АНАЛИТИКЕ НА ПРОИЗВОДСТВЕ ..... 357

Третьяков Д.С.

ГЕНЕРАТИВНЫЕ AI В АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ ..... 360

Третьяков Д.С.

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ. 363

Трибелев А.А.

РЕЗУЛЬТАТЫ ВЕРИФИКАЦИИ ПРИМЕНИМОСТИ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРЕМЕНЕНИЯ В РАСЧЕТАХ ВЕРОЯТНОСТНОГО АНАЛИЗА БЕЗОПАСНОСТИ АЭС 3 УРОВНЯ..... 366

Уточкина Е.С.

СОЗДАНИЕ ФИЛЬТРА КАЛМАНА НА PYTHON ДЛЯ ПОИСКА ПОЛОЖЕНИЯ И СКОРОСТИ ПАДАЮЩЕГО ОБЪЕКТА..... 371

Фальков Г.А.

АДАПТИВНОЕ ОКОННОЕ ПРЕОБРАЗОВАНИЯ ФУРЬЕ ДЛЯ АНАЛИЗА КАЧЕСТВА ЭЛЕКТРОЭНЕРГИИ ВЫСОКОВОЛЬТНОЙ СЕТИ ..... 374

Фонова А.Ю.

УГРОЗЫ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЕНЕРАТИВНОГО ИИ: РИСКИ, СЦЕНАРИИ АТАК И ПОДХОДЫ К ЗАЩИТЕ ..... 378

Фонова А.Ю.

УГРОЗЫ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЕНЕРАТИВНОГО ИИ: РИСКИ, СЦЕНАРИИ АТАК И ПОДХОДЫ К ЗАЩИТЕ ..... 382

Фонова А.Ю.

ЭКОЛОГИЧЕСКИЙ СЛЕД ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СКРЫТЫЕ ИЗДЕРЖКИ РАЗВИТИЯ ТЕХНОЛОГИЙ ИИ..... 387

Фонова А.Ю.

ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАБОЧИЕ ПРОЦЕССЫ СОТРУДНИКОВ IT-КОМПАНИЙ: АНАЛИЗ ВЛИЯНИЯ НА ПРОИЗВОДИТЕЛЬНОСТЬ И ЭФФЕКТИВНОСТЬ ..... 391

Фонова А.Ю.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ: АНАЛИЗ РИСКОВ УТЕЧКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ С ИИ-СИСТЕМАМИ ..... 396

Фонова А.Ю.

ЦИФРОВЫЕ АВАТАРЫ И МЕТАВСЕЛЕННАЯ: КАК ТЕХНОЛОГИИ ИИ МЕНЯЮТ КОММУНИКАЦИЮ И ЦИФРОВУЮ ИДЕНТИЧНОСТЬ ..... 401

Фонова А.Ю.

ИНТЕГРАЦИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС СТУДЕНТОВ ВУЗОВ: ВОЗМОЖНОСТИ, ВЫЗОВЫ И ПЕРСПЕКТИВЫ ..... 405

Фролов О.С.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УПРАВЛЕНИИ ИНТЕЛЛЕКТУАЛЬНЫМИ СИСТЕМАМИ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ..... 409

Фролов О.С.

ВСПЛЫВАЮЩЕЕ МЕНЮ И НИСПАДАЮЩЕЕ МЕНЮ В ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСАХ ..... 414

Худяков М.В.

CI/CD И МОНИТОРИНГ: АВТОМАТИЗАЦИЯ ЦИФРОВЫХ ЭКОСИСТЕМ ..... 418

Худяков М.В.

ВЕБ-САЙТ ЦИФРОВЫХ ЭКОСИСТЕМ И БОТ TELEGRAM КАК ИНСТРУМЕНТЫ РАЗВИТИЯ БИЗНЕСА ..... 424

Худяков М.В.

АРХИТЕКТУРА ЦИФРОВОЙ ЭКОСИСТЕМЫ: КАК СВЯЗАТЬ САЙТ, TELEGRAM-БОТА И ОБЩУЮ БАЗУ ДАННЫХ ..... 428

Худяков М.В.

СЕРДЦЕ ЦИФРОВОЙ ЭКОСИСТЕМЫ РАЗРАБОТКА БЭКЕНДА ДЛЯ СЕТИ КОФЕЕН И ВЕНДИНГА..... 433

Худяков М.В.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ И ИНФРАСТРУКТУРЫ В КОНТЕКСТЕ ЦИФРОВОЙ ЭКОСИСТЕМЫ: ПРИНЦИПЫ И МЕТОДЫ ЗАЩИТЫ ..... 437

Худяков М.В.

API-ДИЗАЙН КАК ОСНОВА БЕСШОВНОЙ ЦИФРОВОЙ ЭКОСИСТЕМЫ ДЛЯ СЕТИ КОФЕЕН И ВЕНДИНГА ..... 443

Худяков М.В.

ОБЛАЧНАЯ ИНФРАСТРУКТУРА КАК ФУНДАМЕНТ МАСШТАБИРОВАНИЯ ЦИФРОВОЙ ЭКОСИСТЕМЫ: АСПЕКТЫ ВЫБОРА И КОНФИГУРАЦИИ ..... 448

Худяков М.В.

БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ CMS СИСТЕМ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ DRUPAL, JOOMALA, WORDPRESS И WEBASYST ..... 454

Чаков И.А., Евтюхов М.С.

ОСОБЕННОСТИ НАСТРОЙКИ И ПРИМЕНЕНИЯ ПРОТОКОЛА IGMPV2 В ОПЕРАЦИОННОЙ СИСТЕМЕ АЛЬТ ..... 459

Чернобровенко А.Е.

КУАЙНЫ ДЛЯ ПОИСКА ПОДМНОЖЕСТВ ЧИСЕЛ С НУЛЕВОЙ СУММОЙ ..... 466

Черновский Д.Д.

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ (GAN) ДЛЯ УЛУЧШЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ..... 472

Черновский Д.Д.

КРИПТОВАЛЮТЫ БЕЗ БЛОКЧЕЙНА: БЕЗОПАСНЫ ЛИ DAG-ПРОТОКОЛЫ (IOTA, HEDERA) ПРОТИВ SYBIL-АТАК ..... 475

Черных А.В.

МЕТОД И СРЕДСТВА ВЫЧИСЛЕНИЯ МЕТОК ПО ТЕХНИЧЕСКИМ ХАРАКТЕРИСТИКАМ КОМПЬЮТЕРНЫХ УСТРОЙСТВ ..... 479

Чжан Ю.

СОЗДАНИЕ ПАРАЛЛЕЛЬНЫХ КОРПУСОВ ХАРАКТЕРИСТИЧЕСКИХ ПРИЗНАКОВ ДИВАНА НА ОСНОВЕ КИТАЙСКИХ И РОССИЙСКИХ LLM ..... 485

Шайдуллина А.Р.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СТРАТЕГИЧЕСКОМ УПРАВЛЕНИИ РИСКАМИ ..... 489

Шевченко А.С.

ОБЗОР ИНФОРМАЦИОННЫХ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ ..... 492

Шевченко П.В.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБНАРУЖЕНИИ КИБЕРАТАК И АНОМАЛИЙ ..... 496

Щукин К.К.

УСТРОЙСТВО И РАЗВИТИЕ РАЗЛИЧНЫХ ХРАНИЛИЩ ДАННЫХ И НАКОПИТЕЛЕЙ ..... 499

Явтуховский Е.Ю., Верещагина Е.А., Ярмонов А.С.

НАБЛЮДАЕМОСТЬ НЕКООПЕРАТИВНЫХ СЕТЕЙ ..... 503

Якимова К.В.,

ИДЕНТИФИКАЦИЯ СПУТНИКА CUBESAT С ПРИМЕНЕНИЕМ МАРКЕРОВ В СИСТЕМЕ ТЕХНИЧЕСКОГО ЗРЕНИЯ ..... 506

[1]Якимова К.В., [2]Кулешов Н.В.

АНАЛИЗ ВОЗМОЖНОСТИ РАЗМЕЩЕНИЯ ИИ НА БОРТУ МАЛОГО КОСМИЧЕСКОГО АППАРАТА ..... 510