

Научный центр «LJournal»

Рецензируемый научный журнал

ТЕНДЕНЦИИ РАЗВИТИЯ НАУКИ И ОБРАЗОВАНИЯ

№114, Октябрь 2024
(Часть 9)



Самара, 2024

T33

Рецензируемый научный журнал «Тенденции развития науки и образования» №114, Октябрь 2024 (Часть 9) - Изд. Научный центр «LJournal», Самара, 2024 - 180 с.

doi: 10.18411/trnio-10-2024-p9

Тенденции развития науки и образования - это рецензируемый научный журнал, который в большей степени предназначен для научных работников, преподавателей, доцентов, аспирантов и студентов высших учебных заведений как инструмент получения актуальной научной информации.

Периодичность выхода журнала – ежемесячно. Такой подход позволяет публиковать самые актуальные научные статьи и осуществлять оперативное обнародование важной научно-технической информации.

Информация, представленная в сборниках, опубликована в авторском варианте. Орфография и пунктуация сохранены. Ответственность за информацию, представленную на всеобщее обозрение, несут авторы материалов.

Метаданные и полные тексты статей журнала передаются в наукометрическую систему ELIBRARY.

Электронные макеты издания доступны на сайте научного центра «LJournal» - <https://ljournal.org>

© Научный центр «LJournal»
© Университет дополнительного
профессионального образования

УДК 001.1
ББК 60

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Чернопятов Александр Михайлович

Кандидат экономических наук, Профессор

Царегородцев Евгений Леонидович

Кандидат технических наук, доцент

Пивоваров Александр Анатольевич

Кандидат педагогических наук

Малышкина Елена Владимировна

Кандидат исторических наук

Ильященко Дмитрий Павлович

Кандидат технических наук

Дробот Павел Николаевич

Кандидат физико-математических наук, Доцент

Божко Леся Михайловна

Доктор экономических наук, Доцент

Бегидова Светлана Николаевна

Доктор педагогических наук, Профессор

Андреева Ольга Николаевна

Кандидат филологических наук, Доцент

Абасова Самира Гусейн кызы

Кандидат экономических наук, Доцент

Попова Наталья Владимировна

Кандидат педагогических наук, Доцент

Ханбабаева Ольга Евгеньевна

Кандидат сельскохозяйственных наук, Доцент

Вражнов Алексей Сергеевич

Кандидат юридических наук

Ерыгина Анна Владимировна

Кандидат экономических наук, Доцент

Чебыкина Ольга Альбертовна

Кандидат психологических наук

Левченко Виктория Викторовна

Кандидат педагогических наук

Петраш Елена Вадимовна

Кандидат культурологии

Романенко Елена Александровна

Кандидат юридических наук, Доцент

Мирошин Дмитрий Григорьевич

Кандидат педагогических наук, Доцент

Ефременко Евгений Сергеевич

Кандидат медицинских наук, Доцент

Шалагинова Ксения Сергеевна

Кандидат психологических наук, Доцент

Катермина Вероника Викторовна

Доктор филологических наук, Профессор

Полицинский Евгений Валериевич

Кандидат педагогических наук, Доцент

Жичкин Кирилл Александрович

Кандидат экономических наук, Доцент

Пузыня Татьяна Алексеевна

Кандидат экономических наук, Доцент

Ларионов Максим Викторович

Доктор биологических наук, Доцент

Афанасьева Татьяна Гавриловна

Доктор фармацевтических наук, Доцент

Байрамова Айгюн Сеймур кызы

Доктор философии по техническим наукам

Лыгин Сергей Александрович

Кандидат химических наук, Доцент

Заломнова Светлана Петровна

Кандидат педагогических наук, Доцент

Биймурсаева Бурулбубу Молдосалиевна

Кандидат педагогических наук, Доцент

Радкевич Михаил Михайлович

Доктор технических наук, Профессор

Гуткевич Елена Владимировна

Доктор медицинских наук

Матвеев Роман Сталинарьевич

Доктор медицинских наук, Доцент

Шамутдинов Айдар Харисович

Кандидат технических наук, Профессор

Найденов Николай Дмитриевич

Доктор экономических наук, Профессор

Романова Ирина Валентиновна

Кандидат экономических наук, Доцент

Хачатурова Карине Робертовна

Кандидат педагогических наук

Кадим Мундер Мулла

Кандидат филологических наук, Доцент

Григорьев Михаил Федосеевич

Кандидат сельскохозяйственных наук

СОДЕРЖАНИЕ

РАЗДЕЛ XXI. ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА	7
Акаев Т.И., Магомадов Ш.А. Цифровая игровая платформа	7
Арзанукаев А.У., Магомадов Ш.А. Виртуальный ассистент для интернет-магазина	9
Ахмадова Э.З., Сайтова Х.С., Магомадов Ш.А. Тенденции и перспективы цифровизации банковской системы	12
Дадаев И.А., Абдурахманов М.Ш., Магомадов Ш.А. Роль платежной системы как инструмент денежно-кредитной политики	14
Димитриев А.П. К исследованию изменения расписания в системе коммутации потребителей мощности при воздействии типа «единичная функция»	18
Зайцев А.Ф. Математическая модель структурно-функциональной организации программно-информационных вычислительных систем	20
Закаев Р.М., Шуева А.А., Магомадов Ш.А. Банкротство и причины возникновения банкротства предприятия	26
Закаев Р.М., Шуева А.А., Магомадов Ш.А. Новейшая или иная концепция понятия «денег» - криптовалюты	29
Закаев Р.М., Шуева А.А., Магомадов Ш.А. Современная интерпретация эволюции понятия «денег»	31
Захаров А. М., Безнос О.С. Современные подходы к защите данных: как сохранить конфиденциальность в эпоху больших данных	34
Илюхина С.В., Недорезов К.А. Панорама степени внедрения искусственного интеллекта и информационных технологий в России и за рубежом	36
Казакова А.В. Классификация DDoS-атак	39
Казакова А.В. Обзор и сравнение алгоритмов глубокого обучения	42
Карклис А.Д., Дроздова А.А. Перспективы развития портала «Наш город» с учетом применения методов интеллектуального анализа текстов	46
Коновалов Г.Г. Анализ сервиса Keycloak: преимущества и недостатки	50
Коновалов Г.Г. Об архитектурных особенностях безопасности языка Java	52
Коновалов Г.Г. Особенности архитектуры и преимущества колоночных баз данных	55
Коновалов Г.Г. Применение нечеткой логики в программировании	58
Коновалов Г.Г. Реализация алгоритма критического пути	61
Коновалов Г.Г. Реализация транспортной задачи с применением методов линейного программирования	64
Кузнецов А.М. Методы статистического анализа, используемые в информационно-аналитических системах социологических исследований	68
Кулешова И.А., Соколов И.В. Изучение методов увеличения качества изображений	73
Лепиев Д.Р., Гайрабеков А.У., Магомадов Ш.А. Понятие и сущность банкротства предприятий	79
Логачев В.О., Лобанов Е.Г., Нагиева А.С., Семиколеннов С.А., Французова Н.Н. It-образование: как изменяются подходы к обучению в сфере технологий и программирования	82
Лукашевич А.В., Кувшинова И.Б. К вопросу о составлении сложного поискового запроса в базе данных ВИНТИ РАН	84

Лукашевич А.В., Кувшинова И.Б., Теплицкая В.С. Общие принципы формирования предметного и объектного указателей на примере Отдела научной информации по астрономии ВИНТИ РАН.....	89
Масликов Т.О. Принципы глубокого обучения и нейросетей	95
Нучаев С-С.Р., Закаев Р.М., Гузуева Э.Р. Сравнительный анализ систем управления контентом (CMS) и искусственного интеллекта (AI).....	98
Павличенко Е.А., Якубайлик О.Э. Региональная система оперативного спутникового мониторинга	100
Савкина А.В., Матвеев Е.С. Формирование базы данных для интернет-площадки.....	103
Серсултанов Х.Р., Магомадов Ш.А. Цифровая игровая платформа	107
Табашников А.П. Подходы к анализу публикационной активности и обзор существующих программных решений	110
Табашников А.П. Угрозы информационной безопасности, векторы атак и концепции хакинга	114
Филюшкин С.В. Применение гетерогенных структур СКУД в современных кибер-физических системах	116
Филюшкин С.В. Принципы разработки универсального алгоритма работы контроллеров СКУД в рамках распределенного объекта.....	124
Фурман И.С., Похорукова М.Ю. Создание игрового калькулятора для настольной игры.	130
Хоманенко С.В. Возможность использования искусственного интеллекта для защиты видеонаблюдения.....	133
Чухров М.М., Белаш В.Ю. Разработка приложения «Планировщик отпусков» с использованием средств VBA	135
Шатаева Л.И., Тасуев А.А., Магомадов Ш.А. Преимущества и недостатки применения блокчейн технологии в банковской сфере.....	138
Шершнёв Д.Ю. Методология атаки и методы защиты веб-сервера	141
Щербань О.В., Аников Д.А., Брежнев А.В. Интеллектуальная система сбора информации о пациентах, предназначенная для медицинских учреждений с использованием медицинского браслета.....	144
Юданов Р.С. Классификация стеганографии по виду покрываемого объекта	151
Юданов Р.С. Методы анализа публикационной активности	154
Юданов Р.С. Основные методы и применение стеганографии в различных областях	158
Юданов Р.С. Современные методы проведения тестирования на проникновение	161
Яблоков Д.С. Методы анализа сетевого трафика.....	163
Яблоков Д.С. Традиционные методы классификации сетевого трафика	166
Яблоков Д.С. Устройство фундаментальной концепции сетевых технологий TCP/IP	169
РАЗДЕЛ XXII. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ	172
Абдразаков В.А., Харченко С.Н. Роль участия искусственного интеллекта в образовании.....	172
РАЗДЕЛ XXIII. НАНОТЕХНОЛОГИИ.....	175
Мукминова И.Р. Функциональная отделка текстиля с использованием полиэлектролитов	175

РАЗДЕЛ XXI. ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Акаев Т.И., Магомадов Ш.А.
Цифровая игровая платформа

ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)

doi: 10.18411/trnio-10-2024-371

Аннотация

В 2010-х годах цифровые игровые платформы значительно изменили сферу игровой индустрии, став одним из её основополагающих элементов. Этот десятилетний период стал временем революционных изменений, которые существенно повлияли на способы распространения игр. С переходом от традиционных физических носителей к цифровому формату игровая индустрия претерпела масштабные преобразования, которые оказали влияние на главных субъектов игровой индустрии — разработчиков и игроков.

Ключевые слова: цифровая игровая платформа, Облачные сервисы, облачный гейминг, экономика.

Abstract

In the 2010s, digital gaming platforms significantly changed the sphere of the gaming industry, becoming one of its fundamental elements. This ten-year period was a time of revolutionary changes that significantly affected the way games were distributed. With the transition from traditional physical media to a digital format, the gaming industry has undergone large—scale transformations that have influenced the main actors of the gaming industry - developers and players.

Keywords: digital gaming platform, Cloud services, cloud gaming, economics.

Цифровая игровая платформа — это программное обеспечение или онлайн-сервис, который предоставляет пользователям доступ к играм в цифровом формате. Цифровые игровые платформы позволяют приобретать, арендовать или получать игры по подписке. Кроме того, такие платформы предлагают различные игровые функции. Благодаря этому игры становятся более привлекательными и доступными для широкого круга пользователей, а также стимулируют развитие интернет-торговли и облачных технологий.

К наиболее популярным цифровым игровым платформам относятся Steam от Valve, PlayStation Store от Sony, Xbox Store от Microsoft, а также мобильные платформы Google Play от Google и AppStore от Apple.

Цифровые игровые платформы обладают рядом существенных преимуществ перед физическими устройствами хранения данных (например, дисками или картриджами). Вот основные из них:

1. **Доступность:** игры можно приобрести и загрузить сразу после покупки, не посещая магазин и не дожидаясь доставки. Это позволяет игрокам начать игру практически мгновенно.
2. **Экономия:** Подписочные сервисы, позволяют игрокам получать доступ к различным играм за фиксированную плату, что значительно экономит деньги по сравнению с покупкой игр по отдельности.
3. **Простота использования:** Цифровые платформы предлагают удобные интерфейсы для управления библиотекой игр, включая функции поиска, сортировки и фильтрации.
4. **Отсутствие риска повреждения:** Цифровые игры не подвержены физическому износу, такому как царапины или повреждение упаковки, что в перспективе обеспечивает их надежное хранение.

Несмотря на свои привлекательные для пользователей преимущества, цифровые платформы имеют немало минусов, например:

1. Подключение к сети: Для активации или загрузки игр требуется стабильное интернет соединение, данная минус может стать главным фактором для приобретения физических копий игр.
2. Права потребителей: Цифровые платформы используют системы защиты цифровых прав, которые могут ограничивать возможность использования игр.
3. Безопасность данных: Данные, которые хранятся на удаленных серверах, могут подвергнуться кибератаке или утечке.

В последнее время цифровые игровые платформы поставили перед собой цель максимально увеличить распространение предоставляемых товаров и услуг, облачные сервисы являются одним из способов достижения этой цели. Так как облачные сервисы доступны на большинстве устройствах имеющих доступ к всемирной паутине и не требуют загрузки игр на устройства. Параллельно с развитием облачных игр растет интерес к облачным технологиям в целом. Компании, предоставляющие облачные сервисы, начинают активно развивать свои предложения для поддержки игровой индустрии. Это включает в себя повышение качества серверов, увеличение пропускной способности сети и разработку специализированных решений для эффективного использования ресурсов. Таким образом, облачные игровые сервисы является двигателем не только для игровой индустрии, но и всей индустрии облачных технологий. Главными поставщиками услуг облачного гейминга являются сервисы: Xbox Cloud Gaming, NVIDIA GeForce NOW, Google Stadia и PlayStation Now.

По состоянию на 2023 год общая капитализация игровой индустрии оценивается более чем в 300 миллиардов долларов. Этот рост обусловлен увеличением числа пользователей, расширением платформ (мобильные игры, ПК, консоли, облачные игры) и растущим интересом к электронным спортивным соревнованиям (киберспорту). Учитывая этот факт, трудно не заметить роль цифровых платформ в экономике. Давайте подробнее рассмотрим, как цифровые игровые платформы влияют на экономику:

1. Создание новых рынков: Цифровые игровые платформы способствовали созданию новых рынков, таких как облачные игры, инди-игры и виртуальная реальность. Эти новые сегменты предлагают разработчикам и издателям возможности монетизации, что приводит к увеличению числа стартапов и малых предприятий в игровой индустрии.
2. Увеличение доходов от продаж: Переход на цифровой формат значительно увеличил выручку от продаж игр. Цифровые платформы, такие как Steam, PlayStation Network и Xbox Live, предоставляют разработчикам возможность напрямую взаимодействовать с потребителями, что позволяет им получать увеличить количество продаж
3. Увеличение числа рабочих мест: Цифровые игровые платформы способствуют созданию рабочих мест в различных секторах, включая разработку игр, маркетинг, обслуживание клиентов и техническую поддержку. Отрасль привлекает талантливых специалистов, что также влияет на образование в области технологий
4. Доступ к глобальному рынку: Цифровые платформы позволяют разработчикам игр выходить на международные рынки без необходимости физического присутствия. Это способствует глобализации игровой индустрии и международной торговли, что может привести к значительному экономическому росту развивающихся рынков.

Заключение

Цифровые игровые платформы произвели революцию в игровой индустрии, изменив способы распространения игр, их монетизации и взаимодействия с ними. Они открыли новые возможности для разработчиков, сделав игры доступными для широкой аудитории, и предоставили игрокам удобные способы покупки и использования контента. В то же время они

стимулировали развитие таких технологий, как облачные сервисы и киберспорт, что, в свою очередь, повлияло на экономику и инновации в других областях. Однако, несмотря на свои многочисленные преимущества, цифровые платформы также сталкиваются с рядом проблем, таких как зависимость от Интернета и ограничения прав пользователей. Тем не менее, их значение для игровой индустрии продолжает расти, создавая новые перспективы для дальнейшего развития и инноваций.

1. Steamworks. Цифровое распространение и публикация игр — Текст: электронный // Steam: [сайт]. — URL: <https://partner.steamgames.com/> (дата обращения: 18.09.2024).
2. Важность маркетинга с влиятельными лицами в игровой индустрии — Текст: электронный // Newzoo: [сайт]. — URL: <https://newzoo.com/influencer-marketing/> (дата обращения: 18.09.2024).
3. Микротранзакции в видеоиграх: преимущества и проблемы — Текст: электронный // Game Developer: [сайт]. — URL: <https://www.gamedeveloper.com/business/microtransactions-in-video-games/> (дата обращения: 18.09.2024).

Арзанукаев А.У., Магомадов Ш.А.

Виртуальный ассистент для интернет-магазина

ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»

(Россия, Грозный)

doi: 10.18411/trnio-10-2024-372

Аннотация

Виртуальный ассистент для интернет-магазина — это программное решение, которое помогает улучшить клиентский опыт и повысить эффективность работы бизнеса. Он может выполнять ряд функций, таких как:

Поддержка клиентов: Ответы на часто задаваемые вопросы, помощь с оформлением заказов и решение проблем.

Персонализированные рекомендации: Анализ покупательских предпочтений и предложение товаров, которые могут заинтересовать клиента.

Автоматизация процессов: Обработка заказов, управление запасами и мониторинг доставки.

Сбор отзывов: Помощь в сборе и анализе отзывов клиентов для улучшения сервиса и продукции.

Маркетинговые акции: Уведомление о специальных предложениях и акциях, направленных на увеличение продаж.

Этот ассистент может работать 24/7, что позволяет магазинам улучшить обслуживание клиентов и повысить конверсию. С его помощью можно не только снизить нагрузку на сотрудников, но и увеличить лояльность клиентов благодаря быстрому и качественному сервису.

Ключевые слова: виртуальный ассистент, интернет-магазин, поддержка клиентов, персонализированные рекомендации, автоматизация процессов, конверсия лояльность клиентов.

Abstract

A virtual assistant for an online store is a software solution that helps to improve customer experience and business performance. It can perform a number of functions such as:

Customer Support: Answering frequently asked questions, helping with ordering and solving problems.

Personalized recommendations: Analyzing customer buying preferences and suggesting products that may interest the customer.

Process Automation: Order processing, inventory management and delivery monitoring.

Feedback gathering: Helping to collect and analyze customer feedback to improve service and products.

Marketing promotions: Notification of special offers and promotions to increase sales.

This assistant can work 24/7, allowing stores to improve customer service and increase conversion rates. With its help, you can not only reduce the workload of employees, but also increase customer loyalty due to fast and high-quality service.

Keywords: virtual assistant, online store, customer support, personalized recommendations, process automation, conversion customer loyalty.

Виртуальный помощник для интернет-магазина — это программный инструмент, созданный для автоматизации взаимодействия с клиентами и оптимизации бизнес-процессов. В его основе лежит искусственный интеллект (ИИ), который позволяет ему обучаться и адаптироваться к потребностям пользователей и магазина. Давайте разберемся подробнее, как работает этот помощник и чем он может быть полезен.

Основными функциями виртуального помощника являются

Поддержка клиентов

Одной из основных задач виртуального помощника является помощь клиентам, которая включает в себя:

Ответы на часто задаваемые вопросы (FAQ): мастер может мгновенно предоставить информацию по таким типичным вопросам, как «Как оформить заказ?», «Какие способы оплаты доступны?», «Сколько стоит доставка?» и т. д. Это снижает нагрузку на службу поддержки.

Навигация по сайту: если клиент не может найти товар или раздел, мастер может направить его на нужную страницу или подсказать категорию товара. Он выступает в роли «виртуального консультанта», экономя время пользователя.

Помощь при оплате: на этапе оформления заказа, если у покупателя возникли трудности, мастер поможет, объяснив, как ввести данные, выбрать способ оплаты или доставки.

Реализация через чат-боты: чаще всего виртуальный помощник работает через чат-боты: на сайте, в мессенджерах (например, WhatsApp или Telegram) или даже в социальных сетях. Клиенты могут задавать вопросы напрямую

Персонализированные рекомендации по товарам

Анализ покупок и интересов: мастер отслеживает поведение покупателя в магазине: какие товары он просматривал, что покупал раньше и какие страницы посещал. На основе этого он может предложить товары, которые могут заинтересовать покупателя. Например, если клиент часто покупает электронику, мастер предложит ему новые модели телефонов или аксессуары.

Перекрестные и дополнительные продажи: мастер может предложить дополнительные продукты (например, аксессуары для основного продукта) или более дорогие и модернизированные версии того, что рассматривает клиент.

Автоматизация процессов

Виртуальный помощник помогает компаниям автоматизировать рутинные задачи, что значительно экономит время:

Обработка заказов: как только клиент размещает заказ, мастер автоматически передает информацию на склад для дальнейшей обработки. Это избавляет от необходимости выполнять работу вручную и снижает вероятность ошибок.

Управление запасами: Мастер отслеживает количество товаров на складе. Если товара нет в наличии, он оповещает менеджеров магазина, что позволяет своевременно пополнить запасы.

Отслеживание доставки: Мастер может отслеживать статус доставки заказов и уведомлять клиента о том, что его посылка находится в пути, прибыла на склад или уже доставлена.

Комментарии и отзывы

Сбор отзывов: после того как клиент получил заказ, мастер может отправить вам запрос на обратную связь. Вы можете спросить, доволен ли клиент продуктом и услугой, и собрать предложения по улучшению.

Управление негативными отзывами: если клиент оставляет негативный отзыв, мастер может автоматически предложить решение проблемы, например возврат денег, замену или скидку на будущие покупки. Это помогает поддерживать лояльность клиентов.

Продвижение акций и скидок

Информирование о скидках: Виртуальный помощник может напоминать клиентам о текущих акциях, скидках и специальных предложениях. Это можно сделать с помощью уведомлений на сайте, электронных писем или сообщений.

Персонализированные предложения: основываясь на предпочтениях клиента, помощник может предложить индивидуальные скидки или промокоды, что повышает вероятность повторных покупок.

Технологическая база

Ассистент работает на основе ряда технологий:

- 1. Искусственный интеллект (AI) и машинное обучение (ML):** эти технологии позволяют ассистенту анализировать данные, понимать поведение клиентов и адаптироваться к их потребностям. Чем больше помощник взаимодействует с клиентами, тем больше он совершенствуется.
- 2. Обработка естественного языка (NLP):** это технология, которая позволяет ассистенту «понимать» человеческий язык. С помощью NLP ассистент может отвечать на вопросы, поддерживать разговор и управлять запросами в режиме реального времени.
- 3. Интеграция с CRM и ERP-системами:** Ассистент часто интегрируется с другими бизнес-системами, такими как CRM (системы управления взаимоотношениями с клиентами) и ERP (системы управления предприятием). Это помогает собирать и анализировать данные о клиентах, заказах, запасах и других бизнес-процессах.

Преимущества для клиентов и компаний

Для клиентов:

Доступность 24/7: помощник всегда на связи, независимо от времени суток. Это особенно удобно для тех, кто совершает покупки ночью или в разных часовых поясах.

Быстрые ответы: Клиенты получают мгновенные ответы, что значительно повышает качество обслуживания и снижает риск того, что они уйдут на сайт конкурента.

Персонализация: покупатели получают рекомендации и скидки, соответствующие их интересам, что делает процесс покупок более удобным и увлекательным.

Для предприятий:

Экономия ресурсов: Виртуальный помощник снижает нагрузку на сотрудников, освобождая их от рутинных задач, таких как ответы на типичные вопросы или обработка заказов.

Увеличение продаж: благодаря рекомендациям, персонализированным предложениям и быстрому обслуживанию клиенты совершают больше покупок и с большей вероятностью вернуться в магазин.

Анализ данных: Ассистент собирает и анализирует множество данных о поведении покупателей, помогая компаниям лучше понять свою аудиторию и усовершенствовать маркетинговые стратегии.

Заключение

В заключение следует отметить, что виртуальный помощник для интернет-магазина — это не просто практичный инструмент, а стратегически важный элемент современной электронной коммерции. Он выполняет множество задач - от помощи клиентам и персонализации их покупок до автоматизации рутинных процессов, таких как обработка

заказов и управление запасами. Благодаря круглосуточной доступности и мгновенным ответам помощник значительно улучшает качество обслуживания клиентов, повышает их удовлетворенность и укрепляет лояльность.

Для предприятий виртуальный помощник означает сокращение операционных расходов, повышение эффективности и увеличение продаж благодаря персонализированным рекомендациям и маркетинговым кампаниям. Кроме того, он предоставляет ценные данные о поведении пользователей, которые помогают лучше понять аудиторию и адаптировать стратегии продаж.

В условиях жесткой конкуренции на рынке электронной коммерции наличие виртуального помощника дает интернет-магазину значительное преимущество, делая процесс покупки более легким и приятным для покупателей, а бизнес - более прибыльным и устойчивым.

1. "Artificial Intelligence for Marketing" (Джим Стерн) — о применении ИИ в маркетинге и персонализации.
2. "AI Superpowers" (Кай-Фу Ли) — о внедрении ИИ в бизнес-среду.
3. "E-Commerce Power: стратегии роста в электронной коммерции"
4. "The Future of Customer Interaction: использования виртуальных ассистентов и чат-ботов в электронной коммерции"

Ахмадова Э.З., Сайтова Х.С., Магоматов Ш.А.

Тенденции и перспективы цифровизации банковской системы

ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»

(Россия, Грозный)

doi: 10.18411/trnio-10-2024-373

Аннотация

Сегодня банки пересматривают бюджеты и расставляют приоритеты на основе актуальной экономической ситуации, реализуя, в первую очередь, наиболее прибыльные потенциально проекты. Развиваются сервисы, направленные непосредственно на российский рынок. Пристальное внимание уделяется решению задач информационной безопасности.

Ключевые слова: цифровизация, банк, ИТ-рынок, смарт-контракты, блокчейн.

Abstract

Today, banks are reviewing budgets and setting priorities based on the current economic situation, implementing, first of all, the most profitable potential projects. Services aimed directly at the Russian market are being developed. Close attention is paid to solving information security problems.

Keywords: digitalization, bank, IT market, smart contracts, blockchain.

Современные инновации способствуют сохранению и увеличению конкурентных преимуществ банка на рынке финансовых услуг, оптимизации всех бизнес-процессов, а также помогает сократить операционные расходы. Автоматизация рабочих мест является одним из важнейших достоинств, так как способствует упрощенному режиму обработки данных, что, в свою очередь, значительно ускоряет операции, связанные с предоставлением кредитов и обслуживания клиентов, а также существенно сокращает время для проведения проверок большого объема информации. Не менее важно, что применение передовых технологий сводит к минимуму вероятность появления ошибок, поскольку устраняется человеческий фактор. Это вызвано тем, что процесс автоматизированной обработки данных использует определенный алгоритм действий, характеризующийся точностью и надежностью. Помимо вышеперечисленного, автоматизация обеспечивает решение таких базовых задач, как ведение бухгалтерского учета, своевременное формирование обязательной финансовой отчетности. Инновационная активность и оперативное реагирование на изменяющиеся потребности

клиентов, внедрение новейших технологий служат залогом успешности и одними из факторов формирования конкурентоспособности кредитного учреждения.

Главными точками роста для развития цифровизации в банках остаются прежние перспективные направления: облака (SaaS, PaaS), аналитика данных, машинное обучение, DevOps. Но реализованы они теперь будут по-другому, с акцентом на отечественные продукты и сервисы. Так, для банков, как и в целом по ИТ-рынку, актуален тренд на миграцию с западных облачных платформ на российские. Повышается востребованность в отечественных программно-аппаратных комплексах (ПАК), в которых вычислительный модуль оптимизирован под работу конкретного ПО.

Среди относительно новых направлений цифровизации стоит отметить технологию NFC, дающую клиентам банка новый пользовательский опыт.

Наконец, еще одной точкой роста для финансовых организаций становится расширение их сотрудничества с ИТ-интеграторами: например, в области создания совместных центров компетенций и центров поддержки зарубежного программного обеспечения. Это позволяет заказчикам реализовать наиболее оптимальную, поэтапную стратегию импортозамещения.

В целом, проекты российских компаний по переходу на импортонезависимые программные и аппаратные решения будут проводиться в течение всего 2024 года.

Смарт-контракты в настоящее время используют программное обеспечение и технологию электронной подписи для идентификации личности. В большинстве случаев для этого требуется вмешательство человека, а для этого требуется регистрация и проверка. Однако эти типы контрактов часто полагаются на посредничество правительств для защиты действительности контракта.

Основное различие между смарт-контрактами и обычными изображено на рисунке



Рисунок 1. Сравнение.

Смарт-контракты работают с технологией блокчейн. Блокчейн — это криптографическая технология, использующая математический код для создания базы данных. Блокчейн по своему замыслу снижает любую возможность подделки данных, поскольку использует сложную математику для решения головоломки, недоступной человеческому пониманию.

Технология Blockchain — это децентрализованная распределенная технология управления данными с помощью шифрования данных, хранения цепочки данных и механизма распределенного консенсуса.

В отличие от традиционной структуры цепочки, хеш-указатель используется в системе блокчейн для достижения логических связей между блоками данных. Структура может эффективно увеличить сложность подделки данных, поскольку данные в блоке данных изменяются, это приведет к изменению значения хэша заголовка последующего блока данных. Кроме того, последующий блок данных содержит информацию предыдущего блока данных, что обеспечивает временную связь между блоками данных.

Одним из самых простых примеров применения искусственного интеллекта в сфере развлечений могут послужить рекомендационные системы на основе машинного обучения таких платформ, как Amazon Prime Video, Netflix и YouTube. Эти системы учатся на данных истории запросов, просмотров, предпочтений и поведении пользователей и создают модели, предлагающие им фильмы, телешоу, короткие видео, книги и другой контент.

На этом примеры использования алгоритмов искусственного интеллекта не заканчиваются. Компания Disney использует интегрировал эти технологии в свои рабочие процессы анимации и визуальных эффектов. Также различные инструменты, на подобие Scriptbook и HyperWrite, показывают хорошие результаты и невероятный потенциал в написании сценариев и повествовании. Они анализируют огромный объем существующих произведений и на их основе создают последовательные повествования на основе выявленных шаблонов и структур.

Заключение

В образовании технологии искусственного интеллекта используются в целях повышения потенциала педагогов, создания и оцифровки лекций и учебных пособий, а также репетиторства. Примером служит Thinkster Math, который описывается разработчиками как программа репетиторства по математике, интегрирующая новаторский ИИ и человеческое взаимодействие для создания персонализированных учебных программ. Также есть программы-чаты, виртуальные ассистенты, программные обеспечения для распознавания речи и не только.

На основе компьютерного зрения были созданы программы, решающие проблемы даже в отрасли сельского хозяйства. При этом создаются самые различные решения: обнаружение болезней и насекомых, распознавание зрелости урожая, оценка почвы, мониторинг здоровья скота и так далее.

Прекрасным примером реализации всех этих идей является британская компания V7 Labs, которая активно разрабатывает технологию для автоматизации и сбора данных, необходимых для машинного обучения.

1. Генкин А., Михеев А. Blockchain: Как это работает и что ждет нас завтра // Издательство Альпина, 2019. С. 20-22.
2. Генкин А. С. Blockchain: Как это работает и что ждет нас завтра/ А. С. Генкин, А. А. Михеев. - Москва: Альпина Паблишер, 2018. - 592 с
3. Букасова А. Ю. Blockchain-технология как инструмент децентрализованного мира // Современные тенденции развития науки и технологий. - 2018. - № 9. - С. 5-9.
4. Винья Пол. Эпоха криптовалют. Как биткоин и blockchain меняют мировой экономический порядок. Москва: Изд-во «Манн, Иванов и Фербер», 2017 (2018). 429 с
6. Власов А. И., Карпунин А. А., Новиков И. П. Системный анализ
7. технологии обмена и хранения данных blockchain // Современные технологии. Системный анализ. Моделирование, 2017.с.49-82

Дадаев И.А., Абдурахманов М.Ш., Магомадов Ш.А.

Роль платежной системы как инструмент денежно-кредитной политики

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-374

Аннотация

В настоящее время устойчивое и бесперебойное функционирование финансового сектора невозможно без высокоэффективной платежной системы, с применением современных форм расчетов Цифровые деньги центрального банка — это центральная система. Платежная система Банка России является составной частью национальной платежной системы. На

законодательном уровне она признается системно значимой платежной системой, через которую реализуется денежно-кредитная и бюджетная политика Российской Федерации.

Ключевые слова: платежная система, финансы, рынок, банк, экономика.

Abstract

Currently, the stable and uninterrupted functioning of the financial sector is impossible without a highly efficient payment system, with the use of modern forms of payment, the digital money of the central bank is the central system. The payment system of the Bank of Russia is an integral part of the national payment system. At the legislative level, it is recognized as a systemically significant payment system through which the monetary and budgetary policy of the Russian Federation is implemented.

Keywords: payment system, finance, market, bank, economy.

Мир несовершенных рынков капитала, в котором значительную роль играет процесс кредитования коммерческих банков, кажется более интересным (и реалистичным). Для рефинансирования собственного кредитования банкам приходится привлекать депозиты или другие заемные средства. Привлечение таких внешних средств, например, посредством вышеупомянутого выпуска банковских облигаций, становится более дорогим в случае повышения денежной процентной ставки, привлекается меньше внешних средств, кредитование банков и, следовательно, финансируемая кредитом часть инвестиций и снижение потребления

Поскольку операции с активами, которые считаются слишком рискованными, можно легче и быстрее наказать за счет вычетов по депозитам, это имеет дисциплинарный и снижающий риск эффект. Это явно положительный вклад цифровых денег центрального банка в стабильность финансового рынка.

Эффективность этого эффекта во многом зависит от наличия страхования вкладов. Если вкладчик-физическое лицо не несет никакого риска в виде (частичной) потери своих вкладов в случае неплатежеспособности банка, он не будет осуществлять никакого мониторинга. Кроме того, сегодня еще существует возможность перевода депозитов из проблемного банка в здоровый банк. Но эти соображения носят микроэкономический характер. На макроэкономическом уровне следует принять во внимание случай общего банковского кризиса. Переводы в здоровые банки здесь обычно невозможны, а страхование вкладов также теряет доверие, поскольку сумма требований к страховой компании значительно превышает ресурсы в случае общего банковского кризиса. Если страховое покрытие считается ненадежным, существует риск сценария массового изъятия средств из банка. Цифровые деньги центрального банка вмешиваются в ситуацию двумя способами. С одной стороны, это вполне надежная защита вкладчиков, поскольку перевод депозитов в центральный банк обеспечивает полную защиту от любой их потери. С другой стороны, цифровые деньги центрального банка облегчают вывод депозитов, поскольку депозиты могут быть беспрепятственно и в любое время переведены из коммерческих банков в центральный банк. Любые сложности, которые могут возникнуть, например, при конвертации депозитов в наличные, устраняются. Как следствие, вероятность таких вычетов, вероятно, возрастет в беспокойные времена.

Потери активов, связанные с общим банковским кризисом, уменьшаются с помощью цифровых денег центрального банка, но вероятность общего банковского кризиса грозит увеличиться в результате более легкого вывода средств. Таким образом, цифровые деньги центральных банков являются палкой о двух концах с точки зрения стабильности финансового рынка. Однако следует прямо отметить, что изложенные соображения содержат высокую степень спекуляций, поскольку на сегодняшний день не существует основательного

теоретического или эмпирического анализа, посвященного цифровым деньгам центрального банка в их взаимодействии со страхованием вкладов и адаптационным поведением вкладчиков и коммерческих предприятий. банки. Здесь существует значительная потребность в исследованиях.

Центральные банки являются стержнем экономической жизни в большинстве современных обществ. Они несут основную ответственность за регулирование денежно-кредитная политика и поэтому оказывают существенное влияние на экономическую ситуацию как внутри своих стран, так и на международном уровне.

Основная цель ЕЦБ – поддерживать стабильность цен. Мы работаем для жителей еврозоны и обеспечиваем сохранение стоимости евро. Здесь вы можете узнать о нашей стратегии денежно-кредитной политики, наших инструментах и о том, как наши меры влияют на вашу повседневную жизнь.

Мы также следим за финансовыми рынками. Это дает нам информацию, необходимую для нашей главной задачи: обеспечения стабильных цен. Это способствует экономическому росту. По сути, центральные банки выполняют четыре основные функции: контроль над денежная масса, мониторинг и регулирование финансовой системы, управление валютными резервами и обеспечение финансовой стабильности.

- контроль над денежной: Покупая и продавая государственные облигации на открытом рынке, центральные банки могут влиять на денежную массу в экономике.
- надзор и регулирование финансовой системы: они контролируют и регулируют банки и другие финансовые учреждения для обеспечения здоровья финансовой системы.
- управление валютными резервами: Центральные банки управляют валютными резервами страны для обеспечения стабильности национальной валюты.
- обеспечение финансовой стабильности. Благодаря своей роли «кредитора последней инстанции» центральные банки могут стабилизировать финансовую систему во время кризиса.

Их роль делает их центральной частью экономической системы, как на национальном, так и на международном уровне.

Например, если центральный банк увеличивает денежную массу, это может привести к падению процентных ставок по кредитам. Это, в свою очередь, может привести к тому, что больше людей и предприятий будут брать займы и тратить деньги, что может стимулировать экономику.

В начале (длинной) цепочки эффектов, посредством которых решения денежно-кредитной политики влияют на уровень цен, находится изменение ключевых процентных ставок, устанавливаемых центральным банком для своих операций денежно-кредитной политики. Это дает центральному банку доминирующее влияние на денежный рынок и, таким образом, может контролировать процентные ставки на денежном рынке. Изменения ставок денежного рынка, в свою очередь, влияют на другие (долгосрочные) процентные ставки.

В процессе цифровизации спрос на наличные деньги все больше вытесняется, а платежные операции приватизируются. Отражением этого развития является потеря власти со стороны центральных банков, их набор инструментов находится под угрозой потери эффективности. Недавно широко обсуждавшаяся реакция центральных банков на эту проблему заключается в создании цифровых денег центрального банка со счетом в центральном банке для каждого. Переход от одной формы денег к ее преемнику всегда отражал технологические разработки. Процесс цифровизации знаменует собой следующий шаг здесь. Поскольку даже самые маленькие суммы теперь могут быть переведены в одноранговом электронном виде в

режиме реального времени, наличные деньги теряют свое сравнительное преимущество и находятся под угрозой вытеснения с платежного рынка. Взгляд на Швецию кажется взглядом в будущее. В дополнение к более широкому использованию дебетовых и кредитных карт, в частности, в Швеции развивается мобильная платежная система Swish. В настоящее время лишь чуть менее 20% всех транзакций в точках продаж обрабатываются наличными, и это тенденция; резко падает. В Германии, которая сравнительно экономна в денежных средствах, соответствующий показатель составляет около 75%, и тенденция несколько снижается. Сокращение наличных денег в Швеции — это процесс рыночной экономики, сопровождающийся повышением эффективности. Возможен ли аналогичный процесс в Германии, хотя банкноты евро являются единственным неограниченным законным платежным средством? Да, потому что, вопреки распространенному мнению, функция законного платежного средства не означает, что необходимо принимать наличные. Принцип свободы договора включает право отказаться от оплаты наличными; Любая компания может включить пункт «без наличных» в свои общие положения и условия.

Основная идея цифровых денег центрального банка очень проста: частные домохозяйства и компании получают прямой доступ к балансу центрального банка, открывая счет в центральном банке и делая депозиты.

В предыдущие годы внедрение не удалось, в том числе, из-за отсутствия технической возможности управления учетными записями, независимого от местоположения. Сегодня де-факто определение деталей конструктивных особенностей находится исключительно в компетенции центральных банков.

Частные депозиты, как и традиционные деньги центрального банка (наличные и резервы), являются пассивом центрального банка. В зависимости от конструкции цифровые деньги центрального банка могут быть ближе к наличным деньгам или к резервам. Хотя наличные деньги обращаются в экономике, но не являются электронными, балансы (резервы) коммерческих банков являются цифровыми, но не обращаются. Цифровые деньги центрального банка сочетают в себе следующие свойства: Цифровые единицы денег центрального банка, как правило, являются предметом торговли и обращения в экономике.

Заключение

Цифровые деньги центрального банка — это центральная система. В отличие от частных цифровых валют, таких как Биткойн или Эфириум, центральный банк является четко идентифицируемым эмитентом, который обеспечивает функционирование системы и принимает решения о «правилах игры» по своему усмотрению. Ответственное учреждение, вероятно, будет преимуществом для всеобщего признания цифровых денег. Если центральный банк в первую очередь хочет компенсировать вытеснение наличных денег, он выбирает DZBG, основанный на стоимости. Следует отличать DZBG на основе счетов, который следует рассматривать как расширение инструментов денежно-кредитной политики. Используя цифровые деньги центрального банка, основанные на стоимости, частные лица предъявляют претензии к центральному банку не в форме счета, а в форме представителей стоимости, так называемых токенов. Простейший вариант жетона, практикуемый уже более 200 лет, — печатная бумага, наличные. Доступ через предоплаченные карты или мобильные приложения — это дополнительные варианты, которые возможны для цифровых денег центрального банка.

1. Sveriges Riksbank: Модели платежей в Швеции, май 2018 г.; а также
2. Deutsche Bundesbank: Платежное поведение в Германии, 2017 г., Четвертое исследование использования наличных и безналичных средств платежа, Франкфурт-на-Майне. М. 2022.
3. Глущенко А.В., Слепов А.П. Заем, кредит и ссуда категориальный анализ
4. // Финансы и кредит. 2022. №14. 181с.
5. Волошин И.В. Анализ денежных потоков коммерческого банка//
6. Банковское дело. 2022. - №9. - 221с.

Димитриев А.П.

К исследованию изменения расписания в системе коммутации потребителей мощности при воздействии типа «единичная функция»

ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»
(Россия, Чебоксары)

doi: 10.18411/trnio-10-2024-375

Аннотация

Исследуется дискретная модель коммутации электрических токов нескольким потребителям при широтно-импульсном регулировании мощности. С целью выработки новой эвристики выдвинута гипотеза о так называемой «локальности» процесса оптимизации расписания коммутаций. Рассмотрена реакция системы на изменение в значении входных данных на единицу. Проведены вычисления эксперименты, частично подтверждающие гипотезу.

Ключевые слова: дискретная система, единичная функция, широтно-импульсное регулирование мощности, оптимизация расписания, пространственная локальность.

Abstract

A discrete model of switching electric currents to several consumers with pulse-width power regulation is investigated. In order to develop a new heuristic, a hypothesis is put forward about the so-called "locality" of the switching schedule optimization process. The system's response to a change in the value of input data per unit is considered. Computations are carried out, partially confirming the hypothesis.

Keywords: discrete system, unit function, pulse-width power regulation, schedule optimization, space locality.

В работах автора [1] и многих других (всего в 32 его научных публикациях) исследуется дискретная система, представляющая собой дискретную модель коммутации токов нескольким потребителям при широтно-импульсном регулировании мощности. Коммутация производится по расписанию, от которого зависит ток нагрузки через силовую сеть, который не должен принимать высокое значение (в идеале – как можно меньшее).

В этой модели входные данные представляют собой набор дискретных значений силы тока $\{i_i\}$ и доли от максимальной мощности $\{p_i\}$ для каждого из n потребителей, где $i=1, \dots, n$, а выходные данные – расписание начал коммутаций в течение периода регулирования.

Сформулирована оптимизационная задача и разработаны громоздкие (последняя версия реализации основного модуля на Delphi состоит из 4249 строк текста программы) и трудоемкие во временном отношении алгоритмы получения приближенного к оптимальному расписания коммутаций. При оптимизации возможно применение некоторых эвристик.

В данной статье с целью выработки одной из эвристик исследуется гипотеза о локальности процесса оптимизации. Предпосылкой к этому служит то, что некоторым процессам присуща локальность. Например, вычислительные процессы обладают пространственной и временной локальностью [3]. А именно, зачастую, если процесс считывал какие-то данные, то существует повышенная вероятность, что в скором времени он снова обратится к ним или к данным, расположенным вблизи от этих данных. На этом наблюдении основан принцип кэширования памяти в вычислительных системах, объективность которого подтверждается наличием аппаратной поддержки кэширования, а также политика упреждающего чтения данных.

Проведем аналогию в терминах оптимизации расписания. Пусть входные данные в рассматриваемой системе коммутации изменяются совсем незначительно. Это моделирует незначительный сдвиг в пространстве входных параметров для расписания. Предполагается, что с некоторой вероятностью оптимальное расписание при таком сдвиге также будет изменяться незначительно либо в некоторых случаях вовсе не изменяться, т.е. будет

обнаруживаться то же или почти то же самое расписание. Если это так, то можно будет не проводить каждый раз процесс оптимизации, который при использовании некоторых алгоритмов занимает длительное время, либо разработать и затем использовать новый, менее затратный метод оптимизации, производящий поиск оптимального расписания в окрестности построенного ранее оптимального расписания. И если с математической точки зрения наличие оптимального расписания только в этой окрестности – не факт, то с инженерной точки зрения это может оказаться приемлемым, поскольку предельное значение силы тока в сети, оговоренное с поставщиком, вероятно, превышено не будет, если оно не превышалось при построенном ранее расписании.

Небольшие изменения во входных данных могут рассматриваться как небольшие воздействия на систему. Нечто подобное имеется в операционном исчислении – единичная функция Хевисайда [5], являющаяся простейшей кусочно-непрерывной функцией (оригиналом), принимающей нулевое значение до нулевого момента времени и единичное значение после этого момента. Она применяется при исследовании изменения поведения системы при изменении влияния на систему, количественно выражаемом в одной единице.

В отношении рассматриваемой дискретной модели единичную функцию может моделировать либо изменение силы тока одного из потребителей на одно минимальное дискретное значение (случай 1), либо изменение доли мощности одного из потребителей также на одно минимальное дискретное значение (случай 2). Прохождению нулевого момента времени будет соответствовать переход к составлению расписания при обновленных исходных данных.

Рассмотрим проведение соответствующего вычислительного эксперимента. С помощью информационной системы [2] для файла входных данных spiral-f1.txt [1] для 40 потребителей проведено четыре эксперимента по изменению входных данных относительно исходного набора значений: 1) изменено значение t_1 с 10 на 11; 2) изменено значение t_4 с 5 на 6; 3) изменено значение p_1 с 12 на 13; 4) изменено значение p_4 с 66 на 67.

Оптимизация расписания проведена по не самому оптимальному по получаемому значению целевой функции, но одному из самых быстрых алгоритмов – на основе сортировки по значению произведения t_i на значение меры близости p_i к половине от максимума для i -го потребителя.

Выходные данные представлены в формате текстового файла, содержащего четыре столбца данных и 40 строк. Столбцы представляют собой поля: значение t_i , значение p_i , момент начала коммутации и исходный номер потребителя. Строки соответствуют потребителям. Значений полей разделяются символами табуляции.

После открытия такого файла его содержимое скопировано в MS Excel, таким образом создавая таблицу. Эта таблица отсортировывалась по первым двум столбцам. Пара этих значений в большинстве случаев идентифицирует потребителя, однако имеются три совпадения. Тем не менее, эти совпадения не препятствуют исследованию. Сортировка потребовалась для визуального сравнения пяти таких таблиц, расположенных рядом.

В результате выявлено следующее. Для случая 2 расписание несколько не изменилось в эксперименте 4. Это является подтверждением выдвинутой гипотезы о локальности, однако одного эксперимента для того чтобы сделать выводы явно недостаточно. В эксперименте 3 расписание изменилось незначительно – только для одного потребителя момент начала коммутации переместился на одну единицу из 100 единиц периода, в течение которого реализуется расписание. Расписание реализуется циклически, поэтому перемещение более чем на 50 единиц означало бы перемещение в обратную сторону на менее чем 50 единиц. Поэтому произошло перемещение на 1 единицу из 50 возможных.

В случае 1 изменения более существенные и рассматриваются далее. В эксперименте 1 изменения в начале коммутаций коснулись не только потребителя с увеличенной t_i , но и еще 7 потребителей, причем изменения значительные – от 12 до 50 дискретных единиц времени. В эксперименте 2 – соответственно изменения коснулись еще 10 потребителей, от 3 до 48 дискретных единиц времени.

Таким образом, имеются предпосылки для подтверждения выдвинутой выше гипотезы о локальности. Несмотря на малое количество проведенных экспериментов, фактор случайности снижен благодаря двойным выборкам и представляется правдоподобным, что подтверждение гипотезы в большей степени относится к изменениям в r_i , чем в t_i .

Однако наличие такой локальности не всегда полезно, о чем говорит следующая ситуация. Рассматриваемая модель расписания применена в шифровании данных, при этом исследовался лавинный эффект, состоящий в том, что минимальные изменения входных данных должны производить максимальное изменение в выходных данных [4]. В области шифрования данных такой эффект является желательным явлением, и наоборот, локальность только вредна. Однако важно то, что лавинного эффекта не просто достичь. Таким образом, эта ситуация – скорее исключение из общего правила.

Положительной стороной, как ожидается, в связи с обнаружением локальности меньше нужно будет производить вычислений при оптимизации, однако с другой стороны это несколько снизит криптостойкость шифра при вышеуказанном шифровании.

1. Дмитриев, А. П. Модели и алгоритмы в системах автоматизированного перевода текста // Прикладная информатика. 2013. № 6 (48). С.45-59. URL: http://appliedinformatics.ru/r/articles/article/index.php?article_id_4=1552 (дата обращения 25.09.2024).
2. Дмитриев, А. П. Информационная система для проведения имитационных вычислительных экспериментов по оптимизации расписаний // Системная инженерия и информационные технологии. 2019. Т. 1. № 2 (2). С. 78-86.
3. Олифер, В. Г. Сетевые операционные системы / В.Г. Олифер, Н.А. Олифер. СПб.: Питер, 2002. - 544 с.
4. Дмитриев, А. П. Алгоритм получения лавинного эффекта в криптосистеме со сниженным эффектом размножения ошибок / А. П. Дмитриев, К. В. Никитин // Состояние и перспективы развития ИТ-образования: Сборник докладов и научных статей Всероссийской научно-практической конференции. Чебоксары: Изд-во Чуваш. ун-та, 2019. С. 189-192.
5. Штокало И.З. Операционное исчисление: обобщения и приложения. Киев: Наука думка, 1972. 304 с.

Зайцев А.Ф.

Математическая модель структурно-функциональной организации программно-информационных вычислительных систем

*Восточно-Сибирский государственный университет технологий и управления
(Россия, Улан-Удэ)*

doi: 10.18411/trnio-10-2024-376

Аннотация

Компьютерные программно-информационные вычислительные системы играют ключевую роль в решении множества существующих проблем, связанных с управлением и обработкой цифровой информации. Информационные вычислительные системы представляют собой сложные программные комплексы, структура и функционирование которых включает в себя множество взаимодействующих компонентов, выполняющих анализ и обработку необходимой информации. Разработка формальных моделей для описания структурно-функциональной организации программно-информационных систем является актуальной задачей, так как позволяет определять их внутреннее устройство, вырабатывать новые принципы их проектирования и реализации, а также оптимизировать алгоритмы их работы.

Целью исследования является разработка математической модели для описания структурно-функциональной организации и функционирования программно-информационных вычислительных систем. Для достижения цели были поставлены следующие задачи:

- проанализировать существующие методы моделирования программно-информационных систем;
- проанализировать существующие используемые подходы к проектированию программно-информационных систем;

-разработать и предложить формальную модель для описания структурно-функциональной организации программно-информационных вычислительных систем.

В процессе исследования были использованы следующие общенаучные методы: анализ, декомпозиция, синтез, структуризация, моделирование, формализация, описание, сравнение, а также теория множеств. В качестве материалов исследования использовались компьютеры, программные инструментальные средства и программное обеспечение.

В результате исследования были проанализированы существующие методы моделирования, а также описаны используемые подходы к проектированию программных систем. Разработана и предложена формальная модель для описания структурно-функциональной организации программно-информационных вычислительных систем, построенная на базе методологии системного анализа и математического моделирования. Предложенная модель позволяет описывать процесс функционирования, а также структуру и взаимодействие компонентов различных программно-информационных систем. Модель может быть использована в процессе разработки программных систем на начальных этапах, связанных с моделированием и проектированием программного обеспечения. Результаты исследования могут представлять научную и практическую ценность для широкого круга специалистов, интересующихся анализом, моделированием, проектированием и реализацией различного рода программных систем.

Ключевые слова: модель программной системы, проектирование программных систем, моделирование систем, компьютерное моделирование, организация программ, вычислительные системы, системный анализ, обработка информации, архитектура систем.

Abstract

Computer software-information computational systems play a key role in solving many existing problems related to management and processing of digital information. Informational computational systems are complex software complexes, the structure and functioning of which include many interacting components that analyze and process the necessary information. The development of formal models to describe the structural and functional organization of software-information systems is an urgent task, as it allows us to determine their internal structure, develop new approaches for their design and implementation, and also optimize their algorithms.

The aim of the study is to develop a mathematical model to describe the structural and functional organization and functioning of software-information computational systems. To achieve the goal, the following tasks were set:

- to analyze the existing methods of modeling software-information systems;
- to analyze the existing approaches to the design of software-information systems;
- to develop and propose a formal model to describe the structural and functional organization of software-information computational systems.

In the process of research, such general scientific methods as analysis, decomposition, synthesis, structuring, modeling, formalization, description, comparison, and set theory were used. Computers, software tools, and software were used as research materials.

As a result of the study, existing modeling techniques were analyzed, and the approaches used to design software systems were given. A mathematical model for describing the structural and functional organization of software-information computational systems, based on the methodology of system analysis and mathematical modeling, has been developed and proposed. The proposed model allows for describing the process of functioning as well as the structure and interaction of components of various software-information systems. The model can be used in the process of software system development at the initial stages related to modeling and software design. The results of the study can be of scientific and practical value to a wide range of specialists interested in the analysis, modeling, design, and implementation of various kinds of software systems.

Keywords: software system model, software system design, system modeling, computer simulation, software organization, computational systems, system analysis, information processing, software architecture.

Введение

Проектирование – процесс структурно-функциональной организации программно-информационных систем в виде совокупности параметров, величин, функций и других характеристик, описываемых в форме, пригодной для их реализации [1]. В настоящее время проектирование выполняется поэтапно в соответствии со стадиями, регламентированными ГОСТ России [2].

После реализации программные системы становятся разработанной информационной технологией (набором инструкций для описания технологического процесса преобразования входной информации в выходную), которая материализуется у заказчиков в виде автоматизированных систем и инструментов их обслуживания. Главную роль в определении архитектуры программных систем играет моделирование структуры системы, моделирование взаимодействия между составными частями системы и моделирование взаимодействия системы с окружающей средой.

Как известно, моделирование является одним из общенаучных методов анализа систем (объектов и процессов) на основе их моделей и применяется в целях познания, исследования, проектирования и принятия решений [3]. Таким образом, при моделировании часто возникает задача формального описания функционирования какой-либо системы в целом. Методология системного анализа включает в себя различные методы моделирования, позволяющие решать две основные задачи проектирования:

- задачу анализа, связанную с изучением результатов и поведения системы в зависимости от ее структуры и значений параметров;
- задачу синтеза, связанную с выбором или определением структуры системы и значений параметров, исходя из желаемых результатов и поведения системы в целом.

Методы моделирования систем

Методы моделирования систем подразделяются на две большие категории: физическое (материальное) и математическое (абстрактное). Математическое моделирование также подразделяют на аналитическое и компьютерное. В настоящее время для анализа сложных динамических систем используется компьютерное имитационное моделирование [4, 5, 6].

Компьютерное имитационное моделирование – метод построения модели существующей или проектируемой системы и проведения с ней различных вычислительных экспериментов. В частном случае имитационное моделирование представляет собой более мощное средство для анализа сложных систем. Этот процесс, тесно связанный с анализом поведения и функционирования систем, в рамках экспериментов с их моделями, называют имитацией или симуляцией.

На рисунке 1 приведена существующая методика построения и исследования системы, с использованием метода компьютерного имитационного моделирования.



Рисунок 1. Методика исследования системы с использованием компьютерного имитационного моделирования.

Компьютерная имитационная модель – логико-математическое описание системы, которое может быть использовано для экспериментирования на компьютере в целях анализа, проектирования и оценки эффективности её функционирования. Составными частями имитационной модели являются: структура системы, т.е. описание совокупности элементов и связей между ними; средства воспроизведения поведения системы; свойства среды, в которой функционирует исследуемая система. Эти части вначале носят логико-математический характер, а после представляются в виде совокупности алгоритмов, описывающих динамику функционирования какой-либо системы [7, 8].

Подходы к проектированию и организации программных систем

Для описания структуры и функционирования систем при компьютерном имитационном моделировании используют такие подходы, как: системная динамика, дискретно-событийное или агентное моделирование.

Агентный подход (агентно-ориентированный) моделирования – обобщенная концепция взаимодействующих друг с другом сущностей (агентов), которыми могут являться программы, устройства, роботы, люди, процессы и др. Основная идея, лежащая в основе подхода агентного моделирования, заключается в построении модели вычислительной мультиагентной системы, представляющей собой набор агентов и позволяющей воспроизводить имитацию вычислений для решения различного рода задач. Многоагентные имитационные модели систем содержат распределённые агенты, которые не имеют возможности достижения общей цели в одиночку и, следовательно, должны взаимодействовать друг с другом [9].

В настоящее время при проектировании сложных программных систем также часто применяют: модульный, компонентный или сервис-ориентированный подходы.

Модульный подход – обобщенная концепция организации различных систем в виде совокупности небольших и независимых частей, называемых модулями. Модули составляют первоначальную основу для компонентов и сервисов.

В одной из работ также был предложен *агентно-модульный подход* к проектированию программных систем [10], который можно схематично изобразить на рисунке 2.



Рисунок 2. Агентно-модульный подход к проектированию программных систем.

Агентно-модульный подход – подход к построению обобщённой модели функционирования программной системы и её алгоритмической реализации, отражающей структурно-функциональную организацию в виде независимых программных модулей (агентов), которые представляют собой отдельные части системы, способные взаимодействовать друг с другом.

Рассматриваемый подход представляет собой последовательность из шести основных этапов, при выполнении которых осуществляются процессы как формального математического

моделирования, так и алгоритмического проектирования программной системы. Подробные действия, выполняемые на каждом из этапов описаны ниже:

1. *Системный анализ.* Выполняется анализ поставленной проблемы, задач и требований к реализуемой системе. Если существует компьютерная модель подобной системы, то выполняется её анализ (структурный, функциональный, параметрический).
2. *Модель (системы).* Из результатов проведенного анализа и поставленных задач описывается общая формальная логико-математическая модель, отражающая структуру и функционирование системы.
3. *Методы решения.* Выбираются и описываются формальные методы (метод) решения поставленных задач, которые взаимодействуя с логико-математической моделью отражают структурно-функциональную организацию системы.
4. *Структурно-функциональный синтез.* Полученные модель и методы используются для реализации отдельных модулей компьютерной модели системы в виде алгоритмов (структур представления данных и функций их обработки).
5. *Параметрический синтез.* Выполняется этап параметрического синтеза, на котором происходит определение и корректировка допустимых численных значений для параметров компьютерной модели системы (значения по умолчанию, постоянные значения, диапазоны значений, типы данных и др.).
6. *Алгоритмы (модулей).* Проводятся вычислительные эксперименты с алгоритмами модулей компьютерной модели системы, а также получение и проверка результатов.

Таким образом, агентно-модульный подход объединяет в себе как подход агентного моделирования, так и подход модульного проектирования программных систем. В представленном подходе агентами являются программные модули, которые вступают в отношение посредничества с другими модулями системы, а также с пользователями и внешними системами (внешней средой). В результате применения агентно-модульного подхода появляется возможность (этап 2) описания структурно-функциональной организации какой-либо программной системы [11], в виде обобщенной математической модели.

Математическая модель структурно-функциональной организации программных систем

Математическая модель структурно-функциональной организации программной системы может быть задана относительно времени t некоторым множеством операторов \overrightarrow{Fs} , которые преобразуют независимые переменные (x_i, p_j, f_k) в соответствии со следующим соотношением:

$$\overrightarrow{Y}(t) = \overrightarrow{Fs}(\overrightarrow{X}, \overrightarrow{P}, \overrightarrow{F}, t),$$

где $\overrightarrow{X}(t) = \{x_1(t), x_2(t), \dots, x_n(t)\}$ – множество входных параметров;

$\overrightarrow{P}(t) = \{p_1(t), p_2(t), \dots, p_n(t)\}$ – множество внутренних параметров системы;

$\overrightarrow{F}(t) = \{f_1(\overrightarrow{X}, t), f_2(\overrightarrow{X}, t), \dots, f_n(\overrightarrow{X}, t)\}$ – множество внутренних (базовых) правил взаимодействия;

$\overrightarrow{Y}(t) = \{y_1(t), y_2(t), \dots, y_n(t)\}$ – множество выходных параметров.

Переменные (x_i, p_j, f_k) являются элементами непересекающихся подмножеств и могут содержать как детерминированные, так и стохастические значения.

Каждый агент из множества (\overrightarrow{Fs}) имеет свой собственный набор параметров:

$$\overrightarrow{Pa}(t) = \{pa_1(t), pa_2(t), \dots, pa_n(t)\},$$

а также набор правил:

$$\overrightarrow{Fa}(t) = \{fa_1(\overrightarrow{X}, t), fa_2(\overrightarrow{X}, t), \dots, fa_n(\overrightarrow{X}, t)\},$$

которые могут осуществлять взаимодействие с другими агентами.

Взаимодействие между агентами происходит посредством вызова их специальных правил (функций с префиксом call_) и может быть описано следующим образом:

$$\vec{Y}_a = Call Fa(\vec{X}_a, t),$$

где:

Fa – имя функции агента;

\vec{X}_a – входные параметры для функции агента;

\vec{Y}_a – возвращенные функцией агента значения результатов.

Текущее состояние системы описывается набором её внутренних параметров $\vec{P}(t)$. Изменение значений данных параметров свидетельствует о переходе системы в другое состояние, согласно определенным базовым правилам $\vec{F}(t)$. Специальные функции агентов (с префиксом call_) могут выполнять базовые правила для изменения значений внутренних параметров и смены состояния системы, а также возвращать ответную реакцию \vec{Y}_a в качестве результата на входные воздействия \vec{X}_a .

Результаты и выводы

В результате исследования была разработана и предложена формальная модель для описания структурно-функциональной организации программно-информационных вычислительных систем. Использование предложенной математической модели позволяет значительно упростить процесс проектирования различных программных систем, делая его более простым, понятным и формализованным. Отличительной особенностью является и то, что подобные модели можно изображать в виде рисунков, отражающих схемы структурно-функциональной организации проектируемых программных систем.

Предложенная модель также может быть применима для проектирования и реализации распределенных программных систем, в которых некоторые данные X сначала передаются узлу, который выполняет функцию агента fa_1 , затем передает результат второму узлу, для вычислений функцией агента fa_2 , и, наконец, третьему узлу, который вычисляет результат функцией агента fa_3 . Подобную модель функционирования можно представить, например, в виде суперпозиции функций: $fa_3 (fa_2 (fa_1 (X, t), t), t)$.

Таким образом, данные могут обрабатываться последовательно или параллельно с помощью функций распределённых и автономных агентов-модулей. Предложенная модель также хорошо сочетается с множеством общеизвестных практических методик проектирования программных систем, например таких как: MVC, MVP, MVVM и других [12].

1. Pyster A., Olwell D., Hutchison N., Enck S., Anthony J., Henry D., Squires A. Guide to the Systems Engineering Body of Knowledge (SEBoK) version 1.0. – Hoboken: The Trustees of the Stevens Institute of Technology, 2012. – 609 p.
2. ГОСТ 2.103-68. Единая система конструкторской документации. Стадии разработки – М.: Стандартинформ, 2007.
3. Королев А.Л. Компьютерное моделирование: учебное пособие / А.Л. Королев – Челябинск: Изд-во Челяб. гос. пед. ун-та, 2019. – 189 с.
4. Черникова О.С. Компьютерное моделирование: учеб. пособие / О.С. Черникова, В.С. Карманов – Новосибирск: Изд-во НГТУ, 2021. – 100 с.
5. Акопов А.С. Имитационное моделирование: учебник и практикум / А.С. Акопов – Москва: Юрайт, 2023. – 389 с.
6. Древис Ю.Г. Имитационное моделирование: учеб. пособие / Ю.Г. Древис, В.В. Золотарёв – 2-е изд. – Москва: Юрайт, 2023. – 142 с.
7. Боев В.Д. Имитационное моделирование систем: учеб. пособие / В.Д. Боев – Москва: Юрайт, 2023. – 253 с.
8. Белякова А.Ю. Имитационное моделирование: учеб. пособие / А.Ю. Белякова – Иркутск: Изд-во ИрГАУ, 2020. – 120 с.
9. Тихвинский В.И. Многоагентное моделирование: учеб.-метод. пособие / В.И. Тихвинский, В.В. Холмогоров, В.А. Морозов – Москва: Изд-во МИРЭА, 2022. – 103 с.

10. Зайцев А.Ф. Агентно-модульный подход к проектированию и реализации программных систем на основе имитационного моделирования / А.Ф. Зайцев // System Analysis & Mathematical Modeling, Т.5, №3, 2023. – С. 338-349 – DOI 10.17150/2713-1734.2023.5(3).338-349
11. Зайцев А.Ф. Системный анализ, классификация и организация программных экспертных систем / А.Ф. Зайцев // Современные научные исследования: проблемы, тенденции, перспективы: сборник научных трудов по материалам XXI Международной научно-практической конференции, Анапа, 17 ноября 2023 года – Анапа: Общество с ограниченной ответственностью «Научно-исследовательский центр экономических и социальных процессов» в Южном Федеральном округе, 2023. – С. 60-75.
12. Garcia R.F. iOS Architecture Patterns: MVC, MVP, MVVM, VIPER, and VIP in Swift / R.F. Garcia – Berkeley: Apress, 2023. – 397 p.

Закаев Р.М., Шуева А.А., Магомадов Ш.А.

Банкротство и причины возникновения банкротства предприятия

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-377

Аннотация

Важным фактором для эффективного существования предприятия является финансовая устойчивость, она выступает преимуществом перед конкурентами так как для инвесторов особенно важна финансовая устойчивость, при вложении средств рассматривают в силах ли компания покрывать свои расходы в противном случае компания считается банкротом. Такие понятия как финансовая устойчивость, финансовое состояние неразрывно связаны с риском банкротства так как там, где нет эффективного финансового функционирования есть риск несостоятельности.

Ключевые слова: риск, банкротство, финансы, бизнес.

Abstract

An important factor for the effective existence of an enterprise is financial stability, it acts as an advantage over competitors, since financial stability is especially important for investors, when investing funds, they consider whether the company is able to cover its expenses, otherwise the company is considered bankrupt. Concepts such as financial stability and financial condition are inextricably linked with the risk of bankruptcy, since where there is no effective financial functioning, there is a risk of insolvency.

Keywords: risk, bankruptcy, finance, business.

Понятия финансовое состояние и финансовая устойчивость связывают с денежным состоянием предприятия. Финансовое состояние предприятия – это сумма определенных показателей на определенный срок, которые позволяют выполнять финансовые обязательства компании, продолжать финансовую и инвестиционную деятельность. Из описанного термина мы понимаем, что финансовое состояние определяет такие направления как инвестиционный и финансовый. Близким к термину «финансовое состояние» является термин финансовый результат, что означает итог в денежном или в другом выражении инвестиционной и финансовой деятельности компании. Для всякого хозяйствующего субъекта характерно наступление кризиса в процессе функционирования и развития. Кризисное состояние для предприятий в условиях рынка это естественное явление.

Банкротство является крайней формой кризисного состояния, когда организация не в силах оплатить задолженности из собственных источников дохода. Банкротство является результатом развития кризисного состояния предприятия. Существует много рассуждений на тему что из себя представляет «кризис», в каких-то направлениях кризис определяется как сочетание таких элементов как опасность и возможность, возможностью кризис считается из-за возможности трансформации бизнеса, но в обычном практическом понимании это невозможность дальнейшего функционирования предприятия в рамках сложившихся условий.

В самом общем виде экономическое содержание банкротства представляет неспособность субъекта рыночных отношений по определенным причинам погасить свою задолженность, невозможность ее погашения в будущем, а также отсутствие оснований для восстановления платежеспособности должника. В научном плане неспособность оплатить по своим долгам как социально-экономическое содержание неплатежеспособности можно охарактеризовать с помощью системы следующих показателей: неплатежеспособность лица; особое имущественное положение должника; уровень эффективности управления финансовыми ресурсами; степень сбалансированности входящих и исходящих денежных потоков.

В определенных случаях следует разделять понятия «несостоятельность» и «банкротство». Такое разделение, основанное на практической необходимости для лиц, являющихся несостоятельными, и лиц, признанных в установленном законом порядке банкротами. В рыночных условиях большое значение имеют вопросы деловой репутации, поэтому для должника будет очень важно называться именно несостоятельным, а не банкротом. В каких-то случаях должник, находящийся в процессе производства по делу о банкротстве, сможет продолжать свою деятельность. В такой ситуации квалификация положения должника как несостоятельность либо как банкротство будет иметь значение как для самого должника, так для реальных и потенциальных партнеров.

Рискообразующие факторы определяющие в будущем возможные отголоски несостоятельности или банкротство компании приводят к последней стадии – финансовый кризис. Чтобы исключить такой исход компании применяют различные методики анализа и оценки своей финансовой деятельности, в надежде локализации исхода и оздоровительных мероприятий в отношении его.

Рискообразующие факторы должны иметь юридический характер для действия со стороны компаний, в случаи если она не сможет выполнять свои обязательства перед дебиторами и кредиторами, то есть его банкротство или несостоятельность должно быть обосновано для дальнейшей возможности принятия оптимизационных мер.

В нынешней экономике неопределенность представляется господствующим фактором. Анализ и оценка риска занимает важное место в системе анализа организаций, наиболее важным анализ рисков является для инвесторов как правило среди вариантов вложения ресурсов выберут тот который меньше подвержен риску.

Вероятность банкротства – это вероятность наступления кризиса на предприятии в последствии чего предприятие не сможет платить по долговой расписке.

При количественной оценке риска целесообразно определять риск исходя из сочетания величины события и вероятности их наступления. На практике производные расчетные значения используются для получения точечной оценки значений риска. При этом вероятность его появления R используется как мера возможности наступления события, как рациональность выбора.

Количественные методы анализа неопределенностей можно разделить на три подкласса, определяющие подход к пониманию неопределенности как таковой:

- неопределенность, когда составляются расчеты на основе классических распределений вероятностей;
- неопределенность, когда расчеты производятся на основе субъективных вероятностей;
- неопределенность, оцениваемая на основе «лингвистической вероятности».

Последствия нежелательного события можно оценивать по различным конкретным параметрам - от экономических до этических или политических. Все сферы ведения бизнеса

подвержены к риску, никакая организация не застрахована от внешних и внутренних рисков в процессе функционирования.

На данный момент в нашей стране за совершения таких действий как умышленное банкротство и фиктивное банкротство установлено уголовное наказание. Также по мнению некоторых специалистов в сфере права к уголовной ответственности стоит привлекать организации, где банкротство наступило по неосторожности, но в данном случае следует учитывать, что в условиях рынка банкротство является естественным процессом и исходя из этого не рассматривать как уголовно наказуемое действие. Несостоятельность организации затрагивает все лица, которые взаимодействуют с организацией, следовательно.

Показатели системы несостоятельности:

Неплатежеспособность лица – отсутствие капитала для оплаты долга. Факт присутствия неплатежеспособности у компании не ставит крест на компании так как она может быть временной и при наличии денежных средств предприятие может расплатиться и вернуть нормальное состояние.

Особое имущественное состояние должника – состояние, когда обязательства превышают сумму активов. Кредиторы обращают внимание на имущество должника чтобы было возможным за счет имущества удовлетворить требования кредиторов.

Уровень эффективности финансового менеджмента – именно эффективное управление финансами является значимым показателем устойчивости организации, ведь при нерациональном использовании финансовых ресурсов не будет платежеспособности.

Заключение

Исследование о банкротстве и причинах возникновения данного явления на предприятии позволяет сделать несколько важных выводов. Во-первых, финансовая устойчивость предприятия играет решающую роль в его успешном функционировании, и недостаток финансовой устойчивости может привести к кризисным состояниям и, в конечном итоге, к банкротству. Во-вторых, понимание показателей финансового состояния и умение оперативно реагировать на изменения на рынке помогает предотвратить финансовые проблемы и поддержать устойчивое развитие предприятия.

Для практического применения результатов исследования рекомендуется предпринимать меры по повышению финансовой устойчивости предприятия, анализировать риски банкротства и разрабатывать стратегии их уменьшения. Также важно улучшить систему управления финансовыми ресурсами и внедрить меры по оптимизации денежных потоков.

Исследование позволяет лучше понять причины банкротства на предприятии и подготовиться к возможным негативным последствиям. Дальнейшие исследования в этой области могут направиться на изучение конкретных случаев банкротства и разработку индивидуальных стратегий предотвращения финансового кризиса.

Таким образом, понимание причин банкротства и разработка эффективных мер по его предотвращению является важной задачей для любого предприятия, стремящегося к устойчивому развитию и процветанию на рынке.

1. Федеральный закон от 03.06.2009 N 103-ФЗ (ред. от 27.12.2019) «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами» // «Парламентская газета», N 31, 09.06.2009.
2. Аналого-цифровые устройства: учебно-методическое пособие / С.Н. Гончаров [и др.] — Саратов: Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 126 с.
3. Басалова Г.В. Основы криптографии: учебное пособие / Басалова Г.В. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с.
4. Ватолина О.В., Данилов С.А. Криптовалюты как новый вид виртуального платежного средства. «Ученые заметки ТОГУ» 2019, Том 6, No 4, С. 717 – 721.

Закаев Р.М., Шуева А.А., Магомадов Ш.А.
Новейшая или иная концепция понятия «денег» - криптовалюты

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-378

Аннотация

Сегодня, в век цифровой трансформации, когда информационные технологии играют важнейшую роль не только в жизни общества, но и в экономике, в частности, использование цифровых денежных средств приобретает все большую популярность. Так, активно развиваются технологии блокчейн, при помощи которых можно существенно сократить транзакционные издержки в масштабе целого рынка, страны и т. д.

Ключевые слова: информационные технологии, криптовалюта, цифровые денежные средства.

Abstract

Today, in the age of digital transformation, when information technologies play a crucial role not only in the life of society, but also in the economy, in particular, the use of digital money is becoming increasingly popular. Thus, blockchain technologies are actively developing, with the help of which it is possible to significantly reduce transaction costs on the scale of an entire market, country, etc.

Keywords: information technology, cryptocurrency, digital money.

Виртуальные торговые площадки и интернет сообщества разрабатывают свои платежные системы и эмитируют собственные цифровые валюты в связи с возникновением у людей желания получить дополнительное средство получения дохода, и совершения финансовых сделок без участия посторонних лиц. Так появляются новые формы виртуальных денег.

Если рассматривать определение криптовалюты, то она представляет из себя один из видов цифровых денег, функционирование которых базируется на алгоритмах шифрования. Данное понятие происходит от греческого слова «криптос», которое переводится как «тайна». Это обусловлено тем, что данная цифровая валюта обеспечивает анонимность проведения сделок, а также тем, что ее сложно подделать.

Еще в последнем десятилетии прошлого века стали высказываться мысли о создании системы, позволяющей шифровать транзакции, совершаемые с денежными средствами. Только в 2008 году удалось полноценно реализовать данную идею, когда появилась первая децентрализованная платежная система, которая не контролируется государством, криптовалюта, которая носит название Bitcoin, а также система технологии Blockchain.

Blockchain представляет из себя информационную цепь баз данных, позволяющих отразить историю операций с биткоинами и их создание. Сложность в копировании биткоинов и проведении иных мошеннических действий с ними состоит в том, что для признания транзакции действительной, необходимо, чтобы ее подтвердили не менее шести блоков, которые входят в цепочку. Так, за подтверждение блоков, операций, выплачивается определенное вознаграждение, которое носит название «майнинг биткоина».

Криптовалюты генерируются при помощи майнинга, являющегося распределенной системой, которая подтверждает ожидающие транзакции включением их в блокную цепь.

Выпуск виртуальных денег представляет собой сложное явление, так как сеть криптовалют постоянно растет. При создании криптовалют майнеры пользуются сверхпроизводительными персональными компьютерами или мощными серверами.

Ключевым отличием криптовалют от привычных видов электронных денег выступает то, что последние требуют определенного физического участия. Так, для перехода в

электронный вид, денежные средства необходимо внести на счет посредством специализированных терминалов или же банка. Если мы говорим об криптовалютах, то их эмиссия осуществляется в сети Интернет и не предполагает физического внесения денег куда-либо. Также у криптовалют отсутствует непосредственная связь с реальной валютной системой.

Исследования в области электронных денег начались в конце прошлого столетия. Как было сказано ранее, впервые идея создание электронных денег была предложена С. Брэндсем и Д. Чаумом. Позже первые наработки в области реализации работ криптографических систем были осуществлены такой компанией, как «DigiCash».

В настоящее время имеются различные виды криптовалют. Представим наиболее известные и широко использующиеся из них [2]:

1. Bitcoin (BTC) – выступает самой известной криптовалютой. Если говорить о механизме реализации работы Биткоина, то он поддерживается такими лицами, как «майнерами», предоставляющими мощность личных компьютеров для осуществления транзакций. В этом и заключается принцип децентрализации, который позволяет не включать в механизм посредников. Некоторые страны на законодательном уровне регламентировали использование биткоина в качестве легального средства платежа.
2. Ethereum (ETH) – Так, в научных трудах ее называют вторым поколением Биткоина. Так, система Эфириум позволяет не только хранить и пересылать цифровую валюту, но и совершать такие операции, как депонирование, инвестирование, кредитование и прочее. Существующая в Эфириум система смарт-контрактов позволяет сформировать базу для новой экономики, которая не зависит ни от государства, ни от банков.
3. Litecoin (LTC) – была создана в 2011 году. Данная цифровая валюта выступает четвертой по капитализации в мире. Ключевым отличием данной цифровой валюты от Биткоина выступает то, что функционал первой в несколько раз шире, так же как и пропускная способность системы. Также у Лайткоина большее количество монет в обращении, которое составляет 84 млн.

Одной из ключевых причин развития цифровых денег послужило повсеместное использование сети «Интернет», которая является условием использования данного вида денежных средств. Также основой популяризации цифровых денежных средств выступает то, что по данным статистики около 70% населения имеет мобильные телефоны, позволяющие подключиться к интернету. Несмотря на многочисленные преимущества криптовалют, обозначенные ниже, стоит отметить и их недостатки. Ключевым из них выступает то, что данная валюта не подкреплена обязательствами. Ценность криптовалют формируется исходя из желания ее пользователей приобрести ее. Здесь имеет место быть рыночный механизм, выражающийся через закон спроса и предложения. Стоит отметить, что зачастую возникают дисбалансы между двумя этими показателями, что подрывает стабильность функционирования криптовалют. С одной стороны, анонимность проведения платежей выступает преимуществом. Но если рассматривать данный вопрос с другого ракурса, то полная анонимность пользователей системы может использоваться в целях осуществления криминальной деятельности. В силу данного факта, большинство государств до сих пор не признают криптовалюты в качестве легального средства платежа.

Каждый владелец криптовалюты имеет цифровой ключ, которые предоставляет доступ к денежным средствам. Если его потерять, то восстановить доступ к имеющимся сбережениям будет невозможно. Также, если владелец криптовалюты желает совершить транзакцию, то выступает необходимым тщательная проверка данных сделки, так как ее нельзя будет отменить и вернуть деньги. Для того чтобы ускорить и облегчить цифровую трансформацию отечественной экономики, государство решило выработать подходы к определению ключевых понятий, используемых в области цифровых технологий. В число данных понятий входит также определение криптовалют. Это связано с тем, что без соответствующей нормативной базы, определяющей криптовалюту как средство платежа, затруднительно дальнейшее развитие

цифровых технологий в стране. Так, одним из ключевых направлений по улучшению правового регулирования цифровой экономики выступает регулирование государством деятельности, связанной с криптовалютами.

Заключение

Проблема правового регулирования операций с криптовалютами актуальна во всех отраслях экономики развитых стран. Преимущественно данная тенденция наблюдается на товарных рынках через динамику использования на них криптовалют. Так, в некоторых крупнейших интернет-магазинах ЕС такая криптовалюта, как биткоин, используется в качестве легального средства платежа. Например, в Швейцарии студенты могут оплатить свое обучение посредством биткоина.

Несмотря на столь широкую популярность и распространённость криптовалют, в особенности биткоина, нельзя сделать вывод о том, что в скором времени данный вид денежных средств заменит фиатные деньги. Также стоит учесть, что уровень капитализации криптовалют намного ниже, чем у других денежных агрегатов.

Анализируя будущее криптовалют, стоит отметить, что они полностью не заменят остальные виды денежных средств, однако точно будут занимать некоторую нишу в системе денежных средств.

1. Федеральный закон от 03.06.2009 N 103-ФЗ (ред. от 27.12.2019) «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами» // «Парламентская газета», N 31, 09.06.2009.
2. Аналого-цифровые устройства: учебно-методическое пособие / С.Н. Гончаров [и др.] — Саратов: Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 126 с.
3. Басалова Г.В. Основы криптографии: учебное пособие / Басалова Г.В. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с.
4. Ватолина О.В., Данилов С.А. Криптовалюты как новый вид виртуального платежного средства. «Ученые заметки ТОГУ» 2019, Том 6, No 4, С. 717 – 721.

Закаев Р.М., Шуева А.А., Магоматов Ш.А. Современная интерпретация эволюции понятия «денег»

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-379

Аннотация

До появления денег существовало множество их прототипов. Так, изначально люди осуществляли товарный обмен. В качестве средства обмена в разных странах могли использоваться шкуры животных, разнообразные камни, соль и т. д. Однако такой способ был недостаточно удобен. Во-первых, было трудно найти человека, который бы владел необходимым тебе товаром. Во-вторых, было сложно договориться о цене товара, из-за чего возникали разногласия. В результате возникла необходимость в создании денег, которые бы имели определенную стоимость и были удобны в использовании.

Ключевые слова: деньги, платежная система, банк, кредит.

Abstract

Before the advent of money, there were many prototypes of them. So, initially, people carried out commodity exchange. Animal skins, various stones, salt, etc. could be used as a means of exchange in different countries. However, this method was not convenient enough. Firstly, it was difficult to find a person who would own the goods you needed. Secondly, it was difficult to agree on the price of the goods, which caused disagreements. As a result, it became necessary to create money that would have a certain value and be convenient to use.

Keywords: money, payment system, bank, credit.

Цифровые деньги (криптовалюта) – это новейшие денежные средства, которые выражаются и обращаются в электронной форме, которые обеспечивают анонимность лиц, которые производят расчеты. Принцип анонимность реализуется посредством специальных криптографических методов.

Двадцать первый это век информационных технологий, который внес новые понятия, такие как «биткойн», «цифровые деньги», «криптовалюты», «блокчейн». Цифровые деньги появились в 2009 году и с тех пор начали активно развиваться, проникая в нашу жизнь и опосредуя экономические отношения.

Тема исследования является актуальной, поскольку с каждым днем растет число экономических субъектов, связывающих себя с криптовалютой. Интерес к ним постоянно растёт и затрагивает финансовую систему, а также мировую экономику в целом. Количество мировых бирж по торговле криптовалютами уже составляет более пятидесяти, а различных криптовалют насчитывается более полутора тысяч.

Первые бумажные деньги появились в Китае в 910 году. Первоначально банкноты выпускались с целью получения по ним определенного количества металлических денег. Однако вскоре их стали использовать как самостоятельные средства платежа. Несмотря на то, что бумажные деньги появились еще в 10 веке, широкое распространение в мире они получили только в 17–18 веках, когда их начали печатать во многих европейских странах. В России они появились в 1769 году при Екатерине II. Бумажные деньги было легко изготавливать, обмениваться ими и хранить их, но они были подвержены инфляции. Для обеспечения эмиссии бумажных денег и их функционирования в странах начали создавать центральные банки, которые стали контролировать денежный оборот.

С развитием банков и системы безналичного расчета в обороте все большую популярность набирали кредитные деньги, которые ранее могли быть выражены в качестве векселей и чеков. Первая кредитная карта была выпущена в 1950-х годах. Далее их начали выпускать и использовать по всему миру. На данный момент оборот средств, получаемых от использования кредитных карт растет с каждым годом.

Электронные деньги, которые используются в Интернете, появились сравнительно недавно, поэтому механизм их использования и применения только развивается. Особенностью электронных денег является то, что они могут использоваться только в рамках конкретной платежной системы эмитента, что приводит к снижению стоимости транзакций. Рынок электронных денежных средств в России регулируется Центральным банком РФ согласно закону «О национальной платежной системе» от 27 июня 2011 г. С каждым днем появляется все больше новых платежных систем. К одним из самых известных на данный момент относят WebMoney, PayPal, Яндекс. Деньги и другие.

Современные функции денег состоят в движении денежных масс, вызванном оборотом капитала, товаров и кредита. Особенностью современных денег является то, что их функционирование включено в круговорот промышленного капитала. Рабочую силу и средства производства покупают за деньги.

С того момента, как правительство России и других стран, использующих свои (национальные) или мировые валюты, отменили их привязку к золотому стандарту, деньги обрели самостоятельную стоимость и приобрели свойство всеобщей обменеваемости. Они стали определять стоимость конкретного товара или услуги и паритет покупательной способности одной национальной валюты по отношению к остальным валютам. Деньги на предприятии теперь не только мера стоимости, но и денежный капитал. Функция меры стоимости теперь устанавливает баланс между стоимостью товаров, необходимых для производства и стоимостью произведенного в конечном итоге товара. При нарушении стоимостных пропорций происходит сокращение производства конечного товара. Для того, чтобы поддерживать рост производства государство должно использовать рыночные методы, такие как повышение покупательной способности своей валюты.

Как и изложено выше, в ходе развития общества и экономических отношений появлялись различные виды денег. Существует много классификаций видов денег. Разберём одну из них.

Товарные деньги или действительные деньги представляют собой конкретный товар, обладающий внутренней стоимостью и конкретной полезностью. Человек, владевший ими, мог использовать их и как деньги, и напрямую как товар. Сначала это были шкуры животных, соль и т.д. В дальнейшем стали использовать драгоценные металлы из-за того, что они обладали следующими свойствами: делимость (слитки, монеты не теряли свою ценность при разделении), признание во всем мире, отсутствие срока годности и т.д. Товарные деньги используются и в современности, например, в условиях экономического кризиса товары, имеющие длительный срок годности, могут быть использованы как средство накопления. Основным недостатком данного вида денег – их дорого изготавливать.

Для удобства проведения финансовых операций на смену товарным деньгам тогда пришли обеспеченные или репрезентативные. Это деньги, которые можно обменять на определенное количество реального актива (в основном, золота или серебра). Однако, после отмены золотого стандарта, такой вид денег фактически не используется потребителями и производителями.

На смену пришли фиатные или бумажные деньги, стоимость которых не равна их номиналу, они не имеют внутренней реальной стоимости. Существуют следующие формы таких денег: наличные и безналичные. Выпуском фиатных денег занимается уполномоченный орган, например, в России это ЦБ. С печати данного вида денег можно получить следующие виды дохода: сеньораж (разница в цене между стоимостью изготовления и обменной стоимостью) и инфляционный налог (доход от выпуска дополнительных денег).

Например, если центральный банк увеличивает денежную массу, это может привести к падению процентных ставок по кредитам. Это, в свою очередь, может привести к тому, что больше людей и предприятий будут брать займы и тратить деньги, что может стимулировать экономику.

Заключение

Электронные деньги, которые появились относительно недавно, относят к современному виду кредитных денег. Они обычно представлены в виде электронных кошельков. Основой таких денег является депозитное обращение. Главными особенностями всех кредитных денег является то, что они выпускаются согласно фактическим и правильно рассчитанным потребностям оборота, имеют соответствующее обеспечение активами банков, выступающих эмитентами.

Произошедший в 2008 году финансово-экономический кризис привел к основательному ухудшению показателей экономически развитых стран, затем перешедший в глобальную рецессию экономики. Это значительно снизило доверие к ведущим мировым валютам, показав, что имеющаяся валютная система имеет существенные недостатки. В посткризисный период активизировались международные дискуссии по вопросам желательных направлений реформирования мировой валютной системы.

1. Федеральный закон от 10.07.2002 N 86-ФЗ (ред. от 30.12.2021) «О Центральном банке Российской Федерации (Банке России)» (с изм. и доп., вступ. в силу с 22.03.2022) // «Собрание законодательства РФ», 15.07.2002, N 28, ст. 2790.
2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2022) // «Собрание законодательства РФ», 31.07.2006, N 31 (1 ч.), ст. 3448.
3. Федеральный закон от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // «Собрание законодательства РФ», 03.08.2020, N 31 (часть I), ст. 5018.

Захаров А. М., Безнос О.С.

**Современные подходы к защите данных:
как сохранить конфиденциальность в эпоху больших данных**

*Кубанский государственный технологический университет
(Россия, Краснодар)*

doi: 10.18411/trnio-10-2024-380

Аннотация

Статья посвящена современным подходам к защите данных в условиях стремительного роста объемов информации, характерного для эпохи больших данных. Рассматриваются основные вызовы, связанные с конфиденциальностью информации, такие как массовый сбор данных, проблемы их безопасного хранения и сложность контроля над ними. Приводятся современные методы защиты данных, включая шифрование, многофакторную аутентификацию, анонимизацию, технологии блокчейн и искусственный интеллект. Отдельное внимание уделяется правовым аспектам защиты данных и их важности для обеспечения безопасности информации в цифровом мире. Также даны рекомендации для пользователей по защите своих личных данных.

Ключевые слова: большие данные, защита данных, конфиденциальность, шифрование, анонимизация, блокчейн, многофакторная аутентификация, искусственный интеллект, персональные данные, кибербезопасность, GDPR.

Abstract

The article is devoted to modern approaches to data protection in the context of the rapid growth of information volumes characteristic of the era of big data. The main challenges related to information confidentiality are considered, such as mass data collection, problems of their secure storage and the complexity of controlling them. Modern methods of data protection are presented, including encryption, multi-factor authentication, anonymization, blockchain technologies and artificial intelligence. Special attention is paid to the legal aspects of data protection and their importance for ensuring information security in the digital world. There are also recommendations for users to protect their personal data.

Keywords: big data, data protection, privacy, encryption, anonymization, blockchain, multi-factor authentication, artificial intelligence, personal data, cybersecurity, GDPR.

Все больше и больше растет популярность технологий. IT-сфера стала неотъемлемым фактором в нашей жизни. Мы живем в то время, когда любое наше действие так или иначе оставляет за собой след в паутине интернета. При таких условиях, важным фактором будет играть конфиденциальность наших данных. Современные подходы к защите данных развиваются параллельно с новыми угрозами, которые появляются в цифровом пространстве [1, 4].

Небезопасное хранение данных – еще одна серьезная проблема. Массовый сбор данных является одним из ключевых вызовов для конфиденциальности. Компании и правительства все больше и больше интересуются сбором личных данных в сети интернет, в основном их собирают, с целью анализа, как поведения людей в сети, так и для рекламных предложений, но участились случаи, когда данными злоупотребляют и пользуются ими для пагубных целей [1]. Даже мастодонты из разных сфер подвержены к крупным утечкам. Хакеры могут получить доступ к серверам и базам данных, содержащим личную информацию миллионов людей. Большинство компаний халатно относятся к кибербезопасности, что, в свою очередь, плачевно сказывается на дальнейших исходах. Большинство пользователей даже не подозревают, что их может ожидать после того, как ставят галочку напротив договора: «соглашение на обработку персональных данных». А это уже должно вызывать сопутствующие вопросы, а кто ответственен за нашу личную информацию [1, 2]?

В нынешнее время существует несколько способов защиты информации, один из способов – кодирование данных. Кодировка данных подразумевает под собой уникальный ключ-код с зашифрованной информацией, подобрать комбинацию ключа практически невозможно, что дает большую лояльность со стороны пользователей [2]. Различные протоколы шифрования, такие как SSL/TLS для защиты интернет-соединений или шифрование на стороне клиента для защиты файлов, широко используются для повышения безопасности. Второй немаловажный способ сохранения конфиденциальности данных – многофакторная аутентификация (MFA), он требует личного участия пользователя, а именно подтверждение паролем и биометрическими данными, что усложняет получение личной информации посторонним людям [3]. Третий подход – анонимизация данных. Она позволяет использовать данные без идентификации личности пользователя, а это значит, что риск вновь снижается из-за того, что анонимная информация не закреплена за каким-либо пользователем [2, 3]. Блокчейн также набирает популярность как средство защиты данных. Блокчейн обеспечивает прозрачность и неизменяемость информации, что делает подделку данных невозможной [2, 6]. Например, технология может применяться для защиты финансовых транзакций и личной информации [2]. Также важен принцип минимизации данных, который предполагает сбор только той информации, которая действительно необходима. Компании начинают осознавать, что чем меньше данных они собирают, тем меньше они подвергаются рискам утечек [4]. Этот подход поддерживается законодательными актами, такими как GDPR (Общий регламент по защите данных) в Европе [3]. В дополнение к этому, современные системы защиты всё чаще используют искусственный интеллект (ИИ) для выявления аномалий в трафике, обнаружения вторжений и предсказания возможных атак. ИИ способен анализировать большие массивы данных в режиме реального времени, что позволяет быстрее реагировать на киберугрозы [4].

Правовая защита данных приобретает всё большее значение. Законы, такие как GDPR в Европейском союзе и CCPA (Калифорнийский закон о защите конфиденциальности потребителей) в США, вводят строгие требования к компаниям по поводу сбора, хранения и использования данных. Эти законы предоставляют пользователям право на доступ к своим данным, их исправление или удаление [4, 5]. GDPR, например, требует от компаний применять подходы «privacy by design», обеспечивающие конфиденциальность на всех этапах проектирования и реализации информационных систем. Нарушения этих норм могут привести к серьезным штрафам [5].

Наконец, важную роль в защите данных сегодня играет искусственный интеллект, который может автоматически выявлять подозрительные активности в сети и предупреждать о возможных кибератаках. Это особенно полезно в больших системах, где человек не всегда может быстро реагировать на угрозы. В будущем, навыки работы с ИИ и кибербезопасностью станут ключевыми для специалистов всех направлений.

Пользователи также могут принимать активные меры для защиты своих данных [6]. Рекомендуется использовать сложные пароли и менять их регулярно, включать многофакторную аутентификацию, быть осторожными при предоставлении личной информации в интернете, использовать VPN для защиты интернет-соединения и ограничивать ненужные разрешения для приложений [5].

В эпоху больших данных возникают не только новые возможности, но и новые угрозы для конфиденциальности [6]. Защита личных данных становится одной из важнейших задач как для компаний и правительств, так и для обычных пользователей. Современные технологии, такие как шифрование, анонимизация и блокчейн, в сочетании с эффективными правовыми нормами и активным участием пользователей, могут обеспечить надежную защиту информации в цифровом мире [5, 6].

1. Лысак, С. В. Защита информации в цифровом обществе. Москва: Издательство "Инфра-М", 2020.
2. Иванов, А. Н. Основы кибербезопасности и защиты информации. Санкт-Петербург: Питер, 2019.
3. Малышев, Д. В. Шифрование и защита данных: теория и практика. Москва: Наука и технологии, 2021.

4. Петров, К. И. Технологии блокчейна и их применение в защите данных. Казань: Казанский государственный университет, 2022.
5. Смирнова, О. В., Федоров, Н. П. Законодательные аспекты защиты данных в эпоху больших данных. Вестник права и информационных технологий, 2023, № 4, с. 22-30.
6. СИСТЕМНЫЙ АНАЛИЗ И СИНТЕЗ ИНФОРМАЦИОННОЙ МОДЕЛИ ОРГАНИЗАЦИИ Безнос О.С. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2007. № 3 (51). С. 140-144.

Илюхина С.В., Недорезов К.А.

**Панорама степени внедрения искусственного интеллекта
и информационных технологий в России и за рубежом**

*Уральский государственный экономический университет
(Россия, Екатеринбург)*

doi: 10.18411/trnio-10-2024-381

Аннотация

Развитие продуктивно-ориентированного производства, увеличение показателей эффективности, базирующихся на инновационных достижениях современных высокотехнологичных сфер экономики, способствует не только непосредственному увеличению прибыльности, но и содействует комплексному решению проблем территориально – пространственного в области инноваций на государственном уровне, в том числе и с применением искусственного интеллекта.

Ключевые слова: искусственный интеллект, инновационное развитие, увеличение эффективности.

Abstract

The development of productively oriented production, an increase in efficiency indicators based on innovative achievements of modern high-tech sectors of the economy, contributes not only to a direct increase in profitability, but also contributes to a comprehensive solution of problems of spatial innovation at the state level, including with the use of artificial intelligence.

Keywords: artificial intelligence, innovative development, increased efficiency.

Объем мирового рынка систем и технологий ИИ по данным Statista и Tractica вырос к 2021г. по сравнению с 2018г. на 267% или 25,36 млрд. долл. США. К 2025г., по прогнозам специалистов, объем мирового рынка искусственного интеллекта, по сравнению с 2016г. вырастет на 58,3 млрд. долл., будет создано 2,3 млн. рабочих мест, на 85% контактной работы с клиентами будет выполнять ИИ, благодаря которому мировой ВВП увеличится на 15,7 трлн. долл. в 2030г.[1] В таб. 1 приведен анализ численности компаний и стартапов в сфере ИИ за 2017г.

Таблица 1

Количество компаний, функционирующих в области ИИ.

	<i>Компании в области ИИ</i>	<i>Стартапы в области ИИ</i>
<i>США</i>	<i>2 905</i>	<i>1393</i>
<i>Китай</i>	<i>709</i>	<i>383</i>
<i>ЕС в т. ч.:</i>	<i>400</i>	<i>524</i>
<i>Франция</i>	<i>136</i>	<i>109</i>
<i>Германия</i>	<i>160</i>	<i>106</i>
<i>Великобритания</i>	<i>366</i>	<i>245</i>
<i>Израиль</i>	<i>173</i>	<i>362</i>
<i>Россия</i>	<i>13</i>	<i>19</i>

Расширяются показатели автоматизации и цифровизации труда, многие бизнес-процессы оптимизируются, повышается объективность и рационализация принимаемых решений, происходит реструктуризация мирового рынка труда (рис.1):

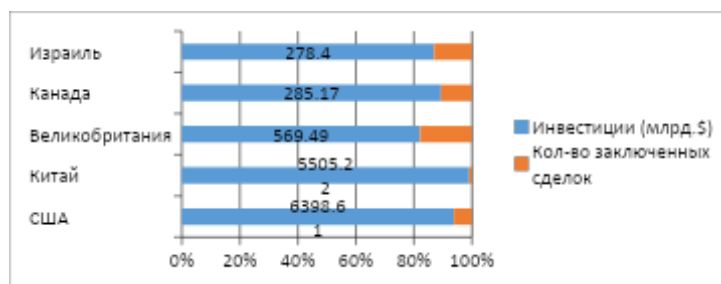


Рисунок 1. Инвестиции в технологии ИИ ведущими странами мира(2019г.).

В Европе проходит большое количество исследований, касающихся так или иначе искусственного интеллекта (ИИ), но при этом на практике, большинство предприятий данными технологиями не пользуются (таб.2):

Таблица 2

Структура данных об использовании предприятиями европейских стран систем искусственного интеллекта (ИИ) на 2020 г., в % к итогу по регионам.

	Восточная Европа	Северная Европа	Западная Европа	Южная Европа	Европа, в целом
Не используют ИИ	95	92	92	92	93
Используют 1 систему ИИ	5	6	7	6	6
Используют 2 системы ИИ	0 (незначительно)	1	1	1	1
Используют 3-4 системы ИИ	0 (незначительно)	1	0 (незначительно)	1	0 (незначительно)

Соответственно, у данного региона большой потенциал в использовании данных технологий, развитии, масштабировании уже установленных на производствах. Сравнивая север, восток, юг и запад Европы, можно сказать о том, что наиболее отсталой в использовании ИИ на предприятиях является Восточная Европа, т.е. стоит сделать акцент на развитии производства с использованием ИИ в данном направлении.

По мнению авторов статьи, бизнес цифровизация в России высокая, что подтверждают накопленные данные по затратам на развитие информационных технологий за 2021 г. российскими компаниями в 3,7 трлн. руб. [2]. Доля новых для мирового рынка инновационных товаров (работ, услуг), в общем объеме отгруженных товаров, выполненных работ, услуг организаций промышленного производства за 8 лет - 0,18% (рис.2):

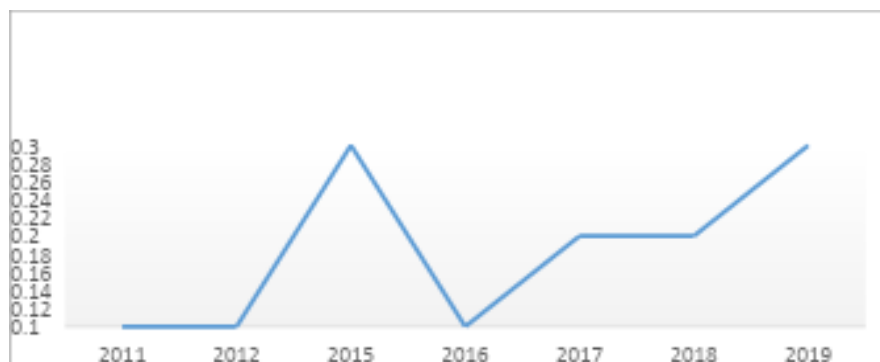


Рисунок 2. Динамика инновационных товаров в России за 2011-2020гг. [5].

В России сферы применения искусственного интеллекта на данный момент времени постоянно растут, это: сельское хозяйство, медицина, промышленность, транспорт, финансы, образование, организация быта, торговля, безопасность.

Использование ИИ в военной сфере: ВВС - второй пилот самолёта, ударно-разведывательные беспилотники, ВС - робот-сапёр, вездеход, наземный робототехнический комплекс, портативный робот-разведчик, ИИ танка РФ Т-14 «Армата». ВМФ – корабельные ракеты с системой наведения «Калибр» и «Яхонт» и др.

ИИ в образовании обеспечивает персонифицированное обучение и проверку заданий в режиме реального времени.

ИИ в торговле: оптовая торговля, розничная торговля, онлайн-торговля, встречная (countertrade) торговля, из дома в дом (house-to-house), консигнационная (consignment trade) со складов за границей. Обороты онлайн-торговли вырастут с 1,5 трлн. до 5 трлн. руб., что составит 10% от общего объема розницы [5].

Искусственный интеллект в аграрном секторе помогает мониторить все процессы, применять беспилотники для сбора и анализа спектральных данных, автоматизация всех процессов при выявлении взаимосвязей при анализе больших данных (машинное обучение, приложения). Что поможет не только непосредственно наблюдать и планировать, но и снизить затраты на ведение агробизнеса, повысить его конкурентоспособность и продовольственную безопасность страны. На рынке сельскохозяйственной робототехники на 55% оснащены молочные фермы, 45% - растениеводство. Наиболее вероятные области применения ИИ в АПК Свердловской области это животноводство -26%, прогноз погоды – 13%, выявление болезней растений и прогноз урожайности – 28% для повышения эффективности ведения хозяйственной деятельности, оптимизации расходов и снижения рисков. У 60% организаций нет возможности для применения ИИ, только у 10% он применяется.

Медицина и здоровье. Размер мирового рынка ИИ в сфере медицины достигнет порядка 30000 млн. долл. США, на данный момент рынок медицинских приложений составляет порядка 7000 млн. долл. США. Выбор методов лечения и постановка диагноза при наличии больших данных из имеющейся медицинской информации о конкретном заболевании при доказанной эффективности врачебной практики. Также в настоящий момент, в том числе из-за пандемии Ковид-19, развивается направление телеметрическая медицина. Это не только помощь высококвалифицированных медиков для жителей отдаленных районов, но и экономия затрат пациентов.

Транспорт: управление информационной системой, мониторинг водителей, облачные сервисы на базе ИИ, профилактическое обслуживание, самоуправляемый транспорт. Объем рынка технологий автономного вождения через 20 лет составит \$560млрд, в 2021г. в мире уже 200 тыс. ед. самоуправляемых машин. В автомобилестроении объем ИИ в 2024г. превысит \$10,73млрд. Многие специалисты склоняются ко мнению, что информационные технологии позволяют по-новому выстраивать исследовательскую деятельность, в том числе и сугубо практической направленности [3]. Активность организаций промышленной направленности в РФ представлена на рис.3:

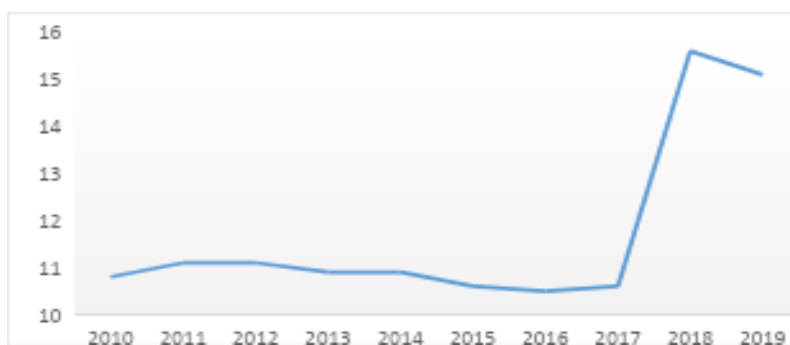


Рисунок 3. Средний совокупный уровень инновационной активности организаций промышленного производства за 10 лет в РФ.

В то же время, инновационное развитие затруднено в силу ряда объективно - субъективных причин: недостаточным финансированием, отсутствием базы и кадров соответствующей квалификации, высокой волатильностью инвестиций в отрасль. Анализ и прогноз отрасли также должен базироваться на актуальных статистических данных не только российской, но и международной статистики [4]. Развитие инноватики должно сопровождаться не только за счет вертикальных связей, но и горизонтальных – сотрудничества организаций между собой.

1. «Методическое пособие по сбору и интерпретации информации об инновациях на основе Oslo Manual. Guidelines for Collecting and Interpreting Innovation Data. 3rd edition. A Joint Publication of OECD and Eurostat. OECD/EC, 2005 (Руководство Осло. Рекомендации по сбору и анализу данных по инновациям. 3-е изд., совместная публикация ОЭСР и Евростата) - <https://ec.europa.eu/eurostat/>
2. Бутко Г.П., Меньшикова М.А., Панов М.А. Пути совершенствования цифровых инструментов в деятельности предприятий // Цифровые модели и решения. 2024. Т. 3, № 1. С. 39–48. DOI: 10.29141/2949-477X-2024-3-1-EDN:PWUVVD.
3. Гавриленко Т.Ю., Проворова И.П. Сетевая экономика как феномен информационного общества. Russian Technological Journal. 2016;4(1):53-61. <https://doi.org/10.32362/2500-316X-2016-4-1-53-61>
4. Илюхин А.А., Илюхина С.В. Управление рисками в организации и информационные технологии. В сборнике: УПРАВЛЕНИЕ ПРОЕКТАМИ: КАРЬЕРА И БИЗНЕС. Материалы III Всероссийской научно-практической конференции. Москва, 2022. С. 76-81. Издательство: Государственный университет управления (Москва).
5. Сайт Министерства экономического развития РФ <https://economy.gov.ru/>

Казакова А.В.

Классификация DDoS-атак

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-382

Аннотация

В статье представлена классификация DDoS-атак, включая их разделение по механизму действия, уровням модели OSI и типам сетевых протоколов. Рассматриваются ключевые методы проведения атак, такие как атаки с использованием флуда, эксплуатация уязвимостей протоколов и атаки на уровне приложений. Описываются примеры различных типов атак, их влияние на сетевую инфраструктуру и методы защиты от них.

Ключевые слова: DDoS-атаки, сетевая безопасность, флуд-атаки, протокольные атаки, атаки на уровне приложений, OSI-модель.

Abstract

The article presents a classification of DDoS attacks, including their separation by mechanism of action, levels of the OSI model and types of network protocols. The key methods of conducting attacks, such as flood attacks, exploiting protocol vulnerabilities and application-level attacks, are considered. Examples of various types of attacks, their impact on the network infrastructure and methods of protection against them are described.

Keywords: DDoS attacks, network security, flood attacks, protocol attacks, application-level attacks, OSI model.

Классификация DDoS-атак (распределённых атак типа "отказ в обслуживании") имеет решающее значение для разработки эффективных стратегий защиты сетей. DDoS-атаки представляют собой угрозы, при которых злоумышленники стремятся нарушить доступность веб-ресурсов, серверов или инфраструктур, насыщая их избыточным трафиком из множества источников. Эти атаки могут быть классифицированы по различным критериям в зависимости

от их механизмов, целей и поведения [1]. Понимание этих классификаций помогает в разработке более целенаправленных и эффективных мер защиты. Рассмотрим ключевые методы классификации DDoS-атак:

1. Протокольные DDoS-атаки. Такие атаки в основном нацелены на следующие большие группы сетевых протоколов: UDP, TCP, другие (ICMP, GRE, IP, ESP, AH, SCTP, OSPF, SWIPE, TLS, Compaq_PEE). Злоумышленники могут потреблять сетевые ресурсы или серверные ресурсы, отправляя запросы, которые требуют значительного времени сервером. Вот несколько примеров наиболее распространенных протокольных DDoS-атак:

Атака IP Null - Согласно техническим стандартам глобальных сетей, заголовок IP-пакета должен содержать информацию об используемом протоколе транспортного уровня в специальном поле – Протокол. Хакеры установили значение этого поля равным нулю. Этот метод позволяет отправлять большое количество пакетов, и никакие брандмауэры или маршрутизаторы не могут этому помешать. Системные ресурсы жертвы начинают постоянно анализировать входящий трафик, и в конечном итоге сервер выходит из строя.

SYN-флуд - Этот тип атаки основан на алгоритме трехэтапного установления связи TCP. Хакер быстро отправляет запросы на подключение к серверу, содержащие поддельный IP-адрес источника. SYN-флуд постепенно занимает всю память таблицы соединений.

UDP-флуд - Во время этой атаки сервер-жертва получает множество UDP-пакетов с разных IP-адресов. Поддельные пакеты UDP перегружают сетевой интерфейс, занимая всю полосу пропускания. Флуд — это огромное количество искаженных сообщений, используемых для создания мощного потока запросов, который перегружает всю выделенную полосу пропускания атакуемого ресурса.

Ping of Death - Эта атака дестабилизирует или приводит к сбою целевого компьютера. Хакер постоянно генерирует пакеты неправильного формата или слишком большого размера, используя простую команду ping. Если атакуемая система основана на стандартном протоколе IPv4, общий размер пакета не может превышать 65 535 байт, иначе система выйдет из строя [2]. В настоящее время некоторые системы работают на обновленной версии протокола IPv6, и хакеры также нашли способы саботировать его. Они отправляют фрагменты искаженных пакетов. Система-жертва пытается их собрать заново, но в результате получается слишком большой размер пакета, что приводит к перегрузке памяти и сбоям в работе.

Сеансовая атака (SlowLoris) - Хакер устанавливает TCP-сеанс между сервером-жертвой и ботом. Когда сеанс успешно установлен, бот злоумышленника не отвечает пакетом ACK, чтобы поддерживать сеанс открытым до тех пор, пока не произойдет тайм-аут сеанса. Пустые сессии потребляют системные ресурсы, в результате чего сервер-жертва выделяет доступные ресурсы для поддержания открытых TCP-сессий с ботами, а затем становится недоступным.

2. Классификация DDoS-атак, основанных на OSI. Данные атаки могут быть направлены на разные уровни, от физического до прикладного, каждый из которых предполагает свои уникальные методы защиты.

Физический уровень: Канал передает необработанные двоичные данные между машинами. Он использует Bluetooth, USB, IrDA, а также концентраторы, розетки и патч-панели.

Пример атаки: Данный уровень может пострадать в результате физического разрушения или любого другого нарушения работы сети. Техногенные сбои приводят к полной непригодности оборудования. На этом уровне невозможны DoS- или DDoS-атаки.

Уровень канала передачи данных: Канальный уровень отвечает за обмен данными между узлами локальной сети. Данные группируются в кадры и передаются на физический уровень. Еще одна функция этого канального уровня — установка сетевым адаптерам уникальных идентификаторов — MAC-адресов.

Пример атаки: наиболее распространенной является лавинная рассылка MAC-адресов. Сетевые коммутаторы перегружены пакетами данных, что приводит к отключению всех портов подключения.

Сетевой уровень: на этом уровне начинают взаимодействовать маршрутизаторы и коммутаторы разных сетей. Маршрутизация основана на преобразовании MAC-адресов в сетевые адреса. Основная цель этого уровня — создать лучший способ передачи данных между устройствами.

Пример атаки: ICMP-флуд, который перегружает целевую сеть сообщениями ICMP. Он направлен на уменьшение пропускной способности и ограничение количества запросов, которые могут быть обработаны по протоколу ICMP.

Транспортный уровень: Он использует протоколы UDP и TCP, а также обрабатывает и транспортирует пакеты данных между узлами связи. Данный уровень контролирует поток информации и обнаруживает ошибки. Если они обнаружены, он повторно отправляет данные [3].

Пример атаки: превышение пороговых значений ширины канала и количества доступных соединений. Наиболее распространенными типами DDoS-атак являются Smurf и SYN-флуд.

Сеансовый уровень: Данный уровень отвечает за взаимодействие между приложениями, а также за установление и завершение соединений и синхронизацию задач ОС.

Пример атаки: злоумышленник использует уязвимости программного обеспечения через Telnet, в результате чего администратор теряет доступ к серверу.

Уровень представления: Уровень кодирует и декодирует данные и адаптирует их для людей или машин понятным образом. Сюда входят видео, аудио, изображения и текстовые данные. Между уровнями 6 и 7 существует протокол SSL. Он обеспечивает клиенту безопасное соединение с сервером и взаимную аутентификацию.

Пример атаки: мусорный флуд SSL. Хакеры генерируют неправильные SSL-запросы для атаки на сервер жертвы. Это замедляет работу ресурсов, поскольку проверка зашифрованных пакетов SSL занимает много времени.

Прикладной уровень: Прикладной уровень полностью работает для пользователя и представляет ему данные в понятном виде.

3. Классификация DDoS-атак по механизму действия. В данной классификации можно выделить 3 группы DDoS-атак с разными механизмами действия: использующие механизм флуда, эксплуатация уязвимости в стеке сетевых протоколов, атаки на уровне приложения. В таблице 1 представлены данные группы и их описание.

Таблица 1

Классификация DDoS-атак по механизму действия, разделённая на три основные группы.

<i>Группа</i>	<i>Тип атаки</i>	<i>Описание</i>
<i>Атаки, использующие механизм флуда</i>	<i>Атака с усилением DNS</i>	<i>Запросы к общедоступному DNS-серверу с последующей переадресацией ответов на сервер-жертву, перегружая его длинными ответами.</i>
<i>Атаки, использующие механизм флуда</i>	<i>DNS-флуд</i>	<i>Массовые DNS-запросы на сервер, вызывая перегрузку ответами на легитимные и поддельные запросы.</i>
<i>Атаки, использующие механизм флуда</i>	<i>Фрагментированный UDP-флуд</i>	<i>Использование больших фрагментированных пакетов для заполнения полосы пропускания, требуя от сервера ресурсы на восстановление данных.</i>
<i>Атаки, использующие механизм флуда</i>	<i>Ping-флуд</i>	<i>Использование ICMP эхо-запросов для вызова сбоя сервера.</i>
<i>Эксплуатация уязвимости протоколов</i>	<i>TOS-флуд</i>	<i>Использование полей TOS и ECN в IP-пакетах для создания иллюзии перегруженности сети и ограничения пропускной способности.</i>
<i>Эксплуатация уязвимости</i>	<i>RST и FIN-флуд</i>	<i>Поддельные пакеты RST или FIN</i>

<i>протоколов</i>		<i>вызывают сбои, так как сервер не может идентифицировать их как легитимные.</i>
<i>Атаки на уровне приложения</i>	<i>DoS-атака на приложение</i>	<i>Использование уязвимостей веб-сайта или приложения, например, через SQL-инъекции, для вызова сбоев.</i>
<i>Атаки на уровне приложения</i>	<i>Фрагментированная HTTP-флуд</i>	<i>Медленная отправка фрагментированных HTTP-пакетов, что позволяет обходить механизмы безопасности.</i>

Классификация DDoS-атак по механизму действия обеспечивает глубокое понимание тактик, используемых злоумышленниками, что критически важно для разработки эффективных стратегий защиты. Включает атаки, нацеленные на сетевые службы, такие как DNS и NTP, которые используют усиление для умножения трафика [4]. Атаки также могут эксплуатировать уязвимости в сетевых протоколах или приложениях, вызывая исчерпание ресурсов и отказ в обслуживании. Каждый тип атаки требует специфического подхода к митигации и защите, что делает анализ механизмов атаки ключевым элементом в сетевой безопасности.

1. DDoS-guard: Классификация DDoS: полное руководство по типам атак [Электронный ресурс]. URL: <https://ddos-guard.net/ru/blog/classification-of-ddos-attacks>. (дата обращения: 10.09.2024.)
2. Цветков А. Ю., Рузманов Е. Ю. Рассмотрение методов тестирования на проникновение для анализа защищенности компании //ББК 3 П27. – 2021. – С. 57.
3. Лаврова Д. С. и др. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика //Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 3. – С. 70-77..
4. HackTheBox. What is network traffic analysis. (2024 blue teamer guide) [Электронный ресурс]. URL: <https://www.hackthebox.com/blog/network-traffic-analysis>. (дата обращения: 11.06.2024.)

Казакова А.В.

Обзор и сравнение алгоритмов глубокого обучения

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-383

Аннотация

В статье проводится обзор и сравнение различных алгоритмов глубокого обучения, используемых в современных задачах анализа данных. Рассматриваются ключевые принципы работы алгоритмов, их преимущества и ограничения при решении сложных задач. Особое внимание уделяется эффективности и точности этих методов при работе с большими объемами данных, а также их адаптивности к разным типам задач.

Ключевые слова: глубокое обучение, алгоритмы, нейронные сети, анализ данных, CNN, машинное обучение.

Abstract

The article provides an overview and comparison of various deep learning algorithms used in modern data analysis tasks. The key principles of algorithms, their advantages and limitations in solving complex problems are considered. Special attention is paid to the effectiveness and accuracy of these methods when working with large amounts of data, as well as their adaptability to different types of tasks.

Keywords: deep learning, algorithms, neural networks, data analysis, CNN, machine learning.

Алгоритмы глубокого обучения играют ключевую роль в современной обработке данных, обеспечивая возможность распознавать сложные шаблоны и делать предсказания на основе больших объемов данных. Рассматриваемые методы включают сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN), в том числе LSTM, каждый из которых имеет свои уникальные преимущества и ограничения в различных сценариях анализа трафика.

Сверточные нейронные сети (CNN) представляют собой особый тип нейронных сетей, которые специализируются на обработке данных в виде сетки. Примерами этого типа данных являются временные ряды и изображения, которые можно рассматривать как одномерную и двумерную сетку пикселей соответственно [1]. Сверточные сети широко использовались в различных реальных задачах, таких как обработка естественного языка (NLP), компьютерное зрение, распознавание речи и т. д. Термин «сверточный» в сверточных нейронных сетях поддерживает идею о том, что CNN используют математическую операцию, называемую сверткой. В своей наиболее распространенной форме оператор свертки представляет собой особый тип линейной операции, которая выполняет интеграл произведения двух функций/сигналов. Другими словами, CNN — это нейронные сети, которые используют операторы свертки вместо общего умножения матриц хотя бы на одном из своих сетевых уровней. CNN применяют три ключевых принципа, которые можно применять для повышения производительности системы машинного обучения за счет сокращения пространства параметров модели: совместное использование параметров или весов, разреженное взаимодействие и эквивариантные представления.

Большая размерность — очевидный недостаток архитектуры нейронных сетей, особенно когда входные данные слишком велики и сложны, например, изображения. Для решения этой проблемы в качестве альтернативы полной связности в архитектуре нейронных сетей был введен оператор свертки (или уровень свертки). Графическое описание глубокой архитектуры CNN представлено на рисунке 1. CNN принимает многоканальные изображения (например, автомобилей и кораблей) в качестве входных данных для целей обучения. CNN использует преимущества нескольких слоев свертки с нелинейными функциями активации для облегчения сложности входных данных (т. е. изображений) и получения выходных данных, т. е. вероятности принадлежности каждого изображения к классу (или категории). В CNN каждая входная зона подключена к выходному нейрону, то есть локальной связности. Каждый уровень использует различные фильтры для распознавания абстрактных понятий, например границ транспортного средства [2]. CNN может изучать функции более высокого уровня, такие как различные детали автомобиля, на более глубоких уровнях. Фильтры в CNN заранее не определены; вместо этого он автоматически изучает значение каждого фильтра на этапе обучения. Более того, CNN использует уровень объединения как метод понижающей выборки. На выходном слое применяется классификатор для использования функций высокого уровня для задачи классификации.

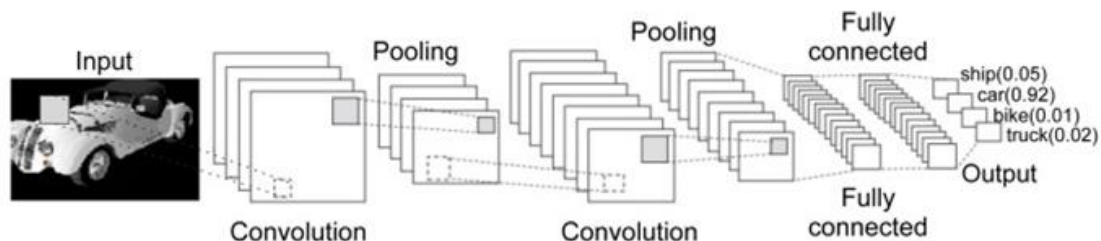


Рисунок 1. Архитектура сверточных нейронных сетей CNN.

Рекуррентные нейронные сети (RNN) представляют собой категорию искусственных нейронных сетей, подходящих для анализа последовательных данных. В отличие от CNN, которые предназначены для работы с данными топологии в виде сетки, например изображениями, RNN представляют собой нейронные сети, которые имеют специализированные характеристики для работы с последовательностью значений x_1, x_2, \dots, x_t . Кроме того, большинство RNN способны обрабатывать последовательности переменной

длины. Главная идея, лежащая в основе рекуррентных сетей и некоторых других методов машинного обучения и статистики, заключается в совместном использовании параметров на разных уровнях модели, чтобы расширить использование модели для экземпляров данных разных форм. Задача совместного использования параметров особенно важна, когда конкретный элемент данных может появляться в нескольких позициях в последовательности. Этот метод оптимизации обычно приводит к значительной экономии памяти в моделях машинного обучения. Также возможно использовать RNN для двумерных пространственных данных, таких как изображения. Ключевое преимущество использования рекуррентных сетей по сравнению с обычными нейронными сетями заключается в том, что RNN может обрабатывать последовательность данных, так что каждый образец можно считать зависимым от предыдущих. Как уже упоминалось, RNN специализируются на моделировании последовательностей, в которых между выборками последовательностей существует сильная последовательная корреляция. На каждом временном шаге RNN использует данные входные данные и информацию, связанную с тем, что уже наблюдалось (т. е. состояние), для генерации выходных данных. Стоит обратить внимание, что эта информация передается посредством рекуррентных соединений между устройствами, как показано на рисунке 2.

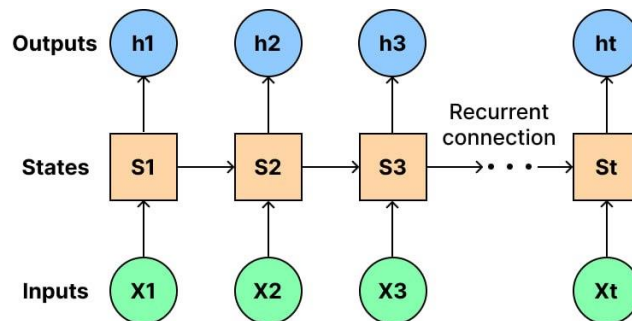


Рисунок 2. Архитектура рекуррентных нейронных сетей.

Предположим, у нас есть последовательность входных элементов

$$x = (x_1, x_2, \dots, x_t).$$

В этом случае RNN выполняет следующие вычисления:

$$S_t = \sigma_s(W_x X_t + W_s S_{t-1} + b_s), h_t = \sigma_h(W_h S_t + b_h).$$

Где S_t — это состояние RNN на временном шаге t и он действует как блок памяти для RNN.

Чтобы вычислить значение S_t , функция входного значения в момент времени $t(x_t)$ и предыдущее состояние RNN, т.е. s_{t-1} было рассчитано. Более того, W_x и W_h веса, которые необходимо изучить в ходе тренировочного процесса, и b_s и b_h являются предубеждениями. В RNN алгоритм обратного распространения ошибки во времени (BPTT) используется для обновления весов или обучения сети.

RNN может использовать самоциклы для хранения градиента недавних входных событий в течение длительного времени. Это основная идея модели долговременной кратковременной памяти (LSTM). Эта функция потенциально важна для широкого спектра приложений, таких как распознавание речи, распознавание рукописного текста, машинный перевод, генерация рукописного ввода, создание титров к изображениям и синтаксический анализ [3]. LSTM был введен для решения двух серьезных проблем, а именно исчезновения градиента и увеличения градиента в первых методах [4]. Более конкретно, при использовании традиционных методов обучения на основе градиента, таких как BPTT и рекуррентное обучение в реальном времени (RTRL), сигналы ошибок могут уменьшаться или увеличиваться при обратном распространении по модели. Сеть LSTM предлагается для решения проблем обратного потока сигналов ошибок путем внедрения идеи использования набора вентиляей. Графическая иллюстрация структуры LSTM представлена на рисунке 3.

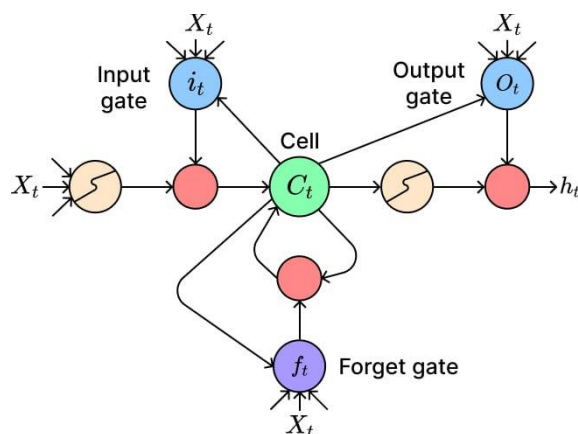


Рисунок 3. Внутренняя структура LSTM.

В этой структуре «Forget gate» решают, какую информацию из состояния ячейки забудут, поскольку они нерепрезентативны. Действительно, forget gate принимают это решение через сигмовидный слой. Forget gate выполняют операцию, отраженную в следующей формуле:

$$F_t = \sigma(W_{xf}X_t + W_{hf}H_{t-1} + W_{cf} \odot C_{t-1} + b_f)$$

В этом выражении \odot - операция Адамара или поэлементное произведение, C_t представляет выходные данные состояния ячейки, H_t обозначает скрытые состояния. Forget gate смягчают исчезновение градиента и увеличение градиента и значительно повышают производительность LSTM, чем RNN.

Другая важная функция LSTM — решить, какую новую информацию следует хранить в состоянии ячейки. С этой целью forget gate i_t решает, какая информация будет обновлена, что отображено в формулах ниже, и эта информация обеспечит обновление старого состояния ячейки (т.е. C_{t-1}).

$$i_t = \sigma(W_{xi}X_t + W_{hi}H_{t-1} + W_{ci} \odot C_{t-1} + b_f)$$

$$i_t = \sigma(W_{xi}X_t + W_{hi}H_{t-1} + W_{ci} \odot C_{t-1} + b_f)$$

$$C_t = F_t \odot C_{t-1} + i_t + \tanh \odot (W_{xc}X_t + W_{hc}H_{t-1} + b_c)$$

И последний шаг LSTM — решить, что должно выводиться на основе состояния ячейки. Это можно сделать с помощью output gate (т.е. o_t), что отражает формула 5, который решает, какая информация о состоянии ячейки пойдет на вывод. Состояние ячейки также проходит через \tanh в формуле 6, а затем умножается на output gate.

$$o_t = \sigma(W_{xo}X_t + W_{ho}H_{t-1} + W_{co} \odot C_t + b_o)$$

$$H_t = o_t \odot \tanh(C_t)$$

Таким образом, были рассмотрены алгоритмы глубокого обучения, такие как сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN) и LSTM. Стоит отметить, что каждый из этих алгоритмов имеет свои особенности, преимущества и недостатки, которые детально отображены в таблице 1.

Таблица 1

Сравнение алгоритмов глубокого обучения.

Алгоритм	Особенности	Плюсы	Минусы
CNN	Эффективны в обработке данных с явной пространственной структурой, таких как изображения.	Высокая точность в распознавании паттернов в данных.	Не оптимальны для анализа временных последовательностей из-за фиксированной структуры входных данных.
RNN	Подходят для работы с последовательностями	Могут обрабатывать данные переменной длины	Страдают от проблемы исчезающего градиента,

	<i>данных благодаря способности передавать скрытое состояние от шага к шагу.</i>	<i>и улавливать временные зависимости.</i>	<i>что затрудняет обучение на длинных последовательностях.</i>
<i>LSTM</i>	<i>Расширение RNN, предназначенное для решения проблемы исчезающего градиента с помощью специальных структурных блоков памяти.</i>	<i>Эффективны в сохранении информации на длительные временные интервалы и в обучении на длинных данных.</i>	<i>Более высокие вычислительные и памятные затраты по сравнению с традиционными RNN.</i>

Данная таблица позволяет оценить, какой алгоритм лучше подходит для конкретных задач в зависимости от характеристик анализируемых данных и требований к задаче анализа сетевого трафика.

1. Катасонов А.И., Кузин Д.И. Исследование разновидностей нейронных сетей и их возможностей для обеспечения безопасности инфокоммуникационных систем//Актуальные проблемы инфотелекоммуникаций в науке и образовании. - Санкт-Петербург, 2024. С. 404-409.
2. Кушнир Д. В., Платонова Т. А., Программирование квантового компьютера и его эмуляция в обеспечении информационной безопасности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 754-758.
3. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.
4. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 193-197.

Карклис А.Д., Дроздова А.А.

**Перспективы развития портала «Наш город»
с учетом применения методов интеллектуального анализа текстов**

*Национальный исследовательский ядерный университет «МИФИ»
(Россия, Москва)*

doi: 10.18411/trnio-10-2024-384

Аннотация

Портал «Наш город» – продукт, разработанный в Москве и направленный на улучшение качества жизни горожан посредством их активного участия в жизни города. На текущий момент портал функционирует 13 лет, но, несмотря на постоянное развитие, он все еще ограничен в наборе тематик, по которым можно оставить обращение.

В статье дана оценка соответствия принципа работы портала «Наш город» требованиям федерального законодательства, а также показана возможность его развития, в том числе расширения перечня тематик, с помощью применения методов интеллектуального анализа текстов.

Ключевые слова: портал «Наш город», работа с обращениями граждан, интеллектуальный анализ текстов, масштабирование сервисов.

Abstract

The «Our City» portal is a product developed in Moscow and aimed at improving the quality of citizens' life through their active participation in the life of the city. Currently, the portal has been operating for 13 years, but despite constant development, it is still limited in the range of topics on which a request can be left.

The article assesses the compliance of operating principles of the «Our City» portal with the requirements of federal legislation, and it also shows the possibility of developing the portal, including expanding the range of topics, using text mining methods.

Keywords: «Our City» portal, working with citizens' requests, text mining, scaling services.

Неотъемлемой частью работы любого органа власти Российской Федерации является взаимодействие с гражданами, которое в современных реалиях обладает тенденцией к переводу в электронный вид.

Отправной точкой в вопросе внедрения электронного формата обращений граждан является издание Федеральных законов от 02 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – 59-ФЗ) [1] и от 27 июля 2010 года № 227-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об организации предоставления государственных и муниципальных услуг» (далее – 227-ФЗ) [2].

Именно в 59-ФЗ на основании 227-ФЗ впервые в определении понятия «обращение гражданина» зафиксирована возможность направления предложения, заявления или жалобы как в письменном или устном, так и в электронном формате, а также в укрупненном виде прописан порядок взаимодействия государственных органов и органов местного самоуправления в электронном виде. Соответственно, с 2010 года обращение в электронной форме приравнивается к письменному обращению.

При этом, регионы вправе уточнять федеральное законодательство на своем уровне. Так, например, на текущий момент Правительство Москвы осуществляет работу с обращениями граждан в соответствии с Регламентом Правительства Москвы [3], который в этой части опирается на 59-ФЗ. Данным Регламентом предусмотрен прием обращений с использованием системы электронного документооборота и с использованием официального сервера Правительства Москвы в сети Интернет, иначе – московский портал государственных услуг.

Помимо этого, у каждого органа исполнительной власти (далее – ОИВ) в обязательном порядке предусмотрена возможность направления обращения гражданином как в личном порядке, через почтовое отделение, курьерами, фельдъегерской службой или посредством почты, так и с помощью обращения в Электронную приемную организации. При этом, если вопрос в обращении выходит за рамки компетенций организации, получившей его, она вправе переадресовать обращение в соответствующий ОИВ с уведомлением гражданина.

Также допускается возможность оставления обращения без ответа, если определить суть обращения невозможно, а в случае, если обращение оформлено не в соответствии с 59-ФЗ, то ОИВ имеет право отклонить обращение с разъяснением порядка рассмотрения обращений.

Помимо вышеописанных способов направления сообщений Московским Правительством активно создаются и развиваются специализированные мобильные приложения и сервисы для взаимодействия с гражданами, самым известным из которых в настоящее время является портал «Наш город», с помощью которого любой гражданин имеет возможность оставить обращение по определенному списку тематик, в основном связанных с содержанием городских объектов.

Данный портал является подсистемой информационной системы публикации данных и приема сообщений, которая создана в целях реализации Указа Президента Российской Федерации от 7 мая 2021 года № 601 «Об основных направлениях совершенствования системы государственного управления» [4].

В соответствии с регламентом обработки информации портала «Наш город» [5] все обращения подразделяются на сообщения и сигналы. Разница заключается в том, что сигнал не предполагает направление ответа заявителю.

Принцип работы портала в части рассмотрения сообщений пользователей, в соответствии с информацией на самом сайте, заключается в следующем:

1. сначала пользователь системы оставляет жалобу в определенном формате;
2. затем модератор рассматривает обращение и принимает решение о публикации – на данной стадии сообщение может быть опубликовано (соответственно, отправлено в ответственный ОИВ), возвращено пользователю на доработку или отклонено по причинам, определенным в правилах обработки сообщений и сигналов [6];

3. если сообщение передано в ОИВ, то ведомство рассматривает обращение, подтверждает/не подтверждает проблему и устраняет ее;
4. далее модератор рассматривает ответ ОИВ на предмет соответствия требованиям и в случае отсутствия замечаний результат рассмотрения обращения публикуется на портале, в противном случае ответ возвращается в ОИВ на доработку;
5. гражданин вправе подтвердить устранение или не устранение проблемы.

Исходя из вышеуказанного представления назначения и функционала портала «Наш город» заметно, что на текущей стадии продукт не является универсальным, то есть гражданин может воспользоваться порталом только в тех случаях, когда его проблема соответствует одной из категорий обращений, рассматриваемых на данном портале.

Важно отметить, что в настоящее время в соответствии с регламентом обработки информации на портале «Наш город» ни сигнал, ни сообщение не являются обращениями граждан в значении понятия, предусмотренного 59-ФЗ, хотя ответы, подготавливаемые ОИВ на сообщения пользователей, соответствуют данному закону, а именно:

1. соблюдаются принципы, указанные в статье 10 59-ФЗ, такие как обязанность ОИВ принимать меры, направленные на восстановление и защиту прав, свобод и законных интересов заявителя, обязанность готовить письменный ответ и уведомления гражданина о направлении его обращения в другой ОИВ (на самом портале публикуется ответ ОИВ с указанием сведений о перенаправлении в другое ведомство) и др.;
2. сроки рассмотрения обращений на портале «Наш город» не превышают сроков, указанных в статье 12 59-ФЗ, в том числе с учетом продления рассмотрения сообщения.

Учитывая вышесказанное, портал «Наш город» может впоследствии быть приведен в соответствие 59-ФЗ в полной мере. Тем не менее, перечень тематик для подачи сообщения на текущий момент сильно ограничен, но при этом обладает потенциалом стать единственным информационным пространством (или его частью конкретно по направлению работы с обращениями граждан), о котором говорится в Стратегии развития информационного общества [7], при условии расширения перечня тематик, совершенствования формы подачи обращений и масштабирования портала на всю страну.

В свою очередь, расширение списка тематик является достаточно проблематичной задачей, так как не все обращения граждан можно привести к унифицированному виду, а спектр поступающих вопросов тяжело спрогнозировать. Рассмотрим данную проблематику и пути ее решения более детально.

В открытых источниках трудно найти сведения о используемых методах расширения перечня тематик портала «Наш город», тем не менее известна практика краудсорсинга, которая позволила за период с 2014 по 2019 год добавить около 60 новых тем для обращений по инициативе граждан [8].

Тем не менее, не все возрастные группы населения города Москвы знакомы с такими краудсорсинговыми проектами и не все в них участвуют. При этом обращения по-прежнему поступают в электронном виде в ОИВ через электронную приемную или на официальные почты ведомств. Учитывая объем поступающих обращений, они могли бы стать основой для определения новых проблемных тем для классификатора на портале «Наш город», а именно можно прибегнуть к интеллектуальному анализу текстов, или технологиям обработки естественного языка.

Обработка естественного языка – достаточно широкое направление, которое в рамках рассматриваемого вопроса можно использовать в целях поиска ключевых словосочетаний в обращениях, для подсчета частоты их встречаемости для определения целесообразности формирования проблемной темы на основе данного словосочетания.

Помимо вышеуказанных данных можно проанализировать отклоненные обращения, если причина их отклонения – несоответствие текста обращения выбранной тематике.

Также для определения тематик можно воспользоваться изучением полномочий ОИВ, но для этого прибегать к внедрению информационных технологий не требуется, при этом тематики, которые определены полномочиями ОИВ, могут быть не востребованы, следовательно, прибегать к изучению общественного мнения или к анализу ранее поступивших обращений на предмет встречаемости обращений по схожей теме все же необходимо.

Чтобы реализовать единое пространство для подачи всех обращений на базе портала «Наш город», необходимо также предусмотреть возможность направления сообщения в открытой форме, причем на уровне модерации обращений можно внедрить все те же механизмы анализа текстов, но уже с целью классификации обращения: такой инструмент может помочь снизить вероятность некорректного выбора адресата пользователем, тем самым избавить ОИВ от рассмотрения обращений, не входящих в их компетенции, и их переадресации в другие ведомства, а также уменьшить долю отклоняемых сообщений.

Таким образом, внедрение инструментов интеллектуального анализа текстов может как способствовать развитию портала «Наш город» в части расширения классификатора проблемных тем, так и оптимизировать процесс модерации сообщений граждан.

Таким образом, если при развитии портала «Наш город» обратиться к технологиям обработки естественного языка, то это позволит расширить действующий классификатор проблемных тем, основываясь на ранее поступавших обращениях, а значит расширится сфера применения портала. Более того, результат интеллектуального анализа текстов способен оптимизировать процесс обработки поступающих сообщений и уменьшить долю некорректно оформленных сообщений (в части выбора темы) и долю отклоняемых обращений.

При таком развитии портала «Наш город» и при условии приведения его принципов работы к требованиям 59-ФЗ, у данного продукта есть все шансы к масштабированию до федерального уровня.

1. О порядке рассмотрения обращений граждан Российской Федерации [Текст]: Федеральный закон от 02 мая 2006 года № 59-ФЗ // Собрание законодательства Российской Федерации – 08.05.2006. № 19. – ст. 2060.
2. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об организации предоставления государственных и муниципальных услуг» [Текст]: Федеральный закон от 27 июля 2010 года № 227-ФЗ // Собрание законодательства Российской Федерации – 02.08.2010. №31. – ст. 4196.
3. О Регламенте Правительства Москвы [Электронный ресурс]: Постановление Правительства Москвы от 21.02.2006 № 112-ПП // URL: О Регламенте Правительства Москвы от 21 февраля 2006 - docs.cntd.ru (дата обращения: 18.09.2024).
4. Об информационных системах, обеспечивающих деятельность Открытого правительства города Москвы [Электронный ресурс]: Постановление Правительства Москвы от 02.04.2013 № 187-ПП // URL: <https://docs.cntd.ru/document/537932962> (дата обращения: 18.09.2024).
5. Регламент обработки информации на портале «Наш город». [Электронный ресурс]: URL: <https://gorod.mos.ru/portal/documents/reglament> (дата обращения: 18.09.2024).
6. Правила обработки сообщений и сигналов на портале «Наш город». [Электронный ресурс]: URL: <https://gorod.mos.ru/portal/documents> (дата обращения: 18.09.2024).
7. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Текст]: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. – 15.05.2017. № 20. – ст. 2901.
8. «Наш город», взгляд изнутри. Как работает портал. [Электронный ресурс]: URL: <https://moscowseasons.com/news/nash-gorod-vzgliad-iznutri-kak-rabotaet-portal/> (дата обращения: 18.09.2024).

Коновалов Г.Г.

Анализ сервиса Keycloak: преимущества и недостатки

*Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/trnio-10-2024-385

Аннотация

В статье рассматриваются ключевые преимущества Keycloak: экономичность, поддержка множества протоколов, возможности масштабирования. Наряду с этим анализируются основные недостатки, такие как сложность настройки, проблемы с производительностью и неудобство интерфейса. В заключении даются рекомендации по использованию Keycloak в зависимости от потребностей и ресурсов организации, помогающие принять обоснованное решение о его внедрении.

Ключевые слова: Keycloak, аутентификация, авторизация, управление доступом, открытый исходный код, многофакторная аутентификация, безопасность, масштабируемость, интеграция.

Abstract

The article discusses the key benefits of Keycloak: cost-effectiveness, support for multiple protocols, and scalability. Along with this, it analyzes the main disadvantages, such as the complexity of setup, performance issues, and inconvenience of the interface. Finally, it provides recommendations on how to use Keycloak depending on the needs and resources of the organization, helping to make an informed decision about its implementation.

Keywords: Keycloak, authentication, authorization, access management, open source, multi-factor authentication, security, scalability, integration.

Keycloak – это мощная система управления доступом с открытым исходным кодом, разработанная компанией Red Hat. Основной задачей Keycloak является обеспечение аутентификации и авторизации пользователей в веб-приложениях и сервисах. Она предоставляет решения для управления пользователями, включающие регистрацию, вход, восстановление пароля, а также поддержку различных протоколов для интеграции с другими системами.

Keycloak поддерживает современные стандарты безопасности, такие как OAuth2, OpenID Connect и SAML, что позволяет легко интегрировать её в существующую инфраструктуру приложений. Она также предоставляет инструменты для управления пользователями и группами, а также возможности для реализации многофакторной аутентификации.

Кроме того, сервис Keycloak выделяется своим гибким и масштабируемым подходом, что делает его подходящим как для малых и средних бизнесов, так и для крупных корпоративных решений. Система предлагает удобные интерфейсы для администрирования и настройки, а это позволяет легко адаптировать её под специфические требования бизнеса.

Одним из ключевых преимуществ Keycloak является его открытый исходный код. Это означает, что пользователи могут свободно использовать, модифицировать и адаптировать систему под свои потребности без необходимости приобретения лицензий. Открытый исходный код также предоставляет возможность глубокой настройки и расширения функционала, что может быть критично для специфических требований бизнеса. Отсутствие лицензионных затрат делает Keycloak экономически привлекательным выбором как для стартапов, так и для крупных организаций.

Как мы уже говорили выше, Keycloak поддерживает несколько широко используемых протоколов аутентификации и авторизации, включая OAuth2, OpenID Connect и SAML. Это позволяет легко интегрировать систему с различными веб-приложениями, мобильными приложениями и корпоративными системами. Поддержка множества протоколов упрощает

реализацию единого входа (SSO) и обеспечивает гибкость при подключении новых сервисов. Пользователи могут выбирать подходящий протокол в зависимости от потребностей и существующей инфраструктуры, что значительно упрощает процесс интеграции.

Keycloak спроектирован с учётом масштабируемости и гибкости, что делает его подходящим для разнообразных сценариев использования. Система может быть настроена для работы в кластеризованном режиме – это позволяет обрабатывать большое количество запросов и обеспечивать высокую доступность. Гибкость Keycloak проявляется в возможности настройки различных аспектов безопасности и управления пользователями, таких как политики паролей, пользовательские атрибуты и роли. Это позволяет адаптировать систему под уникальные требования бизнеса и масштабировать её по мере роста компании.

Keycloak предоставляет встроенную поддержку многофакторной аутентификации (MFA), что значительно повышает уровень безопасности. Пользователи могут настроить различные методы проверки подлинности, включая SMS-коды, электронную почту, и приложения для генерации одноразовых паролей (OTP). Многофакторная аутентификация защищает от несанкционированного доступа и снижает риски, связанные с компрометацией учетных записей. Возможность выбора и настройки различных методов MFA делает Keycloak подходящим решением для организаций с высокими требованиями к безопасности.

Одним из основных недостатков Keycloak является сложность его настройки и конфигурации. Несмотря на мощный функционал, первоначальная установка и интеграция с существующими системами могут потребовать значительных усилий. Администраторам и разработчикам необходимо детально разбираться в архитектуре Keycloak, чтобы правильно настроить сервер, обеспечить безопасность и интеграцию с другими сервисами. Для крупных организаций, где требования к безопасности и масштабируемости высоки, это означает значительные затраты времени и ресурсов.

Keycloak потребляет значительное количество ресурсов, особенно при высоких нагрузках. Когда система обслуживает множество пользователей или работает в условиях, требующих сложных процессов аутентификации, это зачастую приводит к снижению производительности. Высокие требования к вычислительным мощностям вызывают необходимость в оптимизации серверов и инфраструктуры. Для организаций с постоянным ростом пользователей это может стать серьезным препятствием, требующим дополнительных инвестиций в оборудование и оптимизацию.

Документация Keycloak, хотя и является достаточно обширной, не всегда отвечает на все вопросы, возникающие у её пользователей. Проблемы с актуальностью, а также отсутствие полноты некоторых разделов затрудняют процесс обучения и интеграции. Пользователи вынуждены обращаться к сообществу или искать решения на профильных форумах, а это замедляет процесс внедрения и увеличивает риски. Зависимость от сообщества также означает, что уровень поддержки может быть нестабильным, особенно при возникновении специфических или сложных вопросов.

Хотя Keycloak предлагает удобный веб-интерфейс для администрирования, его дизайн и удобство использования часто подвергаются критике. Интерфейс может показаться сложным и неинтуитивным, особенно для новых пользователей. Некоторые задачи, например, настройка сложных политик безопасности или управление группами пользователей, требуют выполнения нескольких неочевидных шагов. Всё это замедляет процесс администрирования и увеличивает вероятность ошибок.

Необходимо отметить, что Keycloak представляет собой мощное и гибкое решение для управления аутентификацией и авторизацией пользователей, обеспечивая значительное количество преимуществ для организаций разного размера. Его открытый исходный код и отсутствие лицензионных затрат делают его привлекательным выбором для многих компаний, особенно для тех, кто ищет экономически эффективные решения. Поддержка множества протоколов, масштабируемость и встроенная поддержка многофакторной аутентификации укрепляют позиции Keycloak как универсального инструмента для обеспечения безопасности и упрощения управления пользователями.

Тем не менее, Keycloak не лишён и недостатков. Сложность настройки и конфигурации может стать значительным барьером для пользователей, не имеющих достаточного опыта. Проблемы с производительностью при высоких нагрузках требуют дополнительных усилий

для оптимизации и масштабирования. Документация и поддержка могут не всегда полностью удовлетворяют потребности пользователей, что добавляет сложности в процессе внедрения. И наконец, интерфейс и пользовательский опыт, хотя и функциональны, не всегда соответствуют требованиям всех администраторов и пользователей.

При выборе Keycloak в качестве решения для управления доступом важно учитывать как его преимущества, так и потенциальные проблемы. Если ваша организация имеет ресурсы для обучения и настройки системы, а также готова инвестировать в оптимизацию производительности, Keycloak может стать отличным выбором благодаря своей гибкости и широкому функционалу. Он подходит для компаний, которым требуется поддержка различных протоколов и возможность масштабирования.

Для организаций, которые ищут решение с более простым процессом настройки и меньшими требованиями к ресурсам, может потребоваться дополнительное рассмотрение альтернативных решений или использование Keycloak в сочетании с внешней поддержкой и консультациями.

В заключение необходимо подчеркнуть, что Keycloak представляет собой мощный инструмент для управления аутентификацией и авторизацией, который, при правильной настройке и оптимизации, может значительно улучшить процессы безопасности и управления пользователями в организации.

1. Chatterjee, A. Applying Spring Security Framework with KeyCloak-Based OAuth2 to Protect Microservice Architecture APIs: A Case Study / A. Chatterjee, A. Prinz // Sensors. – 2022. – Vol. 22, No. 5.
2. Kaczmarek, P. Web security: a quick start introduction to OAuth 2.0 and Keycloak 19.x authorization scenarios / P. Kaczmarek, F. Vandamme // Communication & Cognition. – 2022. – Vol. 55, No. 3-4. – P. 133-160.
3. Коган, М. Keycloak в примерах и фишах / М. Коган, К. Кобылкин // Системный администратор. – 2023. – № 6(247). – С. 16-19.
4. Федоренко, А. В. Использование инструмента Keycloak для реализации систем с единой точкой входа / А. В. Федоренко, А. И. Тымкив // ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК ОСНОВА ЭФФЕКТИВНОГО ИННОВАЦИОННОГО РАЗВИТИЯ : сборник статей Международной научно-практической конференции, Самара, 10 января 2022 года. Том Часть 1. – Уфа: Общество с ограниченной ответственностью «Аэтерна», 2022. – С. 73-75.
5. Федоренко, А. В. настройка инструмента Keycloak для реализации систем с единой точкой входа / А. В. Федоренко, А. И. Тымкив, О. Г. Худасова // Разработка и ПРИМЕНЕНИЕ НАУКОЁМККИХ ТЕХНОЛОГИЙ в ИНТЕРЕСАХ МОДЕРНИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА : сборник статей Международной научно-практической конференции, Таганрог, 20 января 2022 года. Том Часть 1. – Уфа: Общество с ограниченной ответственностью «Аэтерна», 2022. – С. 90-94.
6. Головашов, С. Обзор необходимых функций контроля удалённого доступа, применяемых на практике при использовании KeyCloack / С. Головашов, И. Агатий, В. Марков // Системный администратор. – 2023. – № 11(252). – С. 16-23.

Коновалов Г.Г.

Об архитектурных особенностях безопасности языка Java

*Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/trnio-10-2024-386

Аннотация

В статье рассматриваются архитектурные особенности языка программирования Java, которые обеспечивают безопасность приложений. Описаны ключевые компоненты, такие как виртуальная машина Java (JVM), механизм класслоадеров, модификаторы доступа, Security Manager и политики безопасности. Рассматривается роль каждого из этих элементов в защите программного обеспечения от потенциальных угроз, а также их взаимодействие для обеспечения многоуровневой защиты.

Ключевые слова: архитектура безопасности Java, JVM, класслоадеры, модификаторы доступа, security manager, политики безопасности, защита приложений.

Abstract

The article discusses the architectural features of the Java programming language that ensure application security. Key components such as the Java virtual machine (JVM), classloader mechanism, access modifiers, Security Manager, and security policies are described. The role of each of these elements in protecting software from potential threats is considered, as well as their interaction to ensure multi-level protection.

Keywords: Java security architecture, JVM, classloaders, access modifiers, security manager, security policies, application security.

Безопасность в программировании является одним из ключевых факторов при разработке программного обеспечения, особенно в условиях современного интернета, где кибератаки и уязвимости могут приводить к значительным убыткам. Язык программирования Java, будучи одним из самых популярных и широко используемых языков, обладает встроенными механизмами безопасности, которые защищают приложения от различных угроз. Эти механизмы глубоко интегрированы в архитектуру языка, что делает Java одним из самых безопасных языков для разработки критически важных приложений.

Одной из ключевых особенностей безопасности языка Java является его использование виртуальной машины Java (JVM), которая выполняет байткод и управляет средой выполнения программ. JVM играет центральную роль в обеспечении безопасности Java-приложений, изолируя их от операционной системы и предоставляя защиту от различных угроз.

Когда исходный код Java компилируется, он преобразуется в байткод – платформо-независимый код, который выполняется JVM. Перед выполнением байткод проходит строгую проверку на корректность и безопасность. Этот процесс известен как верификация байткода (Bytecode Verification). Он гарантирует, что байткод не нарушает правил доступа к памяти, не вызывает некорректные операции и не нарушает структуру классов. Верификация байткода предотвращает выполнение потенциально опасного или некорректного кода, что значительно снижает риск возникновения уязвимостей.

Также JVM обеспечивает безопасность за счет механизма обработки исключений. Этот механизм позволяет корректно управлять ошибками, возникающими во время выполнения программы, предотвращая неконтролируемые сбои и утечки данных. Обработка исключений гарантирует, что даже в случае возникновения ошибки приложение продолжит работу в безопасном режиме или будет корректно завершено, что важно для поддержания целостности и безопасности данных.

Модель безопасности Java также включает механизмы на уровне загрузки классов и управления доступом, что также играет важную роль в защите приложений от несанкционированного доступа и выполнения кода. Основными элементами этой модели являются класслоадеры и модификаторы доступа.

Класслоадеры в Java отвечают за загрузку классов в память во время выполнения программы. Важная особенность класслоадеров заключается в их способности разделять пространство имен классов, что позволяет изолировать различные компоненты приложения друг от друга. Это особенно полезно при работе с внешними библиотеками и плагинами, могущими содержать небезопасный код. Например, если злоумышленник попытается внедрить вредоносный код в виде нового класса, который пересекается с уже загруженными безопасными классами, класслоадер предотвратит такие конфликты и защитит приложение.

Java предоставляет гибкую систему модификаторов доступа, контролирующими видимость и доступность классов, методов и полей. Основные модификаторы включают:

- `public`: предоставляет доступ к элементу из любого другого кода;
- `private`: ограничивает доступ только внутри класса;
- `protected`: разрешает доступ из классов одного пакета и из подклассов.
- `default` (по умолчанию): предоставляет доступ только внутри одного пакета.

Эти модификаторы позволяют разработчикам управлять доступом к критически важным данным и функциям, защищая их от несанкционированного использования. Например, использование модификатора `private` для чувствительных данных позволяет предотвратить доступ к ним извне, обеспечивая защиту данных от потенциальных атак.

Класслоадеры и модификаторы доступа работают вместе, создавая мощный механизм контроля доступа к ресурсам. Класслоадеры обеспечивают изоляцию классов, а модификаторы доступа позволяют четко определить, кто и как может взаимодействовать с тем или иным элементом приложения. Это снижает вероятность утечки данных или исполнения нежелательного кода.

Одним из наиболее мощных инструментов обеспечения безопасности в Java является Security Manager – специальный компонент, который контролирует выполнение потенциально опасного кода в приложении. Security Manager работает в сочетании с политиками безопасности, определяющими, какие действия разрешены или запрещены для различных частей кода.

Security Manager выполняет функции «охранника» для приложений, работающих в среде Java. Он контролирует доступ к критическим ресурсам, таким как файловая система, сеть, системные команды и другие чувствительные операции. Когда код пытается выполнить потенциально опасное действие, Security Manager проверяет, разрешено ли это действие согласно текущим настройкам безопасности. Если действие не разрешено, происходит выброс исключения `SecurityException`, и операция блокируется.

Политики безопасности (Security Policies) представляют собой наборы правил, которые определяют, какие действия разрешены для конкретных классов или пакетов. Эти политики могут быть настроены администратором системы или разработчиком приложения, чтобы обеспечить нужный уровень безопасности.

Политики безопасности записываются в виде файлов конфигурации, в которых указывается, какие привилегии предоставляются различным классам. Например, можно создать политику, которая разрешает доступ к определенной директории на диске только для чтения, а доступ на запись – запрещает. Такие политики имеют широкий арсенал настроек, позволяя адаптировать безопасность приложения под конкретные потребности.

Использование Security Manager и политик безопасности позволяет значительно повысить уровень защиты Java-приложений. Они обеспечивают:

- возможность точно настроить, какие действия разрешены для разных частей кода;
- предотвратить выполнения потенциально опасных операций, особенно в среде, где используется код от сторонних поставщиков;
- ограничить доступ к системным ресурсам, минимизируя вероятность злоупотреблений и атак.

И, хотя, начиная с Java 17, Security Manager признан устаревшим и его использование в новых приложениях не рекомендуется, понимание его работы и применение является полезным для поддержки и модернизации существующих систем, где этот компонент уже интегрирован.

В заключение необходимо ответить, что безопасность – ключевой аспект в разработке приложений, и язык Java предоставляет мощные архитектурные инструменты для защиты программного обеспечения от различных угроз. Рассмотренные в статье особенности – виртуальная машина Java (JVM), механизм класслоадеров, модификаторы доступа, а также Security Manager и его политики безопасности, обеспечивают многоуровневую защиту приложений.

JVM, являясь основой выполнения программ на Java, обеспечивает безопасность через проверку байткода и обработку исключений, предотвращая выполнение некорректного и потенциально опасного кода. Механизм класслоадеров и модификаторов доступа помогает изолировать различные компоненты приложения и контролировать доступ к важным ресурсам, предотвращая несанкционированное использование данных и функций.

Security Manager и его политики безопасности предоставляют разработчикам дополнительные инструменты для ограничения выполнения опасных операций, особенно при работе с незнакомым кодом. Несмотря на то, что Security Manager постепенно выводится из активного использования, его концепция остается важной для понимания и поддержания существующих приложений.

В совокупности, все рассмотренные в статье механизмы делают Java надежным выбором для разработки безопасного программного обеспечения, способного противостоять современным угрозам. Разработчикам необходимо учитывать архитектурные особенности языка Java и эффективно использовать их для создания защищенных приложений. В настоящий момент Java продолжает оставаться одним из самых безопасных языков программирования, и его архитектурные решения играют в этом решающую роль.

1. Гаврилов, С. В. Механизмы безопасности Java-приложений / С. В. Гаврилов, П. А. Лотарев, Е. Д. Лунева // Наука. Технология. Производство – 2023 : Материалы Всероссийской научно-технической конференции, посвященной 75-летию ООО «Газпром нефтехим Салават», Салават, 24–28 апреля 2023 года. Том Часть 1. – Салават: Уфимский государственный нефтяной технический университет, 2023. – С. 139-140.
2. Сидоров, И. Д. Безопасность виртуальной машины Java / И. Д. Сидоров, Н. Н. Цопкало // Известия ТРТУ. – 2004. – № 8(43). – С. 132.
3. Сиротский, А. А. Безопасность в Java / А. А. Сиротский, П. И. Кулешов // Современные проблемы информационной безопасности и программной инженерии : Сборник избранных статей научного семинара №1(6) кафедры информационной безопасности и программной инженерии, Москва, 24 января 2014 года / Российский государственный социальный университет, кафедра информационной безопасности и программной инженерии. – Москва: Общество с ограниченной ответственностью «Сам Полиграфист», 2014. – С. 50-56.
4. Часов, Е. А. Разработка и исследование методов повышения безопасности работы Java-приложений / Е. А. Часов, М. А. Марина, Т. В. Касаткин // Экономика и социум. – 2017. – № 9(40). – С. 446-449.
5. Жуматай, Ш. С. Обзор инструментов безопасности языка программирования Java / Ш. С. Жуматай // Молодой исследователь: вызовы и перспективы : сборник статей по материалам ССХI международной научно-практической конференции, Москва, 03 мая 2021 года. Том 16 (211). – Москва: Общество с ограниченной ответственностью «Интернаука», 2021. – С. 242-246.
6. Здитовец, А. Л. Особенности архитектуры бекенда на Java / А. Л. Здитовец // Актуальные исследования. – 2024. – № 2-1(184). – С. 34-40.

Коновалов Г.Г.

Особенности архитектуры и преимущества колоночных баз данных

*Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/trnio-10-2024-387

Аннотация

В статье рассматриваются архитектурные особенности и ключевые преимущества колоночных баз данных в сравнении с традиционными реляционными системами. Обсуждаются механизмы хранения и обработки данных, обеспечивающие высокую производительность при выполнении аналитических запросов и оптимизацию использования ресурсов. Анализируются недостатки колоночных баз данных, затрудняющие их применение в определенных сценариях. Обсуждаются перспективы дальнейшего развития и применения колоночных баз данных.

Ключевые слова: колоночные базы данных, архитектура данных, аналитические запросы, компрессия данных, масштабируемость, производительность, транзакционность.

Abstract

The article examines the architectural features and key advantages of columnar databases compared to traditional relational systems. It discusses data storage and processing mechanisms that provide high performance when executing analytical queries and optimized resource use. It analyzes

the disadvantages of columnar databases that complicate their use in certain scenarios. It discusses the prospects for further development and application of columnar databases.

Keywords: columnar databases, data architecture, analytical queries, data compression, scalability, performance, transactionality.

Колоночные базы данных представляют собой один из ключевых инструментов в современном мире обработки больших данных и аналитики. В отличие от традиционных реляционных баз данных, где данные хранятся построчно, в колоночных базах данных информация организована по столбцам. Такой подход позволяет значительно повысить эффективность работы с данными, особенно в случаях, когда требуется быстро обработать большие объемы информации и выполнить сложные аналитические запросы.

Основное отличие колоночных баз данных заключается в том, как они хранят данные. В традиционных реляционных базах данных информация организована по строкам, каждая из которых представляет собой отдельную запись с различными полями. В колоночных же базах данные хранятся по столбцам, где каждый столбец соответствует одному полю и содержит все значения этого поля для всех записей.

Этот подход имеет ряд преимуществ, особенно ярко проявляющийся при работе с аналитическими запросами, которые часто требуют выборки и агрегации данных по одному или нескольким полям. Поскольку данные одного столбца хранятся компактно и последовательно, колоночные базы данных могут более эффективно извлекать и обрабатывать нужные данные, минимизируя чтение ненужных полей.

Колоночные базы данных также оптимизированы для более эффективного хранения данных. Поскольку все значения в столбце имеют одинаковый тип данных, это открывает возможности для использования специальных алгоритмов сжатия. Методы сжатия, такие как кодирование длин серий (Run-Length Encoding) или словарное сжатие (Dictionary Encoding), значительно уменьшают объем хранимых данных.

Компрессия не только снижает затраты на хранение, но и ускоряет обработку запросов, так как система может обрабатывать данные непосредственно в сжатом виде. Это позволяет быстрее передавать данные в оперативную память и уменьшает объем работы процессора при их декомпрессии.

Колоночные базы данных специально оптимизированы для выполнения запросов, которые задействуют большое количество данных. Благодаря архитектуре хранения данных по столбцам и эффективным механизмам сжатия, такие базы данных быстро обрабатывают запросы, требующие выполнения агрегатных функций, фильтрации данных и других аналитических операций.

Кроме того, многие колоночные базы данных используют технологии векторизации запросов, при которой инструкции процессора применяются сразу к множеству значений, что значительно ускоряет выполнение операций. Это делает колоночные базы данных идеальными для выполнения сложных аналитических запросов, требующих обработки больших объемов данных в реальном времени.

Сама архитектура колоночных баз данных делает их мощным инструментом для аналитики и работы с большими данными, предоставляя возможность быстрее и эффективнее извлекать ценную информацию из огромных массивов данных.

Колоночные базы данных предлагают ряд значительных преимуществ при обработке больших данных и выполнении аналитических задач. Благодаря своей уникальной архитектуре, они обеспечивают высокую производительность, экономию ресурсов и масштабируемость.

Одним из главных преимуществ колоночных баз данных является их высокая производительность при выполнении аналитических запросов. В отличие от традиционных реляционных баз данных, колоночные базы данных позволяют сосредоточить ресурсы на обработке конкретных столбцов, что значительно ускоряет выполнение запросов.

Агрегатные операции, такие как вычисление средних значений, сумм, или других статистических метрик, выполняются значительно быстрее, так как данные уже сгруппированы

по столбцам. Например, если необходимо вычислить сумму значений по определённому столбцу, система может просто прочесть и обработать этот один столбец, не обращаясь к остальным данным. Это особенно полезно в случаях анализа продаж, финансового мониторинга и др.

Колоночные базы данных предлагают высокую эффективность хранения данных за счет использования различных методов сжатия. Поскольку все данные в столбце однотипны, системы могут использовать оптимальные алгоритмы сжатия (Run-Length Encoding или Dictionary Encoding). В некоторых случаях обработка данных может происходить прямо в сжатом виде, что дополнительно ускоряет выполнение запросов.

Колоночные базы данных легко масштабируются, что делает их идеальными для работы с постоянно растущими объемами данных. В таких системах проще реализовать горизонтальное масштабирование, добавляя новые узлы в кластер для увеличения производительности и объема хранения.

Благодаря своей гибкости, колоночные базы данных могут быть адаптированы под различные задачи – от аналитики в реальном времени до долгосрочного хранения архивных данных. Такая универсальность делает их привлекательным выбором для компаний, работающих с большими данными и стремящихся к оптимизации своих аналитических процессов.

Колоночные базы данных особенно эффективны при работе с аналитическими запросами, но они не всегда подходят для обработки транзакционных операций. В тех случаях, когда система должна часто обновлять или вставлять отдельные записи, колоночные базы данных демонстрируют низкую производительность по сравнению с традиционными реляционными базами данных.

В сценариях, где важна скорость выполнения операций вставки, обновления и удаления данных (например, в системах управления заказами или обработке транзакций), традиционные базы данных с построчным хранением данных часто оказываются более эффективными. Это связано с тем, что в колоночных базах данных каждая операция над строкой требует изменения нескольких столбцов, что может привести к повышенной нагрузке на систему и замедлению работы.

В отличие от реляционных баз данных, которые изначально разрабатывались для обработки транзакционных операций, колоночные базы данных не всегда обеспечивают полную поддержку транзакционности (ACID-свойства: атомарность, согласованность, изолированность, долговечность). Некоторые системы могут ограничивать возможности параллельного выполнения транзакций или не предоставлять полной гарантии изолированности.

Это критично в сценариях, где важна высокая надежность и точность выполнения транзакций, например, в финансовых системах или при работе с чувствительными данными. В таких случаях использование колоночных баз данных может потребовать дополнительных мер по обеспечению целостности данных, что может усложнить архитектуру системы.

Колоночные базы данных представляют собой мощный инструмент для работы с большими данными и выполнения сложных аналитических запросов. Благодаря своей уникальной архитектуре, которая предполагает хранение данных по столбцам, эти базы данных предлагают значительные преимущества в производительности, особенно при выполнении операций агрегации и фильтрации данных. Эффективные методы сжатия данных позволяют значительно экономить ресурсы хранения и ускоряют обработку запросов.

Несмотря на все свои достоинства, колоночные базы данных не лишены недостатков. Они слабо подходят для транзакционных операций, где важна высокая скорость обновления и вставки данных, и требуют более сложной настройки и управления. Также ограниченная поддержка транзакций делает их слабо подходящими для систем, требующих строгих гарантий целостности данных.

Тем не менее, колоночные базы данных остаются одним из лучших решений для задач, связанных с аналитикой больших данных, где скорость и эффективность работы играют

ключевую роль. Они продолжают развиваться, предлагая всё больше возможностей для оптимизации работы с данными и расширяя области своего применения.

В заключение необходимо отметить, что в будущем можно ожидать дальнейшего совершенствования колоночных баз данных, улучшения их гибкости и функциональности, что позволит еще более эффективно использовать их в самых разных областях – от бизнес-аналитики до научных исследований и машинного обучения. Важно понимать и учитывать их особенности, чтобы максимально эффективно интегрировать их в инфраструктуру и получить от их использования максимальную выгоду.

1. Шаипов, А. А. Принципы работы колоночной базы данных, ее преимущества и ограничения / А. А. Шаипов // Научно-исследовательский центр «Вектор развития». – 2023. – № 16. – С. 199-204.
2. Сравнения колоночных баз данных / Э. Д. Демидов, Я. М. Сидоренко, А. М. Мацелура, А. Н. Петрова // Наука, инновации и технологии: от идей к внедрению / Редколлегия: А.В. Космынин (отв. ред.) [и др.]. Том 1. – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2022. – С. 199-202.
3. Флоринская, М. В. Современные инструменты построения хранилищ для эффективной работы с Big Data / М. В. Флоринская, А. А. Сидоренко // Вестник Ессентукского института управления, бизнеса и права. – 2019. – № 16. – С. 100-107.
4. Слинкина, Е. В. Тестирование реляционной и колоночной СУБД для работы с аналитической многостроковой информацией / Е. В. Слинкина // Инновационные механизмы и стратегические приоритеты научно-технического развития – УФА: «Аэтерна», 2022. – С. 77-83.
5. Петрова, А. Н. Колоночная модель данных / А. Н. Петрова, А. В. Шатов, В. Ю. Куйдин // Наука, инновации и технологии: от идей к внедрению / Редколлегия: А.В. Космынин (отв. ред.) [и др.]. Том 1. – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2022. – С. 114-116.

Коновалов Г.Г.

Применение нечеткой логики в программировании

*Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/trnio-10-2024-388

Аннотация

В статье рассматривается применение нечеткой логики в программировании. Описаны основные принципы нечеткой логики, её отличие от классической логики, а также ключевые концепции, такие как нечеткие множества и функции принадлежности. Анализируются преимущества и недостатки применения нечеткой логики, её гибкость, способность работать с неопределенными данными и вычислительные сложности.

Ключевые слова: нечеткая логика, программирование, нечеткие множества, функции принадлежности, системы управления, искусственный интеллект, машинное обучение, экспертные системы, неопределенные данные.

Abstract

The article discusses the application of fuzzy logic in programming. It describes the basic principles of fuzzy logic, its difference from classical logic, and key concepts such as fuzzy sets and membership functions. It analyzes the advantages and disadvantages of using fuzzy logic, its flexibility, ability to work with uncertain data, and computational complexities.

Keywords: fuzzy logic, programming, fuzzy sets, membership functions, control systems, artificial intelligence, machine learning, expert systems, uncertain data.

Нечеткая логика (fuzzy logic) представляет собой подход к обработке информации, который позволяет моделировать и управлять неопределенностью и неточностью, характерными для многих реальных систем. Эта концепция была предложена Лотфи Заде в 1965 году как расширение классической булевой логики, которая работает только с бинарными значениями (истинно/ложно). В отличие от нее, нечеткая логика оперирует с градиентными

значениями, что позволяет более точно отражать сложные и многозначные характеристики объектов и процессов.

С течением времени нечеткая логика доказала свою полезность в различных областях, от систем управления до искусственного интеллекта. В современном программировании этот подход нашел широкое применение благодаря своей способности эффективно работать с неопределенностью и приближенностью к реальным условиям.

Нечеткая логика представляет собой обобщение классической булевой логики, позволяя работать с неопределенными и неточными данными. Основная идея заключается в том, что вместо четких истинностных значений «истинно» и «ложно», используются значения в диапазоне от 0 до 1, что позволяет моделировать более сложные и реалистичные ситуации.

Классическая логика оперирует бинарными переменными, которые могут принимать только два значения: 0 (ложь) и 1 (истина). Нечеткая логика, в свою очередь, использует переменные, которые могут иметь любое значение в интервале от 0 до 1. Это позволяет более гибко отражать степени истинности и лжи, что особенно полезно в случаях, когда данные неполные или неточные.

Нечеткое множество представляет собой обобщение классического множества. В классическом множестве элемент либо принадлежит множеству, либо не принадлежит ему. В нечетком множестве принадлежность элемента характеризуется степенью принадлежности, которая выражается числом от 0 до 1. Например, если «х» является членом множества «высокие температуры», его степень принадлежности может быть 0.7, что означает, что температура «х» в некоторой степени считается высокой.

Функция принадлежности описывает степень принадлежности элемента к нечеткому множеству. Это функция, которая принимает значение от 0 до 1 в зависимости от входного параметра. Например, для нечеткого множества «высокие температуры» функция принадлежности может быть задана так, что температуры выше 30°C имеют высокую степень принадлежности (например, 0.9), тогда как температуры ниже 20°C имеют низкую степень принадлежности (например, 0.1).

Нечеткая логика включает в себя несколько ключевых операций, аналогичных классическим логическим операциям, но адаптированных для работы с нечеткими значениями:

1. **Нечеткая конъюнкция (AND):**
Операция нечеткой конъюнкции определяет степень истинности, когда обе условия истинны. Она обычно вычисляется как минимум из степеней принадлежности двух условий. Например, если степень принадлежности первого условия равна 0.7, а второго – 0.5, то степень принадлежности их конъюнкции будет 0.5.
2. **Нечеткая дизъюнкция (OR):**
Операция нечеткой дизъюнкции определяет степень истинности, когда хотя бы одно из условий истинно. Она вычисляется как максимум из степеней принадлежности двух условий. Например, если степень принадлежности первого условия равна 0.7, а второго – 0.5, то степень принадлежности их дизъюнкции будет 0.7.
3. **Нечеткое отрицание (NOT):**
Операция нечеткого отрицания определяет степень ложности условия. Она вычисляется как разность 1 и степень принадлежности условия. Например, если степень принадлежности условия равна 0.7, то степень отрицания этого условия будет 0.3.

Одним из ключевых применений нечеткой логики является управление сложными системами, где точные математические модели создать невозможно. Например, системы управления климатом в помещениях, регулирование скорости автомобилей или роботизированные системы управления полагаются на нечеткую логику для принятия решений в условиях изменяющихся данных.

Нечеткая логика также широко используется в искусственном интеллекте (ИИ) и машинном обучении. В отличие от традиционных алгоритмов, которые требуют четких данных и строгих правил, нечеткие алгоритмы могут работать с приблизительными или частичными данными, что делает их полезными для создания интеллектуальных систем.

В отличие от строго математических моделей, которые требуют точных входных данных, нечеткая логика ближе к человеческому мышлению, где решения часто принимаются

на основе приблизительных данных или субъективных суждений. Это делает её идеальной для систем, которые должны принимать решения в условиях неопределенности, таких как системы поддержки принятия решений, экспертные системы и ИИ-приложения.

Нечеткая логика может эффективно работать с «шумными» данными, то есть данными, которые содержат отклонения или погрешности. Это важно в реальных системах, где входные данные не всегда точны или корректны. Способность нечеткой логики сглаживать такие отклонения позволяет системам сохранять свою функциональность и адекватно реагировать на изменяющиеся условия.

Нечеткие системы относительно легко настраиваются благодаря использованию правил вида «если-то», что позволяет экспертам или разработчикам легко интерпретировать и изменять систему в зависимости от её требований. Например, для создания системы управления температурой можно установить правила типа «если температура высокая, то уменьшить мощность нагрева».

Хотя создание базовых правил нечеткой логики может показаться интуитивным, настройка сложных систем с большим количеством переменных и правил может стать трудоемкой задачей. Для того чтобы система работала эффективно, требуется значительное время для калибровки функций принадлежности и правильного выбора правил. Ошибки на этом этапе могут привести к некорректным результатам или недостаточной точности работы системы.

В крупных системах, где обрабатывается множество нечетких переменных, вычислительная сложность может значительно возрасти. Нечеткая логика требует расчетов для каждой переменной и функции принадлежности, что приводит к увеличению нагрузки на процессоры и замедлению работы системы. Это может стать критическим фактором для реальных приложений с ограниченными ресурсами, таких как встроенные системы или мобильные устройства.

Эффективность нечеткой системы во многом зависит от правильного выбора правил и функций принадлежности. Эти параметры обычно разрабатываются на основе экспертных знаний в конкретной области. В случаях, когда такие знания отсутствуют или не могут быть точно сформулированы, создание точной и надежной системы становится проблематичным.

Нечеткая логика хорошо подходит для задач, где требуется приближенное моделирование, но в некоторых случаях её использование может оказаться недостаточно точным. Например, в системах с очень строгими требованиями к точности или где существуют сложные нелинейные зависимости, нечеткая логика может оказаться менее эффективной по сравнению с традиционными методами, такими как нейронные сети или методы оптимизации.

В заключение необходимо отметить, что преимущества нечеткой логики, такие как гибкость, адаптивность и устойчивость к неопределенности, делают её мощным инструментом в ряде приложений. Однако для успешного применения необходимо учитывать её ограничения: сложность настройки и калибровки, высокие вычислительные затраты и зависимость от экспертных знаний. Важно правильно выбирать задачи для использования нечеткой логики, чтобы максимально эффективно использовать её возможности.

1. Development the information systems with fuzzy logic algorithms and network optimization / A. V. Sinitsyn, N. Yu. Lisay, S. A. Selivanov, A. A. Sinitsyn // *Информация и инновации*. – 2023. – Vol. 18, No. 2. – P. 33-47.
2. Арисов, А. М. Анализ принятия решений на основе нечеткой логики / А. М. Арисов // *Альманах научных работ молодых ученых Университета ИТМО, Санкт-Петербург, 03–06 февраля 2015 года. Том 1*. – Санкт-Петербург: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2015. – С. 38-39.
3. Ризванова, М. Т. Основы нечеткой логики : элективный курс по информатике / М. Т. Ризванова ; Ризванова М. Т.. – Москва : Перо, 2011. – 58 с.
4. Кравец, Е. В. Анализ понятия "нечеткая логика", методы и области применения нечеткой логики / Е. В. Кравец, О. С. Солодова // «Цифра» - реальность, меняющая мир: готовность российской экономики к новым правилам игры : Материалы Национальной научно-практической конференции, Москва, 23 апреля 2019 года. Том 13. – Москва: Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт «Центр», 2019. – С. 110-112.
5. Яхьяева, Г. Э. Теоретико-модельный подход к нечеткой логике / Г. Э. Яхьяева // *Альманах современной науки и образования*. – 2008. – № 12. – С. 252-255.

Коновалов Г.Г.**Реализация алгоритма критического пути***Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/trnio-10-2024-389

Аннотация

В статье рассматриваются алгоритмы критического пути (Critical Path Method, CPM) и их применение в управлении проектами и программировании. Описываются основные этапы выполнения алгоритма, такие как построение сетевой диаграммы, расчет ранних и поздних сроков выполнения задач, а также определение критического пути и временных резервов. Также обсуждается применение CPM в современных системах управления проектами и его влияние на управление ресурсами, сроками и рисками.

Ключевые слова: алгоритм критического пути, CPM, управление проектами, сетевая диаграмма, программирование, графы, временные резервы, оптимизация ресурсов.

Abstract

The article discusses critical path algorithms (Critical Path Method, CPM) and their application in project management and programming. It describes the main stages of the algorithm execution, such as building a network diagram, calculating early and late task deadlines, and determining the critical path and time reserves. It also discusses the application of CPM in modern project management systems and its impact on resource, deadline, and risk management.

Keywords: critical path algorithm, CPM, project management, network diagram, programming, graphs, time reserves, resource optimization.

Алгоритмы критического пути (Critical Path Method, CPM) играют ключевую роль в управлении проектами, где важно не только распределение ресурсов, но и соблюдение сроков выполнения задач. В условиях современного бизнеса, где время – один из самых ценных ресурсов, грамотное планирование и контроль за ходом выполнения проекта становятся важнейшими факторами успеха.

Алгоритм критического пути (Critical Path Method, CPM) – это метод планирования и управления проектами, который позволяет определить последовательность задач, имеющих наибольшее влияние на сроки завершения проекта. Критический путь – это последовательность зависимых задач, каждая из которых не имеет временного резерва. Это означает, что любая задержка выполнения задачи на критическом пути немедленно приводит к увеличению общей продолжительности проекта.

Основная цель CPM – выявить все возможные пути выполнения проекта и найти критический путь, то есть ту последовательность задач, выполнение которых требует наибольшего времени. На основе этого анализа можно:

- определить общую продолжительность проекта;
- найти задачи, выполнение которых можно отложить без ущерба для сроков проекта (задачи с временным резервом);
- обнаружить «узкие» места в плане и выделить задачи, которые требуют особого внимания и контроля.

Для применения CPM проект представляется в виде сетевой диаграммы, которая строится на основе следующих элементов:

- Вехи (events или milestones) – ключевые моменты в проекте, которые обозначают начало или окончание определённых этапов.
- Задачи (activities) – конкретные работы, которые необходимо выполнить. Каждая задача имеет свою продолжительность.
- Зависимости (dependencies) – связи между задачами, которые указывают, какие задачи должны быть завершены перед началом других.

В сетевой диаграмме задачи представляются в виде узлов, а зависимости между ними – в виде направленных рёбер. В результате получается ориентированный граф, где задачи идут последовательно или могут выполняться параллельно.

Алгоритм критического пути (СРМ) предполагает несколько ключевых этапов, которые позволяют определить критический путь и управлять проектом наиболее эффективно.

Построение сетевой диаграммы

Первым шагом является построение сетевой диаграммы проекта. Все задачи проекта представлены в виде узлов (вершин), а зависимости между ними – в виде стрелок (рёбер), которые указывают порядок выполнения задач. Задачи, связанные зависимостями, обозначают этапы, которые необходимо выполнить в определенной последовательности. Эта диаграмма служит базой для дальнейшего анализа и расчета сроков выполнения.

Расчет ранних сроков выполнения задач

На следующем этапе рассчитываются ранние сроки начала и окончания каждой задачи. Этот процесс выполняется путем обхода сетевой диаграммы от начала к концу проекта (прямой проход). Для каждой задачи вычисляется:

- Раннее начало (Early Start, ES) – самый ранний момент, когда задача может начаться, с учетом зависимостей.
- Раннее завершение (Early Finish, EF) – самый ранний момент, когда задача может быть завершена. Вычисляется по формуле:

$$EF = ES + \text{Продолжительность задачи}$$

Расчет поздних сроков выполнения задач

После определения ранних сроков выполнения осуществляется обратный проход (от конца к началу проекта) для вычисления поздних сроков:

- Позднее завершение (Late Finish, LF) – самый поздний момент, когда задача может быть завершена без задержки всего проекта.
- Позднее начало (Late Start, LS) – самый поздний момент, когда задача может начаться без сдвига графика проекта. Вычисляется по формуле:

$$LS = LF - \text{Продолжительность задачи}$$

Определение критического пути

Критический путь – это самая длинная последовательность задач, определяющая минимальное время завершения проекта. Этот путь включает задачи, у которых не остается резерва времени – любые задержки на этих задачах увеличат общую продолжительность проекта. Задачи, которые лежат на критическом пути, имеют равные значения ранних и поздних сроков начала и окончания.

Определение резерва времени для задач

Некритические задачи могут иметь временной резерв, то есть запас времени, который не приведет к сдвигу сроков всего проекта. Этот резерв (или «флоат») вычисляется как разница между поздними и ранними сроками:

$$\text{Резерв времени} = LS - ES$$

Если резерв больше нуля, задача может быть выполнена с небольшой задержкой без риска нарушения сроков всего проекта.

Алгоритм критического пути (СРМ) широко используется в программировании для решения задач, связанных с планированием, оптимизацией и управлением параллельными процессами. Для реализации этого алгоритма важно представить задачи проекта в виде графа, где узлы обозначают задачи, а рёбра – зависимости между ними. Такой подход позволяет моделировать последовательность операций, взаимодействие между задачами и находить оптимальные решения по времени выполнения.

Для представления проекта в виде графа используются различные структуры данных. Одной из самых удобных является ориентированный ациклический граф, где:

- Вершины (узлы) графа представляют задачи или этапы проекта.

- Ребра обозначают зависимости между задачами, указывая, какие задачи должны быть завершены до начала последующих.

Граф является ациклическим, так как в реальных проектах задачи не могут иметь циклических зависимостей (невозможно, чтобы задача зависела от завершения самой себя через цепочку других задач).

Для нахождения критического пути в графе используются известные алгоритмы работы с графами:

- Поиск в глубину (DFS). Этот метод позволяет обойти все вершины графа и найти возможные пути от начальной до конечной задачи. Однако для расчета критического пути этот метод используется в модифицированном виде.
- Топологическая сортировка. Этот алгоритм обеспечивает упорядочивание задач с учетом их зависимостей. Он позволяет вычислить последовательность выполнения задач, начиная с тех, которые не имеют предшественников. После топологической сортировки можно пройти по графу для вычисления ранних и поздних сроков выполнения задач.

Для реализации СРМ в программировании следует выполнить следующие шаги:

1. Представление задач и зависимостей. Проект и его задачи должны быть представлены в виде графа, где каждая задача имеет свои параметры (например, длительность) и зависимости от других задач.
2. Расчет ранних сроков выполнения. Алгоритм начинается с прямого прохода по графу, начиная с вершины, которая не имеет предшественников (например, начало проекта). Для каждой задачи рассчитываются ранние сроки её начала и завершения на основе зависимостей от предыдущих задач.
3. Расчет поздних сроков выполнения. После завершения прямого прохода выполняется обратный обход графа, начиная с последней задачи. На этом этапе вычисляются поздние сроки начала и завершения каждой задачи, что помогает определить, какие задачи имеют временной резерв.
4. Определение критического пути. После расчета ранних и поздних сроков выполнения задач можно найти критический путь. Задачи, у которых ранние и поздние сроки совпадают, входят в критический путь и требуют особого внимания, так как их задержка влияет на общий график проекта.

Алгоритмы критического пути могут применяться для оптимизации параллельных вычислений в программировании. Например, в системах многопоточности или распределённых вычислений задачи, которые могут выполняться параллельно, моделируются с помощью зависимостей на графе. Задачи, находящиеся на критическом пути, определяют время выполнения всей программы, и их выполнение нельзя отложить. Этот подход позволяет эффективно распределять ресурсы и управлять вычислительными процессами.

Программная реализация СРМ позволяет не только находить критический путь, но и выполнять оптимизацию проекта. На основе анализа можно принимать решения о перераспределении ресурсов, добавлении дополнительной рабочей силы или изменении последовательности выполнения задач, чтобы сократить общую продолжительность проекта.

В конечном результате применение алгоритма критического пути в программировании даёт возможность оптимально управлять сложными проектами, минимизировать временные задержки и эффективно использовать ресурсы.

В заключение необходимо отметить, что алгоритмы критического пути играют важную роль в эффективном управлении проектами, позволяя минимизировать задержки, оптимизировать распределение ресурсов и контролировать выполнение задач. Использование СРМ помогает определить ключевые этапы проекта, которые оказывают наибольшее влияние на сроки завершения, и сконцентрировать усилия на задачах, не имеющих временного резерва. Это особенно важно в сложных проектах с большим количеством зависимостей и ограниченными ресурсами.

Применение СРМ в программировании и системах управления проектами стало стандартом в различных отраслях – от строительства и производства до разработки программного обеспечения.

С развитием технологий перспективы использования алгоритмов критического пути продолжают расширяться. Более глубокая интеграция с искусственным интеллектом, прогнозная аналитика и автоматизация управления проектами обещают сделать СРМ ещё более мощным и гибким инструментом в будущем, способным улучшить эффективность работы и управление проектами на всех уровнях.

1. Врублевская, С. С. Алгоритм вычисления нечёткого критического пути / С. С. Врублевская, И. В. Федорова, Б. А. Шиянов // Вестник Воронежского государственного технического университета. – 2007. – Т. 3, № 7. – С. 113-116.
2. Быстров, А. И. О методах определения критического пути в транспортных задачах / А. И. Быстров, Р. З. Гильмутдинов // Вестник БИСТ (Башкирского института социальных технологий). – 2016. – № 1-2(30). – С. 126-131.
3. Плескунов, М. А. Задачи сетевого планирования: Учебное пособие / М. А. Плескунов. – Екатеринбург: Уральский федеральный университет, 2014.
4. Ширипурапу, А. Улучшение алгоритма Дейкстры для оценки характеристик и критического пути проекта / А. Ширипурапу, Р. Ш. Наупада, К. Ш. Рао // Надежность. – 2024. – Т. 24, № 2. – С. 16-23.
5. Сосина, Н. А. Пример оптимизации стоимости сетевого проекта / Н. А. Сосина, С. С. Маштаков // Информационные технологии в моделировании и управлении: подходы, методы, решения : Материалы VI Всероссийской научной конференции с международным участием, Тольятти, 18–20 апреля 2023 года. – Тольятти: Тольяттинский государственный университет, 2023. – С. 248-255.

Коновалов Г.Г.

Реализация транспортной задачи с применением методов линейного программирования

*Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/trnio-10-2024-390

Аннотация

В статье рассматривается реализация транспортной задачи с использованием методов линейного программирования. Описываются основные элементы задачи, приводится математическая модель, а также анализируются методы решения, в частности эвристический и венгерский методы. Представлен пример решения, демонстрирующий применение эвристического подхода для получения начального решения и возможности его оптимизации с помощью линейного программирования.

Ключевые слова: транспортная задача, линейное программирование, оптимизация, эвристический методы, венгерский метод, затраты на транспортировку, ресурсное распределение, математическая модель.

Abstract

The article discusses the implementation of a transport problem using linear programming methods. The main elements of the problem are described, a mathematical model is provided, and solution methods are analyzed, in particular the heuristic and Hungarian methods. An example solution is presented demonstrating the use of a heuristic approach to obtain an initial solution and the possibility of optimizing it using linear programming.

Keywords: transportation problem, linear programming, optimization, heuristic methods, Hungarian method, transportation costs, resource distribution, mathematical model.

Транспортная задача является одним из классических примеров задач линейного программирования. Её суть заключается в оптимизации процесса распределения ресурсов

между несколькими источниками и потребителями таким образом, чтобы минимизировать затраты на транспортировку. Это важная задача находит своё применение в логистике, экономике и планировании, она позволяет эффективно распределять товары, ресурсы или услуги с минимальными затратами на доставку.

Исходные данные задачи включают в себя количество ресурсов, доступных у каждого источника, объем потребностей каждого пункта назначения и стоимость перевозки единицы товара между каждым источником и потребителем.

Основные элементы транспортной задачи:

- Источники – пункты, из которых осуществляется отправка ресурсов. Каждый источник имеет определённый объём товара, который нужно доставить.
- Потребители – пункты назначения, в которые необходимо доставить определённое количество товара.
- Затраты на транспортировку – стоимость перевозки одной единицы товара из источника в конкретный пункт назначения.

Транспортная задача ставится с условием баланса, когда суммарный объём ресурсов, доступных у всех источников, равен суммарной потребности всех пунктов назначения. Это называется «условием баланса», и оно записывается как:

$$\sum_{i=1}^m a_i = \sum_{j=1}^n b_j$$

где a_i – это объём поставок из источника i , а b_j – объём потребностей потребителя j .

Если условие баланса не выполняется (т.е. общие поставки не равны общей потребности), транспортную задачу необходимо преобразовать в сбалансированную путём добавления фиктивного источника или потребителя с нулевыми затратами.

Цель задачи – найти такое распределение ресурсов, которое минимизирует общие затраты на транспортировку, при этом удовлетворяя ограничения по объёмам поставок и потребностей.

Математическая модель транспортной задачи представляет собой задачу линейного программирования, в которой требуется минимизировать затраты на транспортировку при соблюдении ограничений по объёмам поставок и потребностей.

Целью является минимизация общих затрат на перевозку товаров от источников к потребителям. Пусть c_{ij} – это стоимость перевозки единицы товара от источника i к потребителю j , x_{ij} – количество товара, транспортируемого от i к j . Тогда целевая функция, выражающая общие транспортные затраты, имеет вид:

$$Z = \sum_{i=1}^m \sum_{j=1}^n c_{ij} x_{ij}$$

где m – количество источников, а n – количество потребителей. Необходимо минимизировать величину Z , которая представляет собой общие затраты на транспортировку.

Модель включает два типа ограничений:

1. Ограничения по объёмам поставок. Каждый источник i может отправить не больше, чем его общий запас a_i . Это условие записывается так:

$$\sum_{j=1}^n x_{ij} \leq a_i, \quad \forall i = 1, 2, \dots, m$$

2. Ограничения по объёмам потребления. Каждый потребитель j должен получить точно b_j единиц товара. Это ограничение выглядит следующим образом:

$$\sum_{i=1}^m x_{ij} = b_j, \quad \forall j = 1, 2, \dots, n$$

Кроме того, переменные x_{ij} , которые представляют количество товара, не могут быть отрицательными:

$$x_{ij} \geq 0, \quad \forall i, j$$

Таким образом, математическая модель транспортной задачи включает минимизацию целевой функции с учётом ограничений по поставкам и потребностям.

Для решения транспортной задачи существуют различные подходы, среди которых наиболее популярны эвристический и венгерский методы.

Эвристические методы применяются для получения приближённого решения в случаях, когда требуется быстрое нахождение приемлемого результата. Одним из таких методов является метод «минимальной стоимости». Этот метод позволяет быстро распределить ресурсы, основываясь на простых правилах, не обязательно ведя к оптимальному решению, но давая хорошее начальное приближение для последующего уточнения.

Основная идея эвристических методов – начать с одного из источников или потребителей и постепенно распределять товары, минимизируя затраты на каждом шаге. Этот метод даёт базисное решение, которое затем можно улучшать с помощью более точных алгоритмов.

Венгерский метод является более точным и предназначен для решения задач распределения, таких как задача о назначениях, которая является частным случаем транспортной задачи с одинаковыми объёмами поставок и потребностей. Он основан на комбинаторных методах оптимизации и гарантирует нахождение оптимального решения.

Алгоритм венгерского метода включает следующие шаги:

1. Преобразование исходной матрицы затрат для упрощения поиска минимальных значений.
2. Поиск оптимального распределения с использованием чередующихся путей и дуг графа.
3. Итеративное улучшение решения до тех пор, пока не будет найдено минимальное общее значение затрат.

Оба метода могут использоваться для получения начального решения, которое затем можно уточнить с помощью методов линейного программирования. Линейное программирование обеспечивает точное нахождение глобального минимума затрат, учитывая все ограничения.

Рассмотрим небольшой пример транспортной задачи, в котором необходимо распределить товар от трёх источников к трём потребителям с минимальными затратами на транспортировку.

Таблица 1

Первоначальное состояние транспортной задачи.

Потребители	Потребитель 1	Потребитель 2	Потребитель 3	Запасы источника
Источник 1	8	6	10	20
Источник 2	9	12	13	30
Источник 3	14	9	16	25
Потребности	25	25	25	

Задача состоит в том, чтобы минимизировать общие затраты на транспортировку при следующих условиях:

- Запасы источников: 20, 30 и 25 единиц соответственно.
- Потребности потребителей: 25 единиц каждый.

Для начала воспользуемся «методом минимальной стоимости», чтобы найти приближённое решение. На каждом шаге будем выбирать ячейку с наименьшей стоимостью транспортировки и отправлять максимально возможное количество товара.

1. Минимальная стоимость – это 6 (источник 1 → потребитель 2). Отправляем максимум возможного (20 единиц, так как запас у источника 1 – 20). Теперь потребность потребителя 2 снизилась до 5 единиц, а у источника 1 больше нет запасов.
2. Следующая минимальная стоимость – это 9 (источник 3 → потребитель 2). Отправляем максимум возможного (25 единиц, полностью закрыв потребности потребителя 1). Запас у источника 3 теперь равен 0.
3. Потребность потребителя 1 (25 единиц) закрывается из источника 2 (стоимость – 9) и источника 3 (стоимость 14).
4. Потребителю 3 от источника 2 отправляется оставшиеся 10 единиц (стоимость – 13) и от источника 3 оставшиеся 15 единиц (стоимость 16).

Распределение товаров получилось следующим:

Таблица 2

Распределение товаров эвристическим методом.

Потребители	Потребитель 1	Потребитель 2	Потребитель 3	Запасы поставщиков
Источник 1	8	6*20	10	20-20=0
Источник 2	9*20	12	13*10	30-20-10=0
Источник 3	14*5	9*5	16*15	25-5-5-15=0
Потребности потребителей	25-20-5=0	25-20-5=0	25-10-15=0	

Общие затраты на транспортировку рассчитываем по формуле:

$$Z = (20 * 6) + (9 * 20) + (13 * 10) + (14 * 5) + (9 * 5) + (16 * 15) = 120 + 180 + 130 + 70 + 45 + 240 = 785$$

Таким образом, общие затраты на транспортировку составляют 785 единиц.

Полученное решение можно улучшить с помощью линейного программирования. Применяв венгерский метод, можно проверить, является ли это решение оптимальным или есть возможность снизить затраты. Однако для нашего небольшого примера решение эвристического метода уже близко к оптимальному.

В заключение необходимо отметить, что решение транспортной задачи с помощью линейного программирования является мощным и эффективным инструментом для оптимизации распределения ресурсов при минимальных затратах на транспортировку.

Эвристические методы, такие как метод минимальной стоимости, позволяют быстро получить начальное приближённое решение. Хотя этот метод не всегда дает оптимальный результат, он может быть полезен при необходимости быстрой оценки затрат. Более точные алгоритмы, такие как венгерский метод или методы линейного программирования, гарантируют нахождение оптимального решения и могут применяться для задач с любыми объемами поставок и потребностей.

1. Кокурин, Н. С. Решение транспортной задачи методом минимальной стоимости / Н. С. Кокурин // Актуальные проблемы эксплуатации автотранспортных средств – Владимир: Владимирский государственный университет имени Столетовых, 2023. – С. 46-50.
2. Онищук, А. И. Решение транспортной задачи методами линейного программирования / А. И. Онищук, Е. С. Каминская // Научно-техническое творчество аспирантов и студентов – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный технический университет, 2016. – С. 439-441.
3. Шипицына, Р. Е. Об алгоритме решения транспортной задачи линейного программирования / Р. Е. Шипицына // Техника и технологии наземного транспорта – Омск: Сибирский государственный автомобильно-дорожный университет (СибАДИ), 2022. – С. 70-75.
4. Лозгачев, И. А. Подход к решению классической транспортной задачи / И. А. Лозгачев, М. Ю. Корепанов // Уральская горная школа – Екатеринбург: Уральский государственный горный университет, 2016. – С. 191-192.

Кузнецов А.М.

Методы статистического анализа, используемые в информационно-аналитических системах социологических исследований

*Тамбовский государственный технический университет
(Россия, Тамбов)*

doi: 10.18411/trnio-10-2024-391

Аннотация

Статья посвящена рассмотрению особенностей применения методов статистического анализа в информационно-аналитических системах в процессе проведения социологических исследований. Детально описаны наиболее популярные методы и принципы их использования. Представлены результаты экспертного опроса, в рамках которого сравнивались методы статистического анализа с точки зрения их применимости при проектировании архитектуры информационно-аналитической системы.

Ключевые слова: статический анализ, социологические исследования, методы, информация, обработка, прогноз, параметры.

Abstract

The article is devoted to the consideration of peculiarities of application of statistical analysis methods in information-analytical systems in the process of sociological research. The most popular methods and principles of their use are described in detail. The results of an expert survey are presented, which compared the methods of statistical analysis from the point of view of their applicability in designing the architecture of information-analytical system.

Keywords: static analysis, sociological research, methods, information, processing, forecast, parameters.

Введение

Важнейшей особенностью социологического и статистического знания являются их актуальность и оперативность: социология и статистика являются науками, изучающими современную жизнедеятельность общества в контексте текущей ситуации.

Методы статистического анализа данных являются основными инструментами для исследования и понимания социологических процессов и применяются в информационно-аналитических системах (ИАС) для социологических исследований. Они помогают исследователям оперативно принимать обоснованные и актуальные выводы на основе эмпирических данных. Значимость каждого метода может варьироваться в зависимости от конкретного исследования и его конкретных потребностей [1,2].

Информационно-аналитическая система (ИАС) для социологических исследований – это программное обеспечение, предназначенное для сбора, анализа и интерпретации социологических данных. Эта система обычно включает в себя инструменты для проведения опросов, сбора данных, статистического анализа и визуализации результатов.

Методы статистического анализа

- **Дескриптивная статистика (Descriptive Statistics):** Этот метод используется для описания первичных данных, выявления степени достоверности результатов наблюдений и установлению закономерностей изучаемых явлений. Он включает расчет основных статистических характеристик, таких как среднее значение, медиана, стандартное отклонение и корреляция. Это не требует значительных вычислительных ресурсов. Методы дескриптивной статистики широко поддерживаются в программных инструментах и библиотеках, что обеспечивает удобство и совместимость при работе с ними. Эти методы редко применяют при обработке больших данных из-за необходимости выполнения вычислений на всем наборе данных. Множество

инструментов и библиотек (Excel, SPSS, R, Python и др.) доступно для выполнения основных статистических расчетов и представления результатов [3-5].

- **Инференциальная статистика (Inferential Statistics)** или статистика логического вывода применяется для формулировки выводов о генеральной совокупности на основе данных из выборки. Двумя основными типами статистических выводов являются оценка и проверка гипотез. Метод требует более сложных вычислений: статистические тесты гипотез (t-тесты, χ^2 – тесты), интервальные оценки, анализ дисперсии, регрессионный анализ. Метод более сложен для понимания и применения по сравнению с дескриптивной статистикой, но он широко поддерживается различными программными инструментами и библиотеками [6,7].
- **Множественный анализ соответствий (Multiple Correspondence Analysis, MCA):** Этот метод используется для исследования взаимосвязей между несколькими переменными, так как при анализе многомерных социологических данных традиционные методы параметрической статистики, как правило, оказываются неэффективными. Этот вид относится к методам предварительного, или разведочного (exploratory) анализа данных. В этом методе используется графическое представление данных (карты соответствия - correspondence map. Он позволяет анализировать связи и ассоциации между категориями переменных в таблицах сопряженности (двухмерных матрицах) или в виде графической диаграммы, что упрощает визуальное представление и понимание связей между категориями. [8-10].
- **Прогностическая или предикативная статистика (Predictive Analytics):** Этот метод позволяет прогнозировать будущие события и тренды на основе исторических данных с использованием распространенных прогностических математических моделей [11]. В работе [12] подробно описано развитие прогностических методов в социологических исследованиях. Прогностический вид анализа требует больших объемов информации высокой точности. Чем больше данных обрабатывается для построения прогноза, тем важнее точность информации. Предикативная аналитика включает следующие этапы: сбор данных, исследовательский анализ и предикативное моделирование. Наиболее известные прогностические модели, приведены ниже.
 - *Линейная регрессия:* исследует линейную связь между зависимой переменной и одной или несколькими независимыми переменными [13].
 - *Логистическая регрессия:* используется для прогнозирования бинарных или категориальных исходов, когда зависимая переменная является качественной или дискретной [13].
 - *Временные ряды:* анализируют временной компонент данных и используют прошлые значения для прогнозирования будущих. Некоторые из моделей временных рядов включают ARIMA (авторегрессия интегрированного скользящего среднего) и экспоненциальное сглаживание [14].
 - *Методы машинного обучения:* решающие деревья, случайный лес, градиентный бустинг позволяют обрабатывать сложные зависимости между переменными и предсказывать нелинейные решения, например для изучения динамических социальных процессов [15].
 - *Нейронные сети:* используются для прогнозирования и классификации на основе сложных взаимосвязей между переменными. Они позволяют обрабатывать большие объемы данных и выявлять скрытые

закономерности, что особенно важно при анализе социологических данных [16]. Преимущество нейронных сетей заключается в способности к обучению на основе данных и адаптации к изменениям в социальной среде. Однако, для обучения нейронной сети требуются большие объемы данных. Для подтверждения результатов, полученных с помощью нейронных сетей, необходимо проводить дополнительные социологические исследования.

- **Непараметрическая статистика (Nonparametric Statistics):** Этот метод используется, когда данные не соответствуют предположениям параметрической статистики. Он позволяет обрабатывать данные низкого качества, не требует определенной формы распределения данных и позволяет анализировать данные без предположения о параметрах закона распределения. Этот метод помогает выявить нелинейные связи между переменными, а также может работать с интервальными данными [17,18].
- **Разведочный анализ данных (Exploratory Data Analysis - EDA):** Этот метод включает визуальное и статистическое исследование данных для выявления шаблонов, отклонений или потенциальных корреляций в данных. Он часто применяется для выявления тенденций. EDA помогает исследователям получить первичное представление о данных и генерировать статистическую модель для верификации и дальнейшего анализа. Для целей разведочного анализа используют различные библиотеки R и Python [19,20], а также ПО для глубокой обработки и анализа структурированных данных, которое может объединять различные типы данных в сводных отчетах и эффективно визуализировать результат анализа (Tableau) [21,22].
- **Прескриптивный анализ (Prescriptive Analysis):** Этот метод используется для поиска оптимальных решений на основе анализа данных и моделирования. Это новый этап в развитии аналитики данных и заблаговременного оптимизированного принятия решений для повышения эффективности управленческих решений. Подробный обзор развития этого направления, классификация методов прогнозной аналитики и анализ примеров использования этого метода приведен в [23,24]. Прескриптивный анализ включает обработку данных, моделирование, оптимизацию и прогнозирование для поддержки принятия управленческих решений. ПО и библиотеки (пакеты Puomo в Python или IpSolve в R) представляют собой инструменты, которые обеспечивают возможности для построения и решения различных оптимизационных моделей (линейное, нелинейное, целочисленное и смешанное программирование), RapidMiner Studio - комплексная платформа для обработки данных с визуальным дизайном рабочих процессов [25].
- **Механистический анализ (Mechanistic Analysis):** Этот метод исследует причинно-следственные связи и механизмы, лежащие в основе явлений или процессов, анализируя взаимодействие между различными переменными и компонентами системы. Механистическое моделирование и анализ основаны на хорошем понимании функционирования системы, которое возникает на основе многолетнего контролируемого изучения стабильной системы посредством большого числа экспериментов [26]. Для моделирования и объяснения социальных механизмов пользуются различным математическим аппаратом: регрессионный анализ, многомерный статистический анализ (объединяет факторный анализ и множественную регрессию), байесовский анализ, модели выживаемости, логистическая регрессия, временные ряды и др., которые могут быть применены для механистического анализа в зависимости от конкретной ситуации и данных [27]. Для выполнения механистического анализа используются различные статистические и

аналитические программные пакеты и инструменты: SPSS, Stata, R, SAS, Python (библиотеки pandas, scikit-learn, statsmodels для проведения сложного статистического анализа и механистического моделирования).

Частота использования этих методов в социологических исследованиях может варьироваться в зависимости от конкретной области исследования, контекста и целей исследования. Однако, есть несколько факторов, которые могут объяснить частоту использования определенных методов:

Основополагающие принципы: Дескриптивная статистика и инференциальная статистика являются основополагающими принципами в статистическом анализе данных. Они используются для описания и свода данных, а также для формулировки выводов о популяции на основе выборки. Поэтому они широко применяются в большинстве социологических исследований.

Потребность в прогнозировании: В социологических исследованиях часто возникает потребность в прогнозировании будущих событий и трендов на основе исторических данных. Поэтому прогностическая статистика достаточно часто используется, так как позволяет исследователям делать предсказания на основе различных моделей и методов прогнозирования.

Развитие компьютерных технологий: с развитием компьютерных технологий и доступности программного обеспечения, множественный и исследовательский (EDA) анализ, прескриптивный анализ и механистический анализ становятся все более доступными и интегрируются в аналитический процесс. Они предоставляют возможности для более глубокого исследования данных, предсказаний, оптимальных рекомендаций и понимания причинно-следственных связей.

Проведен экспертный опрос, который позволил сравнить методы статистического анализа с точки зрения их применимости при проектировании архитектуры информационно-аналитической системы для социологических исследований по следующим параметрам:

Вычислительная сложность: оценка того, насколько каждый метод требует вычислительных ресурсов, таких как процессорное время и оперативная память или специализированные компьютерные алгоритмы.

Совместимость с программной средой: насколько каждый метод может быть реализован или применен с помощью существующих программных сред и библиотек.

Обработка больших объемов данных: способность каждого метода обрабатывать большие наборы данных или выполнить параллельные вычисления.

Поддержка программного обеспечения и библиотек: качество ПО и библиотек (распространение, наличие обновлений), сообщество пользователей, которые поддерживают эти методы статистического анализа.

Легкость использования и гибкость: легкость понимания, применения и настройки. Гибкость метода в отношении того, насколько его можно адаптировать к различным сценариям или настроить для специфических потребностей.

В экспертной оценке участвовали преподаватели вузов МИРЭА и ТГТУ, которые оценивали каждый показатель по 10-бальной шкале. Результаты оценки приведены в таблице 1.

Таблица 1

Сравнение методов статистического анализа.

Методы статистического анализа	Вычислительная сложность	Совместимость с программной средой	Обработка больших объемов данных	Поддержка ПО и библиотек	Легкость использования и гибкость	ИТОГ
Дескриптивная статистика	9	9	7,5	9,5	8,5	43,5
Инференциальная статистика	7	8,5	6,5	9	6,5	37,5
Множественный анализ соответствий	5	7	5,5	7	6	30,5

Прогностическая/ предикативная статистика	8	9	8,5	8	7,5	41
Непараметрическая статистика	7	8	7,5	8	7	37,5
Разведочный анализ данных (EDA)	8	8,5	7,5	8,5	8	40,5
Прескриптивный анализ	5	7	5	6,5	6	29,5
Механистический анализ по параметрам	5,5	5,5	4,5	5	4,5	25

Заключение

Как следует из анализа таблицы 1 высшие оценки получили методы: дескриптивная статистика, прогностическая/предикативная статистика и разведочный анализ данных (EDA). Таким образом, при разработке архитектуры ИАС социологических исследований необходимо использовать именно эти методы статистического анализа:

- для подсистемы обработки и анализа данных – методы дескриптивной статистики и разведочного анализа данных (EDA),
- для подсистемы проактивного прогнозирования – методы прогностической статистики.

1. Shrutika Sirisilla, "Effective Use of Statistics in Research – Methods and Tools for Data Analysis." Enago Academy. May 19, 2022. <https://www.enago.com/academy/statistics-in-research-data-analysis/>.
2. Кечина Е. А. Взаимодействие социологии и статистики: понятие и структура // Вестник РУДН. Серия: Социология. 2012. №2. URL: <https://cyberleninka.ru/article/n/vzaimodeystvie-sotsiologii-i-statistiki-ponyatie-i-struktura> (дата обращения: 27.12.2023).
3. Ильин В.П. Методические особенности применения дескриптивной статистики в медико-биологических исследованиях // Acta Biomedica Scientifica. 2013. №1 (89).
4. Аннаева М. Применение статистических методов для анализа данных в различных областях // Всемирный ученый. 2023. №9. URL: <https://cyberleninka.ru/article/n/primenenie-statisticheskikh-metodov-dlya-analiza-dannyh-v-razlichnyh-oblastyah> (дата обращения: 27.12.2023).
5. Zhang, Jin & Wang, Yanyan & Zhao, Yuehua & Cai, Xin. (2018). Applications of inferential statistical methods in library and information science. Data and Information Management. 2. 103-120. 10.2478/dim-2018-0007.
6. Adeyemi, T.O. (2009) Inferential Statistics for Social and Behavioural Research. Research Journal of Mathematics and Statistics, 1, 47-54. <https://pdfs.semanticscholar.org/1869/f09205ffbd289f838077c9180a6817491796.pdf>
7. C. A. Hesse, J. B. Ofofu, Statistical methods for the social sciences, 2017, Accra, Ghana, Akrong Publications Ltd. pp.105, ISBN: 978-9988-2-6060-6
8. Сажин Ю.В., Сарайкин Ю.В. Применение множественного анализа соответствий для исследования структуры научно-педагогических кадров исследовательского университета // Вестник НГУЭУ. 2012. №3. URL: <https://cyberleninka.ru/article/n/primenenie-mnozhestvennogo-analiza-sootvetstviy-dlya-issledovaniya-struktury-nauchno-pedagogicheskikh-kadrov-issledovatel'skogo-universiteta> (дата обращения: 27.12.2023).
9. Blasius J. Correspondence Analysis in Social Science Research / Correspondence Analysis in the Social Sciences (pp.23-52). San Diego, CA: Academic Press. 1994
10. Жучкова С. В., Ротмистров А. Н. Поиск многомерной связи категориальных признаков: сравнение CHAID, логлинейного анализа и множественного анализа соответствий // Мониторинг общественного мнения: Экономические и социальные перемены. 2019. № 2. с. 32—53. <https://doi.org/10.14515/monitoring.2019.2.02>.
11. Шляпентох В. Э. Проблемы качества социологической информации: достоверность, репрезентативность, прогностический потенциал, М., ЦСП, 2006, сс. 547-598
12. Chen, Y., Wu, X., Hu, A. et al. Social prediction: a new research paradigm based on machine learning. J. Chin. Sociol. 8, 15 (2021). <https://doi.org/10.1186/s40711-021-00152-z>
13. Корн, Г. А. Справочник по математике для научных работников и инженеров. Определения, теоремы, формулы Пер. со 2-го амер. перераб. изд. И. Г. Арамановича и др.; Под общ. ред. И. Г. Арамановича. - 5-е изд. - М.: Наука, 1984. - 831 с. ил.
14. Vasileiadou E. and Vliegthart R. (2013), "Studying dynamic social processes with ARIMA modelling", International Journal for Social Research Methodology, DOI: 10.1080/13645579.2013.81625

15. Colbaugh, Richard & Glass, Kristin & Bauer, Travis. (2012). Leveraging Sociological Models for Predictive Analytics, URL: https://www.researchgate.net/publication/234005594_Leveraging_Sociological_Models_for_Predictive_Analytics, (дата обращения: 27.12.2023).
16. Di Franco, G., Santurro, M. Machine learning, artificial neural networks and social research. Qual Quant 55, 1007–1025 (2021). <https://doi.org/10.1007/s11135-020-01037-y>
17. Орлов А.И. Современное состояние непараметрической статистики // Научный журнал КубГАУ. 2015. №106. URL: <https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-neparametricheskoy-statistiki> (дата обращения: 27.12.2023).
18. Nikitina M.A., Chernukna I.M. Methods for nonparametric statistics in scientific research. Overview. Part 1. // Теория и практика переработки мяса. 2021. №2. URL: <https://cyberleninka.ru/article/n/methods-for-nonparametric-statistics-in-scientific-research-overview-part-1> (дата обращения: 27.12.2023).
19. Пономарев Д.С. Иерархическая кластеризация на языке R для производственно-экономических показателей пенитенциарной системы // Экономика. Информатика. 2023. №3. С. 34-39.
20. Григорьев Е.А., Климов Н.С. Разведочный анализ данных с помощью Python // E-Scio. 2020. №2 (41). URL: <https://cyberleninka.ru/article/n/razvedochnyy-analiz-dannyh-s-pomoschyu-python> (дата обращения: 29.12.2023).
21. Захарова А.А., Подвесовский А.Г., Лагереv Д.Г. Визуальная аналитика и когнитивные методы для обработки и анализа гетерогенных данных мультисенсорных систем: проблемы и тенденции // Информационные и математические технологии в науке и управлении. 2019. № 4 (16). С. 6074. DOI: 10.25729/2413-0133-2019-4-05
22. Багутдинов Р.А., Саргсян Н.А., Краснопахтыч М.А. 2020. Аналитика, инструменты и интеллектуальный анализ больших разнородных и разномасштабных данных. Экономика. Информатика. 47 (4): 792–802. DOI 10.18413/2687-0932-2020-47-4-792-802.
23. K. Lepenioti, A. Bousdekis, D. Apostolou, G. Mentzas, Prescriptive analytics: Literature review and research challenges, International Journal of Information Management, Volume 50, 2020, pp. 57-70, <https://doi.org/10.1016/j.ijinfomgt.2019.04.003>.
24. Selvaraj, Poornima & Marudappa, Pushpalatha. (2020). A survey on various applications of prescriptive analytics. International Journal of Intelligent Networks. 1. 76-84. 10.1016/j.ijin.2020.07.001.
25. S. Porritt Top Prescriptive Analytics Tools & Software (05.07.2023), URL: <https://technologyadvice.com/blog/business-intelligence/prescriptive-analytics-tools/>, (дата обращения: 29.12.2023)
26. Carl Anderson, Creating a Data-Driven Organization, Ch.5. Data Analysis, 2015, O'Reilly Media, Inc. ISBN: 9781491916919.
27. Holme P. and Liljeros F. (2015) Mechanistic models in computational social science. Front. Phys. 3:78. doi: 10.3389/fphy.2015.00078

Кулешова И.А., Соколов И.В.

Изучение методов увеличения качества изображений

*Московский государственный технический университет им. Н.Э. Баумана
(Россия, Москва)*

doi: 10.18411/trnio-10-2024-392

Аннотация

В данном исследовании рассматривались 3 метода улучшения качества изображений: метод ближайшего соседа, бикубическая интерполяция и интерполяция Ланцоша. Для наглядной демонстрации разницы работы алгоритмов было создано веб-приложение Image Transformer. По обработанным фотографиям было проведено сравнение, сделаны выводы.

Ключевые слова: улучшение изображений, интерполяция, сэмплы, линейная интерполяция, бикубическая интерполяция, интерполяция Ланцоша, качество изображения, веб-приложение, Go, Javascript.

Abstract

In this study, 3 methods of image enhancement were considered: nearest neighbour method, bicubic interpolation and Lanzos interpolation. Image Transformer web application was created to demonstrate the difference in the performance of the algorithms. Comparison was made on the processed photographs and conclusions were drawn.

Keywords: image enhancement, interpolation, samples, linear interpolation, bicubic interpolation, Lanzos interpolation, image quality, web application, Go, Javascript.

Введение

Изображения играют важнейшую роль в нашей жизни, служа средством коммуникации, документирования и выражения эмоций. С появлением цифровых технологий изображения стали неотъемлемой частью нашего повседневного опыта, используемые во всем, от социальных сетей и онлайн-новостей до научных исследований и медицинской диагностики. Однако зачастую мы сталкиваемся с изображениями низкого качества, размытыми и уменьшенными в размерах, оригиналы которых недоступны или утрачены. Обработка изображений предоставляет исследователям ценные инструменты для улучшения качества изображений, расширения их использования и раскрытия скрытых деталей.

Одной из важных задач обработки изображений является улучшение качества изображений, которое включает изменение его пространственного разрешения для улучшения возможности различения определенных деталей. В случае наиболее часто встречающихся цифровых растровых изображений эта задача формулируется как изменение числа пикселей растра, называемое также передискретизацией, а в случае увеличения разрешения – интерполяцией. Существуют различные методы интерполяции, такие как интерполяция по методу ближайшего соседа, бикубическая интерполяция и интерполяция Ланцоша.

Цель этой статьи - исследовать принципы работы этих методов интерполяции и сравнить их эффективность на практике для различных типов изображений. Мы рассмотрим преимущества и недостатки каждого метода и выявим категории задач, в которых каждый из них наиболее подходит.

Основная часть

Интерполяция - это процесс оценки значений в промежуточных точках на основе известных значений в дискретных точках. В контексте изображений дискретные точки соответствуют пикселям. Интерполяция позволяет создавать новые изображения с более высоким разрешением, чем исходные, заполняя пробелы между существующими пикселями. Применение изменения размера изображения может происходить в более широких сценариях: транслитерация изображения, коррекция искажений объектива, изменение перспективы и поворот изображения. Результаты изменения размера сильно различаются в зависимости от типа используемого алгоритма интерполяции.

Следовательно, для более качественного сравнения различных методов интерполяции изображений нужно понять, что же представляет из себя интерполяция более детально. Для этого рассмотрим одномерный сигнал, дискретизируемый с фиксированным интервалом (рис. 1):

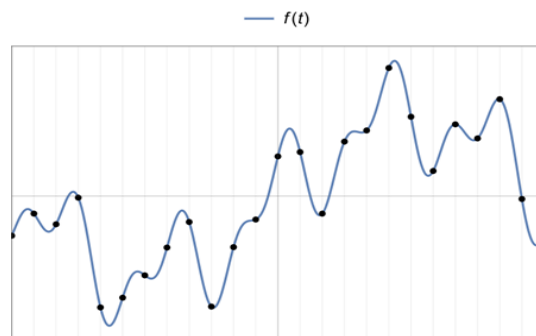


Рисунок 1. Одномерный сигнал, дискретизируемый с фиксированным интервалом.

Такой сигнал, из которого берутся сэмплы [4] (дискретные значения в данном случае), будем называть исходным. Теперь изобразим линейную интерполяцию для данного исходного сигнала (рис. 2):

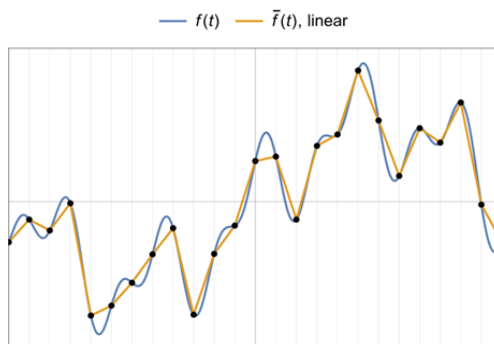


Рисунок 2. Линейная интерполяция для исходного сигнала.

Линейная интерполяция просто соединяет сэмплы прямыми линиями, что показано на рис. 2, следовательно, чем больше сэмплов выбрано, тем лучше будет работать интерполяция. Однако, это не единственный способ улучшить результат интерполяции. Существуют и другие методы интерполяции, которые используют функциональную зависимость [5] между сэмплами. Например, кубическая интерполяция [1] подбирает полином третьей степени между каждой точкой и обеспечивает более плавную интерполяцию (рис. 3):

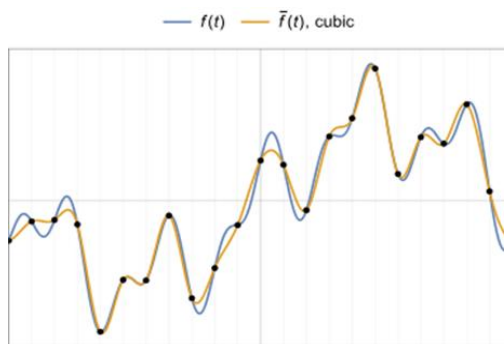


Рисунок 3. Кубическая интерполяция для исходного сигнала.

Но изображения являются двумерными сигналами, требующими более сложных методов интерполяции. Таким образом, двумерная интерполяция осуществляется путем последовательного применения одномерной интерполяции вдоль каждой оси. Для сравнения на рисунки ниже показаны сначала линейная интерполяция, как пример для одномерного сигнала (рис. 4):

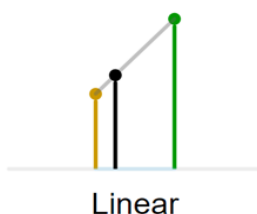


Рисунок 4. Линейная интерполяция.

а затем билинейная интерполяция, как пример для двумерной интерполяции (рис. 5):



Рисунок 5. Билинейная интерполяция.

На данных картинках дискретные сэмплы окрашены, а интерполированные точки черные.

Таким образом, мы рассмотрели принципы интерполяции.

Теперь рассмотрим один из простейших методов интерполяции для изображений: интерполяцию по методу ближайшего соседа. Вместо того, чтобы вычислять среднее значение по каким-либо весовым критериям или генерировать промежуточное значение на основе сложных правил, этот метод просто определяет «ближайший» соседний пиксель и предполагает его значение интенсивности. В результате каждый пиксель просто становится больше.

Сначала рассмотрим это в одномерном случае (рис. 6):

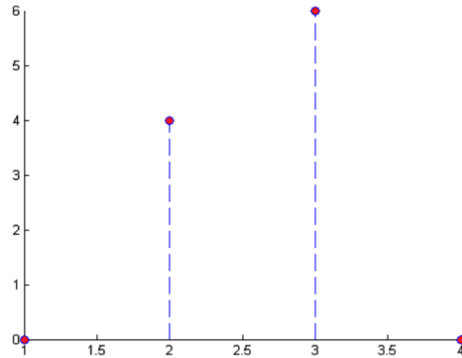


Рисунок 6. Одномерный случай интерполяции по методу ближайшего соседа.

Допустим, мы хотим вставить больше точек данных между точками $x_1 = 2$ и $x_2 = 3$, которые аппроксимируют значения между ними, которые находятся в диапазоне от $f(x_1) = 4$ до $f(x_2) = 6$. Используя интерполяцию ближайшего соседа, наш результат будет выглядеть так:

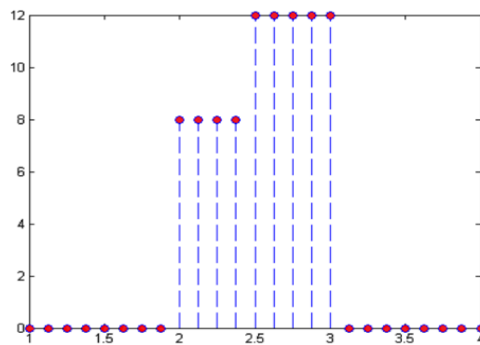


Рисунок 7. Одномерная интерполяция по методу ближайшего соседа.

Выше мы видим, что для каждой точки данных x_i , между нашими исходными точками данных x_1 и x_2 , мы присваиваем им значение $f(x_i)$ на основе того, какая из исходных точек данных была ближе вдоль горизонтальной оси.

Расширяя это на двумерный случай (рис. 8), мы можем изменить размер изображения путем интерполяции пикселей:

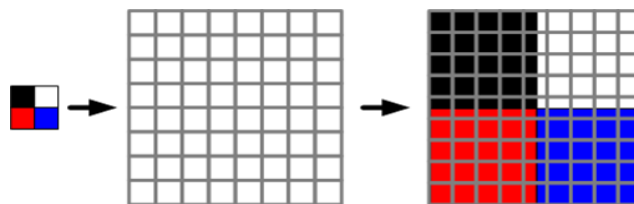


Рисунок 8. Двумерная интерполяция по методу ближайшего соседа.

Теперь рассмотрим чуть более сложный метод интерполяции – бикубическую интерполяцию.

Ранее на рисунке была показана билинейная интерполяция. Бикубическая интерполяция же идёт на один шаг дальше билинейной, рассматривая массив из 4×4 окружающих пикселей — всего 16. Поскольку они находятся на разных расстояниях от неизвестного пикселя, ближайшие пиксели получают при расчёте больший вес. [2] Бикубическая интерполяция производит значительно более резкие изображения, чем интерполяция по методу ближайшего соседа и билинейная, и возможно, является оптимальной по соотношению времени обработки и качества на выходе. По этой причине она стала стандартной для многих программ редактирования изображений (включая Adobe Photoshop), драйверов принтеров и встроенной интерполяции камер.

В вычислительной математике бикубическая интерполяция - расширение кубической интерполяции на случай функции двух переменных, значения которой заданы на двумерной регулярной сетке. Поверхность, полученная в результате бикубической интерполяции, является гладкой функцией, в отличие от поверхностей, полученных в результате билинейной интерполяции или интерполяции методом ближайшего соседа (рис. 9):

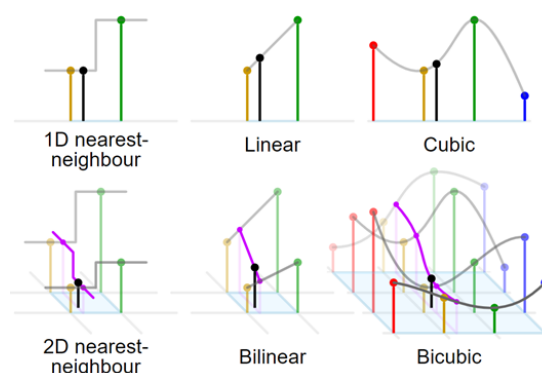


Рисунок 9. Сравнительное изображение различных одномерных и двумерных интерполяций.

А теперь рассмотрим наиболее сложный в математическом плане метод интерполяции – интерполяцию Ланцоша. Данный метод основан на способе математической обработки данных, называемом фильтром Ланцоша. Назван в честь предложившего этот метод обработки данных венгерского учёного Корнелия Ланцоша.

Метод связан с оконной функцией Ланцоша, $L_w(x)$, представляющей собой главный лепесток функции $\text{sinc}(x)$, вне этого лепестка оконная функция равна нулю:

$$L_w(x) = \text{sinc}(x/a).$$

Идея фильтра основана на применении нормированной функции $\text{sinc}(x) = \sin(\frac{f_0}{\pi} x) / \pi x$ с растянутым по оси x главным лепестком и равной нулю вне заданного параметром ширины a интервала. Применение этого фильтра позволяет добиться высокой чёткости изображения, но при обработке возможно появление нежелательных артефактов: появлению вокруг контрастных переходов ярких узких контрастных ореолов, что позволяет сохранить резкость контрастных линий при сохранении достаточной гладкости тональных переходов. Возникновение ореолов обусловлено тем, что при значении параметра $a > 1$ ядро Ланцоша принимает отрицательные значения при некоторых значениях аргумента. Поэтому обработанный сигнал может принимать даже отрицательные значения при положительных значениях выборок.

Фильтр можно применять с различными значениями ядра [3]. Если при билинейном интерполировании для каждого нового пикселя мы рассматривали 4 исходных пикселя, то теперь их может быть 9 (3×3), 25 (5×5), 49 (7×7) и т. д. Оптимальными по качеству и скорости являются размеры 2 и 3.

Для наглядного сравнения данных алгоритмов было создано веб-приложение Image Transformer с бэкендом на языке Go и фронтендом на Javascript (рис. 10). Оно позволяет преобразовать изображение, используя 3 предложенных выше метода: метод ближайшего соседа, бикубический метод или метод Ланцоша.

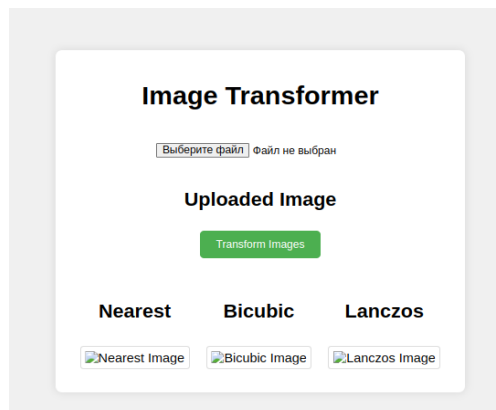


Рисунок 10. Веб-приложение Image Transformer для увеличения качества изображений.

Проверим разницу с помощью веб-приложения. Возьмем фотографию ткани.

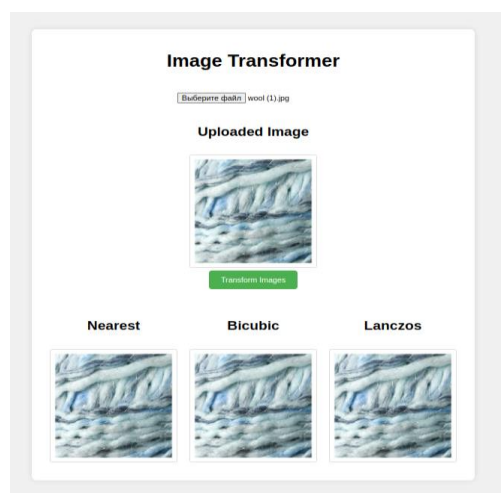


Рисунок 11. Демонстрация работы веб-приложения.

Увеличим изображения, полученные после обработки тремя методами, и сравним качество увеличенных изображений (рис 12). Видны явные различия: менее качественное приближение у метода ближайшего соседа - видны “ступеньки” и резкие переходы, бикубическая интерполяция и интерполяция Ланцоша дают более плавные переходы между пикселями.

Аналогичный результат виден и на обработанной фотографии пирожных (рис. 13).



Рисунок 12. Часть фотографии с изображением шерсти после работы алгоритмов.



Рисунок 13. Часть фотографии с изображением пирожных после работы алгоритмов.

Заключение

Таким образом, были рассмотрены 3 метода: метод ближайшего соседа, бикубическая интерполяция и интерполяция Ланцоша. С помощью веб-приложения наглядно были показаны явные различия алгоритмов в обработке изображений.

1. <https://mazzo.li/posts/lanczos.html>
2. <https://www.geeksforgeeks.org/python-opencv-bicubic-interpolation-for-resizing-image/>
3. https://en.wikipedia.org/wiki/Lanczos_resampling
4. К. Ланцош Практические методы прикладного анализа - М.: Государственное издательство физико-математической литературы, 1961. - 525 с.
5. Привалов А. А. Теория интерполирования функций - Саратов: Издательство саратовского университета, 1990. - 196 с.

Лепиев Д.Р., Гайрабеков А.У., Магомадов Ш.А.

Понятие и сущность банкротства предприятий

ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)

doi: 10.18411/trnio-10-2024-393

Аннотация

Банкротство представляет собой юридически оформленный процесс признания неспособности должника удовлетворить требования кредиторов по обязательным платежам. В экономическом контексте банкротство свидетельствует о критическом финансовом состоянии предприятия, при котором оно не может исполнять свои долговые обязательства. Рассмотрим более детально понятие и критерии банкротства.

Ключевые слова: банкротство, экономика, рассрочка, кредит, задержка платежей.

Abstract

Bankruptcy is a legally formalized process of recognizing the debtor's inability to satisfy creditors' claims for mandatory payments. In an economic context, bankruptcy indicates the critical financial condition of an enterprise, in which it cannot fulfill its debt obligations. Let's take a closer look at the concept and criteria of bankruptcy.

Keywords: bankruptcy, economy, installment plan, loan, payment delay.

В современных условиях нестабильной экономической ситуации и высокой конкуренции вопрос оценки вероятности банкротства предприятий приобретает особую актуальность. Своевременное выявление признаков финансовой неустойчивости и риска банкротства позволяет руководству компаний принимать обоснованные управленческие решения для предотвращения кризисной ситуации и восстановления платежеспособности.

Существует множество методик и моделей для оценки вероятности банкротства предприятий, основанных на анализе различных финансовых показателей. Однако их применение зачастую требует значительных временных и трудовых затрат на сбор и обработку данных, а также проведение расчетов. В этой связи автоматизация процесса оценки банкротства с использованием специализированных программных средств становится актуальной задачей.

Одним из наиболее распространенных и доступных инструментов для автоматизации различных процессов является Microsoft Excel с возможностью создания макросов на языке Visual Basic for Applications (VBA). Разработка макроса для автоматизированной оценки банкротства предприятий в среде MS Excel позволит существенно сократить время и упростить процедуру анализа финансового состояния компаний.

Банкротство — это финансовое состояние предприятия или физического лица, при котором сумма обязательств превышает стоимость активов, и должник не способен погасить свои долговые обязательства. В юридическом смысле банкротство признается судом и может завершиться ликвидацией предприятия или реструктуризацией долгов.

Основными признаками банкротства являются:

Неспособность своевременно выполнить обязательства перед кредиторами.

Отрицательная чистая стоимость активов.

Систематическая задержка платежей по долгам.

Критерии банкротства

Существуют различные критерии для определения банкротства, которые можно разделить на юридические и экономические.

Юридические критерии

Юридические критерии банкротства определяются законодательством конкретной страны и включают в себя следующие ключевые аспекты:

Просрочка платежей по обязательствам: если должник не выполняет свои финансовые обязательства в течение установленного срока (обычно от трех месяцев и более), это может быть основанием для признания его банкротом.

Размер задолженности: законодательством могут быть установлены минимальные суммы задолженности, превышение которых дает основания для инициации процедуры банкротства.

Решение суда: официальное признание банкротства происходит через судебное разбирательство, по результатам которого может быть принято решение о начале процедуры банкротства.

Экономические критерии

Экономические критерии включают анализ финансового состояния предприятия на основе различных показателей и коэффициентов:

Коэффициент текущей ликвидности: показывает способность предприятия покрывать краткосрочные обязательства за счет оборотных активов. Низкий коэффициент указывает на риск неплатежеспособности. Коэффициент финансовой устойчивости: отношение собственного капитала к заемным средствам. Высокий уровень задолженности по сравнению с собственными средствами свидетельствует о высоком риске банкротства. Анализ движения денежных средств: регулярный дефицит денежных средств для покрытия операционных расходов может указывать на потенциальное банкротство.

Модель Альтмана: один из наиболее известных методов прогнозирования банкротства, включающий анализ нескольких финансовых показателей и вычисление Z-коэффициента, который позволяет оценить вероятность банкротства предприятия. Каждый из этих критериев предоставляет важную информацию о финансовом состоянии предприятия и помогает вовремя выявить признаки финансовых трудностей. Понятие и критерии банкротства являются основополагающими элементами для понимания процесса признания несостоятельности предприятия. Юридические и экономические аспекты банкротства помогают комплексно оценить финансовое состояние организации и принять обоснованные решения для предотвращения или управления процессом банкротства. В дальнейшем исследовании будут рассмотрены методы оценки банкротства, а также возможности их автоматизации с помощью макросов в MS Excel. Банкротство предприятий может быть вызвано различными факторами, как внешними, не зависящими от деятельности самой компании, так и внутренними, связанными с ошибками в управлении и организации бизнес-процессов. Рассмотрим основные причины возникновения банкротства более подробно.

Внешние причины:

1. Экономические кризисы и спады в экономике. В период экономического кризиса снижается покупательская способность населения, падает спрос на товары и услуги, что негативно сказывается на финансовом состоянии многих предприятий.
2. Изменения в законодательстве и нормативно-правовом регулировании. Ужесточение требований, введение новых налогов и сборов могут привести к росту издержек и снижению прибыльности бизнеса.
3. Усиление конкуренции на рынке. Появление новых игроков, более эффективных технологий или продуктов у конкурентов может привести к оттоку клиентов и потере доли рынка.
4. Форс-мажорные обстоятельства (стихийные бедствия, военные конфликты, эпидемии и т.д.), которые могут нарушить производственные и логистические процессы компании.

Внутренние причины:

1. Неэффективное управление и стратегические ошибки руководства. Отсутствие четкой стратегии развития, просчеты в инвестиционной и маркетинговой политике, неспособность адаптироваться к изменениям рынка.
2. Низкая рентабельность и убыточность основной деятельности. Если предприятие работает с низкой маржинальностью или вообще несет убытки, рано или поздно оно столкнется с проблемами платежеспособности.
3. Чрезмерная закредитованность и неэффективное управление оборотным капиталом. Высокая долговая нагрузка, особенно при недостатке ликвидных активов, может привести к неспособности обслуживать кредиты и накапливанию просроченной задолженности.
4. Низкая квалификация персонала и ошибки в производственных процессах. Некачественная продукция, брак, простои производства ведут к дополнительным издержкам и потерям прибыли.
5. Недостатки в системе внутреннего контроля и учета. Отсутствие должного контроля за движением финансовых потоков и активов компании может привести к хищениям и злоупотреблениям.

Зачастую банкротство является следствием совокупности нескольких факторов, как внешних, так и внутренних. Своевременное выявление негативных тенденций и принятие соответствующих мер позволяет предотвратить наступление банкротства предприятия.

Заключение

Методы оценки банкротства предприятия варьируются от качественных экспертных оценок до сложных количественных моделей. Использование различных методов позволяет получить всестороннюю картину финансового состояния предприятия и сделать более точные прогнозы о его платежеспособности. В рамках данной дипломной работы особое внимание будет уделено разработке автоматизированного инструмента для оценки банкротства на основе количественных методов, что позволит значительно упростить и ускорить процесс анализа.

1. Федеральный закон "О несостоятельности (банкротстве)" от 26.10.2002 N127-ФЗ.
2. Альтман Э.И. Финансовые критерии прогнозирования угрозы банкротства // США: экономика, политика, идеология. - 1972. - № 5.
3. Терехин В.И. Финансовый менеджмент: учебное пособие. - М.: ИНФРА М, 2019.
4. Шеремет А.Д., Негашев Е.В. Методика финансового анализа деятельности коммерческих организаций. - М.: ИНФРА-М, 2021.
5. Бланк И.А. Основы финансового менеджмента. - М.: Эльга, Ника-Центр, 2018.

Логачев В.О., Лобанов Е.Г., Нагиева А.С., Семиколеннов С.А., Французова Н.Н.
**ИТ-образование: как изменяются подходы к обучению
в сфере технологий и программирования**

*Поволжский государственный университет телекоммуникаций и информатики
(Россия, Самара)*

doi: 10.18411/trnio-10-2024-394

Аннотация

В статье рассмотрены современные изменения в подходах к ИТ-образованию, связанные с развитием технологий, цифровизацией и изменяющимися потребностями рынка труда. Проанализированы тенденции в обучении программированию и внедрение новых образовательных форматов, таких как гибридное и дистанционное обучение, микрокурсы и самообучающиеся платформы. Обсуждается роль практико-ориентированного подхода, интерактивных методов обучения и международных образовательных стандартов в подготовке ИТ-специалистов. Особое внимание уделено влиянию искусственного интеллекта и машинного обучения на процесс обучения и разработке персонализированных образовательных траекторий.

Ключевые слова: ИТ-образование, программирование, цифровизация, гибридное обучение, дистанционное обучение, самообучение, искусственный интеллект, образовательные технологии, образовательные платформы, практико-ориентированное обучение.

Abstract

The article examines modern changes in approaches to IT education, driven by technological advancements, digitalization, and the evolving needs of the labor market. It analyzes trends in programming education and the introduction of new educational formats, such as hybrid and distance learning, microcourses, and self-learning platforms. The role of practice-oriented approaches, interactive teaching methods, and international educational standards in preparing IT specialists is discussed. Special attention is given to the impact of artificial intelligence and machine learning on the learning process and the development of personalized educational pathways.

Keywords: IT education, programming, digitalization, hybrid learning, distance learning, self-learning, artificial intelligence, educational technologies, educational platforms, practice-oriented learning.

Введение

Современный мир быстро изменяется под влиянием технологий, и образование в сфере ИТ становится одной из ключевых областей, требующих адаптации к новым вызовам. Технологии и программирование являются основой цифровой трансформации, которая затрагивает все сферы человеческой деятельности. Это ставит перед системой образования новые задачи по подготовке специалистов, способных эффективно работать в условиях постоянно меняющегося технологического ландшафта. В данной статье рассматриваются изменения в подходах к ИТ-образованию, вызванные цифровизацией, новыми требованиями рынка труда и инновационными образовательными технологиями.

Основные изменения в подходах к ИТ-образованию

Гибридные и дистанционные форматы обучения

С развитием технологий, особенно в условиях пандемии COVID-19, дистанционные и гибридные формы обучения стали обязательной частью образовательного процесса. В ИТ-образовании эти форматы проявили особую эффективность, поскольку позволяют студентам осваивать материал в удобном темпе и на практике применять полученные знания. Онлайн-платформы, такие как Coursera, edX, и Udemu, предоставляют доступ к курсам ведущих университетов мира, что позволяет расширить возможности для самообучения.

Преимущества гибридного и дистанционного обучения включают гибкость в выборе времени и места обучения, возможность для студентов из разных стран получать образование у

лучших преподавателей, доступ к разнообразным учебным материалам и ресурсам. Эти форматы также поддерживают взаимодействие между студентами и преподавателями через цифровые платформы. Особенно эффективным гибридное обучение оказалось в высшем образовании, где оно позволяет сочетать традиционные методы обучения с современными цифровыми инструментами.

Персонализированное обучение и искусственный интеллект

Искусственный интеллект (ИИ) активно внедряется в образовательные системы, предлагая персонализированные траектории обучения, адаптированные к уровню подготовки и потребностям каждого студента. Такие технологии позволяют автоматически анализировать успехи обучающихся и предоставлять индивидуальные рекомендации для дальнейшего изучения тем.

Применение ИИ в IT-образовании помогает не только в автоматизации проверочных заданий и оценок, но и в разработке адаптивных образовательных программ, учитывающих сильные и слабые стороны студентов. Например, платформы, использующие ИИ, могут предлагать дополнительные задания для закрепления знаний или адаптировать сложность материалов под текущий уровень подготовки студента. Кроме того, такие системы помогают сократить разрыв между теорией и практикой за счет внедрения практических заданий, моделирующих реальные задачи из сферы программирования и разработки.

ИИ также позволяет проводить оценку больших массивов данных об обучении студентов, выявляя типичные ошибки и проблемные зоны. Это дает преподавателям возможность более эффективно работать с каждым учеником, предлагая персонализированные рекомендации и корректируя образовательные траектории. Применение ИИ способствует созданию обучающих платформ, которые не только передают знания, но и помогают глубже понять их применение на практике.

Практико-ориентированное обучение

Одной из ключевых тенденций в IT-образовании является переход от теоретических знаний к практико-ориентированному подходу. Традиционные лекции все чаще заменяются интерактивными форматами, такими как проектное обучение, хакатоны и работа в командах над реальными проектами. Это способствует развитию у студентов критического мышления, умения решать сложные задачи и работать в условиях неопределенности.

Практико-ориентированный подход включает использование проектных задач, отражающих реальные потребности бизнеса. Например, работа над проектами для заказчиков из индустрии позволяет студентам не только применять знания, но и получать навыки взаимодействия с клиентами, управления проектами и работы в команде. Это значительно повышает качество подготовки специалистов и их готовность к профессиональной деятельности. Многие образовательные программы в IT-сфере уже активно внедряют подобные методы, делая акцент на практическом опыте, который студенты получают во время обучения.

Микрообучение и образовательные платформы

Современные образовательные платформы предлагают различные форматы микрообучения, что делает процесс обучения более гибким и адаптивным. Микрокурсы и сертификаты становятся важным инструментом для быстрого освоения новых навыков и технологий. Это особенно актуально в сфере IT, где технологии развиваются стремительными темпами, и непрерывное обучение становится необходимостью для профессионального роста.

Компании, такие как Google, Microsoft и IBM, предлагают собственные образовательные программы и сертификации, которые ориентированы на быстрое освоение конкретных навыков. Этот подход значительно сокращает время, необходимое для приобретения новых компетенций, и позволяет специалистам оставаться конкурентоспособными на рынке труда. Кроме того, микрообучение способствует более эффективному восприятию материала за счет его дробления на небольшие порции, что упрощает усвоение информации.

В образовательной системе микрообучение получает признание как метод, дополняющий традиционные формы образования. Оно позволяет студентам гибко планировать учебный процесс, комбинировать различные форматы обучения и получать доступ к актуальным знаниям в любое удобное время. В результате такие подходы способствуют росту числа специалистов, которые не только владеют основами программирования, но и постоянно обновляют свои знания.

Влияние международных стандартов на IT-образование

Интеграция международных образовательных стандартов и лучших практик становится важным элементом в процессе подготовки IT-специалистов. Программы обучения аккредитуются на международном уровне, что позволяет студентам получать признанные квалификации и сертификаты, востребованные на глобальном рынке труда.

Одним из таких стандартов является программа CDIO (Conceive — Design — Implement — Operate), направленная на подготовку инженеров и IT-специалистов через интеграцию теории и практики. Важной особенностью программы является ориентация на разработку реальных проектов и решений, что помогает студентам не только осваивать технологии, но и развивать навыки командной работы и управления проектами. CDIO подчеркивает важность интеграции научных знаний и инженерных навыков, что особенно актуально в контексте подготовки специалистов в области информационных технологий.

Программы, соответствующие международным стандартам, также обеспечивают возможность участия студентов в глобальных образовательных инициативах и международных стажировках. Это расширяет их карьерные перспективы и открывает доступ к ведущим мировым технологиям и методам обучения.

Заключение

Изменения в IT-образовании отражают общие тенденции цифровой трансформации и быстро меняющегося рынка труда. Гибридные и дистанционные формы обучения, персонализированные траектории обучения с использованием ИИ, практико-ориентированные подходы и новые образовательные форматы, такие как микрокурсы, создают благоприятные условия для подготовки квалифицированных IT-специалистов. Эти изменения способствуют созданию системы образования, которая способна не только удовлетворять текущие потребности рынка, но и гибко адаптироваться к будущим вызовам.

1. Глушкова, А. И. Современные тенденции IT-образования в условиях цифровой трансформации // Высшее образование сегодня. – 2022. – № 8. – С. 45–52.
2. Иванов, И. В., Петров, К. А. Персонализированное обучение и искусственный интеллект: новый подход в IT-образовании // Вестник науки и образования. – 2023. – № 3. – С. 12–18.
3. Smith, J., & Brown, R. The role of artificial intelligence in personalized learning for IT education // International Journal of Educational Technology. – 2021. – Vol. 14. – P. 88–96.
4. Марков, В. Н. Гибридное обучение в высшей школе: перспективы и вызовы // Образование и информационные технологии. – 2021. – № 6. – С. 73–79.
5. Технологии программирования и образовательные платформы: вызовы и перспективы // Программирование и информационные системы. – 2022. – № 4. – С. 29–34.

Лукашевич А.В., Кувшинова И.Б.

К вопросу о составлении сложного поискового запроса в базе данных ВИНТИ РАН

*Всероссийский институт научной и технической информации
(Россия, Москва)*

doi: 10.18411/trnio-10-2024-395

Аннотация

Приводится пример составления поискового запроса в базе данных ВИНТИ РАН, отражающего тематику, состоящую из гиперонимов, в частности, на тему «Аэрокосмические исследования Арктики».

Ключевые слова: ВИНТИ РАН, базы данных, запросы в базы данных.

Abstract

An example of compiling a search query in the VINITI RAS database is given, reflecting a topic consisting of hyperonyms, in particular on the topic of “Aerospace research in the Arctic”.

Keywords: VINITI RAS, databases, database queries.

Введение

База данных (БД) ВИНТИ РАН (далее – БД ВИНТИ) [1] используется в качестве источника данных для наукометрического анализа. Она является надежным библиографическим источником и имеет уникальные возможности для анализа, недоступные в других БД, поскольку все документы в БД ВИНТИ РАН проходят аналитико-синтетическую обработку в Отделах научной информации ВИНТИ РАН [2].

Общие правила и примеры составления кратких поисковых запросов в БД ВИНТИ можно найти на сайте ВИНТИ [1]. Если при открытии Базы данных ВИНТИ РАН On-line перейти в раздел «Помощь», то пользователям можно найти подробные описания поисковых операторов, видов поиска, результатов поиска и другие функции. В разделе «Как найти» можно найти инструкцию как найти «одно или несколько слов» с примерами. Самый большой по количеству искомых терминов приведенный пример содержит только четыре термина. С этой страницы также можно попасть на Ютуб-канал VINITI RAS [3], на котором есть ролики, обучающие составлять простые запросы. Самым сложным из предлагаемых на канале запросов является поиск по словосочетанию. Цель статьи – дать пример составления сложного поискового запроса в БД ВИНТИ для темы «Аэрокосмические исследования Арктики». При всей краткости наименования заявленной темы, запрос оказался очень объемным, поскольку оба понятия (и «аэрокосмические исследования», и «Арктика») являются гиперонимами и включают в себя множество гипонимов.

Сравнение выборок, составленных по одному поисковому термину, и объединенных выборок, полученных по нескольким синонимичным терминам, показывает, что "для корректного мониторинга потока НТИ рекомендуется использовать объединенную выборку, как статистически более значимую и однородную" [4]. Для выбора наиболее полного поискового запроса были рассмотрены различные комбинации терминов, их синонимы и гипонимы на русском и английском языке.

Подбор терминов поискового запроса

При выборе нужных терминов, из которых будет состоять запрос, необходимо использовать только те термины, которые не имеют омонимов и не являются частью других слов. Так, например, термин "БЛА" (беспилотные летательные аппараты) использовать в запросах не рекомендуется, поскольку он является частью слова "благодарит" и других.

В статье мы не будем описывать все поисковые операторы и поисковые поля БД ВИНТИ, так как эта информация представлена на сайте. Напомним особенность этой БД — чтобы найти все термины, начинающиеся с заданного фрагмента (неполного слова), необходимо использовать специальный знак усечения — \$ в конце слов без пробела [1]. Можно задать ограничение на максимальное число символов после знака \$. Например, фрагменту мор\$2 соответствуют слова — море, моря, морем, но не морской.

Все термины, которые будут использоваться для запроса, мы разделили на две части: левая (Арктическая) часть и правая (аэрокосмическая) часть (см. Рис. 1). Между ними в дальнейшем в общем поисковом запросе будет стоять поисковый оператор "и".



Рисунок 1. Подбор терминов для поискового запроса к теме «Аэрокосмические наблюдения Арктики».

В правой (аэрокосмической) части термины будут состоять из одиночных слов (например, "satellite") и словосочетаний (например, "беспилотные летательные аппараты"). А вот с левой (арктической) частью возникли вопросы, ведь Арктика является большим регионом (гиперонимом), включающим в себя множество других географических объектов (гипонимов). Чтобы расширить условия поиска и получить больше результатов, мы поставили своей задачей добавить в поисковый запрос большую часть из них. Вопрос о южной географической границе Арктики не однозначен [6]. В наш запрос были добавлены только те географические объекты, которые точно являются Арктикой согласно мнению всех ученых. То есть такие, которые расположены севернее южной границы тундры и июльской изотермы 10°C на суше (5°C – на море), а также севернее Северного полярного круга. В запрос включались только такие из них, названия которых не дают омонимов. Например, полуостров Ямал пришлось исключить из-за одноимённой авиакомпании. Остров Гренландию нельзя включать, так как часть его находится южнее Северного полярного круга, но Гренладское море можно, потому что оно севернее. Однако это не значит, что документы, посвященные исследованию Гренландии, не появятся в поиске. Если автор включил в документ слово Арктика, то документ, посвященный Гренландии, все-равно будет показан в результатах поиска. Всё множество географических объектов, которые включает в себя Арктика, мы разделили на три группы: моря, архипелаги и острова, полуострова и города. Для каждой группы терминов была составлена таблица. Приводим пример такой таблицы для группы морей (см. табл. 1).

Таблица 1

Термины для составления поискового запроса по теме
Аэрокосмические исследования Арктики. Арктическая часть, группа «моря».

Русское название	сокращение для БД ВИНТИ	перевод на английский
Баренцево море	Баренцев\$ adj мор\$2	Barents Sea
Карское море	Карско\$ adj мор\$2	Kara Sea
Море Лаптевых	мор\$2 adj Лаптевых	Laptev Sea
Восточно-Сибирское море	Восточно-Сибирск\$ adj мор\$2	East-Siberian Sea
Чукотское море	Чукотск\$ adj мор\$2	Chukchi Sea
Море Бофорта	мор\$2 adj Бофорта	Beaufort Sea
Гренладское море	Гренландск\$ adj мор\$2	Greenland Sea
Море Линкольна	Линкольна adj мор\$2	Lincoln Sea

Сбор поискового запроса из отдельных частей

После подбора отдельных терминов можно перейти к сбору поискового запроса.

Сначала соберем отдельно каждую группу терминов «морской группы» из арктической части. Объединим отдельно все названия морей через оператор «or» в общую скобку, а слово «море» присоединим к этой скобке с помощью оператора «adj» (adj между словами означает, что оба слова должны встретиться одно за другим. Его удобно использовать для нахождения словосочетаний) [1]. Прделаем эту операцию для русских и английских названий отдельно. Важно отметить, что в БД ВИНТИ лучше не использовать кавычки, они не всегда работают правильно, все кавычки нужно заменять на скобки. Таким образом, часть поискового запроса, связанная с морями Арктики, будет выглядеть так:

((Баренцев\$ or Карско\$ or Лаптевых or Восточно-Сибирск\$ or Чукотск\$ or Бофорта or Гренландск\$ or Линкольна) adj мор\$2) or ((Barents or Kara or Laptev or East-Siberian or Chukchi or Beaufort or Greenland or Lincoln) adj sea)

Часть поискового запроса, связанная с архипелагами и островами Арктики, будет выглядеть так:

((Франца-Иосифа\$ or Нов\$2 or Северн\$) adj Земл\$2) or (Franz adj Josef adj Land) or ((Novaya or Severnaya) adj Zemlya) or Шпицберген or Svalbard or ((Новосибирск\$ or Врангеля or Ян-Майен) adj остров\$2) or (((New adj Siberian) or Wrangel or (Jan Mayen))) adj Island\$1)

Часть поискового запроса, связанная с полуостровами и городами Арктики, будет выглядеть таким образом:

((Таймыр or Гыданск\$3) adj полуостров) or Певек or ((Таумур or Gyda) adj Peninsula) or Pevek

Рекомендуется проверять каждый небольшой фрагмент запроса на его работоспособность с целью исключения возможных ошибок при его составлении.

Соберем запрос арктической части. Он будет выглядеть так:

Арктика or Arctica or ((Баренцев\$ or Карско\$ or Лаптевых or Восточно-Сибирск\$ or Чукотск\$ or Бофорта or Гренландск\$ or Линкольна) adj мор\$2) or ((Barents or Kara or Laptev or East-Siberian or Chukchi or Beaufort or Greenland or Lincoln) adj sea) or ((Франца-Иосифа\$ or Нов\$2 or Северн\$) adj Земл\$2) or (Franz adj Josef adj Land) or ((Novaya or Severnaya) adj Zemlya) or Шпицберген or Svalbard or ((Новосибирск\$ or Врангеля or Ян-Майен or Элсмир) adj остров\$2) or (((New adj Siberian) or Wrangel or (Jan Mayen) or Ellesmere) adj Island\$1) or ((Таймыр or Гыданск\$3) adj полуостров) or Певек or ((Таумур or Gyda) adj Peninsula) or Pevek

Запрос аэрокосмической части будет состоять из отдельных понятий и выглядеть так:

космич\$ or спутник\$ or satell\$ or spac\$ or aerospac\$ or аэрокосм\$ or (aero\$ adj spac\$) or (аэро\$ adj косм\$) or spacecraft or spaceship or ((space or aerospace) adj vehicle) or (unmanned adj aerial adj vehicle) or UAV or UAS or drones or copters or quadcopters or (беспилотные adj летательные adj аппараты) or БПЛА or дрон\$ or коптер\$

Кажется, что основная работа сделана, осталось только взять обе части в скобки, поставить между ними оператор «and» и задать все прочие условия поиска, как это всё описано в инструкции [1]. Хотелось бы обратить внимание читателей на условия поиска, ведь важно не только то, что мы будем искать, но и где. Представляется особенно важным правильное заполнение полей документов, по которым будет проведен поиск, см. Рис. 2.

Рисунок 2. Помощь по работе с Базой Данных ВИНТИ РАН. Как работать со страницей Поиск. Инструкция на сайте ВИНТИ.

Для наукометрического анализа документов не подходит поиск «везде», нам необходимо, чтобы поисковые термины находились в наиболее значимых полях: заглавие, ключевые слова и реферат. Такое ограничение позволит нам исключить термины поиска в пристатейной библиографии (например, журнал с названием Арктика), и в названиях организаций авторов (например, Арктический институт). Такая возможность в БД ВИНТИ есть, поэтому выбираем необходимый вариант в выпадающем списке (Загл/Кл.слова/Реф.).

Как же разместить сам запрос? На Рис. 2 мы видим два поля для запроса, пока не понятно, зачем нам второе поле, которое нужно «при необходимости». Как же будет работать поиск, если мы соберем наш запрос в одно поле и поставим ограничивающие условия «Загл/Кл.слова/Реф» (Рис. 3)?

Рисунок 3. Неправильно заданные условия поиска.

Поиск будет производиться следующим образом: будет проверяться есть ли термин как из «арктической», так и из «аэрокосмической части», в заголовке, потом в ключевых словах, потом в реферате, то есть, в одном поле должны присутствовать термины обеих частей. Таким образом, документ, где в названии есть «Баренцево море», а «спутниковые наблюдения» в ключевых словах, будет отброшен. По нашему мнению, такой документ является релевантным. Поэтому важно использовать и вторую строчку предлагаемой поисковой формы, важно искать и «арктические термины» во всех полях, и «аэрокосмические термины» во всех трёх полях, а не только в каком-то одном поле.

На Рис. 4 показано как правильно поместить наш запрос в поисковых полях.

Рисунок 4. правильно заданные условия поиска.

В конечном итоге мы получили вот такой запрос:

((Арктика or Arctica or ((Баренцево or Карское or Лаптевых or Восточно-Сибирск\$ or Чукотск\$ or Бофорта or Гренландск\$ or Линкольна) adj мор\$2) or ((Barents or Kara or Laptev or East-Siberian or Chukchi or Beaufort or Greenland or Lincoln) adj sea) or (Франца-Иосифа or Нов\$2 or Северн\$) adj Земл\$2) or (Franz adj Josef adj Land) or ((Novaya or Severnaya) adj Zemlya) or Шпицберген or Svalbard or ((Новосибирск\$ or Врангеля or Ян-Майен or Элсмир) adj остров\$2) or (((New adj Siberian) or Wrangel or (Jan Mayen) or Ellesmere) adj Island\$1) or Таймыр or Гыданск\$3 полуостров or Певек or ((Таумуг or Gyda) adj Peninsula) or Pevek):TI,AB,KW AND (космич\$ or спутник\$ or satell\$ or spac\$ or aerospace\$ or аэрокосм\$ or (aero\$ adj spac\$) or (аэро\$ adj косм\$) or spacecraft or spaceship or ((space or aerospace) adj vehicle) or (unmanned adj aerial adj vehicle) or UAV or UAS or drones or copters or quadcopters or (беспилотные adj летательные adj аппараты) or БПЛА or дрон\$ or коптер\$):TI,AB,KW

Можно ограничить поиск с помощью выбора тематического фрагмента, ретроспективы или года издания, языка, раздела тематики. Как это сделать, хорошо и подробно описывается на сайте ВИНТИ РАН [1].

Заключение

На примере своего опыта надеемся, что данная статья окажет помощь пользователям БД ВИНТИ при составлении собственных поисковых запросов, включающих множество терминов.

1. База данных ВИНТИ РАН. – URL: <http://bd.viniti.ru/>
2. Лукашевич А. В. Возможности наукометрического анализа публикаций, посвященных применению военных беспилотников, по БД ВИНТИ РАН / А. В. Лукашевич // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2023. – № 6. – С. 19–29.
3. ВИНТИ РАН Всероссийский институт научной и технической информации РАН. – URL: <https://www.youtube.com/@viniti-ras/featured>
4. Теплицкая В. С. О некоторых особенностях формулировки поисковых запросов при мониторинге потока научно-технической литературы в области астрономии/ Теплицкая В.С. // Материалы 10-й Научной конф. с межд. участием, посвященной 70-летию ВИНТИ РАН «Научная информация в современном мире: глобальные вызовы и национальные приоритеты» (НТИ-2022), 25–26 октября 2022 г., Москва. – Москва: ВИНТИ РАН 2022. – 564 с. – С. 121–129.
5. Котляков В. М. и др. Арктика / В. М. Котляков, В. Е. Хаин [и др.] // Большая российская энциклопедия. – URL: <https://bigenc.ru/c/arktika-d5074d>

Лукашевич А.В., Кувшинова И.Б., Теплицкая В.С.
**Общие принципы формирования предметного и объектного указателей
на примере Отдела научной информации по астрономии ВИНТИ РАН**

*Всероссийский институт научной и технической информации
(Россия, Москва)*

doi: 10.18411/trnio-10-2024-396

Аннотация

Описываются основные принципы формирования указателей в отдельных выпусках Реферативного журнала ВИНТИ РАН в Отделе научной информации по астрономии. Подтверждено, что различия при формировании указателей разными людьми минимальны. Исключительную важность представляет актуализация словаря ключевых слов-дескрипторов. Даны практические рекомендации по ведению таких словарей.

Ключевые слова: ВИНТИ РАН, ключевые слова, словарь ключевых слов, информационно-поисковый тезаурус, дескрипторы, аскрипторы.

Abstract

The basic principles for forming indexes in individual issues of the Abstract journal VINITI RAS in the Department of Scientific Information on Astronomy are described. It is confirmed that the differences in forming indexes by different people are minimal. Updating the dictionary of keywords-descriptors is of exceptional importance. Practical recommendations for maintaining such dictionaries are given.

Keywords: VINITI RAS, keywords, dictionary of keywords, information retrieval thesaurus, descriptors, ascriptors.

Введение

Реферативный журнал (РЖ), выпускаемый Всероссийским институтом научной и технической информации (ВИНИТИ) РАН, состоит из сводных томов и отдельных выпусков. Выпуски Реферативного журнала, выпускаемые Отделом научной информации (ОНИ) по астрономии, снабжаются различными указателями: Авторский указатель, Указатель источников, Предметный и Объектный указатели. Ключевые слова (КС) в отдельных выпусках РЖ подбираются не только выпускающим редактором. При формировании выпусков КС также подбираются другими редакторами и референтами. После этого автоматически формируются указатели, которые корректирует выпускающий редактор.

Цель данной статьи – на примере правил формирования Предметного и Объектного указателей в ОНИ по астрономии дать некоторые методические рекомендации к составлению инструкции правил подбора ключевых слов для РЖ ВИНТИ.

Правила формирования Предметного и Объектного указателя

В ОНИ по астрономии при подборе КС для каждого конкретного документа КС не пишутся в строчку, а должны соединяться парами: главное слово и поясняющее. Тогда в Предметном и Объектном указателях они будут видны читателям как словари, помогающие пользователю найти то, что его интересует.

Приведем пример формирования Предметного указателя. Допустим, читателя интересует лазерное сканирование лесов. Он смотрит в Предметный указатель, находит ключевое слово "леса" и под ним поясняющие слова, среди них видит "сканирование лазерное воздушное" и "сканирование лазерное наземное", после этого читатель уже смотрит в журнале только те документы, на которые указывают нужные ему пары КС, а не все документы, в которых речь идет о лесах. (См. рис. 1.)

ландшафты	
картографирование экологическое	139
ледники	
космические исследования	88
плотность льда	88
потери льда	88
леса	
высота деревьев	279
полсье измерения	279
сканирование лазерное воздушное	277, 279, 280, 282, 283
сканирование лазерное наземное	277, 279
совместная регистрация облака точек	277
летно-съёмочная аппаратура	
системы спутниковой навигации	238
лидары	
архитектурные обмеры	291
облака точек	291
Луна	
вулканизм	177
геологические образования	177, 178
геологические процессы	177

Рисунок 1. Предметный указатель РЖ 52. Геодезия и аэросъемка, № 12, 2019 г. Фрагмент.

Подобным же образом формируется Объектный указатель, в котором читатель может найти ссылки на документы с упоминанием интересующих его объектов. Это могут быть, например, географические объекты, искусственные спутники Земли, организации и т.п. (См. рис. 2).

Swarm	92
TerraSAR-X	90
компании	
Геоскан	21
Кредо-Диалог	325, 326
Ракурс	29
общества	
АО "УГОК"	247
ОАО "Холопеничи"	336
ПАО "НПО "Алмаз"	129
организации	
Библиотека Бодлея в Оксфордском университете	5
Гидрометцентр России	69
планеты	
Марс	179, 180, 189
Меркурий	181, 198

Рисунок 2. Объектный указатель РЖ 52. Геодезия и аэросъемка, № 12, 2019 г. Фрагмент.

Формируемые указатели можно назвать Информационно-поисковыми тезаурусами, составляемыми для каждого конкретного номера РЖ, поскольку они описывают отношения между терминами предметной области [1; 2; 3, с. 5–7]. По своему построению такие указатели относятся к типу тезаурусов, выделяющих среди своих лексических единиц дескрипторы (авторизованные термины) и недескрипторы (аскрипторы) [4].

В каждом РЖ ОНИ по астрономии есть свои списки наиболее употребляемых КС-дескрипторов. Для формирования Предметного и Объектного указателей существует два разных списка КС-дескрипторов. КС этих двух указателей могут быть разными, а могут повторяться.

Для того, чтобы КС соединялись в пары, им присваиваются метки. Метки, используемые в ОНИ по астрономии: АКК, КК, К, Н и ОКК. Если в конце метки стоит буква К (АКК, КК, К и ОКК), то это КС из Списка дескрипторов, и такое КС является дескриптором.

КС не из Списка дескрипторов (аскрипторы) имеют метку Н, все остальные КС с другими метками должны быть из Списка дескрипторов.

АКК и К — это метки, используемые для Предметного указателя, ОКК — для Объектного указателя, КК — более сложная и редко используемая метка, может использоваться и в том, и в другом указателе. Более подробно правила формирования Предметного указателя

публиковались ранее в статье сотрудников ОНИ по астрономии [5]. Перечислим значение этих меток подробнее.

Значение разных меток КС, используемых в РЖ ОНИ по астрономии

Метка АКК — главное КС, ставится в начале Предметного описания документа. Это КС является главным для всех поясняющих слов. При желании редактора таких меток со своими поясняющими словами в одном документе может быть несколько.

Метка К — поясняющее КС из Списка дескрипторов.

Метка Н — поясняющее КС, не принадлежащее Списку дескрипторов. Таким образом, КС с меткой Н — КС-аскрипторы. Используется как в Предметном, так и в Объектном указателе.

Метка ОКК. КС с такой меткой могут использоваться только в Объектном указателе. Метка ОКК ставится для КС-дескрипторов при объектном описании документа. Это КС является главным для всех объектов одного типа. Таких меток со своими поясняющими словами в одном документе может быть несколько. Метка ОКК Объектного указателя выполняет те же функции, что и метка АКК Предметного указателя. Однако есть своя специфика в том, что для КС метки ОКК используется Список дескрипторов Объектного указателя, количество КС в котором значительно меньше.

Основная функция метки КК — дублировать главную метку АКК в Предметном указателе или ОКК в Объектном указателе. Поэтому она может использоваться и в том, и в другом указателе.

Когда документу присваиваются КС, нами предполагается, что необходимо учитывать следующее условие: КС в большинстве случаев должны браться из Словаря КС-дескрипторов. Ведь "словарь нужен для обеспечения стабильности терминологии. В условиях постоянного реформирования ... реформаторы не всегда задумываются о последствиях, которые следует ожидать от изменений в нормативных и методических документах. Слово, включенное в словарь, уже является критерием его существования... Замена одного слова на другое не так безобидна, как кажется. Изменения в понятийно-терминологическом аппарате сказываются на поиске опубликованных и неопубликованных документов (диссертации, научные отчеты, депонированные рукописи)." [6, с. 215].

Полнотекстовый поиск часто может не дать полноты имеющейся информации, вследствие синонимии, полисемии и омонимии [7, с. 398–409].

В своей монографии "Основы информатики", опубликованной в 1968 году, авторы предвидели ситуацию с высоким уровнем информационного шума при использовании Интернета. Информационно-поисковый тезаурус, который используется для увеличения полноты выдачи результатов в дескрипторных информационно-поисковых системах с ограниченным объемом данных, способен улучшить точность информационного поиска в Интернете. "Особую важность имеет функция информационно-поискового тезауруса – быть пособием, которое бы помогало ищущему информацию находить правильные дескрипторы для выражения его информационной потребности." [8, с. 35–36].

Подготовку РЖ ведут разные редакторы и референты, большинство из них осуществляет и процедуру составления "Предметного образа документа" (ПОД), который включает в себя КС и рубрикационные шифры описываемого документа. При этом каждый сам подбирает КС к реферируемым документам, это могут быть как КС-дескрипторы, так и КС-аскрипторы.

По нашему мнению, все авторские КС-аскрипторы, которые могут быть заменены КС из Списка дескрипторов, должны быть по возможности заменены. В этом и заключается одна из основных задач редактирования КС выпускающим редактором.

Приведем пример замены авторских КС (см. рис. 3 и 4). Документ был опубликован в № 7 за 2016 г. РЖ 73. Исследование Земли из космоса (РЖ 73). Издательский номер документа — 16.07–73.35, заголовок статьи: Атмосферная коррекция спутниковых изображений цвета

океана в присутствии полупрозрачных облаков. (Оригинальное название — Atmospheric correction of satellite ocean-color imagery in the presence of semi-transparent clouds).

под	
АКК	атмосферная коррекция
Н	изображения цвета океана
Н	полупрозрачные облака
Н	восстановление концентрации хлорофилла
ОКК	аппаратура
Н	MODIS

Рисунок 3. Авторские КС в Предметном образе документа (ПОД) 16.07-73.35. Скриншот программы "Автоматизированное рабочее место корректора–референта–редактора (АРМ КОРЕФ)".

Вводим новое КС из Списка дескрипторов "дешифрирование изображений", объединяющее аналоги большинства авторских КС, присутствующие в Списке дескрипторов. Новый ПОД см. на рис. 4.

под	
АКК	атмосферная коррекция
Н	изображения цвета океана
Н	полупрозрачные облака
Н	восстановление концентрации хлорофилла
ОКК	аппаратура
Н	MODIS

Рисунок 4. КС выпускающего редактора в Предметном образе документа (ПОД) 16.07–73.35. Скриншот программы "Автоматизированное рабочее место корректора–референта–редактора (АРМ КОРЕФ)".

Таким образом, здесь три авторских КС-аскриптора были заменены редактором, выпускающим РЖ73, на 3 КС-дескриптора.

Хорошо это или плохо? Чем больше и разнообразнее КС, тем более точно отражена область поиска. Но с другой стороны — большее количество КС увеличивает объем указателей и тем самым затрудняет сам поиск.

Использование разных КС разными редакторами

Кажется, что очевидно и без наблюдений, что субъективизм в этой работе неизбежен. Достаточно ли приведенных нами общих указаний для уменьшения субъективизма?

Интересно сравнить, как разные люди применяют разные КС. Ведь можно индексировать документы большим количеством КС, но при этом использовать в своей работе ограниченное количество самих слов. Для ограничения этого количества и призваны служить словари дескрипторов. Увеличение разнообразия КС, присваиваемых документу, хорошо для тех КС, которых являются дескрипторами, поскольку это означает, что КС в Словаре дескрипторов правильно подобраны. Но хорошо ли увеличение КС с меткой Н, ведь это КС-аскрипторы?

В 2018 и 2019 гг. Отдел научной информации (ОНИ) по астрономии ВИНТИ выпускал четыре отдельных выпуска РЖ. Один из них – выпуск РЖ 52. Геодезия и аэросъемка (РЖ 52), в котором с 2019 г. изменился выпускающий редактор. В 2019 году нами были подробно рассмотрены изменения указателей РЖ 52, связанные со сменой выпускающего редактора. Для этого были выбраны выпуски РЖ 52 за полгода: с 1 по 6 номер 2018 г. и с 1 по 6 номер 2019 г.

Различий в принципах формирования указателей разными людьми почти нет. Была выявлена даже некоторая закономерность процентного соотношения усилий, затраченных редакторами при подборе КС Предметного указателя.

Проверка закона Парето для Предметного указателя

Закон Парето формулируется так: "20% усилий дают 80% результата, а остальные 80% усилий — лишь 20% результата". В нашем случае, предположим, что затраченные усилия — это те КС, которые референты и редакторы присвоили каждому документу, а результат — те КС, которые увидят пользователи в Предметном указателе. Ведь если КС "леса" авторы изначально написали как минимум 5 раз в 5 документах (см. Рис. 1. номера документов 277, 279, 280, 282, 283), то в Предметном указателе эти 5 одинаковых КС сольются друг с другом, это будет одно и то же КС, и встретится уже 1 раз.

Процентное соотношение затраченных усилий при подборе КС у обоих редакторов совпало — 65% дескрипторов и 35% аскрипторов. Также близко процентное соотношение результата — 25% дескрипторов и 75% аскрипторов.

Таким образом, при подборе КС для Предметного указателя Закон Парето не выполняется, но есть сходство в рассчитанных соотношениях, несмотря на то, что редактировали Предметный указатель разные люди.

У обоих редакторов совпали наиболее употребимые КС-дескрипторы. По количеству КС на 1 документ формирование Поискового образа документа получилось одинаковым, за исключением метки Н.

Частично различия обусловлены тем, что составляли указатели разные люди. Также, возможно, что менее опытные выпускающие редакторы используют для поискового образа документа больше обобщающих понятий, а также больше разных КС именно из-за своей неопытности, поскольку еще не имеют своих устойчивых "любимых" КС и чаще заглядывают в Список возможных дескрипторов.

Периоды исследования выявили, что как минимум половина всех КС из Списков дескрипторов не используется. В то же время у каждого выпускающего редактора в Предметном указателе есть КС-аскрипторы, которые используются часто и поэтому должны быть внесены в Список дескрипторов Предметного указателя.

Подобные исследования важны для актуализации Списка дескрипторов, для определения наилучшего и наименьшего Списка дескрипторов каждого указателя, с помощью которого возможно максимально удовлетворять поисковые запросы пользователей для каждого выпуска РЖ. В ОНИ по астрономии такая работа проводится ежегодно всеми выпускающими редакторами.

Практические шаги или рекомендации к ведению списков дескрипторов и КС выпускающим редакторам

С учетом нашего многолетнего опыта работы мы предлагаем такую работу разделить на три блока: работа с КС-аскрипторами, работа с КС-дескрипторами и окончательное редактирование Списков ключевых слов-дескрипторов.

Работа с КС-аскрипторами предполагает 8 этапов: (1) получение в Отделе программных систем ВИНТИ РАН списка "КС-аскрипторов с метками Н" за прошедший год; (2) выделение из списка "КС-аскрипторов с метками Н" КС Предметного указателя с частотностью больше 10 (частотные КС); (3) сбор информации о необходимости введения новых КС у редакторов и референтов (предложенные КС); (4) оценка КС, предложенных референтами и редакторами, на

предмет – действительно ли это часто употребляемые КС; (5) если предложенные референтами и редакторами КС действительно часто использовались, хотя бы 5 раз в год, то добавление к предложенным КС аналогов, синонимов, частных вариантов; (6) исследование частоты употребления аналогов предложенных КС в списке "КС-аскрипторов с метками Н"; (7) оценка частотных и предложенных КС методом сравнения с КС, используемыми во всем РЖ ВИНТИ РАН, с помощью поиска КС в классификационной схеме "Рубрикатор ВИНТИ (текущий)" [9]; (8) принятие решения о внесении или не внесении предложенных КС в Список дескрипторов.

Работа с КС-дескрипторами может быть разделена на шесть шагов: (1) получение в Отделе программных систем ВИНТИ РАН списка "КС-дескрипторов с метками К" (с метками АКК, КК и К); (2) внесение списка "КС-дескрипторов с метками К" в файл для сравнения с такими же КС, полученными в прошлые годы; (3) выделение КС, подлежащих удалению, таких, которые не использовались или использовались 1 раз в течение 10 лет; (4) выделение КС-кандидатов, подлежащих удалению, таких, которые использовались 2—5 раз в течение 10 лет и не использовались в последние годы; (5) перевод некоторых КС, подлежащих удалению, в КС-кандидаты, подлежащие удалению, по просьбе редакторов и референтов; (6) принятие решения об удалении КС из Списка дескрипторов.

Редактирование Списка КС-дескрипторов состоит из 4 этапов: (1) внесение частотных и предложенных КС в Список дескрипторов и удаление из него КС, подлежащих удалению; (2) распечатка списков КС, внесенных в Словарь дескрипторов в текущем году для редакторов и референтов; (3) распечатка списков КС-кандидатов, подлежащих удалению в будущем, для обращения на них особого внимания редакторов и референтов. (4) распечатка окончательных Словарей дескрипторов для Предметного и для Объектного указателя.

Выводы:

- 1) предложены основные принципы формирования Предметного и Объектного указателя в реферативных журналах Отдела научной информации по астрономии ВИНТИ РАН;
- 2) подтверждено, что различий в принципах формирования указателей разными людьми почти нет;
- 3) доказано, что исключительную важность представляет актуализация Словарей дескрипторов;
- 4) даны практические рекомендации о взаимодействии выпускающего редактора с научными редакторами и референтами и принятии тех или иных решений по ведению списков КС-дескрипторов.

1. ГОСТ 7.74-96 Информационно-поисковые языки. Термины и определения.
2. Лафтими, И. Информационно-поисковые тезаурусы: основные понятия, назначение и методика разработки. Отраслевой рыболовный тезаурус. / И. Лафтими // Молодой ученый. – 2012. – № 7. – С. 164-166.
3. Лавренова, О. А. Методика разработки информационно-поискового тезауруса / О. А. Лавренова. – Москва : Издательство "Пашков дом", 2001. – 55 с.
4. ГОСТ 7.25-2001 Информационно-поисковый тезаурус. Одноязычный. Правила разработки, структура, состав и форма представления.
5. Седякина, А. Н. "Способ формирования предметного указателя для Реферативного журнала" / А. Н. Седякина, И. Б. Кувшинова, Н. Л. Лукашевич // Материалы 8-ой Международной конференции НТИ-2012, Москва, 28–30 ноября 2012 г., с. 242–244, ВИНТИ РАН, 2012.
6. Полонский, В. М. Зачем нужен словарь? / В. М. Полонский // Наука и школа. – 2019. – № 1. – С. 214–226.
7. Михайлов, А. М. Основы информатики. / А. М. Михайлов, А. И. Черный, Р. С. Гиляревский. – Москва : Академический научно-издательский, производственно-полиграфический и книгораспространительский центр РАН "Издательство "Наука", 1968. – 756 с.
8. Гиляревский, Р. С. Рубрикатор как инструмент информационной навигации : рубрикатор и сферы его применения, иерархические и фасетные классификации, рубрикаторы органов НТИ, рубрикация поисковых машин, интернета, навигация на основе классификации информационных ресурсов / Р. С. Гиляревский, А. В. Шапкин, В. Н. Белоозеров ; Р. С. Гиляревский, А. В. Шапкин, В. Н. Белоозеров. – Санкт-Петербург : Профессия, 2008.
9. Рубрикатор ВИНТИ (текущий) – URL: <http://scs.viniti.ru/rubtree/main.aspx?tree=RV>

Масликов Т.О.

Принципы глубокого обучения и нейросетей

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)

doi: 10.18411/trnio-10-2024-397

Аннотация

В статье исследуются основные принципы глубокого обучения и нейронных сетей, включая ключевые концепции. Рассматриваются их роль и значимость в построении современных моделей машинного обучения, а также их влияние на способность нейронных сетей обучаться на сырых данных, генерировать обобщенные знания и адаптироваться к различным типам задач.

Ключевые слова: глубокое обучение, нейронные сети, обратное распространение, функции активации, оптимизация моделей, машинное обучение.

Abstract

The article explores the basic principles of deep learning and neural networks, including key concepts. Their role and importance in the construction of modern machine learning models are considered, as well as their impact on the ability of neural networks to learn from raw data, generate generalized knowledge and adapt to various types of tasks.

Keywords: deep learning, neural networks, back propagation, activation functions, model optimization, machine learning.

Глубокое обучение и нейронные сети в последние годы стали основой многих революционных достижений в области искусственного интеллекта и машинного обучения. Эти технологии позволяют компьютерам обучаться на больших объемах данных, выявлять сложные зависимости и создавать модели, которые превосходят традиционные алгоритмы. Основная идея глубокого обучения заключается в использовании многослойных нейронных сетей, где каждый слой сети отвечает за извлечение все более абстрактных признаков из данных. Это позволяет моделям обучаться представлениям данных на различных уровнях сложности, начиная от простых элементов, таких как линии и границы, до более сложных структур, таких как объекты и концепции [1].

Принципы глубокого обучения и нейронных сетей являются фундаментальными для современного искусственного интеллекта и машинного обучения. Вот основные из них:

Искусственные нейронные сети (ИНС) - вдохновлены структурой и функционированием мозга человека и состоят из слоёв нейронов, которые обрабатывают информацию, передавая сигналы от входного слоя к выходному. Они обозначены в виде кружков, которые отражены на рисунке 1. Нейроны связаны между собой.

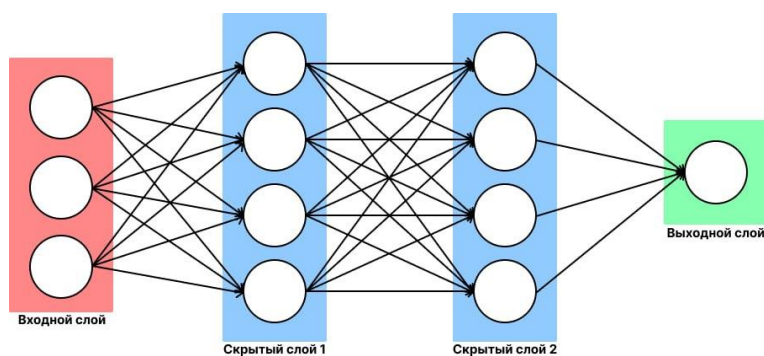


Рисунок 1. Устройство нейросетей.

Существует три вида слоев нейронов: входной слой, скрытые слои, выходной слой. Для описания работы устройства нейросетей применим, для наглядности, авиа-терминологию, что отражено на рисунке 2. Входной слой получает входные данные. В нем 4 нейрона: начальный пункт полета, конечный пункт полета, дата вылета, авиакомпания. От этого слоя входные данные транслируются на первый скрытый слой [2].

В скрытых слоях выполняют математические операции с данными. Одна из трудностей при создании нейросетей – определить количество скрытых слоев и сколько нейронов в каждом слое. Глубокое обучение потому и называется глубоким, что количество скрытых слоев больше одного.

Выходной слой выдает, что получилось в итоге, то есть примерную оценку стоимости рейса.

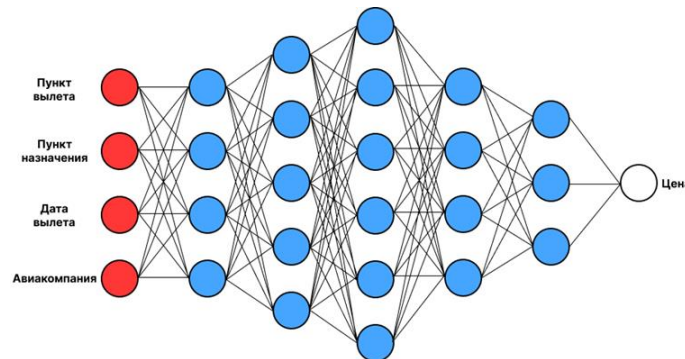


Рисунок 2. Взаимодействие нейронов в слоях нейросети.

Каждая связь между нейронами имеет вес, который определяет важность входного значения, что отражено на рисунке 3. Изначально веса произвольные. Для оценки стоимости авиарейса одним из важнейших параметров является дата вылета. Следовательно, связи с нейроном даты вылета будут обладать большим весом.

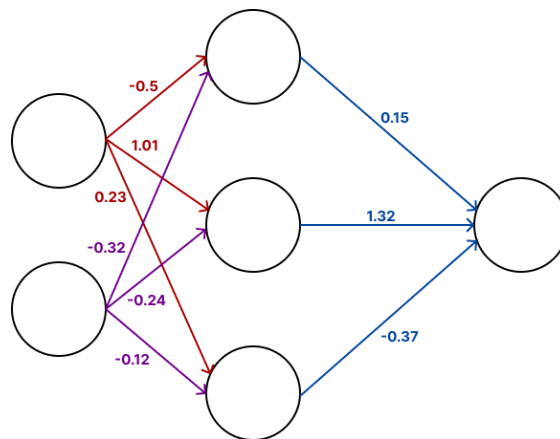


Рисунок 3. Связи нейронов в нейросети.

У каждого нейрона есть функция активации. Если простыми словами, одна из ее задач – «стандартизация» выходных данных. После того, как входные данные прошли через все слои нейросети, выходной слой выдает выходные данные.

Обучение ИИ – сложнейший этап глубокого обучения. Во-первых, набор данных должен быть огромным. Во-вторых, ресурсы для вычислений должны быть очень большими. В случае с сервисом по оценке стоимости авиарейсов, необходимы данные о стоимости билетов за прошлые периоды. Комбинаций аэропортов и дат вылета очень много [4]. Поэтому придется работать с очень большим количеством вариантов цен на билеты. Для обучения машины потребуется задать входы из набора данных и сравнить полученные выходы с выходами из набора данных. Поначалу выходы будут неверными. После обработки, можно создать функцию стоимости, которая показывает, насколько неверными были выходы ИИ в сравнении с

реальными выходами. В идеале, она должна иметь нулевое значение. Это произойдет, когда выходы ИИ совпадут с выходами из набора данных.

Глубина обучения, или глубокое обучение (Deep Learning), — это подмножество машинного обучения, которое включает в себя использование глубоких нейронных сетей. Термин "глубокий" относится к количеству слоёв в нейронной сети. В традиционных нейронных сетях обычно есть только один скрытый слой между входным и выходным слоями, в то время как глубокие нейронные сети имеют два или более скрытых слоя [5]. В таблице 1 ниже, представлены основные элементы глубокого обучения.

Таблица 1

Основные элементы глубокого обучения.

<i>Элемент</i>	<i>Описание</i>	<i>Преимущества</i>
<i>Многослойность</i>	<i>Глубокие нейронные сети содержат несколько скрытых слоёв между входным и выходным слоями. Каждый слой состоит из нейронов, которые обучаются на основе взвешенных входных данных и функции активации.</i>	<i>Глубокие нейронные сети могут обучаться на сырых данных, автоматически извлекая необходимые признаки.</i>
<i>Иерархия признаков</i>	<i>Нейроны в более глубоких слоях сети учатся на основе более высокоуровневых абстракций, представленных выходными данными предыдущих слоёв.</i>	<i>Глубокие нейронные сети могут обобщать знания и распознавать шаблоны в новых данных.</i>
<i>Обратное распространение (Backpropagation)</i>	<i>Процесс, с помощью которого нейросеть обновляет свои веса в ответ на ошибку между предсказанными и истинными значениями.</i>	<i>Способность корректировать ошибки и повышать точность предсказаний.</i>
<i>Функции активации</i>	<i>Функции активации, такие как ReLU или сигмоид, вводят нелинейность, что позволяет сети учиться и представлять более сложные шаблоны.</i>	<i>Позволяют сети учиться более сложным шаблонам и улучшать предсказания.</i>
<i>Оптимизация</i>	<i>Алгоритмы оптимизации, такие как стохастический градиентный спуск (SGD), используются для минимизации функции потерь и настройки весов нейронной сети.</i>	<i>Минимизируют функцию потерь и повышают эффективность обучения.</i>

Глубокое обучение и нейронные сети оказали значительное влияние на развитие современных технологий и продолжают оставаться ключевым элементом в области искусственного интеллекта. Как показано в статье, основные элементы глубокого обучения, такие как многослойность, иерархия признаков, обратное распространение, функции активации и оптимизация, являются основополагающими для создания моделей, способных решать сложные задачи. Данные методы обеспечивают высокую точность и эффективность при работе с большими объемами данных, а также адаптивность к различным типам задач. Перспективы дальнейшего развития этих технологий обещают ещё большее влияние на различные отрасли, включая анализ данных, прогнозирование и кибербезопасность, что делает глубокое обучение одной из самых значимых областей исследований в современном мире.

1. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 193-197.
2. Катасонов А.И., Кузин Д.И. Исследование разновидностей нейронных сетей и их возможностей для обеспечения безопасности инфокоммуникационных систем//Актуальные проблемы инфотелекоммуникаций в науке и образовании. - Санкт-Петербург, 2024. С. 404-409.

3. Skine. Интуитивное глубокое обучение, часть 1a: Введение в нейронные сети [Электронный ресурс]. URL: <https://skine.ru/articles/377412/>. (дата обращения: 14.09.2024.)
4. Лаврова Д. С. и др. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 3. – С. 70-77.
5. Кушнир Д. В., Платонова Т. А. ПРОГРАММИРОВАНИЕ КВАНТОВОГО КОМПЬЮТЕРА И ЕГО ЭМУЛЯЦИЯ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 754-758.

Нучаев С-С.Р., Закаев Р.М., Гузуева Э.Р.
Сравнительный анализ систем управления контентом (CMS)
и искусственного интеллекта (AI)

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-398

Аннотация

Современные системы управления контентом (CMS) и решения на основе искусственного интеллекта (AI) кардинально изменили методы управления веб-контентом. CMS делают процесс создания сайтов доступным благодаря шаблонам и плагинам, тогда как AI-системы ориентированы на динамическое обновление и персонализацию, благодаря использованию алгоритмов машинного обучения и анализу больших данных. В этой статье проведен сравнительный анализ двух подходов, чтобы выявить их ключевые преимущества и недостатки, а также рассмотреть их применимость в различных типах проектов.

Ключевые слова: CMS, система управления контентом, искусственный интеллект, AI, веб-сайт.

Abstract

Modern content management systems (CMS) and solutions based on artificial intelligence (AI) have radically changed the methods of managing web content. CMS make the process of creating websites accessible through templates and plugins, whereas AI systems are focused on dynamic updating and personalization through the use of machine learning algorithms and big data analysis. This article provides a comparative analysis of the two approaches to identify their key advantages and limitations, as well as to consider their applicability in various types of projects.

Keywords: CMS, content management system, artificial intelligence, AI, website.

В наше время наблюдается все большее увеличение популярности систем управления контентом (CMS) таких как WordPress занимающую большую долю рынка, до OpenCart и Tilda более понятных для обычных пользователей. Свою популярность они обрели среди тех людей, которые хотят разработать свой собственный сайт, но не имеют глубоких знаний в программировании. Но в последнее время технология искусственного интеллекта развивается в масштабной прогрессии. Благодаря внедрению систем искусственного интеллекта появляется возможность проводить более глубокий анализ рынка, поведения человека на сайте и автоматическая адаптация под те или иные запросы.

Основные преимущества и недостатки CMS

Системы управления контентом (CMS) – имеют понятный интерфейс для разработки и управления веб-сайта. Хотя при разработке человеку и нет необходимости писать код, но он ограничен представленными шаблонами и плагинами.

К основным достоинствам систем управления контентом можно отнести:

1. Интуитивно понятный интерфейс. Разработчики могут выбрать понравившийся шаблон из библиотеки, и в последствии менять в его по своему усмотрению.

2. Легкая масштабируемость. Большинство систем управления контентом имеют возможность расширить функциональность сайта благодаря внедрению плагинов и модулей.
3. Безопасность. В корпоративных CMS таких как 1С-Битрикс, особое внимание уделено безопасности клиентов.
4. Сообщество. Преимущество разработки сайта на CMS заключается еще в том, что они имеют большое сообщество разработчиков. Благодаря этому имеется возможность найти ответ на возникший вопрос на разных интернет-ресурсах.
5. SEO-оптимизация. Большинство систем управления контентом имеют встроенные инструменты для оптимизации сайта под разные поисковые системы, это позволяет улучшить видимость сайта в сети.

К недостаткам систем управления контентом можно отнести:

1. Ограниченность разработки. Хотя CMS и дают большую возможность для разработки веб-сайта, но действительно серьезные проекты трудно создать без хороших знаний в программировании.
2. Постоянные обновления. В системах управления контентом часто происходят обновления безопасности и производительности. Данный процесс может быть долгим и трудоемким, особенно для больших сайтов.
3. Риск потери данных. Из-за санкций некоторые CMS которые не были разработаны в нашей стране могут приостановить свою работу когда захотят, так, например с 12 сентября один из популярных сервисов Wix приостановил свою работу в нашей стране и заблокировал всех ее пользователей, предоставив при этом меньше трех суток для миграции на другие платформы.

Основные преимущества и недостатки AI-систем

К преимуществам систем искусственного интеллекта можно отнести:

1. Адаптивность. Искусственный интеллект может в режиме реального времени отслеживать поведение пользователей на сайте, адаптироваться и менять код под их запросы. Такие веб-сайты имеют большие возможности, и благодаря такому подходу в разработке конверсия на сайте может возрасти в несколько раз.
2. Автоматизация. Управление сайтом с внедрением искусственного интеллекта дает возможность автоматизировать не только создание новых страниц и контента, но и SEO-оптимизацию с минимальным участием человека в этом.
3. Безопасность. Искусственный интеллект имеет возможность постоянного мониторинга подозрительной активности на сайте и благодаря этому предотвращать возможные атаки.

Недостатки AI-систем:

1. Ресурсоемкость и затратность. Для внедрения систем искусственного интеллекта требуется большое количество вычислительных мощностей, следовательно возрастают затраты на разработку, а это целесообразно только для больших проектов.
2. Интеграция. Использование систем AI в разработке требует специализированных знаний и долгосрочной поддержки. Хотя системы искусственного интеллекта и развиваются большими шагами, но эта система все еще не идеальна и требует постоянного внимания человека.

Таблица 1

Сравнительный анализ CMS и AI систем.

Функция	CMS	AI
Доступность	Простота настройки и доступность	Сложность интеграции и настройки
Персонализация	Ограниченность шаблонами и плагинами	Высокая степень адаптивности

<i>Поддержка</i>	<i>Есть</i>	<i>Нет</i>
<i>Автоматизация</i>	<i>Ограничена возможностями плагинов</i>	<i>Высокая автоматизация процессов</i>
<i>Анализ данных</i>	<i>Ограничена возможностями плагинов</i>	<i>Глубокий анализ</i>
<i>Масштабируемость</i>	<i>Зависит от выбора CMS и плагинов</i>	<i>Зависит от данных и машинного обучения</i>
<i>Стоимость</i>	<i>Есть как полностью бесплатные, так и коммерческие решения</i>	<i>Высокие затраты на разработку</i>

Примеры использования

Системы управления контентом (CMS) - являются идеальным выбором для пользователя, который планирует создать собственный веб-сайт например: блог, интернет-магазин или сайт-визитку. Используя готовые шаблоны и плагины у пользователя появляется возможность разработать и запустить сайт за короткий промежуток времени.

Системы искусственного интеллекта (AI) – являются хорошим выбором для больших проектов таких как маркетплейсы которые имеют большое количество пользователей. Благодаря внедрению искусственного интеллекта появляются возможности автоматической автоматизации большинства процессов на сайте.

Заключение

Системы управления контентом и AI-системы имеют разные роли в разработке и управлении веб-контентом. Главное преимущество CMS это предоставление готовых шаблонов и плагинов для быстрой и эффективной разработки. Поэтому CMS являются отличным выбором для тех, кто хочет разработать небольшой средний проект, не имея при этом глубоких знаний в программировании. AI-системы, же более подходящие для масштабных проектов, которые требуют большей автоматизации процессов и более глубокого анализа входящих данных. Какую же систему выбрать зависит от времени, масштабов и бюджета проекта.

1. Что Такое WordPress? Обзор Самой Популярной CMS. — Текст: электронный // Hostinger : [сайт]. — URL: <https://www.hostinger.ru/rukovodstva/chto-takoe-wordpress-obzor-populjarnoj-cms/> (дата обращения: 25.05.2024).
2. Как создать сайт с помощью нейросети. — Текст: электронный // habr: [сайт]. — URL: <https://habr.com/ru/articles/816549> (дата обращения: 25.05.2024).
3. Горнаков С.Г. Осваиваем популярные системы управления сайтом. - М.: ДМК Пресс, 2019. – 336 с.
4. Как создать сайт с помощью нейросети: ТОП-25 ИИ для создания сайта. — Текст: электронный // craftum: [сайт]. — URL: https://craftum.com/blog/ispolzovanie-nejrosetej-v-sozdanii-sajtov-top-10-servisov/?is_ai_link_active=true
5. Гениатулина Е.В. CMS - системы управления контентом. – Н.: Издво-НГТУ, 2019. – 63 с.

Павличенко Е.А., Якубайлик О.Э.

Региональная система оперативного спутникового мониторинга

*Федеральный исследовательский центр
«Красноярский научный центр СО РАН»
(Россия, Красноярск)*

doi: 10.18411/trnio-10-2024-399

Аннотация

В статье рассматривается общая структура и особенности реализации программного обеспечения региональной системы оперативного космического мониторинга на базе приемных станций данных дистанционного зондирования Земли в г. Красноярске. Система решает задачи первичной обработки принимаемых данных ДЗЗ, создания производных тематических информационно-продуктов, формирования архивов спутниковой информации.

Ключевые слова: данные дистанционного зондирования Земли, система оперативного космического мониторинга, AQUA, NOAA, TERRA, спутниковый приемный комплекс, архив данных ДЗЗ.

Abstract

The article discusses the overall structure and features of the software implementation of the regional operational space monitoring system, based on receiving stations for Earth remote sensing data in Krasnoyarsk. This system solves the problems of primary processing of the received remote sensing data, creating derived thematic information products, and forming satellite information archives.

Keywords: Earth remote sensing data, operational space monitoring system, AQUA, NOAA, TERRA, satellite receiving station, remote sensing data archive.

Создание комплекса приема и обработки данных с космических аппаратов дистанционного зондирования Земли (ДЗЗ) позволяет использовать принятую информацию с минимальной задержкой в различных системах принятия решения и управления регионального уровня и упростить доступ к тематическим продуктам ДЗЗ для научных исследований.

В настоящее время корпорация Роскосмос создает Единую территориально-распределенную информационную систему дистанционного зондирования Земли (ЕТРИС ДЗЗ), призванную обеспечить целевое применение отечественной группировки космических аппаратов дистанционного зондирования Земли из космоса и предоставления информации ДЗЗ и информационных продуктов на ее основе широкому кругу потребителей. ЕТРИС ДЗЗ создана как территориально-распределенная сеть станций и комплексов, обеспечивающих приём и обработку информации с российских КА ДЗЗ, а также её доведение потребителям. В перечень наземных объектов ЕТРИС ДЗЗ входят несколько центров приема на территории России и за ее пределами [1]. Данная система является федеральной и основана на приеме и обработке данных с отечественных спутников, имеет свой геопортал для обеспечения доступа к данным и нацелена на решение задач как на федеральном, так и на региональном уровнях. Недостатком этой системы можно назвать невозможность получения данных за длительный период наблюдений, небольшое количество тематических продуктов, большое время доступа к данным, также, остается необходимость локального хранения больших объемов данных при работе с большой территорией или на больших временных отрезках.

Созданная в Красноярском научном центре СО РАН система приема и обработки данных ДЗЗ работает на прием данных с метеорологических спутников NASA и Китая, а также на закачивание данных высокого разрешения со спутников Landsat и Sentinel-2. Система нацелена на работу на региональном уровне и обеспечении данными дистанционного зондирования научных работ по изучению лесного покрова, сельскохозяйственных угодий и водных объектов.

Приемный комплекс системы основан на базе двух станций приема УниСкан-36 [2] производства компании «Сканэкс», одна из которых была приобретена Сибирским федеральным университетом, и в настоящее время находится в оперативном управлении ФИЦ КНЦ СО РАН. За этот период на обеих станциях приемного комплекса была проведена модернизация программного обеспечения для возможности приема и включения в расписание нового спутника программы Suomi-NPP – NOAA-21, запущенного в конце 2022 года (запуск состоялся 10 ноября 2022 г., а выход на оперативный режим 29 марта 2023 г.).

Аппаратно-программное обеспечение регионального центра ДЗЗ строится по модульному принципу, как совокупность функционально самостоятельных компонентов. Логическими единицами системы являются группы серверов обработки спутниковых данных: 1) приема, 2) предварительной обработки, 3) тематической обработки. Программное обеспечение реализуется в сервис-ориентированной архитектуре, на основе открытого и свободно распространяемого программного обеспечения. Интерфейс пользователя создается на основе стандартного веб-браузера, с использованием технологий геоинформационных веб-систем и геопорталов, концепции инфраструктуры пространственных данных.

Создание интерактивных веб-сервисов оперативного представления и экспресс-анализа спутниковой информации в «квазиреальном» режиме времени – конечные данные становятся доступными в течение часа после завершения сеанса приема. Для спутниковых данных

основных низкоорбитальных метеорологических спутников (Terra/Aqua, Suomi NPP/NOAA-20/NOAA-21) автоматически формируется коллекция мультимасштабных композитных изображений с популярными комбинациями спектральных каналов, значимыми характеристиками (вегетационные индексы, яркостная температура, и др.). Географическое положение Красноярска в центре России обеспечивает практически ежедневное покрытие значительной части территории страны несколько раз в сутки.

Развиваемая в ФИЦ КНЦ СО РАН система оперативного космического мониторинга в части программного обеспечения для приема данных построена на основе пакета IPOPP (International Planetary Observation Processing Package) [3], который включает предварительную обработку принятых данных и большое количество специализированных программных пакетов тематической обработки данных дистанционного зондирования для спутников NASA. Данный пакет расширяет возможности поставляемого коммерческого пакета программ обработки данных спутниковой информации от фирмы «Сканэкс». В настоящее время он стал одним из стандартов де факто в дистанционном зондировании Земли и позволяет с наименьшими усилиями организовать оперативную работу. Кроме графической оболочки, IPOPP имеет набор инструментов командной строки для выполнения различных операций, настроек и мониторинга работы.

В составе IPOPP имеется набор специализированных пакетов обработки спутниковых данных, называемые научными алгоритмами – Science Processing Algorithms (SPA). Результатом работы пакета программ этих алгоритмов являются различные тематические продукты: активные пожары (Active Fires MOD14), содержание аэрозолей в атмосфере – Aerosol SPA, алгоритм картирования гарей, алгоритм вычисления температуры земной поверхности и другие алгоритмы, для спутников Aqua/Terra и NOAA-20/JPSS-1. Выходные продукты имеют различные файловые форматы и разделяются по уровням обработки – от 0-го до 2-го уровня. Выходные данные программного пакета IPOPP разбиваются по каталогам уровней обработки. Для возможности использования полученных тематических продуктов в геопортале и обеспечения доступа к данным для реализации научных исследований, тематические продукты спутниковых данных необходимо упорядочить и систематизировать на сервере хранения. Для этого был разработан набор вспомогательных программ и сервисов, который кроме систематизации выходных продуктов обеспечивает автоматизацию процесса подачи принятых данных для вычисления и последующего хранения в архивах [4].

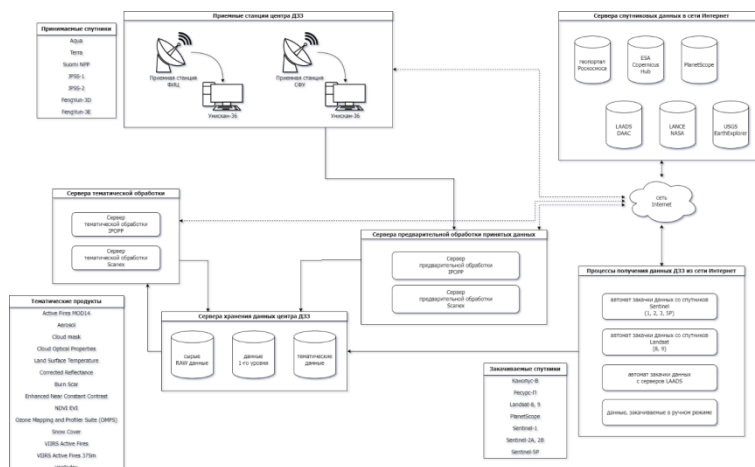


Рисунок 1. Общая схема получения, обработки и хранения спутниковых данных в региональном центре ДЗЗ.

Формируемый каталог данных дистанционного зондирования ФИЦ КНЦ СО РАН не ограничивается информацией, поступающей с приемных комплексов УниСкан-36 – он пополняется данными, поступающими с российских космических аппаратов через геопортал Роскосмоса и данными, принимаемыми зарубежными спутниками Sentinel, Landsat, и др. Общая схема приема, обработки, загрузки и хранения данных представлена на Рисунке 1.

Российские спутниковые данные поступают через геопортал Роскосмоса. На сегодняшний день – в основном это снимки со спутника Канопус-В. Данные централизованно загружаются для нужд всех подразделений, входящих в ФИЦ КНЦ СО РАН, по общей заявке для всех подразделений. Доступ к данным осуществляется по локальной сети ФИЦ КНЦ СО РАН через созданный геопортал.

Для спутниковых данных Sentinel и Landsat разработаны программные сервисы, обеспечивающие полностью автоматизированное скачивание данных и упорядоченное хранение, их предварительную обработку, формирование информационных продуктов для визуализации на собственном геопортале. Процедуры получения данных используют Sentinel Hub API и учитывают существующие особенности режимов доступа к данным [5].

На основе принимаемой спутниковой информации решаются различные научно-исследовательские и прикладные задачи – выявление температурных аномалий и пожаров, динамики растительного покрова, определение различных характеристик облачности и аэрозолей, оценка состояния снежного покрова и связанное с ним моделирование паводковых ситуаций.

1. Ромашкин В.В., Лошкарев П.А., Федоткин Д.И., Тохиян О.О., Арефьева Т.А., Мусиенко В.А. ЕТРИС ДЗЗ – современные решения в развитии отечественной наземной космической инфраструктуры дистанционного зондирования земли из космоса // Современные проблемы дистанционного зондирования Земли из космоса. 2019. Т. 16. № 3. С. 220-227.
2. Гершензон О.Н., Маслов А.А. Оперативный спутниковый мониторинг на базе универсальной приемной станции УниСкан™ // Гео-Сибирь. 2005. Т. 5. С. 46-50.
3. Patrick L. Coronado, John Overton, Kelvin W. Brentzel. International Polar-Orbit Processing Package Framework for Earth Remote Sensing Science Data Processing // URL: https://directreadout.sci.gsfc.nasa.gov/publications_documents/IPOPP_Framework.pdf (дата обращения: 30.09.2024).
4. Павличенко Е. А. Программа автоматизации обработки архивных и оперативных данных со спутников MODIS/AQUA И NPP/NOAA20 с использованием комплекса IPOPP // Свидетельство о регистрации программы для ЭВМ 2022664753, 04.08.2022.
5. Павличенко Е. А. Программа автоматической зачатки архивных и оперативных данных со спутников Sentinel-1, 2A, 2B, 5P // Свидетельство о регистрации программы для ЭВМ 2022664714, 04.08.2022.

Савкина А.В., Матвеев Е.С.

Формирование базы данных для интернет-площадки

*Мордовский государственный университет им. Н.П. Огарёва
(Россия, Саранск)*

doi: 10.18411/trnio-10-2024-400

Аннотация

В статье рассматривается создание базы данных для хранения информации для успешного управления чат-ботом, как одной из составных частей программного обеспечения интернет-площадок. Для правильного взаимодействия её с остальными объектами надо учитывать различные взаимосвязи между отдельными сущностями, их внутреннюю структуру и типы отношений. В статье приводятся диаграммы, представляющие логическое представление модели: диаграмма классов, диаграмма развертывания, ER-диаграмма.

Ключевые слова: чат-бот; база данных; диаграмма классов; диаграмма развертывания; ER-диаграмма.

Abstract

The article discusses the creation of a database for storing information for the successful management of a chatbot, as one of the components of the software of Internet platforms. For its proper interaction with other objects, it is necessary to take into account the various relationships

between individual entities, their internal structure and types of relationships. The article provides diagrams representing the logical representation of the model: class diagram, deployment diagram, ER diagram.

Keywords: chatbot; database; class diagram; deployment diagram; ER diagram.

Для формирования базы данных необходимо сформировать диаграмму классов, которая является основным логическим представлением модели и служит для представления статической структуры модели системы в терминологии классов объектно-ориентированного программирования. Диаграмма классов может отражать, в частности, различные взаимосвязи между отдельными сущностями предметной области, такими как объекты и подсистемы, а также описывает их внутреннюю структуру и типы отношений.

Диаграмма классов взаимодействия приведена на рисунке 1.

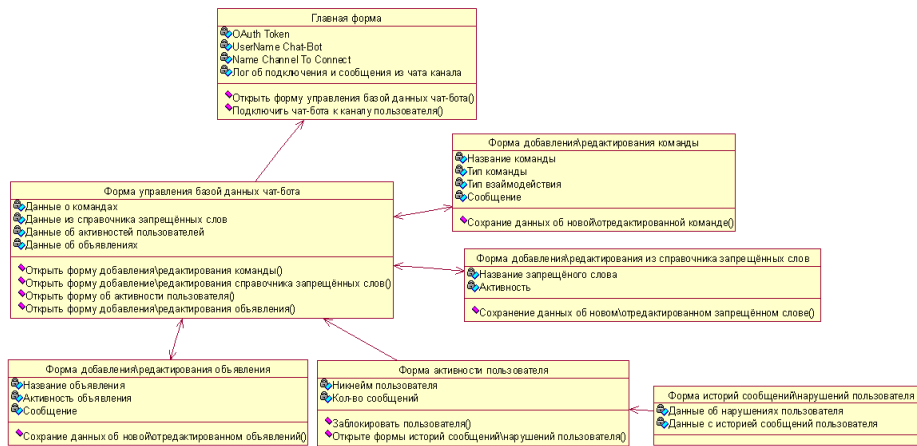


Рисунок 1. Диаграмма классов системы.

На спроектированной диаграмме классов представлены основные классы системы, такие как: главная форма, форма управления базой данных чат-бота, форма добавления и редактирование команды, форма добавления и редактирование из справочника запрещённых слов, форма добавления и редактирования объявления, форма активности пользователя, форма историй сообщений и нарушений пользователя, а также как администратор взаимодействуют с приложением и как в системе происходит взаимодействие между элементами.

С технической точки зрения интернет площадка состоит из трех основных компонентов: устройство пользователя, сервер API Twitch, база данных. Под устройством пользователя подразумевается компьютер, имеющий доступ в Интернет. Диаграмма развертывания для такой системы представлена на рисунке 2.

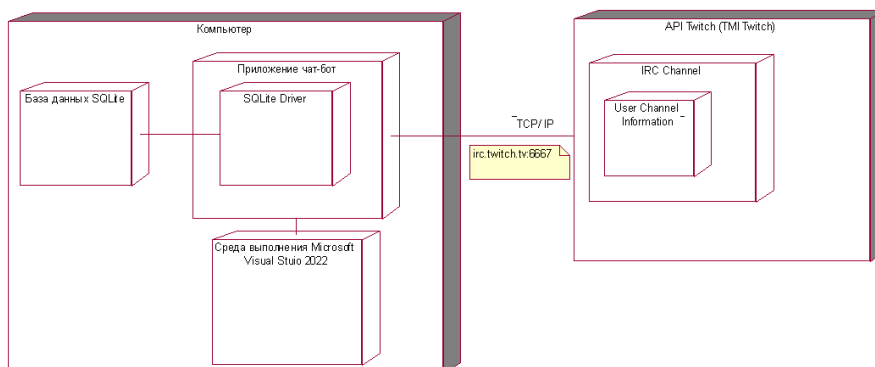


Рисунок 2. Диаграмма развёртывания.

Для успешного проектирования информационной системы одним из главных этапов является построение ER-диаграммы, которая помогает провести анализ требований к будущему программному продукту, она показывает отношения наборов сущностей, хранящихся в базе данных. Сущность в этом контексте – это объект, компонент данных. Эти объекты могут иметь атрибуты, определяющие его свойства. Благодаря определению сущностей, атрибутов и отображению взаимосвязей между ними ER-диаграмма иллюстрирует логическую структуру базы данных. Такие диаграммы чаще всего применяются при проектировании реляционных баз данных, но могут составляться и для не реляционных баз. В нашем случае ER-диаграмма составлена для базы данных SQLite. Одной из главных особенностей SQLite является простота в использовании и интеграции. База данных SQLite представляет собой единственный файл, который может быть легко встроен в приложение или использован как локальное хранилище данных. Он не требует настройки сервера и может работать на различных платформах, включая Windows, macOS, Linux и мобильные устройства. SQLite обладает высокой производительностью и небольшим потреблением ресурсов, что делает его идеальным выбором для мобильных приложений, встроенных систем, настольных программ и других сценариев, где требуется небольшой и эффективный механизм хранения данных.

SQLite поддерживает широкий набор функциональности, включая создание таблиц, индексов, представлений, триггеров и сохранение данных в различных форматах, таких как числа, строки, даты и бинарные объекты, а также поддерживает расширяемость через использование плагинов и пользовательских функций. Частичная реализация кода будет иметь вид:

```
private void dataBase_btn_Click(object sender, EventArgs e)
{
    Form2 dataBaseForm = new Form2();

    if (dataBaseForm.ShowDialog() == DialogResult.OK)
    {
        Settings.Default["AnnounRate"] =
(Convert.ToDouble(dataBaseForm.rateAnnouInput.Text));
        Settings.Default.Save();

        SQLiteManagement.ClearAndUpdateTable("datacmd", dataBaseForm.cmdToDB, 4,
new List<string>
{
    "cmd",
    "value",
    "type",
    "use"
});

        SQLiteManagement.ClearAndUpdateTable("announcement",
dataBaseForm.announToDB, 3, new List<string>
{
    "name",
    "text",
    "enabled"
});
        SQLiteManagement.ClearAndUpdateDirForbWordTable(dataBaseForm.forbWordsT
oDB);
    }
    ...
}
```

ER-диаграмма представлена на рисунке 3.

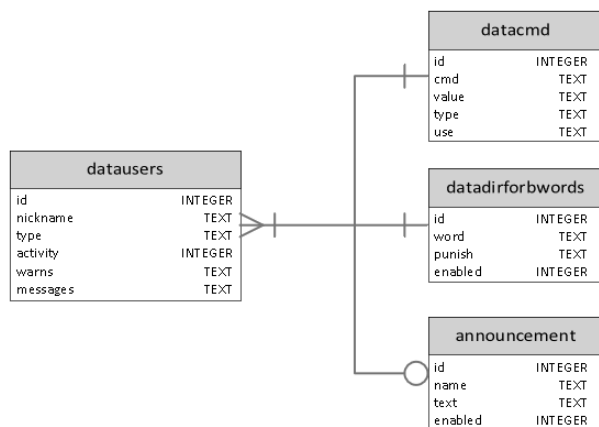


Рисунок 3. ER-диаграмма.

На данной диаграмме представлена структура базы данных. Некоторые сущности имеют общий набор полей, а также уникальные для каждого типа поля. Глобально приложение состоит из четырёх доменных сущностей взаимодействующие с чат-ботом, команда для взаимодействия, объявления, а также справочника запрещённых слов.

Рассмотрим более подробно как храниться информация о командах взаимодействия с чат-ботом, справочнике запрещённых слов, а также объявлений. В таблице команды для взаимодействия с чат-ботом созданы несколько колонок: команда, значение команды, тип использования, а также кто может его использовать.

Вид таблицы команды для взаимодействия с чат-ботом представлен на рисунке 4.

	cmd	value	type	use
	Фильтр	Фильтр	Фильтр	Фи...
1	!rand	rand{0,100}	0	0
2	!clear	/clear	1	1
3	!about	Создатель чат...	0	0
4	!social	vk - vk.com/...	0	0
5	!db	На кубике: ...	0	0
6	!d12	На кубике: ...	0	0

Рисунок 4. Таблица команд для взаимодействия с чат-ботом.

В данной таблице мы можем наблюдать уже созданные в системе команды для взаимодействия с чат-ботом. Администратор в приложение при создании команды указывает необходимые данные, если поля при сохранении данных отсутствуют приложение потребует заполнить необходимые поля, либо закрыть форму создания команды.

В колонке «type» указывается какой тип сообщение будет выводиться в чат, если при создании администратор указывает поле как «Текст», то в чат будет выводиться текстовое сообщение, в таблице базе данных значение указывается как «0». Если будет указано в поле как «Действие», то в чат будет выводиться как команда, которая выполняется уже на сайте чата, в таблице базе данных значение указывает как «1».

В колонке «use» указывается на кого чат-бот будет реагировать этой командой, если при создании администратор указывает поле как «Все», то чат-бот обязан реагировать на эту команду от всех пользователей чата, написавших её, в таблице базе данных значение указывается как «0». Если будет указано как «Модератор», то чат-бот обязан реагировать на эту

команду только от модераторов данного чата, в таблице базы данных значение указывается как «1».

Для хранения справочника запрещённых слов была создана отдельная таблица. В данной таблице были созданы несколько колонок: слово, наказание, а также статус.

Вид таблицы справочника запрещённых слов представлен на рисунке 5.

	word	punish	enabled
	Фильтр	Фильтр	Фильтр
1	Дурак	0	1

Рисунок 5. Таблица справочника запрещённых слов.

В колонке «punish» указывается какое наказание будет выдано пользователю чата, если при создании администратор указывает «Предупреждение», то чат-бот выдает начислит одно предупреждение и заблокирует пользователя на 10 секунд, в таблице базы данных значение указывается как «0». Если при создании указать «Блокировка», то чат-бот заблокирует пользователя чата навсегда, в таблице базы данных значение указывается как «1».

В колонке «enabled» указывается включено ли в обработку слово. Если при создании администратор указывает «Включено», то чат-бот будет проверять сообщение содержащее это слово, в таблице базы данных значение указывается как «1». Если при создании указывается «Выключено», то чат-бот не будет проверять сообщение, содержащее это слово, в таблице базы данных значение указывается как «0».

1. Вендров А. М. CASE-технологии. // Современные методы и средства проектирования информационных систем. М., 2004. - 238 с.
2. Лоре А. Проектирование веб-API / А. Лоре; [перевод с английского Д. А. Беликова]. М., 2020. – 440 с. – ISBN 978-5-97060-861-6.
3. Тузовский А. Ф. Проектирование и разработка web-приложений. М. 2018. – 218 с. – ISBN 978-5-534-10017-4.
4. SQLite – Wikipedia: сайт. – URL: <https://ru.wikipedia.org/wiki/SQLite> (дата обращения 03.06.2023). – Режим доступа: свободный. – Текст: электронный.

Серсултанов Х.Р., Магомадов Ш.А.

Цифровая игровая платформа

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-401

Аннотация

В 2023 году цифровые игровые платформы приобрели ключевое значение в распространении и продвижении игрового контента. Такие платформы, как Steam, Epic Games Store и консольные магазины, стали важными элементами экосистемы игр, предоставляя разработчикам возможности для выхода на глобальный рынок. Современные тенденции включают использование цифровых платформ для прямого взаимодействия с аудиторией, интеграции микротранзакций и маркетинга с помощью инфлюенсеров.

Ключевые слова: цифровая платформа, видеоигры, маркетинг, программные инструменты, игровая экосистема.

Abstract

In 2023, digital gaming platforms have become a key component in the distribution and promotion of game content. Platforms such as Steam, Epic Games Store, and console stores have emerged as crucial elements of the gaming ecosystem, providing developers with opportunities to reach global markets. Modern trends include using digital platforms for direct audience engagement, integrating microtransactions, and influencer marketing.

Keywords: digital platform, video games, marketing, software tools, gaming ecosystem.

Цифровые игровые платформы играют важную роль в индустрии видеоигр, предоставляя разработчикам возможность напрямую продавать и продвигать свои проекты. С развитием технологий и увеличением числа игроков по всему миру, такие платформы обеспечивают глобальный доступ к играм и становятся важным элементом экосистемы цифрового маркетинга. Эти платформы также способствуют развитию современных бизнес-моделей, таких как подписки, микротранзакции и DLC (загружаемый контент).

Цифровые игровые платформы предоставляют множество возможностей для маркетинга и взаимодействия с пользователями. К основным инструментам относятся:

1. Магазины приложений и игр: Платформы, такие как Steam, PlayStation Store и Google Play, позволяют разработчикам размещать игры на глобальном рынке, получая доступ к миллионам пользователей.
2. Рейтинговые системы и обзоры: Пользователи могут оставлять отзывы и оценки, что помогает формировать общественное мнение о продукте и влияет на его популярность.
3. Интеграция социальных сетей: Взаимодействие с игроками через платформы и социальные медиа позволяет компаниям использовать инфлюенсеров и стримеров для продвижения своих игр.
4. Микротранзакции: Многие платформы интегрируют микротранзакции, что помогает разработчикам зарабатывать на бесплатных или условно-бесплатных играх через продажи внутриигровых предметов.

Современные цифровые платформы играют важную роль в маркетинговой стратегии игр. Важнейшими тенденциями стали:

- Реклама через стримеров и инфлюенсеров: Стримеры и популярные игроки, используя такие платформы, как Twitch и YouTube, создают бесплатные рекламные кампании для игр, влияя на целевую аудиторию.
- Микротаргетинг и персонализация: Платформы могут использовать данные о поведении игроков для создания персонализированных предложений, улучшая пользовательский опыт.
- Виртуальные события и турниры: Многие компании используют платформы для проведения виртуальных мероприятий и киберспортивных турниров, что помогает вовлекать новых пользователей.

Цифровые игровые платформы оказали значительное влияние на динамику рынка видеоигр. С одной стороны, они упростили доступ малым и независимым разработчикам к глобальной аудитории, что позволило инди-проектам конкурировать с крупными издателями. С другой стороны, цифровые платформы стали средой для интенсивной конкуренции, где успех игры во многом зависит от маркетинговых усилий, пользовательских обзоров и продвижения через алгоритмы рекомендаций. Кроме того, использование игровых подписок (например, Xbox Game Pass) и раннего доступа стимулирует вовлечение игроков и поддерживает интерес к проектам еще на этапе их разработки.

С развитием технологий, таких как облачные вычисления и искусственный интеллект, цифровые игровые платформы продолжают эволюционировать. Облачные платформы, такие как Google Stadia и NVIDIA GeForce Now, предлагают возможность играть в высокопроизводительные игры без необходимости владения мощным оборудованием, что расширяет доступность игр для широкой аудитории. Искусственный интеллект, в свою

очередь, помогает улучшить рекомендации контента, анализируя предпочтения пользователей и предлагая игры, которые соответствуют их интересам. В будущем ожидается дальнейшая интеграция платформ с технологиями виртуальной и дополненной реальности, что создаст новые возможности для взаимодействия с игровым контентом и продвижения продуктов через новые форматы.

Современные цифровые игровые платформы не только предоставляют доступ к играм, но и активно развивают социальные функции, способствующие взаимодействию между игроками. Социальные сети, встроенные в платформы, такие как Steam, PlayStation Network и Xbox Live, позволяют пользователям общаться, делиться игровыми моментами, организовывать совместные сессии и соревнования. Эти функции стимулируют создание игровых сообществ, что способствует увеличению вовлеченности пользователей и формированию лояльной аудитории. В будущем можно ожидать еще большего углубления социальных аспектов, включая интеграцию с платформами стриминга, что сделает процесс игры и взаимодействия с другими игроками еще более интерактивным и персонализированным.

Цифровые игровые платформы также изменили подходы к монетизации игр. В дополнение к традиционным покупкам игр, активно используются модели free-to-play, которые основываются на микротранзакциях, внутриигровых покупках и подписках. Такая модель позволяет привлечь большее количество игроков, снижая барьер для входа, но одновременно создавая возможности для постоянного дохода от активных пользователей. Кроме того, игровые платформы все чаще фокусируются на улучшении пользовательского опыта через персонализацию интерфейса, удобные методы оплаты и интеграцию социальных элементов, что способствует удержанию аудитории и созданию активного сообщества вокруг игр.

Заключение

Цифровые игровые платформы становятся неотъемлемой частью современной игровой индустрии, обеспечивая глобальную взаимосвязь между разработчиками и игроками. Они не только предлагают удобный и доступный способ распространения игр, но и предоставляют возможность выстраивать долгосрочные отношения с пользователями через цифровые экосистемы. На этих платформах игроки могут находить новые проекты, участвовать в игровом процессе, взаимодействовать с сообществом и вносить вклад в развитие игр через отзывы и рейтинги.

Успех на цифровых платформах требует от разработчиков и издателей внедрения передовых маркетинговых подходов. Одним из ключевых факторов является сотрудничество с инфлюенсерами, которые помогают создавать доверие к бренду и расширять аудиторию, продвигая игры на глобальном уровне. Благодаря популярности стриминговых сервисов и социальных сетей, влияние таких маркетинговых кампаний стало значительно выше, чем в традиционных рекламных каналах. Это позволяет не только привлечь внимание к игре, но и увеличить её продажи в краткосрочной и долгосрочной перспективе.

Кроме того, персонализация предложений играет важную роль в повышении уровня вовлеченности пользователей. Современные цифровые игровые платформы предлагают персонализированные рекомендации на основе предпочтений игроков, что способствует увеличению времени, проводимого в игре, и повышению лояльности аудитории. Это достигается с помощью анализа данных о поведении игроков, что позволяет предлагать контент и внутриигровые акции, адаптированные под каждого пользователя.

Микротранзакции также стали важным элементом монетизации игр на цифровых платформах. Они позволяют не только увеличивать доходы разработчиков, но и обеспечивают игрокам возможность персонализировать свой игровой опыт через покупку дополнительных предметов, косметических улучшений или контента. Однако для успешного использования данной модели важно поддерживать баланс между привлекательностью микротранзакций и их влиянием на игровой процесс, чтобы не снижать удовлетворенность пользователей.

Цифровые игровые платформы трансформируют игровой рынок, предлагая новые возможности для продвижения игр и взаимодействия с игроками. Для успешного продвижения и монетизации на этих платформах необходимо учитывать современные тенденции в маркетинге, включая работу с инфлюенсерами, персонализацию предложений и внедрение микротранзакций, создавая тем самым устойчивую экосистему, которая способствует росту и развитию игровой индустрии.

1. Steamworks. Цифровое распространение и публикация игр — Текст: электронный // Steam: [сайт]. — URL: <https://partner.steamgames.com/> (дата обращения: 18.09.2024).
2. Важность маркетинга с влиятельными лицами в игровой индустрии — Текст: электронный // Newzoo: [сайт]. — URL: <https://newzoo.com/influencer-marketing/> (дата обращения: 18.09.2024).
3. Микротранзакции в видеоиграх: преимущества и проблемы — Текст: электронный // Game Developer: [сайт]. — URL: <https://www.gamedeveloper.com/business/microtransactions-in-video-games/> (дата обращения: 18.09.2024).

Табашников А.П.

**Подходы к анализу публикационной активности
и обзор существующих программных решений**

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-402

Аннотация

В статье рассматриваются подходы к анализу публикационной активности и даётся обзор существующих программных решений для обработки и визуализации данных. Также обсуждаются качественные методы, включая анализ контекста цитирования и экспертную оценку. Особое внимание уделяется программным решениям, которые позволяют автоматизировать процесс анализа и эффективно визуализировать результаты.

Ключевые слова: публикационная активность, количественные методы, качественные методы, визуализация данных, цитирование, программные решения.

Abstract

The article discusses approaches to the analysis of publication activity and provides an overview of existing software solutions for data processing and visualization. Qualitative methods are also discussed, including citation context analysis and peer review. Special attention is paid to software solutions that allow you to automate the analysis process and effectively visualize the results.

Keywords: publication activity, quantitative methods, qualitative methods, data visualization, citation, software solutions.

Подходы к анализу публикационной активности можно разделить на традиционные и современные, каждый из которых имеет свои преимущества и ограничения. Традиционные подходы основываются на проверенных временем методах библиометрии и наукометрии, которые используют статистические и математические инструменты для оценки научной деятельности. Современные подходы включают в себя использование машинного обучения и текстового анализа, предлагая новые возможности для обработки и интерпретации больших объемов данных.

Традиционные подходы к анализу публикационной активности основываются на проверенных временем методах библиометрии и наукометрии. Эти методы используют статистические и математические инструменты для оценки научной продуктивности и влияния исследователей, организаций и научных журналов [1]. Основные традиционные подходы, а также их описание, представлены в таблице 1.

Таблица 1

Описание основных традиционных подходов.

<i>Подход</i>	<i>Описание</i>	<i>Преимущества</i>	<i>Ограничения</i>
<i>Наукометрический анализ</i>	<i>Количественное исследование динамики научного развития с использованием метрик (индекс Хирша, SNIP, SJR).</i>	<i>Выявление ключевых тенденций, оценка эффективности научных программ.</i>	<i>Может быть сложен в интерпретации, требует качественных данных.</i>
<i>Библиометрический анализ</i>	<i>Количественное исследование научных публикаций с использованием различных метрик (количество публикаций, число цитирований, индекс Хирша, импакт-фактор).</i>	<i>Объективные данные, возможность сравнительного анализа.</i>	<i>Не всегда учитывает качество публикаций и контекст цитирования.</i>
<i>Цитатный анализ</i>	<i>Изучение паттернов цитирования научных работ для выявления наиболее влиятельных публикаций.</i>	<i>Помогает понять распространение идей и влияние работ.</i>	<i>Может быть предвзятым в пользу популярных тем, не учитывает контекст.</i>
<i>Анализ соавторства</i>	<i>Исследование сотрудничества между учеными, анализ научных сетей.</i>	<i>Выявление ключевых коллективов, понимание структуры сотрудничества.</i>	<i>Может не отражать все аспекты взаимодействий между учеными.</i>

Следующим подходом к анализу публикационной активности является современный. Данные способы предоставляют более гибкие и точные инструменты для исследования научной продуктивности и влияния. Они позволяют автоматизировать и улучшить процессы анализа, предоставляя глубокие и комплексные данные для принятия обоснованных решений и стратегического планирования в области науки и исследований. Классификация основных современных методов анализа публикационной активности отражена в таблице 2.

Таблица 2

Классификация основных современных методов.

<i>Подход</i>	<i>Описание</i>	<i>Преимущества</i>	<i>Ограничения</i>
<i>Машинное обучение</i>	<i>Использование алгоритмов для классификации, кластеризации и предсказания тенденций в научных данных.</i>	<i>Выявление скрытых паттернов, автоматизация анализа, высокая точность.</i>	<i>Требует больших объемов данных и вычислительных ресурсов.</i>
<i>Текстовый анализ (NLP)</i>	<i>Обработка и анализ текстовых данных для выявления ключевых тем и тенденций.</i>	<i>Автоматизация анализа содержания, создание карт знаний, выявление новых направлений.</i>	<i>Сложность обработки и интерпретации естественного языка.</i>
<i>Анализ социальных сетей</i>	<i>Исследование структуры и динамики взаимодействий между исследователями и научными коллективами.</i>	<i>Визуализация научных сотрудничеств, оценка влияния сетевых взаимодействий.</i>	<i>Может быть сложен в интерпретации сетевых данных.</i>
<i>Big Data и Data Mining</i>	<i>Обработка и анализ больших объемов данных для извлечения полезной информации.</i>	<i>Высокая точность и эффективность анализа, автоматизация процессов.</i>	<i>Требует больших вычислительных ресурсов и навыков работы с данными.</i>
<i>Анализ цитатного контекста</i>	<i>Изучение контекста, в котором упоминаются научные работы.</i>	<i>Понимание использования и восприятия результатов исследований.</i>	<i>Сложность в обработке и интерпретации контекстуальных данных.</i>

Семантический анализ	Использование ИИ для понимания смысла текстов и выявления отношений между понятиями.	Глубокий анализ содержания, выявление скрытых связей и паттернов.	Требует сложных алгоритмов и мощных вычислительных ресурсов.
----------------------	--	---	--

Таким образом, благодаря проведенному анализу традиционных и современных подходов можно сделать вывод, что их сочетание может обеспечить наиболее полное и комплексное понимание публикационной активности. Традиционные методы предоставляют надежную базу для количественного анализа, в то время как современные методы позволяют учитывать качественные аспекты и анализировать большие и сложные данные [3]. Комбинированное использование этих подходов способствует более точному и всестороннему анализу, что важно для принятия обоснованных решений в области науки и исследований.

Существует множество программных решений для анализа публикационной активности, предназначенных для оценки научной продуктивности и влияния. Данные инструменты могут быть, как бесплатными и простыми в использовании, так и сложными коммерческими платформами с широкими функциональными возможностями. В этом разделе будут рассмотрены наиболее известные и широко используемые программные решения.

InCites от Clarivate Analytics — это мощная аналитическая, коммерческая платформа, предназначенная для глубокого анализа научной деятельности и публикационной активности. Интеграция с базой данных Web of Science обеспечивает доступ к высококачественным данным, что делает InCites одним из наиболее авторитетных инструментов в этой области. Платформа предлагает обширные возможности для анализа цитирований, научной продуктивности и сотрудничества [4]. InCites помогает выявлять ключевые научные направления, оценивать влияние публикаций и определять наиболее продуктивных авторов и организации. Одна из важных функций InCites — анализ сотрудничества, который визуализирует и анализирует взаимодействия между учеными, организациями и странами. Это помогает понять структуру научных сетей и выявить ключевых партнеров. Платформа также предоставляет возможности для оценки научных журналов, что помогает исследователям выбирать наиболее подходящие издания для публикации своих работ. Как выглядит интерфейс данной программы можно изучить на рисунке 1.

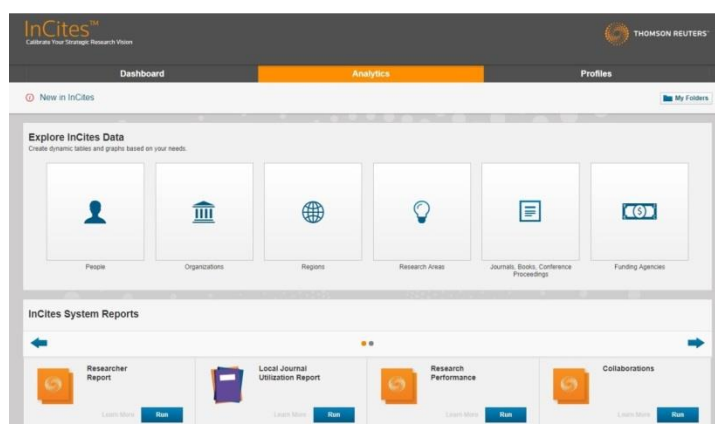


Рисунок 1. Интерфейс платформы InCites.

SciVal также является коммерческим продуктом. Данный аналитический инструмент представлен компанией Elsevier, и работает на основе информации из базы данных Scopus. SciVal предоставляет обширные возможности для анализа публикационной активности, включая оценку продуктивности, выявление научных трендов, анализ сотрудничества и стратегическое планирование. SciVal позволяет исследователям и администраторам создавать визуальные отчеты и дашборды, которые помогают наглядно представлять данные. Преимущества SciVal включают доступ к данным из Scopus, мощные аналитические

инструменты и гибкость настройки отчетов. Основным ограничением является высокая стоимость лицензии, что может быть препятствием для небольших учреждений и индивидуальных пользователей.

Dimensions — это комплексная аналитическая платформа, которая объединяет данные о публикациях, цитированиях, грантах, клинических испытаниях и патентах. Она предоставляет широкий спектр инструментов для анализа научной деятельности, включая библиометрический анализ, выявление исследовательских трендов и оценку научного влияния. Dimensions предлагает мощные функции поиска и фильтрации данных, что позволяет исследователям быстро находить релевантную информацию. Преимущества Dimensions включают интеграцию различных типов данных и возможность проведения комплексного анализа. Однако, как и другие коммерческие платформы, Dimensions требует значительных финансовых вложений для доступа к полной функциональности.

Следующим для рассмотрения будет предложен VOSviewer. Данный продукт является бесплатным инструментом для построения и визуализации библиометрических карт. Он позволяет исследователям создавать карты соавторства, карты цитирования и карты терминов на основе данных из Scopus, Web of Science и других источников. VOSviewer поддерживает анализ больших объемов данных и предоставляет мощные функции для визуализации научных сетей и выявления ключевых паттернов. Преимущества VOSviewer включают бесплатный доступ, мощные функции визуализации и поддержку различных источников данных [2]. Основное ограничение заключается в необходимости предварительной подготовки данных, что может требовать дополнительных усилий и навыков. Как выглядит интерфейс данного продукта отобразено на рисунке 2.

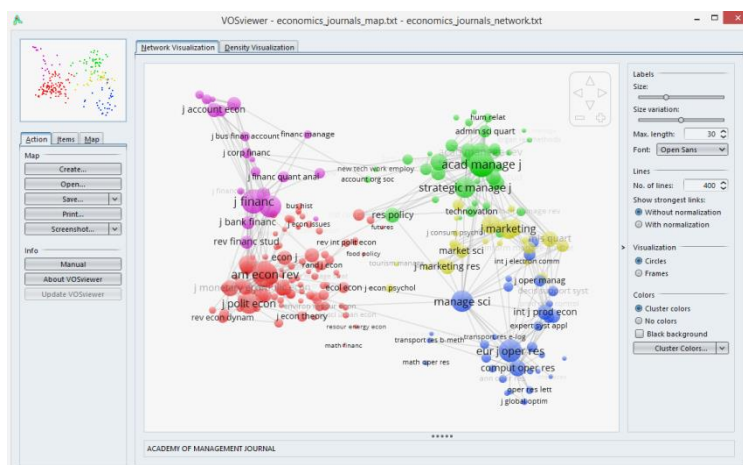


Рисунок 2. Интерфейс VOSviewer.

Таким образом, выбор конкретного программного решения зависит от потребностей и ресурсов пользователя. Комбинированное использование различных инструментов может обеспечить наиболее полное и точное понимание публикационной активности, что способствует повышению эффективности научных исследований и управления научной деятельностью.

1. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
2. VOSviewer. [Электронный ресурс]. URL: <https://www.vosviewer.com/>. (дата обращения: 30.09.2024.)
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

Табашников А.П.

Угрозы информационной безопасности, векторы атак и концепции хакинга

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)

doi: 10.18411/trnio-10-2024-403

Аннотация

В статье рассматриваются ключевые угрозы информационной безопасности, векторы атак и концепции хакинга. Описаны основные угрозы, такие как вредоносное программное обеспечение, фишинг, атаки на веб-приложения, DDoS-атаки и хищение личных данных. Особое внимание уделено различным типам хакинга, включая белый, черный и серый хакинг, их особенности и правовые аспекты.

Ключевые слова: информационная безопасность, векторы атак, вредоносное ПО, фишинг, DDoS-атаки, хищение данных.

Abstract

The article discusses the key threats to information security, attack vectors and hacking concepts. The main threats such as malware, phishing, attacks on web applications, DDoS attacks and identity theft are described. Special attention is paid to various types of hacking, including white, black and gray hacking, their features and legal aspects.

Keywords: information security, attack vectors, malware, phishing, DDoS attacks, data theft.

Векторы атак в области информационной безопасности представляют собой разнообразные методы, посредством которых злоумышленники могут стремиться получить несанкционированный доступ к системам, сетям или данным. Существует множество угроз для информационной безопасности, каждая из которых обладает своим специфическим вектором атаки:

Вредоносное программное обеспечение. Оно представляет собой компьютерную программу, созданную с намерением нанести вред или причинить ущерб пользователям компьютера или сети. Вредоносное ПО может принимать различные формы, включая вирусы, троянские программы, шпионское ПО, рекламное ПО и другие. Они могут распространяться через различные каналы, включая вложения электронной почты, зараженные веб-сайты или через съемные носители. После установки на компьютер, вредоносное ПО может выполнять различные деструктивные действия, такие как кража личной информации, повреждение или удаление данных, замедление работы системы или даже полное отключение компьютера [1].

Фишинг. Он представляет собой метод кибератаки, направленный на получение конфиденциальной информации, такой как логины, пароли или данные банковских карт или любой другой ценной для злоумышленника информации путем обмана пользователей. Атака обычно осуществляется через электронную почту, социальные сети или сайты, имитирующие настоящие. Злоумышленник создает поддельный сайт или отправляет письмо от имени доверенной организации, запрашивая у жертвы личные данные [2]. Когда жертва предоставляет свои данные на фальшивом сайте или в ответе на поддельное письмо, злоумышленник получает доступ к этой информации и может использовать ее для своих целей.

Атаки на веб-приложения, направленные на уязвимости в приложениях: злоумышленники могут использовать SQL-инъекции или межсайтовый скриптинг для получения доступа к базе данных или похищения информации о пользователях. Принцип работы этих атак предлагается рассмотреть ниже:

- SQL-инъекция работает следующим образом: когда пользователь вводит данные через форму или другое поле ввода на веб-странице, эти данные могут быть использованы в SQL-запросе без необходимой проверки или очистки.

Если данные содержат SQL-команды, они могут изменить структуру базы данных, получить доступ к конфиденциальной информации или даже полностью взять под контроль приложение;

- Межсайтовый скриптинг работает следующим образом: злоумышленник внедряет клиентский скрипт в страницу веб-сайта. Когда жертва посещает эту страницу, скрипт выполняется на стороне клиента, что может привести к утечке чувствительной информации, перехвату сессий или выполнению других действий от лица жертвы. XSS-атаки часто происходят, когда данные пользователя отображаются обратно без надлежащей очистки и экранирования специальных символов.

DDoS-атака. Атака на информационную систему или сеть, которая направлена на создание условий, при которых пользователи не могут получить доступ к ресурсам системы или сети из-за значительного увеличения нагрузки на нее. Работает это следующим образом: злоумышленник использует большую сеть компьютеров (ботнет), которые одновременно отправляют огромное количество запросов к целевому серверу или сайту. Эти запросы настолько велики, что сервер не справляется с ними, и в результате становится недоступным для обычных пользователей. Принцип работы DDoS-атаки изображен на рисунке 1.

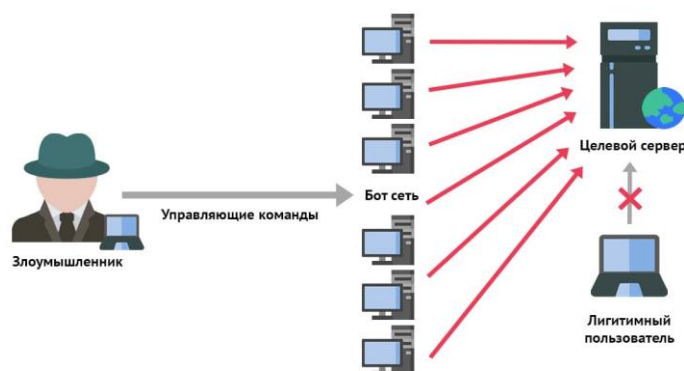


Рисунок 1. Принцип работы DDoS-атаки.

Хищение личных данных в области информационной безопасности. Это процесс незаконного получения и использования конфиденциальной информации о конкретном человеке или организации. Это может включать такие данные, как имена, адреса, номера телефонов, финансовая информация, медицинские записи и другие личные сведения. Хищение личных данных может происходить различными способами, включая хакерские атаки на компьютерные системы, кражу бумажных документов, использование социальных инженерных методов для обмана людей и получения доступа к их личным данным. После того, как злоумышленники получают доступ к личной информации, они могут использовать ее для мошенничества, кражи личности, шантажа или других преступлений.

Хакинг представляет собой процесс применения знаний и навыков для достижения определенной цели, часто связанный с информационными технологиями. Концепции хакинга включают следующие аспекты:

Белый хакинг, также известный как этичный хакинг или сканирование уязвимостей, представляет собой процесс тестирования безопасности компьютерных систем или сетей с целью выявления и устранения уязвимостей до того, как они будут использованы злоумышленниками. Это законная практика, которую используют специалисты по безопасности для оценки защищенности систем и помощи организациям в улучшении их мер безопасности. Белые хакеры обычно имеют разрешение на проведение таких тестов и следуют определенным правилам и процедурам, чтобы минимизировать риск нарушения работы системы или потери данных [3].

Черный хакинг, также известный как криминальный хакинг или киберпреступность, представляет собой незаконную практику использования компьютерных технологий для несанкционированного доступа к системам или сети с целью нанесения вреда, кражи информации или получения финансовой выгоды. Черные хакеры обычно действуют скрытно и стараются избежать обнаружения, используя различные методы, такие как взлом паролей, создание вредоносных программ или использование уязвимостей в системах. Черный хакинг является преступлением во многих странах и влечет за собой юридические последствия.

Серый хакинг, также известный как хакинг на грани, представляет собой практику тестирования безопасности компьютерных систем или сетей, которая находится на границе между белым и черным хакингом. Это означает, что действия серого хакера могут быть законными в некоторых контекстах, но незаконными в других. Например, серый хакер может взломать систему без разрешения владельца, но с целью показать уязвимости и помочь улучшить безопасность, а не с целью нанесения вреда или получения личной выгоды. Однако, поскольку действия серого хакера могут быть несанкционированными, они могут быть незаконными в некоторых юрисдикциях [4].

1. Кушнир Д. В., Платонова Т. А. ПРОГРАММИРОВАНИЕ КВАНТОВОГО КОМПЬЮТЕРА И ЕГО ЭМУЛЯЦИЯ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 754-758.
2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
3. Цветков А. Ю., Рузманов Е. Ю. РАССМОТРЕНИЕ МЕТОДОВ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПАНИИ //ББК 3 П27. – 2021. – С. 57.
4. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения //Интеллектуальные технологии на транспорте. – 2018. – №. 3 (15). – С. 47-54.

Филюшкин С.В.

**Применение гетерогенных структур СКУД
в современных кибер-физических системах**

*ООО «Лайнком»
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-404

Аннотация

Данная статья подчеркивает растущее значение гетерогенных систем СКУД в различных областях, таких как умные города, кибер-физические системы (КФС), промышленная автоматизация и системы умного дома. Контроль доступа (Access Control) является критическим компонентом безопасности КФС, обеспечивая защиту от несанкционированного доступа и потенциальных угроз. Часто система контроля и управления доступом (СКУД) в этих случаях представляет собой гетерогенную структуру, объединяющую устройства и протоколы различных типов. Более подробно рассмотрены назначение и состав, а также ключевые методы контроля доступа и угрозы, с которыми сталкиваются эти системы.

Ключевые слова: кибер-физические системы (КФС), контроль доступа (Access Control), система контроля и управления доступом (СКУД), гетерогенные системы СКУД, промышленная автоматизация, безопасность, неавторизованный доступ, протоколы, методы контроля доступа, потенциальные угрозы, модель угроз, внутренний контроль.

Abstract

This article highlights the growing importance of cyber-physical systems (CPS) in various fields such as smart cities, industrial automation, and smart home systems. Access control is a critical

component of CPS security, providing protection against unauthorized access and potential threats. Often, access control systems (ACS) in these cases represent a heterogeneous structure, integrating devices and protocols of various types. This paper will explore in more detail the purpose and composition of heterogeneous ACS, as well as key access control methods and challenges faced by these systems.

Keywords: cyber-physical systems (CPS), access control, access control system (ACS), heterogeneous systems, industrial automation, security, unauthorized access, protocols, access control methods, potential threats, threat model, internal control.

Методы контроля доступа

Рассмотрим несколько методов, которые используются для обеспечения контроля доступа в КФС:

1. Рольное управление доступом (RBAC):
Эта модель широко применяется в КФС благодаря своей гибкости и возможностям управления доступом [1] на основе ролей пользователей. Каждому пользователю назначается роль, а доступ к ресурсам предоставляется в зависимости от его роли. Например, инженер может получить доступ к одному набору данных, а системный администратор — к другому. Это упрощает управление большими системами с множеством пользователей, а также улучшает безопасность за счет четкого разграничения прав доступа.
2. Атрибутное управление доступом (ABAC):
ABAC основан на использовании атрибутов субъектов (пользователей), объектов (ресурсов) и условий (контекста) для принятия решений о предоставлении доступа. Эта модель обеспечивает более детализированное управление доступом и учитывает контекстные условия, такие как местоположение пользователя, время запроса доступа или состояние устройства. Это делает систему более гибкой и адаптируемой к сложным и динамическим условиям эксплуатации.
3. Контроль доступа на основе политики (PBAC):
PBAC использует предопределенные политики для управления доступом и принятия решений на основе формализованных правил. Этот подход позволяет автоматизировать принятие решений, делая процесс более быстрым и предсказуемым. Политики могут включать набор условий и действий, которые выполняются при определенных событиях или запросах.
4. Биометрические методы:
Биометрия становится все более популярной в СКУД благодаря возможности обеспечить высокий уровень безопасности и удобства. Отпечатки пальцев, распознавание лиц, голосовая идентификация и другие методы биометрической аутентификации позволяют предоставить доступ только авторизованным лицам, что исключает возможность использования утраченных или украденных учетных данных и аппаратных средств доступа.

Системы контроля доступа (СКУД) играют ключевую роль в обеспечении безопасности современных организаций. Они регулируют доступ к физическим и информационным ресурсам, что делает их важным элементом безопасности. СКУД могут различаться по своему устройству, функциональности и масштабируемости. Важно понимать различные типы таких систем для правильного выбора решения под конкретные условия.

СКУД можно разделить на несколько категорий в зависимости от их архитектуры и способов управления:

Автономные СКУД

Автономные СКУД — это простейшие системы, работающие без подключения к сети или центральному серверу. Они идеально подходят для небольших объектов, где требования к

интеграции с другими системами минимальны. Автономные системы работают локально, управляя доступом непосредственно на контроллере. [2]

Основные характеристики автономных СКУД:

Независимость от сети связи: не требуется подключения к серверу, что снижает зависимость от внешних систем.

Простота установки и эксплуатации: Быстрое развертывание без необходимости сложных настроек.

Ограниченные возможности: Невозможность интеграции с другими системами безопасности или удаленного управления.

Сетевые (централизованные) системы

Сетевые системы СКУД обеспечивают централизованное управление доступом с помощью единого сервера, координирующего все контроллеры и устройства. Они предлагают расширенные возможности для интеграции с другими системами и обеспечивают высокую масштабируемость.

Основные преимущества сетевых СКУД:

Централизованное управление: вся информация об управлении доступом хранится и обрабатывается на центральном сервере.

Масштабируемость: легко расширяются за счет добавления новых контроллеров и устройств.

Интеграция: могут быть связаны с другими системами, такими как видеонаблюдение или системы сигнализации.

Универсальные системы

Универсальные СКУД сочетают возможности как автономных, так и сетевых систем. Они могут работать как локально, так и через сеть, обеспечивая высокую гибкость. Такие системы часто применяются в средних и крупных организациях, где требуется гибкость и возможность масштабирования.

Характерные черты универсальных СКУД:

Гибкость в управлении: возможность работы в автономном или сетевом режимах.

Поддержка сложных сценариев: можно использовать различные сценарии управления доступом для разных объектов.

Легкость интеграции: Универсальные системы поддерживают работу с оборудованием различных производителей.

Биометрические системы

Биометрические СКУД обеспечивают высокий уровень безопасности, идентифицируя людей по уникальным физическим или поведенческим характеристикам, таким как отпечатки пальцев, радужка глаза или голос. Эти системы применяются в организациях с особыми требованиями к безопасности.

Основные преимущества биометрических СКУД:

Высокая надежность идентификации: Биометрические данные практически невозможно подделать.

Уникальные персональные данные: использование биометрии позволяет точно определить личность.

Интеграция с другими системами безопасности: Биометрические данные могут использоваться вместе с другими методами контроля доступа для создания многослойной системы безопасности, в том числе и для идентификации личности допускаемой на защищаемый объект системой СКУД.

Распределенные системы СКУД

Распределенные системы СКУД — это более сложные архитектурные решения, которые обеспечивают управление доступом на большом количестве удаленных объектов. Такие системы позволяют координировать работу нескольких удаленных точек, часто через Интернет или выделенные каналы связи.

Особенности распределенных СКУД:

Гибкость управления: Каждая точка контроля доступа может работать независимо, при этом данные централизованно обрабатываются.

Управление удаленными объектами: Система позволяет контролировать доступ на удаленные объекты и интегрировать различные устройства, находящиеся на значительном расстоянии друг от друга.

Повышенная надежность: благодаря распределенной архитектуре, при сбоях в одном участке системы остальные продолжают работать без перерыва.

Распределенные системы СКУД востребованы на предприятиях с несколькими филиалами или распределенными объектами, такими как складские помещения, удаленные офисы и промышленные площадки.

Гетерогенные системы СКУД

Введем понятие гетерогенной системы СКУД. Это системы контроля доступа, которые включают оборудование от разных производителей, что позволяет объединять различные устройства и технологии в одну единую систему. Однако, использование гетерогенных систем может приводить к ряду сложностей, таких как несовместимость протоколов, проблемы с интеграцией оборудования и сложность управления регистрами контроллеров.

Гетерогенные системы СКУД особенно актуальны на объектах, которые распределены, как территориально, так и административно. Это могут быть крупные предприятия с множеством филиалов или объекты с различными уровнями доступа и ответственности. Применение гетерогенных систем СКУД позволяет объединить уже имеющееся оборудование с новыми решениями, не требуя полной замены всей системы, что способствует экономии ресурсов и времени. [3]

Основные особенности и проблемы использования гетерогенных систем СКУД можно представить в таблице 1.

Таблица 1

Основные особенности и проблемы использования гетерогенных систем СКУД.

Параметр	Преимущества	Проблемы и сложности
Использование оборудования разных производителей	Позволяет интегрировать разнородные устройства СКУД, уже существующие в системе	Возможны проблемы совместимости из-за разных протоколов и стандартов
Гибкость в настройке	Системы могут адаптироваться под конкретные задачи, используя разные технологии	Требуется квалифицированный персонал для настройки и управления
Экономия на модернизации	Не требуется полная замена системы, можно добавлять новые компоненты постепенно	Могут возникать затраты на создание адаптеров или программных шлюзов
Масштабируемость	Систему легко расширить за счет добавления новых устройств от разных производителей	Сложность обеспечения единого уровня безопасности на всех объектах
Применение на распределенных объектах	Обеспечивает централизованное управление доступом на удаленных филиалах	Необходимость надежной связи между объектами и центром управления
Управление регистрами контроллеров	Можно интегрировать устройства с различными протоколами для максимальной гибкости	Разные контроллеры могут использовать несовместимые команды и протоколы

Примеры применения гетерогенных систем:

1. Крупные корпорации с многочисленными офисами и филиалами могут использовать оборудование от разных производителей для управления доступом, включая старые и новые устройства, поддерживая единую систему безопасности.
2. Производственные объекты могут интегрировать специализированные системы для отдельных зданий или зон, сохраняя общую инфраструктуру.

3. Административные комплексы часто нуждаются в гибкой настройке уровней доступа, что достигается с помощью различных типов контроллеров и устройств, работающих в единой системе.

Таким образом, гетерогенные системы СКУД находят широкое применение на объектах, которые требуют гибкости и многоуровневой защиты, обеспечивая надежное управление доступом из единого удаленного территориально центра, даже при использовании разнородных технологий.

Системы СКУД применяемые в Кибер-физических системах

Несмотря на преимущества описанных методов, системы контроля доступа в КФС сталкиваются с рядом угроз, которые требуют дальнейшего исследования и разработки решений.

1. Гетерогенность устройств:
КФС часто состоят из множества различных устройств и систем, которые могут использовать разные протоколы и стандарты безопасности. Это создает сложности в их интеграции и управлении доступом, так как необходимо обеспечить совместимость между различными компонентами системы. В связи с этим, гетерогенные системы СКУД требуют разработки универсальных протоколов и методов синхронизации для эффективной работы.
2. Масштабируемость:
По мере роста числа подключенных устройств и пользователей КФС возрастает необходимость в масштабируемых решениях для управления доступом. Системы должны быть способны обрабатывать большое количество запросов на доступ в реальном времени, при этом сохраняя высокую производительность, надежность и безопасность. Масштабируемость особенно важна в условиях умных городов и крупных промышленных объектов, где могут быть задействованы тысячи устройств.
3. Безопасность и конфиденциальность:
Защита данных и обеспечение конфиденциальности информации являются ключевыми аспектами контроля доступа в КФС и СКУД. В условиях постоянного обмена данными между устройствами и серверами, необходимо гарантировать, что информация остается защищенной от потенциальных атак и несанкционированного доступа. Важную роль в этом играют шифрование данных, аутентификация и мониторинг доступа. [4]
4. Эффективность и производительность:
Системы контроля доступа должны обеспечивать быструю и надежную работу даже при высоких нагрузках. Это требует оптимизации процессов обработки запросов и передачи данных, а также минимизации задержек в доступе к критическим ресурсам. Эффективность системы также влияет на её способность предотвращать атаки и обеспечивать своевременное реагирование на угрозы.

Перспективы и направления будущих исследований

Для того чтобы преодолеть текущие вызовы и повысить уровень безопасности и эффективности контроля доступа в СКУД, авторы предлагают несколько перспективных направлений для дальнейших исследований:

Интеграция систем СКУД с искусственным интеллектом (ИИ):

Использование ИИ и методов машинного обучения для разработки адаптивных и интеллектуальных систем контроля доступа. Такие системы могут автоматически изменять политики доступа в зависимости от поведения пользователей, времени суток или текущих угроз. Это позволит сделать системы более динамичными и эффективными в условиях быстро изменяющейся среды.

Блокчейн-технологии:

Блокчейн [4] может быть использован для создания децентрализованных и защищенных систем управления доступом, которые обеспечивают неизменяемость и прозрачность всех транзакций (в применении к СКУД - это передача ID между системой управления и контроллером). Применение блокчейна позволяет избежать единой точки отказа и предоставляет более высокую степень безопасности данных и доступа. Применение блокчейна в системе контроля и управления доступом (СКУД) может значительно повысить безопасность, прозрачность и устойчивость таких систем. Вот несколько ключевых областей применения блокчейна в СКУД:

Безопасность данных доступа: Блокчейн позволяет хранить информацию о доступе пользователей и действий в системе (входы, выходы, запросы на доступ) в неизменяемой и распределённой базе данных. Это предотвращает манипуляции с данными или их несанкционированное изменение.

Децентрализация управления: В традиционных системах СКУД обычно есть центральный сервер или контроллер, через который проходят все действия. Использование блокчейна позволяет децентрализовать управление системой, обеспечивая независимость от единой точки отказа и улучшая устойчивость к взломам.

Аутентификация и идентификация: Блокчейн может быть использован для безопасной аутентификации пользователей без необходимости хранения личных данных в центральной базе. Это возможно через использование децентрализованных идентификаторов (DID), где пользователи имеют криптографические ключи для подтверждения своей личности.

Прозрачность и аудит: Все транзакции, связанные с доступом, могут быть записаны в блокчейн, что обеспечивает полную прозрачность и возможность проведения аудита. Это полезно для отслеживания действий и обеспечения безопасности на объектах с высокими требованиями.

Смарт-контракты: Блокчейн позволяет интегрировать смарт-контракты в СКУД. Например, доступ в помещение может быть автоматически разрешён или заблокирован в зависимости от условий, заданных в смарт-контракте (оплата аренды, выполнение определённых обязательств и т.д.).

Защита от внутренней угрозы: за счёт неизменяемости данных в блокчейне и распределённого хранения информация о доступах и действиях сотрудников будет защищена от внутренних злоумышленников, поскольку все изменения фиксируются и легко отслеживаются. [5]

Интеграция с IoT-устройствами: Многие современные системы СКУД используют устройства интернета вещей (IoT). Блокчейн может улучшить безопасность взаимодействия IoT-устройств между собой и с системой контроля доступа, минимизируя возможность подмены или взлома данных.

Таким образом, блокчейн может повысить надёжность, защиту и прозрачность систем контроля доступа, особенно в критически важных объектах с высокими требованиями к безопасности.

Многофакторная аутентификация:

Усиление безопасности за счет внедрения многофакторной аутентификации, которая использует несколько методов идентификации, таких как пароли, биометрические данные и токены. Многофакторная аутентификация снижает вероятность несанкционированного доступа и делает систему более устойчивой к атакам.

Сетевые протоколы и стандарты безопасности:

Необходимо продолжать разработку и стандартизацию сетевых протоколов, которые обеспечат эффективную интеграцию различных устройств в КФС и СКУД. Кроме того, требуется развивать методы обеспечения безопасности при передаче данных, такие как сквозное шифрование и аутентификация устройств на всех уровнях сети.

Централизованное управление гетерогенной системой СКУД на базе единого программного обеспечения.

В гетерогенных системах СКУД, которые включают оборудование от различных производителей, ключевым аспектом является возможность централизованного управления. Центральная система управления должна быть способна координировать работу всех устройств, обеспечивая унифицированный контроль и мониторинг доступа на различных объектах и площадках. Для этого используется единое программное обеспечение (ПО), которое интегрирует все компоненты системы, независимо от их производителя или используемых протоколов.

Основные функции централизованного управления на базе единого ПО:

Унификация интерфейса управления:

Единое ПО предоставляет операторам единый интерфейс для управления всеми компонентами системы, включая устройства разных производителей. Это снижает необходимость в обучении персонала работе с несколькими системами и упрощает управление доступом.

Мониторинг в реальном времени:

Программное обеспечение позволяет отслеживать состояние всех устройств в режиме реального времени, включая активные контроллеры, сенсоры и замки. Это повышает оперативность и точность работы системы, особенно на объектах, распределенных географически.

Интеграция с другими системами безопасности:

Единое ПО может быть интегрировано с другими системами безопасности, такими как видеонаблюдение, пожарная сигнализация, системы учета рабочего времени и др. Это создает комплексное решение, которое обеспечивает более высокий уровень защиты.

Централизованное управление политиками доступа:

Программное обеспечение позволяет централизованно задавать политики доступа для разных уровней сотрудников или групп пользователей, что особенно важно для распределенных объектов. Это также упрощает управление изменениями в системе, например, при появлении новых филиалов или сотрудников.

Обработка и хранение данных:

Все события и данные, связанные с доступом, собираются и хранятся в централизованной базе данных. База данных находится на защищенном сервере в зашифрованном виде. Обмен данными с периферийными устройствами производится при помощи идентификационных номеров, что позволяет избежать кражи персональных данных. Централизация обработки данных позволяет вести полную отчетность и анализировать события для улучшения безопасности и оперативного реагирования на инциденты.

Таблица 2

Преимущества централизованного управления гетерогенной СКУД.

<i>Параметр</i>	<i>Преимущества</i>
<i>Единая точка управления</i>	<i>Управление всеми компонентами системы через один интерфейс</i>
<i>Масштабируемость</i>	<i>Легкость добавления новых устройств и объектов без изменения архитектуры ПО</i>
<i>Снижение сложности управления</i>	<i>Уменьшение необходимости изучения разных программ и протоколов</i>
<i>Интеграция разнородных устройств</i>	<i>Возможность объединить устройства разных производителей под единой системой</i>
<i>Безопасность и контроль данных</i>	<i>Централизованное хранение данных и журналов событий для повышения безопасности</i>
<i>Оперативность и мониторинг</i>	<i>Отслеживание и управление доступом в режиме реального времени</i>

Примеры применения централизованного управления:

1. Крупные корпорации с множеством офисов и филиалов: Единое программное обеспечение позволяет централизованно управлять доступом ко всем филиалам, что исключает необходимость индивидуальной настройки для каждого офиса и упрощает масштабирование системы.

2. Производственные объекты и распределенные сети: В компаниях с несколькими производственными объектами можно интегрировать различные устройства контроля доступа, используемые на каждом из объектов, и управлять ими централизованно.
3. Правительственные и административные здания: В учреждениях с разными уровнями доступа (государственные здания).

Централизованное управление гетерогенной системой СКУД на базе единого программного обеспечения представляет собой стратегический подход к координации различных систем контроля доступа, использующих оборудование от разных производителей. В условиях распределенных и многоуровневых объектов, централизованное управление значительно упрощает процесс администрирования, позволяет объединить разнородные системы в одну сеть и обеспечить более высокий уровень безопасности. [6]

Преимущества централизованного управления гетерогенной системой СКУД:

1. Упрощенная интеграция разнородного оборудования: Единое программное обеспечение (ПО) выступает как платформа, способная работать с контроллерами, считывателями и другими компонентами СКУД разных производителей. Это исключает необходимость индивидуального управления каждой системой.
2. Централизованное управление доступом: с помощью одного интерфейса можно контролировать и управлять доступом на всех объектах, независимо от их географического расположения. Все данные собираются в одной базе данных, что позволяет лучше анализировать доступ и реагировать на угрозы.
3. Унификация интерфейса и логики управления: Пользователи взаимодействуют с одной программной платформой, что упрощает обучение персонала и повышает эффективность работы. Нет необходимости изучать несколько разных интерфейсов для каждого типа контроллера.
4. Единая система отчетности и мониторинга: Централизованное ПО собирает и обрабатывает данные с разных устройств, формируя единую систему отчетов. Это упрощает мониторинг событий и обеспечивает прозрачность процессов на всех уровнях.
5. Управление безопасностью на удаленных объектах: Централизованная система позволяет управлять доступом на распределенных объектах в режиме реального времени, что особенно важно для крупных корпораций и объектов с филиальной структурой.
6. Гибкость и масштабируемость: ПО может легко масштабироваться, добавляя новые устройства и расширяя систему без необходимости полной замены оборудования. Это особенно важно для организаций, которые растут или изменяют свою структуру.

Таблица 3

Архитектура централизованной гетерогенной системы СКУД.

Компонент системы	Функция
<i>Единое программное обеспечение</i>	<i>Управление доступом, сбор данных, мониторинг, настройка контроллеров</i>
<i>Контроллеры различных производителей</i>	<i>Управление регистрами, связь с исполнительными устройствами</i>
<i>Считыватели разных типов (RFID, биометрия)</i>	<i>Идентификация персонала и контроль доступа</i>
<i>Центральный сервер</i>	<i>Хранение базы данных событий, управление пользователями и распределение прав</i>
<i>Удаленные объекты (офисы, филиалы)</i>	<i>Контролируемые устройства, подключенные к центральной системе через сеть</i>
<i>Оповещающие и исполнительные устройства</i>	<i>Сигнализация, турникеты, двери, ворота</i>

Таким образом, контроль доступа в кибер-физических системах является важным компонентом обеспечения безопасности закрытых территорий и критически важных объектов. Гетерогенные системы СКУД, интегрирующие различные методы и протоколы контроля доступа, представляют собой перспективное решение для повышения надежности и гибкости охранных систем. В будущем интеграция ИИ, блокчейн-технологий и многофакторной аутентификации позволит значительно улучшить безопасность и производительность этих систем, обеспечивая более высокую степень защиты от киберугроз и несанкционированного доступа.

1. Левшун Д.С., Чечулин А.А., Котенко И.В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. No 4. С. 114–123. DOI:10.31854/1813-324X-2019-5-4-114-123
2. Raj Rajkumar, Dionisio de Niz, Mark Klein "Cyber-Physical Systems: Challenges and Solutions". Journal Addison-Wesley, 2022. ISBN-13: 978-0-321-92696-8
3. Zhang, L., & Wu, H. "Access Control in Heterogeneous Systems: An Overview". International Journal of Security Systems, 2021.
4. Brown, J. "Blockchain Applications in Access Control Systems". Security Innovations, 2022.
5. Hu F., Lu Y., Vasilakos A.V., Hao Q., Ma R., Patil Y., et al. Robust Cyber-Physical Systems: Concept, Models, and Implementation // Future Generation Computer Systems. 2016. Vol. 56. PP. 449–475. DOI:10.1016/j.future.2015.06.006
6. Srivastava A., Morris T., Ernster T., Vellaithurai C., Pan S., Adhikari U. Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information // IEEE Transactions on Smart Grid. 2013. Vol. 4. Iss. 1. PP. 235–244. DOI:10.1109/TSG.2012. 2232318

Филюшкин С.В.

**Принципы разработки универсального алгоритма работы контроллеров СКУД
в рамках распределенного объекта**

ООО «Лайнком»
(Россия, Санкт-Петербург)

doi: 10.18411/trnio-10-2024-405

Аннотация

В данной статье рассматриваются один из вариантов методов разработки универсального алгоритма работы централизованного программного обеспечения для гетерогенных систем СКУД. Описываются основные элементы управления контроллерами различных производителей оборудования единым центром. Рассматривается комбинированный вариант управления с использованием облачной и локальной структуры. Приведены методы взаимодействия с аппаратной частью, элементами интерфейса пользователя. Проводится математический анализ методов использования оптимальных команд для работы контроллера.

Ключевые слова: гетерогенные системы СКУД, алгоритм работы с контроллером, интерфейс, контроллер, программное обеспечение, внутренний контроль.

Abstract

This article examines one of the methods for developing a universal algorithm for centralized software for heterogeneous access control systems (ACS). The main elements of controlling controllers from various equipment manufacturers through a unified center are described. A combined control method using both cloud and local structures is considered. Methods of interaction with hardware and user interface elements are provided. A mathematical analysis of optimal command usage for controller operation is conducted.

Keywords: heterogeneous ACS systems, controller operation algorithm, interface, controller, software, internal control.

Современные системы контроля управления доступом (СКУД) являются критически важными компонентами безопасности на режимных объектах. Основная функция СКУД заключается в ограничении и управлении доступом на защищаемую территорию. В последние годы наблюдается рост количества решений, предлагаемых на рынке, в частности, контроллеров производителей оборудования Parsec, Gate. Несмотря на разнообразие доступных технологий, существует необходимость в разработке универсального алгоритма, который позволит интегрировать различные гетерогенные устройства СКУД в единую систему, повышая таким образом уровень защищенности и снижая операционные расходы.

Цель и задачи исследования

Целью данной работы является разработка универсального алгоритма работы с контроллерами СКУД Parsec, Gate, а также анализ мер внутренней безопасности, обеспечивающих защиту режимных объектов. Для достижения поставленной цели в ходе исследования необходимо решить следующие задачи:

1. Провести сравнительный анализ контроллеров Parsec, Gate.
2. Разработать универсальный алгоритм взаимодействия с этими контроллерами.
3. Исследовать методы защиты данных и управления доступом на уровне контроллеров.
4. Провести тестирование и оценку разработанного алгоритма на практических примерах.

Обзор существующих решений

1. Современные тенденции в системах контроля доступа
Современные системы СКУД стремятся к повышению уровня безопасности за счет внедрения многоуровневых систем аутентификации, интеграции с системами видеонаблюдения и учета рабочего времени. Важную роль играет поддержка шифрования и других методов защиты данных на всех уровнях. Для систем, таких как Gate и Parsec, это особенно важно, так как они предназначены для использования на объектах с высокими требованиями к безопасности. [1]
2. Сравнительный анализ контроллеров Parsec, Gate.

Нашей исследовательской группой был проведен анализ сильных сторон и недостатков протоколов работы контроллеров Parsec, Gate по основным критериям:

1. Общие характеристики протоколов: типы данных, поддерживаемые команды, структура сообщений.
2. Методы шифрования и защиты данных.
3. Сетевые возможности и требования.
4. Поддержка интеграции с другими системами.[2]
5. Уровень отказоустойчивости и безопасности.

Были изучены теоретические материалы:

Контроллеры Parsec

Parsec – это система, ориентированная на крупные и средние объекты, предоставляющая комплексные решения для управления доступом. Контроллеры Parsec обладают мощными вычислительными возможностями, поддерживают различные методы аутентификации, включая биометрию, и интеграцию с системами видеонаблюдения и учета рабочего времени. Протоколы обмена данными в системе Parsec строятся на базе современных стандартов безопасности, таких как SSL/TLS.

Контроллеры Parsec известны своей высокой степенью интеграции с другими системами и поддержкой различных методов аутентификации. Это делает их популярным выбором для крупных объектов. Однако, как отмечают многие исследователи, сложность интеграции и настройки может стать проблемой при использовании в системах с нестандартными требованиями [3].

Контроллеры Gate

Система Gate известна своей высокой надежностью в сложных сетевых условиях, а также способностью работы в распределенных системах. Контроллеры Gate поддерживают широкий спектр методов идентификации, включая карты доступа, PIN-коды и биометрические данные. Особенностью данных контроллеров является использование защищенных протоколов передачи данных и встроенные механизмы шифрования, что делает их устойчивыми к атакам, таким как "человек посередине" (MITM).

Контроллеры Gate обладают высокой надежностью и способностью работать в распределенных сетях. Особенностью этих устройств является их устойчивость к сетевым атакам благодаря встроенным механизмам шифрования. Это делает их привлекательными для использования на режимных объектах [4].

Таблица 1

Анализ основные аспекты протоколов контроллеров Gate-8000-Ethernet и Parsec NC8000.

Параметры	Gate 8000 Ethernet	Parsec NC8000
1. Общие характеристики протоколов		
Тип данных	Поддержка различных форматов данных, включая ASCII и двоичные форматы	Поддержка двоично-десятичного формата данных (BCD) для временных параметров, встроенная поддержка дат
Команды	Набор команд для управления функциями контроллера (доступ, мониторинг, диагностика)	Команды для управления доступом, синхронизации времени, управления реле и другими функциями
Структура сообщений	Стандартная структура с заголовком, телом и контрольной суммой	Сообщения состоят из кода команды и параметров, представленных в BCD-формате
2. Методы шифрования и защиты данных		
Шифрование	Базовые механизмы защиты через контрольные суммы и шифрование сообщений	Дополнительные уровни защиты с использованием уникальных идентификаторов и шифрования данных
Безопасность	Аутентификация команд, защита данных при передаче	Встроенные средства защиты от несанкционированного доступа, мониторинг состояния питания и защиты корпуса
3. Сетевые возможности и требования		
Интерфейсы связи	Поддержка RS-485 и Ethernet для локальных и удаленных подключений	Поддержка RS-485 и Ethernet, выбор интерфейса осуществляется аппаратно
Автономная работа	Нет	Возможность автономной работы с копией баз данных
Обезличенная идентификация	Поддержка	Поддержка
4. Поддержка интеграции с другими системами		
Интеграция с другими системами	Легкая интеграция с системами сторонних производителей, гибкость для различных сценариев контроля доступа	Совместимость с более старыми версиями оборудования Parsec, поддержка аппаратных и программных расширений
5. Уровень отказоустойчивости и безопасности		
Отказоустойчивость	Встроенные механизмы защиты данных и контроля доступа	Высокий уровень надежности за счет встроенных часов реального времени, релейных расширителей
Дополнительные функции безопасности	Нет	Мониторинг состояния питания и защита от вскрытия

Проведем математический анализ протоколов Gate и Parsec 8000D, чтобы выявить их общие черты и различия, а затем создать универсальную формулу или алгоритм, который будет учитывать специфику обоих протоколов. Для этого нам необходимо разделить работу на следующие этапы:

Анализ протоколов [5]

Прежде чем перейти к математическому анализу, нужно понять основные элементы протоколов:

Структура команд:

Какие команды присутствуют в каждом протоколе, их формат и семантика.

Форматы данных: Как представлены данные в каждом из протоколов (например, байтовая структура, числовые форматы, типы данных).

Типы событий:

Какие события поддерживаются каждым из протоколов (например, доступ предоставлен, доступ отклонен, тревога).

Идентификация пользователей: Какие механизмы используются для идентификации пользователей (например, UID, MAC-адреса).

Механизмы передачи данных: Как осуществляется обмен данными между устройствами (например, TCP/IP, специальный бинарный формат).

Построение полиномов

Для упрощения анализа можно представить каждый протокол в виде набора переменных или функций, описывающих его поведение. Например:

Пусть $G(x)$ — функция, описывающая протокол Gate.

Пусть $P(y)$ — функция, описывающая протокол Parsec 8000D.

Каждая функция может быть представлена в виде полинома или набора полиномов, где переменные x и y могут представлять разные параметры или команды протоколов. [6]

Универсальный алгоритм

Предположим [7], что оба протокола можно представить в виде линейных или нелинейных комбинаций этих переменных. Тогда универсальный алгоритм можно попытаться выразить через универсальную функцию $PU(z)$, которая будет являться линейной комбинацией $G(x)$ и $P(y)$:

$$PU(z) = \alpha G(x) + \beta P(y) + \gamma,$$

где:

α и β — коэффициенты, которые зависят от специфики реализации и особенностей систем.

γ — некоторая константа, отражающая особенности обмена данными между системами или другие специфические характеристики.

Оптимизация и проверка

На этапе оптимизации необходимо:

Уточним значения коэффициентов α , β и γ на основании реальных данных или моделирования.

Проведем тестирование на различных наборах данных, чтобы убедиться в работоспособности алгоритма.

Перед разработкой универсального алгоритма обработки событий, который будет объединять протоколы контроллеров GATE-Ethernet и Parsec 8000D, мы провели анализ таблицы команд каждого из контроллеров.

Результатом анализа команд каждого контроллера, стало математическое представление команд.

Представим каждую категорию команд в виде функции, где каждая функция будет представлять определенный набор команд:

$U_p(y)$ - функции работы с пользователями;

$S_p(y)$ - функции конфигурации и настройки;

$M_p(y)$ - функции управления режимами работы;

$A_p(y)$ - функции управления доступом;

$R_p(y)$ - функции сброса и очистки данных;

$T_p(y)$ - функции синхронизации и управления временем;

$P_1 \dots P_n$ – тип команды контроллера Parsec 8000D.

$Pz.1 \dots Pz.n$ – тип регистра команды контроллера Parsec 8000D.

Тогда можно представить команды Parsec в виде суммы этих функций:

$$P(y) = U_p(y) + S_p(y) + M_p(y) + A_p(y) + R_p(y) + T_p(y),$$

где каждая подфункция описывает различные группы команд, такие как работа с пользователями, конфигурация, управление режимами, доступ и т.д.

Определение подфункций для Parsec 8000D

Функции работы с пользователями $U_p(y)$:

$$U_p(y) = fP1(y) + fP2(y) + fP3(y) + fP4(y) + fP5(y) + fP6(y)$$

Функции конфигурации и настройки $C_p(y)$:

$$C_p(y) = fP1.1(y) + fP1.2(y) + fP1.3(y) + fP1.4(y) + fP1.5(y)$$

Функции управления режимами работы $M(y)$:

$$M_p(y) = fP2.1(y) + fP2.2(y) + fP2.3(y) + fP2.4(y) + fP2.5(y)$$

Функции управления доступом $A(y)$:

$$A_p(y) = fP3.1(y) + fP3.2(y) + fP3.3(y) + fP3.4(y) + fP3.5(y) + fP3.6(y)$$

Функции сброса и очистки данных $R(y)$:

$$R_p(y) = fP4.1(y) + fP4.2(y) + fP4.3(y) + fP4.4(y) + fP4.5(y)$$

Функции синхронизации и управления временем $T_p(y)$:

$$T_p(y) = fP5.1(y)$$

Аналогичным образом можно представить команды Gate Ethernet в виде функции:

$$G(x) = UG(x) + CG(x) + MG(x) + AG(x) + RG(x) + TG(x)$$

Функции конфигурации и настройки $C_G(x)$:

$$C_G(x) = fG1.1(x) + fG1.2(x) + fG1.3(x) + fG1.4(x) + fG1.5(x)$$

Функции управления режимами работы ($M(x)$):

$$M_G(x) = fG2.1(x) + fG2.2(x) + fG2.3(x) + fG2.4(x) + fG2.5(x)$$

Функции управления доступом $A_G(x)$:

$$A_G(x) = fG3.1(x) + fG3.2(x) + fG3.3(x) + fG3.4(x) + fG3.5(x) + fG3.6(x)$$

Функции сброса и очистки данных ($R(x)$):

$$R_G(x) = fG4.1(x) + fG4.2(x) + fG4.3(x) + fG4.4(x) + fG4.5(x)$$

Функции синхронизации и управления временем $T_G(x)$:

$$T_G(x) = fG4.1(x)$$

Объединение протоколов в универсальный алгоритм

Если известно, что $G(x)$ и $P(y)$ различаются только в определенных аспектах, то универсальный алгоритм можно выразить как:

$$U(z) = \alpha P(y) + \beta G(x) + \gamma$$

После формализации функций обоих протоколов можно объединить их в универсальный алгоритм. Поскольку, оба протокола имеют схожие категории функций, что позволяет объединить их следующим образом [9]:

При объединении двух различных протоколов (Parsec 8000D и Gate Ethernet) возникает необходимость уравнивания их особенностей и приоритетов. Каждому из протоколов присваивается определённый весовой коэффициент, который отражает степень важности или значимости информации, получаемой от каждого из протоколов в итоговой формуле.

Эта формула является основой для разработки универсального алгоритма [10] обработки событий системы контроля доступа, который обрабатывает данные с устройств, работающих по разным протоколам, и настраивается в зависимости от конкретных требований и условий эксплуатации системы.

α — это весовой коэффициент, который зависит от приоритета или специфики протоколов, которые отражают вклад протокола Parsec 8000D в общий алгоритм. Этот коэффициент может зависеть от того, насколько важны данные, поступающие от устройств, работающих по протоколу Parsec 8000D, для всей системы.

Например, если Parsec 8000D используется для более точной идентификации пользователей или сложной логики доступа, его вес может быть выше.

β — весовой коэффициент для протокола GATE-Ethernet определяет значимость данных, поступающих по протоколу GATE-Ethernet. Как и в случае с α , значение β зависит от роли этого протокола в общей системе контроля доступа. Если, например, GATE-Ethernet отвечает за управление основными элементами (такими как замки, реле и другие исполнительные устройства), его вес также может быть увеличен [11].

γ — константа для учета специфики системы

Константа γ введена в уравнение для учета специфических условий или особенностей системы, которые не покрываются ни одним из протоколов. Эта константа может:

- обеспечивать базовое значение для компенсации несовершенств протоколов или учитывать специфические требования системы.
- учитывать непредвиденные факторы, такие как задержки в передаче данных, погрешности в работе оборудования или другие внешние условия.

Значения α , β и γ должны быть выбраны или вычислены на основе практических испытаний системы или анализа требований.

Обозначим основные подходы к присвоению значений:

Анализ приоритетов системы:

Если в системе основное внимание уделяется контролю доступа и безопасности, тогда большее значение (α или β) будет присвоено тому протоколу, который лучше справляется с этими задачами.

Тестирование системы:

На этапе тестирования может быть выполнено измерение эффективности каждого из протоколов. На основе этого выбираются значения, которые минимизируют ошибки и обеспечивают надёжную работу системы.

Эмпирическое определение:

α и β можно определить эмпирически на основе наблюдений и накопленного опыта эксплуатации системы. Если по статистике протокол Parsec 8000D чаще участвует в обработке критических событий, его вес α увеличивается.

Таким образом, в процессе тестирования можно собрать статистические данные о том, как часто и в каких условиях каждый из протоколов демонстрирует наилучшую производительность. Это позволит выявить закономерности, такие как время реакции на команды, стабильность передачи данных и надёжность при обработке критических событий. [12]

Оптимизация системы

На основе полученных данных можно внести коррективы в алгоритмы работы системы, выделяя больший приоритет тем протоколам, которые лучше справляются с ключевыми задачами. Например, если Parsec 8000D более стабильно работает при большом количестве подключений или лучше обрабатывает события безопасности, его вес (α) в общей схеме управления будет увеличен, а другие протоколы, такие как Gate, могут быть использованы в менее критических сценариях, что повысит общую отказоустойчивость системы.

Дальнейшее развитие системы

В процессе эксплуатации также может производиться корректировка весов α и β в зависимости от изменения рабочих условий и задач. Таким образом, система сможет адаптироваться к новым требованиям и нагрузкам, обеспечивая максимальную эффективность и безопасность работы гетерогенных систем СКУД на длительной основе.

Проведённый анализ эффективности протоколов Gate и Parsec NC8000D на этапе тестирования позволяет выявить ключевые аспекты их использования в рамках гетерогенной системы СКУД. Определение значений параметров α и β на основе эмпирических данных играет важную роль в обеспечении надёжной и оптимальной работы системы. Протокол Parsec 8000D, демонстрируя лучшие результаты при обработке критических событий, может иметь более высокий вес в конечной системе, что гарантирует стабильную работу при повышенных требованиях к безопасности. В то же время протокол Gate может использоваться для менее ресурсоёмких задач, таких как мониторинг доступа или управление дополнительными элементами системы, что позволяет сбалансировать нагрузку и повысить общую отказоустойчивость.

Тестирование каждого из протоколов выявляет важные различия в их производительности, что помогает оптимизировать использование ресурсов системы, а также минимизировать потенциальные ошибки и сбои. Такой подход позволяет гибко настраивать работу системы в зависимости от конкретных задач, распределять нагрузки и использовать наиболее подходящий протокол в зависимости от текущих условий эксплуатации. [8]

Разработка и тестирование универсального алгоритма для управления гетерогенными системами СКУД представляет собой сложную задачу, требующую учёта множества факторов. Протоколы Gate и Parsec NC8000D, будучи основными элементами такой системы, должны быть тщательно протестированы на предмет производительности, надёжности и безопасности.

Эмпирическое определение параметров α и β позволяет системе адаптироваться к изменяющимся условиям эксплуатации, распределяя приоритеты между протоколами в зависимости от их эффективности.

Таким образом, на основе данных, полученных на этапе тестирования, можно не только оптимизировать работу системы, но и обеспечить её гибкость в долгосрочной перспективе. Адаптивность алгоритма и возможность корректировки весов протоколов обеспечат системе способность эффективно справляться с критическими событиями, гарантируя высокий уровень безопасности и устойчивости к сбоям.

1. Левшун Д.С., Чечулин А.А., Котенко И.В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. No 4. С. 114–123. DOI:10.31854/1813-324X-2019-5-4-114-123
2. Левшун Д.С., Чечулин А.А., Котенко И.В. Проектирование безопасной среды передачи данных на примере протокола I2C // Защита информации. Инсайд. 2018. No 4 (82). С.54–62. DOI:10.31854/1813-324X-2019-5-4-114-123
3. L. Johnso, "Challenges and Solutions in Implementing Parsec Control Systems" (L. Johnson et al., International Journal of Network Security, 2021)
4. P. Brown et al., "Distributed Access Control Systems: A Case Study of Gate Controllers" (P. Brown et al., Journal of Information Security, 2020)
5. Hu F., Lu Y., Vasilakos A.V., Hao Q., Ma R., Patil Y., et al. Robust Cyber-Physical Systems: Concept, Models, and Implementation // Future Generation Computer Systems. 2016. Vol. 56. PP. 449–475. DOI:10.1016/j.future.2015.06.006
6. Srivastava A., Morris T., Ernster T., Vellaithurai C., Pan S., Adhikari U. Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information // IEEE Transactions on Smart Grid. 2013. Vol. 4. Iss. 1. PP. 235–244. DOI:10.1109/TSG.2012.2232318
7. Strzelecki A., Rizun M. Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping //Sustainability. - 2022. - Т. 14. - №. 10. - С. 1-17. <https://doi.org/10.3390/su14105866>
8. Zhuang Y. et al. Research on big data access control mechanism //International Journal of Computational Science and Engineering. - 2023. - Т. 26. - №. 2. - С. 192-198. <https://doi.org/10.1504/IJCSE.2023.129738>
9. Jiang R. et al. T-RBAC Model Based on Two-Dimensional Dynamic Trust Evaluation under Medical Big Data //Wireless Communications and Mobile Computing. - 2021. - Т. 2021. - С. 1-17. <https://doi.org/10.1155/2021/9957214>
10. Gupta M., Patwa F., Sandhu R. Object-tagged RBAC model for the Ha-doop ecosystem //IFIP Annual Conference on Data and Applications Security and Privacy. - Cham : Springer International Publishing, 2017. - С. 63-81. https://doi.org/10.1007/978-3-319-61176-1_4
11. Servos D., Osborn S. L. Current research and open problems in attribute-based access control //ACM Computing Surveys (CSUR). - 2017. - Т. 49. - №. 4. - С. 1-45. <https://doi.org/10.1145/3007204>
12. Zeng W., Yang Y., Luo B. Content-based access control: Use data content to assist access control for large-scale content-centric databases //2014 IEEE International Conference on Big Data (Big Data). - IEEE, 2014. - С. 701-710. <https://doi.org/10.1109/BigData.2014.7004294>

Фурман И.С., Похорокова М.Ю.

Создание игрового калькулятора для настольной игры

Технический институт

ФГАОУ ВО "Северо-Восточный федеральный университет имени М.К. Аммосова"

(Россия, Нерюнгри)

doi: 10.18411/trnio-10-2024-406

Аннотация

В современном мире настольных игр часто возникают различные инструменты, упрощающие механику и повышающие удобство для игроков и мастеров подземелий. Представленный калькулятор значительно упрощает процесс броска кубиков, обеспечивая гибкость и точность, необходимые для расчета результатов в самых разных игровых ситуациях. Пользователи могут вводить пользовательские значения кубиков, что позволяет выполнять практически любые броски. В статье рассматривается процесс создания калькулятора на языке C#.

Ключевые слова: игровой калькулятор, бросок кубика, бонус, windows forms, C#.

Abstract

In the modern world of board games, various tools often arise that simplify the mechanics and increase the convenience for players and dungeon masters. The presented calculator greatly simplifies the process of rolling dice, providing the flexibility and accuracy necessary to calculate the results in a variety of gaming situations. Users can enter custom dice values, which allows you to make almost any throws. The article discusses the process of creating a calculator in C#.

Keywords: game calculator, dice roll, bonus, windows forms, C#.

Игровая индустрия, как часть этого мира, продолжает динамично развиваться, предлагая всё новые и инновационные способы взаимодействия с информацией и обучения через игровые механизмы. В этом контексте особенно актуальной становится разработка специализированных приложений, таких как калькуляторы очков и генераторы для настольных ролевых игр, например, Dungeons & Dragons (D&D). Эта игра сочетает в себе элементы стратегии, фантазии и командного взаимодействия, предлагая уникальный опыт погружения в мир приключений. Игра основана на системе правил, которая определяет возможности персонажей и исход событий. Игроки используют специальные кубики для определения исхода своих действий, а также калькуляторы очков и генераторы сценариев для создания и оптимизации своих персонажей и приключений.

Выбор языка C# для разработки игрового калькулятора Dungeons & Dragons был обусловлен несколькими важными факторами. C# и платформа .NET предлагают мощные инструменты для создания Windows Forms приложений, что значительно упрощает разработку интуитивно понятного и функционального пользовательского интерфейса. Это позволило быстро создать интерфейс, который удовлетворяет потребности игроков и ведущих в процессе игры. C# обладает богатой экосистемой библиотек и инструментов, которые облегчают разработку. Например, стандартные библиотеки C# обеспечивают легкий доступ к генерации случайных чисел, что является ключевым элементом при реализации бросков кубиков. Благодаря .NET Core, программы на C# могут быть кроссплатформенными, что открывает возможность переноса программы на другие операционные системы, если это потребуется.

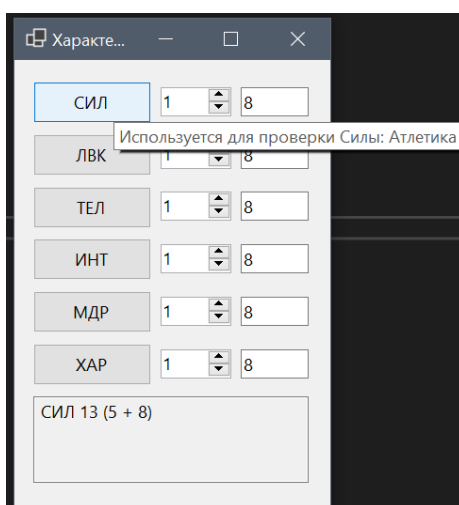


Рисунок 1. Окно «Характеристик игрока».

Окно «Характеристик игрока» представляет собой панель с кнопками характеристик, при наведении на которые высвечиваются подсказки с дополнительными характеристиками,

которые проверяются этой характеристикой. Правее есть уровень характеристики, который даёт бонус к броску, вычисляемый по игровым правилам. Ещё правее находятся окна итогового бонуса к броску, которые можно редактировать в случае временного повышения характеристик, обусловленного игровой ситуацией. В поле ниже отображается результат последней проверки характеристики игрока и то, как он был получен, перед скобками стоит сумма брошенного кубика и бонуса, внутри скобок число слева – результат броска двадцатигранного кубика, а число справа – добавленный бонус.

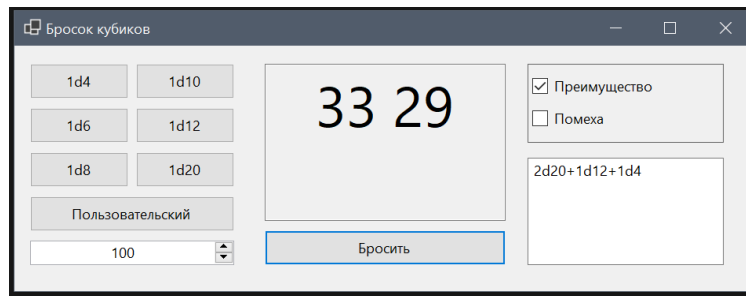


Рисунок 2. Окно «Бросок кубиков».

Калькулятор включает кнопки для броска стандартных кубиков, таких как d4, d6, d8, d10, d12, d20 и d100. Эти кубики могут использоваться по отдельности или комбинироваться для более сложных бросков. Помимо стандартных вариантов, калькулятор поддерживает возможность добавления произвольного количества граней кубика, что позволяет адаптировать его под любые игровые ситуации.

Простой и понятный интерфейс позволяет легко задавать и комбинировать различные броски. При удержании клавиши Shift, несколько типов кубиков можно добавить в одно выражение, например, для броска $2d8 + 1d12$.

Калькулятор автоматически парсит введенное выражение и выполняет бросок соответствующего количества кубиков, отображая итоговый результат. Это исключает ошибки и значительно ускоряет игровой процесс. Встроенные функции для учета преимуществ или помех особенно важны при проведении бросков на атаку или проверки навыков.

Пользователь может легко настраивать выражение броска и адаптировать его под текущую игровую ситуацию. Это полезно для опытных игроков, которым нужны гибкие инструменты для управления сложными механиками.

Метод `rollButton_Click` убирает пробелы из введенного выражения, выполняет бросок кубиков и сохраняет результат. Если активировано преимущество, выполняется дополнительный бросок, и выбирается наилучший результат. Если активирована помеха, выполняется дополнительный бросок, и выбирается наихудший результат. Выводит результат в текстовое поле, учитывая преимущества и помехи. Метод `RollDice` разделяет выражение на части по знаку +, чтобы обработать каждый кубик отдельно. Для каждой части выражения разделяет строку на количество кубиков и количество граней, проверяет корректность формата и значения, выполняет бросок для каждого кубика и суммирует результаты, возвращает итоговую сумму бросков. Работа над проектом позволила приобрести ценный опыт в создании приложений на языке программирования C#. В процессе разработки были использованы современные методы программирования и принципы объектно-ориентированного дизайна. Были успешно разработаны и реализованы ключевые алгоритмы для данного калькулятора, включая генерацию бросков кубиков, редактирование оружия, ведения боя и проверки характеристик персонажа.

Проведенное тестирование продемонстрировало высокую стабильность и надежность программы. Выявленные в ходе тестирования недочеты были успешно устранены, что способствовало повышению качества и удобства использования приложения.

Практическое применение D&D не ограничивается только развлечением. Эта игра способствует развитию множества навыков: от стратегического планирования и командной работы до креативности и принятия решений. Игра требует от игроков аналитического мышления, воображения и способности быстро адаптироваться к меняющимся условиям. Кроме того, D&D часто используется в развивающих целях, так как она помогает развивать коммуникативные навыки и учит работе в команде.

1. Innovations in Dice Simulation Software: Advances and Applications / E. S. Johnson, M. L. Roberts, A. D. Hughes // 18th International Conference on Computational Games. ICCG '20. Volume 3: Software Engineering, Los Angeles, USA, 12–14 марта 2020 года. Vol. 3. – Los Angeles, USA: Tech University Press, 2020. – P. 87-98.
2. А. Н. Иванов. Программные методы генерации случайных чисел для игр и симуляторов / А. Н. Иванов // Вестник информационных технологий. – 2024. – № 3(112).
3. Л. И. Смирнова. Эффективные алгоритмы генерации случайных чисел в C# / Л. И. Смирнова // Информатика и разработки. – 2022. – № 3(67).
4. М. С. Петров. Интерфейс пользователя в WinForms: создание и настройка / М. С. Петров // ТехноМир. – 2024. – № 1(90). – EDN KPLRZT.
5. Н. А. Гончарова. Основы работы с событиями в WinForms / Н. А. Гончарова // Научный журнал по программированию. – 2023. – № 2(56).
6. П. В. Кулинча. Безопасность в C#: методы обеспечения безопасности при разработке приложений на C# / П. В. Кулинча // Дневник науки. – 2023. – № 6(78).

Хоманенко С.В.

**Возможность использования искусственного интеллекта
для защиты видеонаблюдения**

*Донской Государственный Технический Университет
(Россия, Ростов-на-Дону)*

doi: 10.18411/trnio-10-2024-407

Аннотация

В статье рассматривается применение видеоаналитики, её развитие и перспективы. Обсуждается проблема уязвимости систем видеонаблюдения и возможность применения искусственного интеллекта для их защиты.

Ключевые слова: видеоаналитика, видеонаблюдение, искусственный интеллект, информационная безопасность.

Abstract

The article discusses the use of video analytics, its development and prospects. The problem of vulnerability of video surveillance systems and the possibility of using artificial intelligence to protect them are discussed.

Keywords: video analytics, video surveillance, artificial intelligence, information security.

Применение искусственного интеллекта в системах видеонаблюдения берет свое начало с 2000-х годов, в этот момент начинают активно развиваться сетевые видеокамеры, появляется профессиональное программное обеспечение для управления оборудованием. Нейросетевые технологии выводят видеонаблюдение на совершенно другой уровень. Система наблюдения становится гораздо эффективнее, появляются новые инструменты для анализа, охраны и защиты объектов инфраструктуры. Впервые становится возможным автоматизировано отслеживать и идентифицировать людей, а также анализировать траекторию движения объекта. Такие методы хорошо работали только в хороших условиях освещенности и требовали

значительных вычислительных ресурсов. Благодаря использованию технологии глубокого обучения удалось решить эти проблемы. Нейросети обучались на реальных примерах, собранных с камер видеонаблюдения в различных условиях, что позволило добиться высокой точности анализа видео и появиться новым функциям обнаружения. Видеоаналитика в системах видеонаблюдения позволила автоматизировано контролировать периметр и производственные процессы, распознавать лица, отслеживать и анализировать поведение людей и объектов, обеспечивать безопасность сотрудников и предприятия, а также в кратчайшие сроки оповещать оператора о каком-либо инциденте.

Компания Markets and Markets, провела исследование и сделала подробный отчет [1], согласно которому рынок видеоаналитики в период с 2023 по 2028 год будет демонстрировать значительный рост. Ожидается, что его объем увеличится с 8,3 до 22,6 млрд долларов при среднегодовом темпе роста 22,3%.

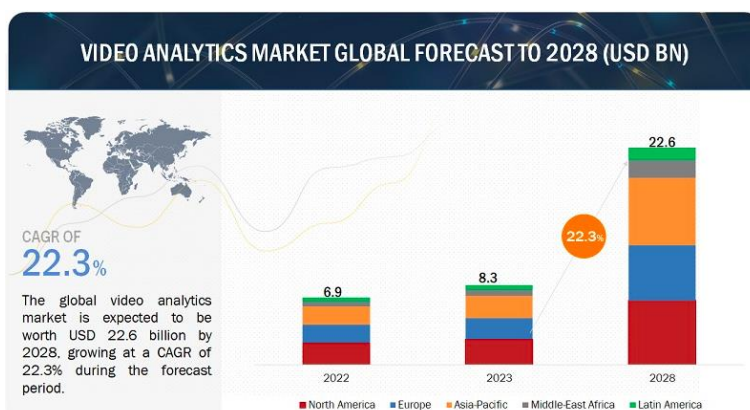


Рисунок 1. Глобальный прогноз развития рынка видеоаналитики до 2028 года.

Потребность в повышении уровня безопасности в городах, включая отслеживание транспортных средств и людей, анализ дорожного движения, обнаружение оставленных предметов, а также мониторинг посетителей в торговых центрах, будет способствовать увеличению спроса на внедрение систем видеоаналитики.

Для пользователей, которые планируют использовать систему видеоаналитики, обеспечение конфиденциальности и безопасности данных должно являться основополагающими принципами. В зависимости от задач, видеоаналитика может быть реализована как отдельное программное обеспечение, которое установлено в камеру видеонаблюдения или отдельный физический сервер, так и в виде облачного ресурса, который может находиться в любой точке мира и обрабатывать видеопоток в реальном времени.

При выборе реализации видеоаналитики необходимо учесть такие факторы: какая информация будет передаваться, какие данные будут обрабатываться, кто получит доступ к управлению системой, а также соответствие системы необходимым стандартам безопасности. Как и любая другая технология, видеоаналитика может иметь уязвимости в системе безопасности. Если данные, передаваемые между камерой и системой, не защищены должным образом, злоумышленник может получить к ним доступ. Также существует риск кибератак на систему, если в программном обеспечении устройства есть уязвимости.

Так, в апреле 2023 года лаборатория FortiGuard Labs компании Fortinet, специализирующаяся на исследованиях и разработках в области кибербезопасности, выявила резкий рост атак [2], использующих уязвимость CVE-2018-9995, обнаруженную еще в 2018 году. Эта уязвимость позволяла злоумышленникам обойти аутентификацию в видеорегистраторах DVR 4104/4216 компании ТВК и получить доступ администратора, а затем использовать видеоданные.

Согласно данным поставщика, установлено свыше 600 000 камер и 50 000 DVR устройств по всему миру в банках, правительственных зданиях и других объектах критической

инфраструктуры. Устройства компании ТВК продаются под различными торговыми марками, такими как Novo, CeNova, QSee, Pulnix, XVR 5 в 1, Securus, Night OWL, DVR Login, HVR Login и MDVR.

В ходе дальнейшего исследования были обнаружены камеры видеонаблюдения и видеорегистраторы компаний Argus, Axis, MYPower и Vacon, которые также подвергались атакам [3]. Уязвимости CVE-2018-15745, CVE-2018-10661, CVE-2018-10662 и CVE-2016-20016 могли позволить злоумышленникам обойти контроль доступа и раскрыть небезопасный интерфейс, что привело бы к получению доступа в систему, а также к ряду других проблем, таких как доступ к файлам, выполнение произвольных команд операционной системы от имени пользователя root и удаленное выполнение кода. В настоящий момент не известно о каких-либо исправлениях, предоставленных поставщиком продукции ТВК.

Для предотвращения подобных инцидентов и повышения уровня безопасности устройств видеонаблюдения, возможно применить искусственный интеллект, который позволит:

1. Обнаруживать подозрительные действия путем непрерывного мониторинга системных журналов.
2. Анализировать сетевой трафик для обнаружения кибератак.
3. Находить уязвимости при установке оборудования и программного обеспечения.
4. Повысить уровень надежности аутентификации.
5. Постоянно отслеживать работу системы.
6. Мгновенно принимать меры для защиты.

В условиях, когда видеоаналитика становится всё более востребованной, а характер киберугроз стремительно меняется, допустимо предположить рост числа атак на инфраструктуру, содержащую как персональные данные, так и информацию, имеющую критически важное значение для безопасности города или государства. Для предотвращения таких ситуаций необходимо использовать современные методы защиты, основанные на искусственном интеллекте.

1. Video Analytics Market by Offering, Application (Intrusion Management, Incident Detection, and Traffic Monitoring), Deployment Model, Type, Vertical (Critical Infrastructure, Government & Defense, and Manufacturing) and Region - Global Forecast to 2028 // Markets and Markets : сайт. – URL: https://www.marketsandmarkets.com/Market-Reports/intelligent-video-analytics-market-778.html?utm_source=prnewswire&utm_medium=referral&utm_campaign=paidpr (дата обращения: 07.04.2024).
2. Detection Spike Observed for DVR Authentication Bypass Vulnerability (CVE-2018-9995) // Fortiguard : сайт. – URL: <https://www.fortiguard.com/threat-signal-report/5152> (дата обращения: 11.04.2024).
3. Active Exploitation of Multiple Vendor Camera System Attack // Fortiguard : сайт. – URL: <https://www.fortiguard.com/threat-signal-report/5162/active-exploitation-of-multiple-vendor-camera-system-attack> (дата обращения: 12.04.2024).

Чухров М.М., Белаш В.Ю.

Разработка приложения «Планировщик отпусков» с использованием средств ВВА

*Калужский государственный университет имени К.Э. Циолковского
(Россия, Калуга)*

doi: 10.18411/trnio-10-2024-408

Аннотация

В статье рассматриваются вопросы, связанные с проектированием и разработкой приложения «Планировщик отпусков». Обосновывается актуальность данного приложения,

рассматриваются различные способы его реализации. Также представлены требования к конечному продукту и описан процесс его создания.

Ключевые слова: Excel, VBA, отдел кадров, приложение.

Abstract

The article discusses issues related to the design and development of the Vacation Planner application. The relevance of this application is substantiated, various ways of its implementation are considered. The requirements for the final product are also presented and the process of its creation is described.

Keywords: Excel, VBA, HR, application.

У каждой компании или предприятия имеется штат сотрудников (кадров). Для учета и координирования деятельности сотрудников необходимы специальные приложения. Для некоторой организации потребовалось приложение «Планировщик отпусков». На протяжении длительного периода использовался аналог данного приложения, однако, в какой-то момент у заказчика в приложении перестали проводиться расчёты: происходило принудительное закрытие приложения, и образовались проблемы, связанные с работой данного программного продукта. В связи с этим появилась необходимость использования иного решения. Основное приложение, которое использовалось на предприятии, прекратило поддержку функциональности, тем самым став менее актуальным на рынке.

Кроме того, заказчиком была обозначена необходимость реализации дополнительной функции, которая отвечала бы за игнорирование кадров при дальнейших расчётах. Это нужно для тех сотрудников, кто по какой-либо причине был уволен из организации.

Итак, можно обозначить следующие требования к конечному программному продукту:

1. Разработка основной таблицы "Планировщик отпусков".
2. Разработка подсчётов авансовых и остаточных отпусков.
3. Реализация возможности игнорирования при расчётах сотрудников в случае увольнения из предприятия.
4. Реализация отправки уведомлений сотрудникам, которые должны уйти в отпуск в течение 21 дня.
5. Разработка автоматического формирования уведомления для сотрудника в виде официального документа.
6. Разработка функции, которая формирует график пересечений отпусков.
7. Разработка функции, которая создаёт унифицированную форму для отчёта.

В процессе разработки приложения изучены возможные варианты для реализации конечного продукта:

- Разработка ПО на языке Python с собственным интерфейсом.
- Разработка Excel-приложения на языке VBA [2].
- Разработка приложения на базе онлайн таблиц написанное на языке Java Script.
- Разработка 1С приложения.

У каждого из вышеперечисленных средств, есть достоинства и недостатки. Рассмотрим их подробнее, чтобы определиться с выбором средств разработки. Сравнительная характеристика процессов разработки ПО на языке Python с собственным интерфейсом представлена в таблице 1.

Таблица 1

Использование средств языка Python для создания приложения.

Достоинства	Недостатки
Данное приложение будет полностью самостоятельным	В данное приложение сложнее интегрировать какое-либо обновление в программную часть кода без потери данных
У данного приложения будет собственный интерфейс	Нужно отдельно реализовывать импорт данных

Разработка Excel-приложения на языке VBA обладает такими достоинствами как: более обширный функционал (в сравнении с Java Script), возможность одновременно взаимодействовать со всеми инструментами из пакета Microsoft Office, отсутствие необходимости импортировать конечные таблицы, так как они уже по умолчанию находятся в Excel приложении. Однако, присутствует и недостаток: низкий уровень защищённости программного кода

В таблице 2 представлены достоинства и недостатки разработки приложения на базе онлайн таблиц, написанного на языке Java Script.

Таблица 2

Использование языка Java Script для создания приложения.

<i>Достоинства</i>	<i>Недостатки</i>
<i>Обновление данных в режиме реального времени</i>	<i>Данный язык очень ограничивает разработчика и пользователя во взаимодействии со всеми необходимыми инструментами для выполнения всех функций конечного продукта</i>
<i>Не нужно тратить на память устройства, так как все таблицы будут находиться на облачном хранилище</i>	<i>Ограниченный функционал разработки</i>

Разработка 1С приложения позволила бы реализовать все требования к конечному продукту, однако, и в этом случае отметим низкий уровень защищённости программного кода и тот факт, что такое приложение будет не всегда автономным, так как на устройстве должно изначально быть установлено отдельное ПО для просмотра и/или взаимодействия.

Проведя анализ программных средств разработки приложений, можно сделать вывод, что конечный продукт лучше реализовывать в 1С или в VBA. Автор данной статьи выбрал VBA так как этот язык является оптимальным решением для разработки конечного продукта.

На этапе проектирования был рассмотрен аналог excel-приложения [3] для планирования отпусков. За основу конечного приложения были взяты из аналога excel-приложения макеты листа «планировщик» (рис. 1) и макет листа «пересечение отпусков».

Рисунок 1. Лист «планировщик».

Анализируя макет листа «планировщик» (рис. 1), можно заметить, что отсутствует возможность внесения сотрудника в список уволенных сотрудников или возможность выставления какого-либо тега, помечающего сотрудника как уволенного из предприятия. Следовательно, макет данного листа должен быть изменён.

Рисунок 2. Лист «сформировать график».

Также при изучении данного excel-приложения был открыт лист «сформировать график» (рис. 2). Пользователь видит на листе две кнопки, после нажатия которых выполняются соответствующие макросы. Данный способ реализации вызова функций/макросов не является оптимальным, так как лист или кнопка по некоторым причинам могут быть удалены, или вовсе ссылка на макрос может открепиться от кнопки.

В связи с этим возник вопрос: возможно ли кнопку встроить в интерфейс excel-приложения? Ответ оказался положительным. К сожалению, у компании Microsoft нет возможности редактировать интерфейс инструментов, но такая возможность есть, с использованием редакторов, разработанных пользователями. В качестве примера и дальнейшей разработки интерфейса excel-приложения, был взят редактор Ribbon XML Editor [1] от Новикова М.Г.

Рассмотрим основной функционал RibbonXMLEditor:

1. XML-описание интерфейса ленты оперативно строится, кроме того быстро работают команды, контекстное меню, панель быстрого доступа. Представлен кнопочный интерфейс, а также возможность выбора функциональных элементов из списка.
2. Реализована возможность использования внешних иллюстраций для настройки интерфейса разрабатываемого приложения.
3. Синхронизация и внедрение элементов интерфейса в документы Word, Excel, PowerPoint или Access поддерживается.
4. Есть возможность импорта/экспорта xml-макета интерфейса в файл настроек ленты.
5. Присутствует функция построения основе полученного xml-кода модуля ".bas" для VBA с шаблонами процедур обратного вызова.

Таким образом, за счет использования редактора Ribbon XML Editor получилось реализовать приложение, отвечающее всем поставленным требованиям.

В статье были рассмотрены возможные способы реализации приложения для планирования отпусков для отдела кадров. Анализ недостатков существующего приложения помог выявить его ограничения и недочеты. В результате были сформулированы рекомендации для создания приложения, чтобы оно стало более эффективным инструментом для отдела кадров.

1. Новиков М.Г. Ribbon XML Editor / Новиков М.Г. [Электронный ресурс] // Макс.мск.рус : [сайт]. — URL: <http://xn--80auew.xn--j1adp.xn--p1acf/products/ribbonxmleditor/ribbonxmleditor.html> (дата обращения: 12.04.2024).
2. Справочник по языку Visual Basic (VBA) для приложений / [Электронный ресурс] // learn.microsoft.com : [сайт]. — URL: <https://learn.microsoft.com/ru-ru/office/vba/api/overview/language-reference> (дата обращения: 12.04.2024).
3. Умный график отпусков – 2024 / [Электронный ресурс] // Система Главбух : [сайт]. — URL: <https://1gl.ru/#/document/16/129271> (дата обращения: 12.04.2024).

Шатаева Л.И., Тасуев А.А., Магомадов Ш.А.
Преимущества и недостатки применения блокчейн технологии
в банковской сфере

*ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-10-2024-409

Аннотация

Начало цифровой трансформации пришлось именно на банковскую среду, как на центральную составляющую экономики. Причиной этому является то, что в первую очередь банки более восприимчивы и адаптивны к изменениям внешних факторов воздействия, а инновационный потенциал помогает банковскому учреждению непрерывно совершенствоваться

процесс предоставления банковских услуг, создавать и реализовывать совершенно новые для российского финансового рынка банковские продукты.

Ключевые слова: бухгалтерский учет, банк, облачные технологии, большие данные, блокчейн.

Abstract

The beginning of the digital transformation took place precisely in the banking environment, as a central component of the economy. The reason for this is that, first of all, banks are more receptive and adaptive to changes in external factors, and the innovative potential helps a banking institution to continuously improve the process of providing banking services, create and implement banking products that are completely new to the Russian financial market.

Keywords: accounting, banking, cloud technologies, big data, blockchain.

Современные инновации способствуют сохранению и увеличению конкурентных преимуществ банка на рынке финансовых услуг, оптимизации всех бизнес-процессов, а также помогает сократить операционные расходы. Автоматизация рабочих мест является одним из важнейших достоинств, так как способствует упрощенному режиму обработки данных, что, в свою очередь, значительно ускоряет операции, связанные с предоставлением кредитов и обслуживания клиентов, а также существенно сокращает время для проведения проверок большого объема информации. Не менее важно, что применение передовых технологий сводит к минимуму вероятность появления ошибок, поскольку устраняется человеческий фактор. Это вызвано тем, что процесс автоматизированной обработки данных использует определенный алгоритм действий, характеризующийся точностью и надежностью. Помимо вышперечисленного, автоматизация обеспечивает решение таких базовых задач, как ведение бухгалтерского учета, своевременное формирование обязательной финансовой отчетности. Инновационная активность и оперативное реагирование на изменяющиеся потребности клиентов, внедрение новейших технологий служат залогом успешности и одними из факторов формирования конкурентоспособности кредитного учреждения.

Цифровизация банков осуществляется в трех направлениях:

1. Первый путь развития основывается на выпуске инновационных банковских продуктов, среди которых можно выделить сервис кредитного брокера, который способен оформлять заявки на предоставление потребительского кредита и ипотеки без непосредственного привлечения специалистов; биометрическую идентификацию; cashback – сервисы и многие другие. Постоянное наблюдение трендов и точное выявление потребностей клиентов – определяющие факторы для появления актуальных идей. Еще один важный аспект – скорость вывода инноваций на рынок: чем быстрее банк запускает качественно новые услуги и продукты, тем больше конкурентных преимуществ он приобретет.
2. Второе направление – процессные инновации, ориентированные на кратное сокращение и минимизацию затрат, связанных с банковскими операциями. Цифровизация основополагающих процессов в банках, к которым относят продажи новых продуктов и сервисное обслуживание в офисах, позволяет сократить их стоимость на 40-60%.
3. Третье направление базируется на инновациях в бизнес-моделях посредством создания экосистем, развития партнерских отношений с другими субъектами банковской сферы, предоставление банковских услуг под чужим брендом. Постепенный переход от классического формата к банковской экосистеме предполагает усиленное внимание к запросам клиентов. Необходимым умением стало выстраивание активного взаимодействия с технологическими компаниями при разработке и внедрении инновационных решений, аутсорсинге инноваций и т.д. Партнерами банков становятся социальные сети и операторы связи, предоставляющие доступ к общей информации о клиентах.

Рассмотрим примеры инновационных банковских разработок в известных банках:

В ноябре 2023 года Сбербанк презентовал систему искусственного интеллекта GigaChat, способную выполнять множество интеллектуальных задач, включая генерирование текста, участие в дискуссиях, создание кода. А включение в действие Kandinsky открывает возможности для создания изображений. Следует отметить, что финансовый эффект от применения инновационных разработок в 2023 году Сбербанка нарастающим итогом, начиная с 2021 года, составил 800 млрд. руб. прибыли. В дальнейшем планируется увеличение инвестиций банка в развитие искусственного интеллекта примерно в полтора раза до 450 млрд. руб. В 2024–2026 годах Сбербанк намерен перейти на человекоцентричную модель с фокусом на глубокое использование искусственного интеллекта. Новый AI-помощник направлен на ликвидацию так называемого цифрового разрыва на территории страны, поскольку станет доступен всем пользователям, а также он не требует специальных знаний. ИИ «нового поколения» обеспечит перевод многих задач в автоматизированный режим.

Финансы и банковское дело: блокчейн может использоваться для улучшения процессов передачи денег, управления счетами и обеспечения безопасности финансовых транзакций.

Логистика и цепи поставок: блокчейн позволяет отслеживать перемещение товаров и сократить время и затраты на управление цепями поставок.

Управление данными и цифровая идентификация: блокчейн может обеспечить уверенность в истинности и безопасности хранимых данных, что особенно важно при обмене информацией в интернете.

Медицина и здравоохранение: блокчейн помогает создать единую платформу для обмена медицинской информацией между различными учреждениями и специалистами

Децентрализованные приложения: блокчейн может быть использован для создания децентрализованных приложений, которые не подвержены цензуре и могут функционировать независимо от централизованных серверов.

Умные договоры: блокчейн позволяет автоматизировать исполнение договоров и условий с помощью умных контрактов, что повышает прозрачность и надежность сделок.

Голосование и выборы: блокчейн может использоваться для обеспечения прозрачности и безопасности выборов, путем создания системы электронного голосования на основе технологии блокчейн.

Интеллектуальная собственность: блокчейн может сделать процесс управления правами интеллектуальной собственности более эффективным и прозрачным, минимизируя риски нарушения авторских прав и пиратства.

Известно, что в 2024 году РНКБ примет участие в тестировании цифрового рубля, запуск которого намечен на 2025 год. Цифровой рубль объединяет свойства как наличных, так и безналичных денег, выполняя основные функции денег. Внедрение цифрового рубля позволит совершать платежи быстрее, удобнее, и самое главное, безопаснее.

Финансовые вложения в цифровые реформы для небольших банков могут быть рискованными из-за недостатка опыта, а потери от неудачной трансформации могут привести к банкротству. Поэтому важно найти узко специализированный сегмент и сосредоточиться на нем. Недостаток средств не должен останавливать малых игроков в проведении цифровизации: можно сосредоточиться на развитии ключевых технологий или использовать аутсорсинг. Как крупные, так и малые компании могут использовать технологии анализа больших данных для создания моделей прогнозирования кредитных рисков, что позволит предлагать индивидуальные условия клиентам и оптимально использовать ресурсы.

Несмотря на недавние потрясения в экономике, особенно санкционное давление и временный спад, отключение банков от SWIFT, российская финансовая система достойно выдержала испытания. Банковский сектор успешно выполнил запланированные мероприятия по цифровизации и продолжает инвестировать в развитие информационных технологий по сегодняшний день.

Агентство цифрового аудита SDI360 в 2023 году провело исследование на предмет цифровой зрелости 60 крупнейших коммерческих банков страны. Основными критериями

рейтинга стали представленность кредитной организации в цифровом пространстве, продвижение, удобство коммуникаций клиентов с банком, а также развитие онлайн-продаж. Рассмотрим таблицу 1, в которой продемонстрированы результаты исследования, посвященного уровню цифровизации банковской отрасли.

Интересны сведения, приведенные по критерию представленности российских банков в сети Интернет:

1. Ярко выражена перегруженность банковских сайтов технологиями, тем не менее 43% банков обеспечивают высокую скорость загрузки сайтов.
2. Самой актуальной социальной сетью среди исследуемых банков стала VK, в контент на этой платформе активно вкладываются 83% банковских учреждений, однако регулярно публикуют информацию 67% банков.
3. 22% банков развивают каналы на YouTube, российский аналоговый видеохостинг Rutube на данный момент не пользуется подобной популярностью, только три банка, а именно «Промсвязьбанк», «МТС Банк» и «Газпромбанк» — инвестируют в этот видеохостинг.
4. Банки инвестируют и в более молодые платформы: 82% участников банковского сектора используют Telegram для коммуникации с аудиторией.

Заключение

Таким образом, применение инновационных технологий в банковском секторе имеет огромные перспективы для улучшения качества обслуживания клиентов, оптимизации бизнес-процессов и повышения конкурентоспособности банков. Развитие рынка финансовых технологий, использование искусственного интеллекта, блокчейн-технологий и многих других инноваций открывает новые возможности для банковской отрасли. Банки, которые активно внедряют новые технологии, смогут значительно увеличить свою эффективность и привлекательность для клиентов. Инновации играют ключевую роль в развитии банковского сектора и будут продолжать диктовать его маршрут в будущем.

1. Генкин, А. Блокчейн: Как это работает и что ждет нас завтра / А. Генкин, А. Михеев. — Москва : Альпина Паблишер, 2018. — 592 с. — ISBN 978-5-9614-6558-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/82585.html> (дата обращения: 14.05.2023)
2. Киселев, А. А. Технология блокчейн в финансировании проектов : учебное пособие для СПО / А. А. Киселев, В. Д. Сухов. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. — 103 с. — ISBN 978-5-4488-1331-3, 978-5-4497-1521-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/117302.html> (дата обращения: 14.05.2023)
3. Максуров, А. А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование : монография / А. А. Максуров. — 2-е изд. — Москва : Дашков и К, 2021. — 212 с. — ISBN 978-5-394-04198-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/107773.html> (дата обращения: 14.05.2023)

Шершнёв Д.Ю.

Методология атаки и методы защиты веб-сервера

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-410

Аннотация

В статье анализируется методология атаки на веб-сервер, включая этапы сбора информации, сканирования уязвимостей, перехвата сессионных данных и взлома паролей. Описаны основные классы ошибок, возникающих на уровне веб-серверов, и их последствия для безопасности. Также рассматриваются методы защиты веб-серверов, такие как сегментация сети, система обнаружения изменений и регулярный аудит безопасности.

Ключевые слова: атака на веб-сервер, защита веб-сервера, SQL-инъекции, DDoS-атаки, сегментация сети, аудит безопасности.

Abstract

The article analyzes the methodology of attacking a web server, including the stages of collecting information, scanning vulnerabilities, intercepting session data and cracking passwords. The main classes of errors that occur at the web server level and their security implications are described. Methods of protecting web servers, such as network segmentation, a change detection system and regular security audits, are also considered.

Keywords: web server attack, web server protection, SQL injection, DDoS attacks, network segmentation, security audit.

Атака на веб-сервер представляет собой спланированную последовательность действий, известную как методология атаки, которую злоумышленник применяет для достижения своей цели. Хакеры осуществляют атаку на веб-сервер поэтапно, на каждом этапе стремясь получить информацию о слабых местах веб-сервера и несанкционированный доступ к нему.

Предлагается выделить три основных класса ошибок, возникающих на уровне серверов:

- Ошибки, ведущие к нарушению конфиденциальности информации. Они позволяют неавторизованным пользователям получать доступ к закрытым данным, обходя механизмы аутентификации или просматривая исходный код важных приложений.
- Ошибки, вызывающие атаки типа DoS. Они носят исключительно разрушительный характер, поскольку приводят к тому, что сервер становится неспособным выполнять свои обычные функции из-за обработки большого количества ложных запросов.
- Ошибки, позволяющие выполнение на сервере неавторизованного кода. Благодаря им злоумышленники могут запускать на сервере программы, которые не предназначены для общего доступа, а также отправлять на сервер собственный исполняемый код. Последний вариант характерен для ошибок, связанных с переполнением буфера.

Сбор информации о целевом сервере осуществляется с использованием различных инструментов и методов, включая сервис Whois.net и Whois Lookup, позволяющие определить сетевую информацию веб-сервера, такую как доменное имя и IP-адрес.

В процессе зеркального отображения веб-сайта хакер копирует весь сайт и его содержимое на локальный диск, что позволяет ему получить ценную информацию о структуре каталогов и файловой системе целевого веб-сервера.

Следующий этап – сканирование на уязвимости – предназначен для обнаружения слабых мест на целевом веб-сервере или в сети. Затем злоумышленник ищет способы эксплуатации найденных уязвимостей, используя известные эксплойты, доступные на сайтах SecurityFocus и Exploit-DB.

Перехват сессионных данных позволяет злоумышленнику получить несанкционированный доступ к целевому веб-серверу, используя методы социальной инженерии, атаки типа XSS или специальные инструменты, такие как Burp Suite.

Последний этап – взлом паролей. Этот этап предполагает попытку взлома паролей, обнаруженных на предыдущих этапах или после закрепления в системе. Для этого злоумышленник может использовать различные методы, включая простое угадывание пароля, радужную атаку и вычисление хэша пароля, а также автоматизированные средства, такие как Hashcat, THC.

Подытожив всё вышеперечисленное, предлагается алгоритм поведения хакера при атаке на веб-сервер на рисунке 1.

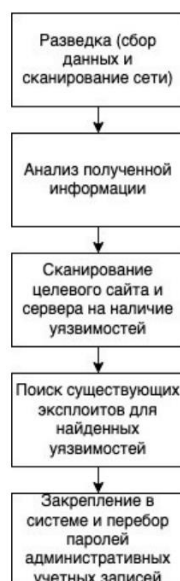


Рисунок 1. Алгоритм хакерской атаки на веб-сервер.

При рассмотрении методологии атаки на веб-сервер важно не только понимать, как злоумышленники могут использовать уязвимости, но и разрабатывать адекватные методы защиты для минимизации рисков. Каждая обнаруженная слабость может быть преобразована в сильную сторону системы, если разработать и внедрить соответствующие защитные механизмы. Именно на основе понимания техники атак, таких как SQL-инъекции, атаки типа "отказ в обслуживании" (DDoS), межсайтовые скрипты (XSS), можно формировать эффективные методы защиты веб-сервера. Теперь рассмотрим ключевые подходы и технологии, которые помогут предотвратить большинство угроз и усилить безопасность сервера.

Существует несколько методов защиты веб-серверов от различных видов атак, такие как:

Сегментация сети. Сегментация сети представляет собой стратегию разделения компьютерной сети на несколько отдельных областей, каждая из которых имеет свою специфическую функцию и уровень доступа. Идеальная инфраструктура веб-хостинга включает в себя три основных сегмента: интернет-сегмент, сегмент безопасности защищенного сервера (DMZ) и внутреннюю сеть (Рисунок 2). DMZ, или Demilitarized Zone, выступает в роли буфера между внутренней сетью организации и внешними сетями, такими как Интернет, обеспечивая дополнительный уровень безопасности для внутренних систем. Размещение веб-сервера в DMZ, изолированном от общей и внутренней сети веб-хостинга, является первым шагом в обеспечении его безопасности. Это разделение позволяет администраторам устанавливать брандмауэры и применять правила контроля доступа для управления интернет-трафиком, направляемым в DMZ, и трафиком внутренней сети. В сегментированной сети попытка взлома одного сегмента не позволит злоумышленнику поставить под угрозу безопасность других сегментов.

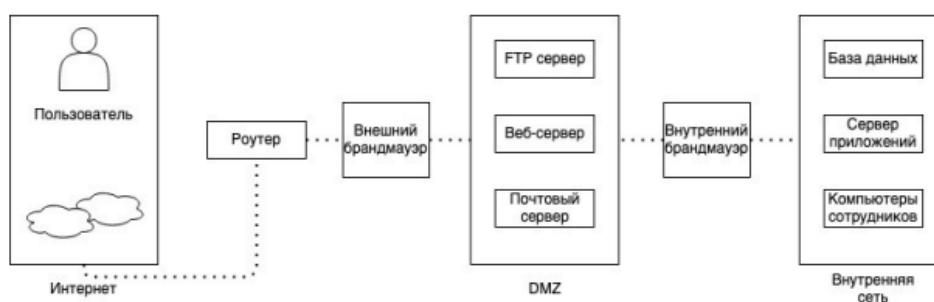


Рисунок 2. Сеть веб-хостинга с использованием DMZ.

Обнаружение попыток взлома: злоумышленник, получивший доступ к веб-серверу и поставивший под угрозу безопасность, может попытаться установить бэкдоры (скрипты), которые позволят ему нанести дополнительный ущерб бизнесу компании. После установки бэкдора на веб-сервер, размер зараженных файлов автоматически увеличивается. Предлагается использовать систему обнаружения изменений веб-сайта (WDS), которая представляет собой сценарий, выполняющийся на сервере и предназначенный для обнаружения изменений, внесенных в любые исполняемые файлы, или появления новых файлов на веб-сервере. Система оповещает пользователя о необходимости принятия соответствующих мер.

Своевременное выполнение аудита безопасности: этот процесс позволяет выявить уязвимости безопасности веб-сервера до того, как злоумышленник попытается осуществить вторжение в сеть. Своевременное выполнение аудита безопасности представляет собой процесс оценки соответствия системы требованиям по безопасности и выявления возможных уязвимостей и рисков. Аудит безопасности включает планирование, сбор информации, анализ, подготовку отчета и реализацию рекомендаций. Регулярное проведение аудита помогает организациям поддерживать надежность и защищенность своих информационных систем, а также повышает осведомленность персонала о рисках и мерах безопасности.

1. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 193-197.
2. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
3. Миняев А. А. Метод оценки эффективности системы защиты информации территориально- распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
4. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.

Щербань О.В., Аников Д.А., Брежнев А.В.

Интеллектуальная система сбора информации о пациентах, предназначенная для медицинских учреждений с использованием медицинского браслета

*Высшая школа кибертехнологий, математики и статистики
Российский экономический университет имени Г.В. Плеханова
(Россия, Москва)*

doi: 10.18411/trnio-10-2024-411

Аннотация

Статья рассматривает значимость и преимущества внедрения интеллектуальной системы сбора данных о пациентах для медицинских учреждений. Поднимается вопрос о том, насколько важным является переход к цифровизации здравоохранения и созданию электронных методов мониторинга состояния здоровья пациентов. Эти методы объединяют разнообразные медицинские данные и обеспечивают их доступность и безопасность. Также в статье обсуждаются основные аспекты такой системы, включая стандартизацию медицинской документации и меры по обеспечению конфиденциальности информации. Преимущества автоматизации медицинской отчетности и оптимизации взаимодействия медицинских учреждений через единую систему также рассматриваются.

Ключевые слова: искусственный интеллект, медицина, цифровизация здравоохранения, интеграция медицинских данных, автоматизация медицинской отчетности.

Abstract

The article examines the significance and advantages of implementing a unified system for collecting patient data for medical institutions. The question is raised about the importance of the transition to digitalization of healthcare and the creation of electronic methods for tracking the well-

being of patients, combining a variety of medical data and ensuring their accessibility and protection. The article also highlights the main elements of such a system, including the unification of medical records and measures to ensure the confidentiality of information. The advantages of automating medical reporting and optimizing the interaction of medical institutions through a single system are considered.

Keywords: artificial intelligence, medicine, digitalization of healthcare, integration of medical data, automation of medical reporting.

Актуальность данной темы состоит в том, что в настоящее время остро стоит вопрос о решении следующей социально значимой проблемы: медицинские учреждения сталкиваются с необходимостью эффективного и безопасного обмена информацией о пациентах. Внедрение интеллектуальной системы сбора информации может улучшить уровень медицинского обслуживания, сократить время, затрачиваемое на поиск и анализ данных, повысить безопасность хранения конфиденциальной информации пациентов, а также снизить вероятность ошибок в диагностике и лечении благодаря автоматизации таких процессов, как сбор данных о состоянии пациента, сведение данных из его медицинской истории, а также прогнозирование его состояния и диагностика при помощи экспертных систем. Это способствует более эффективному взаимодействию между различными медицинскими учреждениями, что крайне важно в условиях увеличения объемов информации и повышенных требований к качеству медицинской помощи.

Цель представленного исследования заключается в глубоком анализе и детальном описании инновационной интеллектуальной системы, специально разработанной для эффективного сбора и управления информацией о пациентах, с уникальной адаптацией к потребностям медицинских учреждений. Основное внимание уделяется не только техническим аспектам системы, но и ее практическим преимуществам и вызовам, которые могут возникнуть при ее внедрении. Исследование стремится выявить оптимальные подходы к интеграции этой системы в работу медицинских учреждений, а также проанализировать потенциальные пути для улучшения процесса ее использования.

Задачи проекта. В ходе работы над проектом перед нами стояли пять основных задачи:

1. определить, какие данные о пациентах необходимо собирать;
2. определить способы сбора анализируемых данных;
3. определить и описать алгоритмы для экспертной системы;
4. описать способы взаимодействия системы с врачами в медицинских учреждениях;
5. внедрить систему, которая позволяет облегчить работу медицинских сотрудников.

Научная новизна. Концептуальная модель экономически эффективно автоматизирует сбор жизненных показателей о пациентах, включая историю болезни из единой медицинской информационно-аналитической системой (ЕМИАС) и текущий анализ, для использования ее в медицинских учреждениях, а также помогает заранее перед консультацией со специалистом выдвинуть предположительный диагноз и систему лечение, который основывается на обширной энциклопедической базе исследованных заболеваний и бота-голосового помощника, который перед приемом у специалиста уточняет симптомы болезни.

Методы и методологии. Для полноценного функционирования интеллектуальной системы сбора информации, необходимо задействовать следующие компоненты:

Во-первых, наша интеллектуальная система должна быть взаимосвязана с единой медицинской информационно-аналитической системой (ЕМИАС) города Москвы, которая разработана с целью улучшения качества и доступности медицинской помощи в государственных учреждениях здравоохранения. Эта интеграция обеспечит эффективное взаимодействие между нашей интеллектуальной системой и историей заболеваний каждого человека, содержащейся в базе данных ЕМИАС [4]. Такое взаимодействие позволит нашей системе автоматически анализировать медицинскую историю пациента, выявлять его

предыдущие заболевания, особенности лечения, реакции на терапию и другие важные медицинские данные. Это позволит нашей системе фокусироваться на наиболее значимых аспектах заболеваний и показателях здоровья для каждого конкретного человека, учитывая его индивидуальные особенности и историю болезни. Кроме того, благодаря интеграции с ЕМИАС, система будет в состоянии предоставлять более точные и персонализированные рекомендации по диагностике, лечению и профилактике заболеваний, основываясь на данных, хранящихся в обширной базе медицинской информации города Москвы. Это значительно повысит качество медицинского обслуживания, сделав его более адаптированным и улучшить доступность медицинской помощи в целом.

Во-вторых, интеллектуальная система должна обладать функцией синхронизации с обширной энциклопедической базой данных заболеваний, которая включает в себя огромный объем исследовательской информации. Эта база данных состоит из детальных описаний различных заболеваний, включая список симптомов, характерных для каждого заболевания, и методы их лечения, основанные на актуальных медицинских данных и практиках. При получении информации о пациенте, система автоматически просматривает эту базу данных, чтобы выявить возможные соответствия с его симптомами и состоянием здоровья. Система включает в себя механизм анализа и сопоставления симптомов пациента с известными заболеваниями из базы данных. Это позволяет системе формулировать предварительные диагнозы или предположения о возможных заболеваниях, что в свою очередь облегчает и ускоряет процесс определения дальнейших медицинских действий. Важно подчеркнуть, что эта система включает в себя не только описания заболеваний и их симптомов, но и актуальные методы лечения, что позволяет медицинскому персоналу быстро ознакомиться с возможными вариантами терапии и немедленно начать подбор наиболее эффективного курса лечения для каждого конкретного случая. Такой комплексный подход значительно улучшает качество медицинского обслуживания и обеспечивает более эффективное и целенаправленное лечение для пациентов.

В-третьих, важно встроить в интеллектуальную систему бота-голосового помощника, который играет значимую роль в повышении эффективности обслуживания клиентов. После подачи клиентом запроса на консультацию с медицинским специалистом, данный бот не только принимает информацию, но и активно взаимодействует с клиентом. Он задает дополнительные вопросы, уточняя симптомы и другие аспекты, необходимые для полноценного анализа обстановки. Затем, используя полученные сведения, бот сужает круг вероятных заболеваний, что в конечном итоге позволяет оптимизировать затраты времени и ресурсов медицинского персонала. Кроме того, этот бот автоматически обновляет информацию в медицинской карточке пациента, дополняя ее новыми данными, полученными в ходе взаимодействия. Это обеспечивает актуальность информации и гарантирует своевременное оказание медицинской помощи с максимальной точностью. Подобный подход к взаимодействию с клиентами содействует улучшению качества обслуживания и способствует увеличению уровня доверия к медицинской системе в целом.

Объект исследования. Мы фокусируемся на описании процесса сбора информации о физическом самочувствии пациентов, что включает в себя данные о текущем состоянии здоровья и анализ прежних и настоящих заболеваний. Наша задача состоит в изучении особенностей этого процесса, охватывая методы сбора данных, их достоверность, а также оценку эффективности использования полученной информации в лечебной практике.

Предмет исследования. Наше исследование занимается анализом и изучением процесса автоматизации сбора информации о медицинской истории пациента и отслеживания при помощи медицинского браслета ключевых показателей жизнедеятельности. Мы стремимся глубоко понять и охватить этот процесс, рассмотрев его в различных аспектах, включая внедрение информационных технологий, разработку программного обеспечения, а также взаимодействие с персоналом медицинских учреждений и самими пациентами.

Проблематика. Интеллектуальная система сбора информации о пациентах позволяет решать сразу ряд проблем, связанных с работой медицинских учреждений. Различные данные о пациентах, включая информацию об их текущем состоянии, а также данные из медицинской карты, хранятся децентрализованно и не системно, что способствует как и низкому качеству обслуживания пациентов, так и усложнения ведения профессиональной деятельности медицинских сотрудников, включая диагностирование заболеваний и отслеживание состояния пациента в комплексном режиме. Описываемая система может предложить решение данных проблем за счет автоматизации процессов сбора, хранения и анализа данных о пациентах, а также обеспечить защиту конфиденциальных данных и данных, попадающих под определение медицинской тайны.

Требования к автоматизации. Система представляет собой совокупность компонентов и процессов, таких как: базы данных для хранения медицинских записей, алгоритмы обработки и анализа этих данных с целью выявления заболеваний, интерфейсы взаимодействия пациентов и медицинских работников с данной системой, а также со специальным браслетом, собирающим различные показатели пациента.

Собираемые данные и их использование. В рамках системы предполагается получение данных из нескольких источников.

Во-первых, показатели, получаемые при помощи специального браслета (пульс, кровяное давление, сатурация, температура тела и другие показатели). Данные должны быть представлены в числовом формате в единицах измерения, соответствующих показателю, передаваться на смартфон пользователя через bluetooth и отображаться в личном кабинете в клиентском приложении пользователя [1]. На основе этих данных интеллектуальная система на сервере позволяет поставить предварительный диагноз пациенту и назначить лечение [2]. Также в случае ухудшения показателей приложение должно уведомить пользователя о необходимости посещения врача, а в случае опасности для жизни пользователя немедленно вызвать скорую помощь [5].

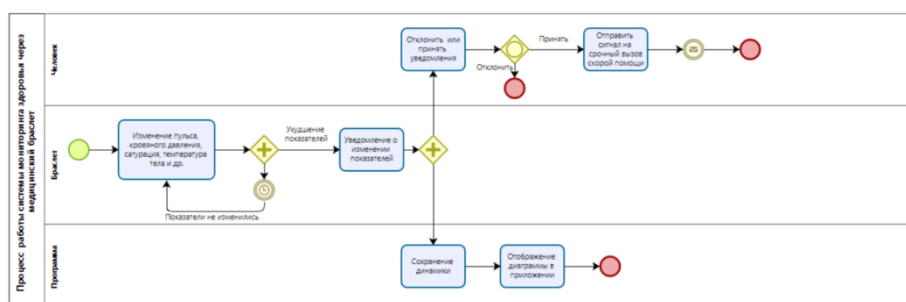


Рисунок 1. Процесс работы системы мониторинга здоровья через медицинский браслет.

Во-вторых, данные, получаемые при создании личного кабинета пациента (ФИО, адрес проживания, паспортные данные, номер полиса ОМС).

В-третьих, данные, получаемые при оформлении пациентом электронной заявки на посещение медучреждения в личном кабинете в приложении или на сайте (общее самочувствие и описание симптомов в свободной форме, также возможен смешанный вариант с заполнением специальной формы). После того, как пациент оставил заявку, с ним по телефону связывается голосовой помощник, который собирает дополнительную информацию о самочувствии и симптомах пациента для определения интеллектуальной системой профиля врача, к которому необходимо записать пациента, а также, если это возможно, поставить предварительный диагноз. Решения принимаются на основе заранее прописанных линейных алгоритмов в случае работы с данными из форм и при помощи языковых моделей в случае работы с описанием симптомов в свободной форме [4].

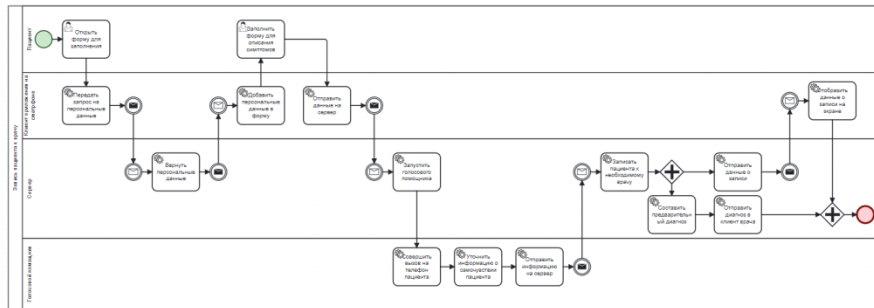


Рисунок 2. Процесс записи пациента к врачу при помощи мобильного приложения и голосового помощника.

В-четвертых, данные, получаемые при осмотре врачом в медучреждении и при дальнейшем исследовании и лечении (общее самочувствие, описание симптомов в свободной форме, пульс, кровяное давление, сатурация, температура тела, различные анализы крови, снимки КТ, описания исследований УЗИ, ЭКГ, результаты других исследований). Все эти данные вносятся в электронную медицинскую карту пациента врачом при проведении осмотра или автоматически в случае исследований, проводимых при помощи электронного оборудования.

В-пятых, данные из медицинской карты пациента (истории болезней и методы лечения). Последняя категория данных представляет собой архивную информацию, включающую в себя истории болезней других пациентов и справочную информацию.

Экспертная система, основанная на алгоритме случайного леса, нейронных сетях и логистической регрессии, использует данные из четырех последних групп для составления предварительного диагноза и предложения варианта лечения. Алгоритм случайного леса позволяет анализировать данные и выявлять важные признаки, которые могут указывать на определенные заболевания или состояния пациента. Нейронные сети используются для обучения модели на большом объеме данных и выявления сложных взаимосвязей между различными параметрами. Логистическая регрессия помогает предсказывать вероятность возникновения конкретного заболевания на основе имеющихся данных [3].

Описание компонентов системы. В основе системы лежит клиент-серверная архитектура со следующими компонентами:

- Клиентский сервер, на котором находятся экспертные системы и сервисы принятия решений, описанных выше. Также он должен обеспечивать взаимодействие с пациентом при помощи голосового помощника.
- Сервер базы данных, на котором хранятся все данные о пациентах и их историях болезней, а также справочная информация.
- Клиент пациента в виде мобильного приложения или сайта, который должен обладать следующим функционалом:
 1. Возможность самостоятельного указания персональных данных пациента, включая данные о его состоянии здоровья;
 2. Возможность отслеживания показателей, считываемых специальным браслетом;
 3. Возможность просмотра своей истории болезни и медицинской карты, а также назначенного лечения;
 4. Возможность записи на прием к врачу при помощи электронной заявки.
- Клиент врача в виде десктопного приложения или сайта, который должен обладать следующим функционалом:
 1. Просмотр электронных заявок пациентов с описаниями их симптомов;
 2. Возможность просмотра и редактирования истории болезни пациента;
 3. Возможность просмотра всех предварительных диагнозов, поставленных на разных этапах обследования пациента (при помощи браслета, на основе данных о симптомах, полученных при заполнении заявки и при

взаимодействии с голосовым помощником) и рекомендуемого лечения, предлагаемых системой, и возможность их редактирования при необходимости;

4. Возможность постоянного отслеживания показателей пациента, собираемых с его носимого браслета.

Преимущества интеллектуальной системы сбора информации о пациентах. Во время разработки на начальных стадиях важно ответить на вопрос: “Как данная система упростит деятельность медицинского учреждения?”. По нашему мнению можно выделить ряд следующих преимуществ:

1. Благодаря синхронизации с базами данных медицинских исследований и клинической практики, система имеет доступ к обширному объему медицинской информации. Это позволяет ей быстро анализировать симптомы и другие клинические данные пациента и сопоставлять их с известными заболеваниями и их характеристиками. Благодаря этому, система может автоматически формулировать предположения о возможных диагнозах в значительно более короткие сроки, чем традиционные методы диагностики;
2. Система взаимодействует с энциклопедической базой данных заболеваний, которая содержит информацию о тысячах заболеваний, их симптомах, признаках и методах лечения. Это позволяет системе быстро отфильтровывать и анализировать множество возможных диагнозов, исключая менее вероятные варианты и сужая круг возможных болезней.
3. Интеграция с ЕМИАС позволяет системе получать доступ к медицинской истории пациента и предыдущим диагнозам, что дополнительно ускоряет процесс постановки диагноза и позволяет более точно адаптировать лечение к индивидуальным потребностям каждого пациента;
4. Система предлагает наиболее подходящие методы лечения, учитывая индивидуальные особенности пациента, его медицинскую историю и реакцию на предыдущие методы терапии. Это помогает минимизировать риски нежелательных побочных эффектов и повышает эффективность лечения;
5. Пациенты получают необходимое лечение быстрее. Это сокращает время ожидания на прием к врачу и уменьшает нагрузку на медицинские учреждения, что в конечном итоге способствует повышению доступности медицинской помощи для всех;
6. Позволяет медицинскому персоналу сосредоточиться на более сложных случаях и тех, которые требуют особого внимания, в то время как система автоматически обрабатывает более рутинные задачи, такие как анализ симптомов и истории болезни. Это повышает эффективность работы медицинского персонала и улучшает качество обслуживания.

Недостатки и ограничения данной технологии. Разумное понимание слабых сторон системы позволяет не только эффективнее использовать ее преимущества, но и работать над их устранением.

1. Несмотря на продвинутые алгоритмы и базы данных, интеллектуальные системы могут быть ограничены в точности постановки диагноза, особенно в случаях, когда симптомы неоднозначны или редки. Это может привести к ошибкам в диагностике и назначении лечения;
2. Интеллектуальные системы могут быть ограничены в своей способности понимать человеческие эмоции, индивидуальные предпочтения и контекст человеческого состояния. Это может привести к недостаточному учету психологических аспектов заболевания и чувств пациента.
3. Использование медицинских данных требует высокого уровня конфиденциальности и безопасности, чтобы защитить личную информацию

пациентов от несанкционированного доступа и утечек. Недостаточные меры защиты могут создать риски для конфиденциальности пациентов.

4. Интеллектуальные системы требуют надежного интернет-соединения, аппаратного обеспечения и программного обеспечения для своей работы. Сбои в электропитании, проблемы с сетью или ошибки программного обеспечения могут привести к простоям и недоступности системы.
5. Важным аспектом медицинской помощи является взаимодействие между врачом и пациентом. Интеллектуальные системы могут не всегда обеспечивать такой уровень взаимодействия, который мог бы быть обеспечен человеком, что может отрицательно сказаться на уровне комфорта и доверия пациента к системе.

Обсуждение. С развитием цифровых технологий и распространением носимых устройств сбор и анализ данных о состоянии здоровья становятся доступнее и более широко распространены. Это открывает новые возможности для интеграции таких данных в сферу страхования здоровья.

Страхование жизни и здоровья — это финансовый продукт, который обеспечивает защиту финансового благополучия в случае болезни, травмы или смерти страхователя. Обычно страховая компания выплачивает страховое возмещение при наступлении страхового случая, такого как смерть страхователя или диагностика тяжелого заболевания. Страхование жизни может также включать дополнительные опции, например, накопительную часть, которая позволяет накапливать средства на будущее, или возможность получения страховой суммы при инвалидности. Страхование здоровья, в свою очередь, обеспечивает покрытие расходов на медицинское обслуживание и лечение в случае болезни или травмы.

Среди преимуществ интеграции данных о здоровье в сферу страхования можно выделить следующие:

- *Улучшение подбора страховых продуктов.* Собранные и анализируемые данные позволяют фонду страхования жизни и здоровья более точно определить риски и потребности клиентов, что способствует созданию более индивидуализированных страховых продуктов.
- *Снижение рисков и затрат.* Благодаря более точной оценке здоровья клиентов на основе данных фонд может эффективно управлять рисками и минимизировать потери, что в конечном итоге может снизить стоимость страховых премий и обеспечить более адекватное ценообразование.
- *Повышение уровня обслуживания клиентов.* Интеграция данных позволяет фонду предоставлять клиентам более качественное обслуживание, реагируя на изменения в их состоянии здоровья и предоставляя индивидуальную поддержку и советы по управлению здоровьем.
- *Продвижение здорового образа жизни.* Предоставление доступа к инструментам и ресурсам для активного отслеживания и улучшения здоровья может мотивировать клиентов к более здоровому образу жизни, что в конечном итоге снижает риски для фонда и улучшает общее благосостояние клиентов.

Заключение. Применение искусственного интеллекта в сфере медицинской помощи играет ключевую роль в улучшении стандартов здравоохранения и оптимизации обслуживания пациентов. Важно заметить, что недостатки потенциальной информационной системы могут быть преодолены или смягчены с развитием технологий, улучшением алгоритмов и оптимизацией использования таких систем. Однако для успешной интеграции интеллектуальных систем в медицинскую практику необходимо уделить должное внимание

обучению медицинского персонала по их применению, обеспечению безопасности и конфиденциальности медицинских данных пациентов, а также учитывать потребности и предпочтения пациентов при разработке и внедрении таких систем. Решения на основе искусственного интеллекта в области медицины представляют собой мощный инструмент, который способен кардинально изменить методы диагностики, лечения и управления здравоохранением. Правильное применение и развитие таких систем помогут улучшить доступность и качество медицинской помощи, а также повысить эффективность работы медицинского персонала.

1. "Интеллектуальные системы сбора информации о пациентах на основе медицинских браслетов" - И. И. Иванов, В. П. Петров. (дата обращения: 14.03.2024)
2. "Медицинские браслеты: технологии и применение в современной медицине" - А. С. Смирнов, Е. В. Иванова. (дата обращения: 16.03.2024)
3. "Применение носимых устройств в медицине" - Л. Н. Ковалев, В. А. Иванов. (дата обращения: 16.03.2024)
4. "Интеллектуальные системы сбора и анализа медицинской информации" - Е. Г. Смирнова, А. А. Кузнецов. (дата обращения: 18.03.2024)
5. "Технологии носимой электроники в медицине: возможности и перспективы" - В. И. Зубков, О. П. Николаева. (дата обращения: 19.03.2024)
6. ИТ в здравоохранении. Открытые системы. [электронный ресурс] – URL: <http://www.osp.ru/medit/2015/11/13047519.html> (дата обращения: 19.03.2024)
7. Развитие информационного общества. Зинина Л.И., Петрова Е.С., Аникина Н.В., Бажанова С.В., Глухова Т.В., Ефремова Л.И., Иванова И.А., Кузнецов А.Ф., Соколова М.Ю., Федякова Н.Н. Монография / Зинина Л. И. [и др.]; науч. ред. Л. И. Зинина. Саранск, 2010. – 9 с. (дата обращения: 20.03.2024)
8. Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 г., «Собрание законодательства РФ», 31.07.2006 г., № 31 (1 ч.), ст. 3451. (дата обращения: 20.03.2024)
9. Эльянов М. М. Медицинские информационные технологии. Каталог. Вып. 5. - М.: Третья медицина, 2005. - 320 с. (дата обращения: 20.03.2024)
10. Разработка и внедрение нового режима «Листы назначений» в медицинскую информационную систему / А. И. Ленчик, Т. А. Панфилова, А. В. Липатов / Решетневские чтения. 2018. Т. 2. С. 277-279. (дата обращения: 20.03.2024)

Юданов Р.С.

Классификация стеганографии по виду покрываемого объекта

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-412

Аннотация

В статье рассматриваются различные виды стеганографических объектов в зависимости от типа покрываемого носителя, такие как сетевая, лингвистическая, аудио и видео стеганография. Описаны основные методы сокрытия данных в изображениях и аудиофайлах, а также использование интернет-протоколов и текстов для встраивания секретной информации.

Ключевые слова: стеганография, сетевая стеганография, лингвистическая стеганография, аудио стеганография, видео стеганография, защита информации.

Abstract

The article discusses various types of steganographic objects depending on the type of covering medium, such as network, linguistic, audio and video steganography. The main methods of hiding data in images and audio files, as well as the use of Internet protocols and texts for embedding classified information, are described.

Keywords: steganography, network steganography, linguistic steganography, audio steganography, video steganography, information security.

В зависимости от типа покрываемого объекта существуют различные виды стеганографических объектов, которые показаны в таблице 1.

Таблица 1

Классификация стеганографии по виду покрываемого объекта и их описание.

Вид стеганографии	Описание
Сетевая стеганография	Использование интернет-протоколов, таких как TCP/IP, для скрытия информации в сетевых пакетах данных.
Лингвистическая стеганография	Встраивание секретных сообщений в текст с использованием синонимов, грамматических конструкций и кодов.
Стеганография в цифровых изображениях	Встраивание данных в цифровые изображения с использованием методов, таких как LSB и дискретное косинусное преобразование.
Видео стеганография	Соккрытие информации в видеокадрах и аудиотреках видеороликов, используя методы, такие как DWT и фазовое кодирование.
Аудио стеганография	Встраивание секретных сообщений в аудиофайлы с использованием методов LSB, фазового кодирования и эхо-кодирования.

Различные виды стеганографических объектов применяются для обеспечения безопасности, как это показано на рисунке 1.



Рисунок 1. Классификация стеганографии по виду покрываемого объекта.

Сетевая стеганография основывается на внедрении скрытой информации в различные интернет-протоколы, такие как TCP/IP (Transmission Control Protocol/Internet Protocol). Встраивание возможно на всех уровнях модели OSI (Open Systems Interconnection). В таблице 2 наглядно показаны возможности встраивания информации в различные уровни модели OSI. Этот подход позволяет передавать скрытую информацию незаметно, используя стандартные сетевые коммуникации. Применение стеганографии на уровне сетевых протоколов значительно усложняет задачу обнаружения и извлечения скрытых данных, так как информация может быть встраиваемая на любом из семи уровней OSI: физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном [1].

Таким образом, каждый уровень предоставляет свои собственные возможности и методы для сокрытия данных, что делает сетевую стеганографию мощным инструментом для обеспечения конфиденциальности и безопасности передачи данных в сетях.

Таблица 2

Возможность встраивать информацию в подчиненные уровни OSI.

Уровни модели OSI	Способность к встраиванию
Прикладной уровень	Использование обычной стеганографии
Уровень представления	Встраивание в поля сообщений
Сеансовый уровень	Мониторинг удаленных сайтов
Транспортный уровень	Встраивание в неиспользуемые поля протоколов TCP
Сетевой уровень	Встраивание в свободные поля IP-пакетов
Физический уровень	Использование конфликтных ситуаций: «0» – отправить пакет после некоторой задержки, «1» – отправить пакет сразу после конфликта

Что касается ТСР-заголовков, то на рисунке 2 наглядно показана возможность встраивания информации в заголовки ТСР [2]. Поля, закрашенные зеленым цветом, указывают на то, что в них можно встроить информацию без каких-либо проблем; а поля, закрашенные красным цветом, указывают на внедрение информации про некоторых условиях.

Порт отправителя				Порт получателя			
Порядковый номер							
Порт подтверждения							
Смещение данных	Резерв	U	A	P	R	S	F
		R	C	S	S	Y	I
		G	K	H	T	N	Размер Окна
Контрольная сумма				Указатель срочности			
Опции						Выравнивание	

Рисунок 2. Возможность встраивания в заголовки ТСР.

Также стоит отметить VoIP (Voice Over IP)-стеганографию, которая представляет собой разновидность сетевой стеганографии в реальном времени, которая использует протоколы VoIP и трафик в качестве скрытого канала для передачи секретных сообщений. В контексте VoIP-стеганографии встраивание конфиденциальной информации в определенные пакеты осуществляется таким образом, что «потеря пакетов» не оказывает негативного влияния на качество передаваемого голоса.

Одним из часто используемых методов стеганографии, применяемых как в древности, так и в современности, являются методы лингвистической стеганографии. Эти методы позволяют скрывать информацию в текстовых файлах, интегрируя её в сам смысловой контекст текста, что обеспечивает защиту информации от попыток удаления, даже при переводе текста на другой язык. Часто используются те же алгоритмы, которые применялись много веков назад, но адаптированные к цифровому формату.

Основными преимуществами методов лингвистической стеганографии являются простота реализации и высокая степень скрытности, что затрудняет обнаружение факта передачи скрытой информации сторонними наблюдателями. К недостаткам данных методов можно отнести низкую скорость передачи информации и сложность автоматизации процессов, что, как правило, требует участия человека-оператора для встраивания и извлечения информации.

Наиболее известным методом лингвистической стеганографии является метод синонимов. Алгоритм этого метода довольно прост в реализации: в исходном покрывающем объекте (в данном случае в текстовом контексте) осуществляется поиск слов, к которым можно подобрать синонимы. Обычно такие слова заранее определены в словаре синонимов, где уже указано, какой синоним из пары соответствует передаче «1», а какой — «0». При этом могут использоваться как абсолютные, так и относительные синонимы [3].

Абсолютные синонимы — это слова или фразы, которые можно заменить другими словами или фразами в любом контексте без изменения семантики исходного текста; например, пара слов «счастливый» и «радостный», «идти» и «шагать» и прочее. Относительные синонимы, напротив, — это слова или фразы, которые могут заменять друг друга не всегда, а только в определённых контекстах, если замена не нарушает исходной семантики предложения; например, пары «выпустить пар» и «успокоиться», «выпустить пар» и «открыть крышку» (кипящей кастрюли). Таким образом, при использовании относительных синонимов необходимо учитывать контекст ПО.

Стеганография применяется для встраивания секретных сообщений в изображения, которые являются наиболее популярными покрывающими объектами. Это связано с тем, что изображения обладают большим пространством для скрытия информации и высокой избыточностью в представлении данных. Общие методы стеганографии делятся на два типа:

методы, основанные на использовании пространственной области, и методы, основанные на области преобразования.

Методы, основанные на пространственной области, являются более широко применяемыми по сравнению с методами на основе области преобразования. Наиболее распространённым алгоритмом стеганографии для изображений является алгоритм встраивания в наименее значащий бит (НЗБ). Этот метод заключается в замене наименее значащих битов пикселей изображения битами скрываемой информации.

Преимуществом методов на основе пространственной области является их простота и эффективность, что позволяет легко реализовать алгоритмы на практике. Однако, они могут быть более уязвимы к стеганализу и атакам, направленным на обнаружение скрытой информации. Методы на основе области преобразования, такие как DCT или дискретное преобразование Уолша (DWT), предлагают большую устойчивость к таким атакам, так как встраивание информации происходит в частотной области изображения. Это делает их менее заметными, но более сложными в реализации и требующими больших вычислительных ресурсов [4].

Видео-стеганография представляет собой расширение методов стеганографии, применяемых к изображениям. Видеопоток фактически состоит из серии последовательных и равномерно распределённых во времени неподвижных изображений (кадров), сопровождаемых аудио. Поэтому многие методы стеганографии, разработанные для изображений, могут быть адаптированы для видео-стеганографии. Видео является весьма перспективным типом покрывающего носителя, так как позволяет встраивать значительное количество секретных данных.

Аудио стеганография представляет собой метод встраивания секретных сообщений в аудио файлы. Этот метод обладает высокой надёжностью, но имеет ограничение по объёму данных, которые можно скрыть. Аудио стеганография применяется для встраивания данных в звуковые файлы форматов WAV, AU, MP3 и других. Существуют различные методы аудио стеганографии, включая кодирование НЗБ, фазовое кодирование, использование широкополосных сигналов и эхо-сигналов. Эти методы обеспечивают надёжную защиту данных и минимальное искажение оригинального аудиоконтента, что делает их привлекательными для использования в различных приложениях, требующих высокой степени конфиденциальности.

1. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография. СПб.: Изд-во СПбГУТ, 2016.
2. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
3. Цветков А. Ю., Рузманов Е. Ю. РАССМОТРЕНИЕ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ //ББК 3 П27. – 2021. – С. 55.
4. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 193-197.

Юданов Р.С.

Методы анализа публикационной активности

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-413

Аннотация

В статье рассматриваются методы анализа публикационной активности, включая количественные подходы, такие как подсчет публикаций и индекс Хирша, а также качественные, например, экспертная оценка и анализ контекста цитирования. Особое внимание уделяется визуализации данных, которая помогает выявить ключевые тенденции и закономерности в научной деятельности.

Ключевые слова: публикационная активность, количественные методы, качественные методы, индекс Хирша, цитирование, визуализация данных.

Abstract

The article discusses methods for analyzing publication activity, including quantitative approaches such as counting publications and the Hirsch index, as well as qualitative ones, such as peer review and citation context analysis. Special attention is paid to data visualization, which helps to identify key trends and patterns in scientific activity.

Keywords: publication activity, quantitative methods, qualitative methods, Hirsch index, citation, data visualization.

Анализ публикационной активности включает в себя разнообразные методы, которые можно разделить на количественные и качественные. Количественные методы позволяют объективно измерить научную продуктивность и влияние, используя различные числовые показатели. Эти методы основываются на сборе и анализе данных о количестве публикаций, их цитируемости и других метриках, что позволяет оценить вклад исследователей и организаций в развитие науки.

Количественные методы анализа публикационной активности фокусируются на измерении числовых показателей, которые отражают продуктивность и влияние научных работ. Эти методы обеспечивают объективные данные, которые можно сравнивать и анализировать для оценки научной деятельности. Основные подходы отражены в таблице 1.

Таблица 1

Описание основных количественных методов.

<i>Метод</i>	<i>Описание</i>	<i>Преимущества</i>	<i>Ограничения</i>
<i>Количество публикаций</i>	<i>Подсчет общего числа научных публикаций исследователя, группы или организации за определенный период времени.</i>	<i>Простота измерения и интерпретации, возможность быстрого получения данных.</i>	<i>Не всегда отражает качество работы, так как большое количество публикаций не обязательно свидетельствует о высоком научном уровне.</i>
<i>Число цитирований</i>	<i>Количество раз, когда работа была процитирована в других научных публикациях.</i>	<i>Позволяет оценить признание работы в научном сообществе, указывает на влияние публикации.</i>	<i>Может быть предвзятым в пользу популярных или модных тем, не учитывает контекст цитирования.</i>
<i>Импакт-фактор</i>	<i>Среднее количество цитирований статей, опубликованных в научном журнале за определенный период (обычно два года).</i>	<i>Общеизвестный и признанный показатель, помогает сравнивать журналы.</i>	<i>Не учитывает контекст цитирования, неравномерно распределен между областями знаний.</i>
<i>Индекс Хирша (h-индекс)</i>	<i>Показатель, который учитывает как количество публикаций, так и их цитируемость. Исследователь имеет индекс h, если h его статей процитированы не менее h раз.</i>	<i>Учитывает как продуктивность, так и влияние, балансируя между числом публикаций и их качеством.</i>	<i>Может быть завышен за счет умеренно цитируемых публикаций, не учитывает разницу в цитируемости по областям знаний.</i>

Количественные методы предоставляют объективные и измеримые данные, которые помогают оценить научную продуктивность и влияние исследований. Однако важно помнить, что они имеют свои ограничения и могут быть дополнены качественными методами для получения более полной картины.

Качественные методы анализа публикационной активности предоставляют глубокое понимание содержания и значимости научных работ. В отличие от количественных методов, которые фокусируются на числовых показателях, качественные методы направлены на более детальную оценку качества научных публикаций, их влияния и контекста использования. Эти

методы включают экспертную оценку, анализ содержания публикаций и контекста цитирования.

Экспертная оценка является одним из ключевых качественных методов, в рамках которого специалисты в определенной научной области проводят всесторонний анализ научных работ. Эксперты оценивают не только методологию и результаты исследований, но и их новизну, оригинальность, вклад в науку и потенциальное влияние на дальнейшие исследования. Экспертные оценки могут учитывать множество факторов, таких как сложность и инновационность подходов, актуальность исследуемой темы и качество интерпретации полученных данных. Этот метод помогает выявить сильные и слабые стороны научных работ, что способствует более точной и объективной оценке их значимости.

Анализ содержания публикаций представляет собой еще один важный качественный метод. В этом подходе внимание уделяется глубинному изучению текстов научных работ. Анализируются основные гипотезы, методология, результаты и выводы исследования. Особое внимание уделяется тому, насколько тщательно исследователь проработал свою тему, использовал ли он адекватные методы исследования и насколько убедительно он представил свои результаты. Качественный анализ содержания позволяет выявить наиболее значимые и перспективные работы, а также определить направления, которые требуют дальнейшего изучения.

Контекст цитирования также играет важную роль в качественном анализе публикационной активности. Этот метод включает изучение контекста, в котором работы упоминаются в других научных публикациях. Важно не только знать, сколько раз работа была процитирована, но и понять, в каком контексте это произошло. Например, цитата может быть использована для подтверждения основных результатов исследования, для критики или для обсуждения в контексте более широкого научного вопроса. Анализ контекста цитирования помогает оценить истинное влияние работы на научное сообщество и понять, как результаты исследования воспринимаются и используются другими учеными.

Таким образом, качественные методы анализа публикационной активности предоставляют более глубокое и многогранное понимание научной деятельности. Они позволяют учитывать не только количественные аспекты, но и качество, значимость и контекст использования научных работ. Это особенно важно для комплексной оценки научной продуктивности и влияния, а также для принятия обоснованных решений в области управления научными исследованиями и разработки стратегий развития научных направлений.

Еще одним важным аспектом методов анализа публикационной активности является визуализация данных. Данный инструмент позволяет наглядно представить сложные данные и выявить скрытые закономерности и тенденции. Методы визуализации помогают исследователям, администраторам и политикам быстрее и легче понимать результаты анализа, принимая обоснованные решения на основе представленных данных. Далее рассмотрим основные способы визуализации данных:

Графики и диаграммы являются базовыми инструментами визуализации данных. Они включают в себя линейные графики, гистограммы, круговые диаграммы и столбчатые диаграммы. Линейные графики часто используются для отображения изменений публикационной активности во времени, показывая динамику числа публикаций или цитирований. Гистограммы и столбчатые диаграммы помогают сравнивать показатели между разными авторами, учреждениями или временными периодами. Круговые диаграммы используются для иллюстрации долей различных категорий, таких как распределение публикаций по типам или тематикам.

Сетевые графы предоставляют возможность визуализации сложных взаимоотношений и связей между элементами публикационной активности. Например, графы соавторства показывают, как исследователи сотрудничают друг с другом, образуя научные сети. Узлы в таких графах представляют собой авторов, а ребра — совместные публикации. Анализ сетевых графов позволяет выявить ключевые фигуры и группы в научном сообществе, а также понять структуру и динамику научных сотрудничеств. Пример сетевого графа можно рассмотреть на рисунке 1.

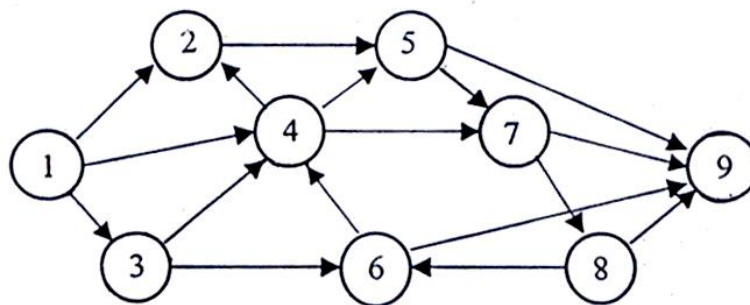


Рисунок 1. Сетевой граф.

Карты соавторства являются специфической формой сетевых графов, которые фокусируются на взаимодействиях между авторами. Они помогают визуализировать, как распределены научные сотрудничества в различных географических регионах или между различными учреждениями. Карты соавторства могут быть полезны для выявления основных центров научной активности и анализа географического распределения научных исследований.

Тепловые карты предоставляют визуализацию плотности или интенсивности публикационной активности в различных областях. Они часто используются для отображения количества публикаций или цитирований в определенных географических регионах или научных областях. Тепловые карты помогают быстро идентифицировать регионы с высокой или низкой активностью и могут быть полезны для анализа концентрации научных исследований.

Тематические карты позволяют визуализировать распределение публикаций по различным научным темам или областям знаний. Такие карты помогают понять, какие темы являются наиболее популярными или значимыми в определенной области, и могут выявить основные направления исследований. Тематические карты также полезны для анализа трендов и выявления новых, возникающих областей научных исследований.

Дашборды (панели мониторинга) объединяют несколько методов визуализации данных в одном интерфейсе, предоставляя комплексный обзор ключевых метрик и показателей публикационной активности. Дашборды позволяют пользователям легко переключаться между различными визуализациями и получать актуальную информацию в реальном времени. Они могут включать графики, диаграммы, карты и другие визуальные элементы, предоставляя полное представление о публикационной активности.

Интерактивные визуализации представляют собой продвинутые методы визуализации данных, которые позволяют пользователям взаимодействовать с данными. Такие визуализации позволяют масштабировать, фильтровать и исследовать данные более детально, предоставляя пользователю возможность настроить отображение информации под свои потребности. Интерактивные визуализации часто используются в веб-приложениях и аналитических инструментах для предоставления более гибких и адаптивных возможностей анализа.

Методы визуализации данных являются неотъемлемой частью анализа публикационной активности, предоставляя исследователям и администраторам мощные инструменты для понимания и интерпретации сложных данных. Визуализация помогает выявить важные тенденции, взаимодействия и паттерны, которые могут быть неочевидны при использовании только числовых методов анализа. Таким образом, использование визуализационных методов значительно улучшает качество и эффективность анализа публикационной активности, способствуя принятию более обоснованных и информированных решений.

1. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
2. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

3. ТЕХНОЛОГИЯ ОЦЕНКИ КАЧЕСТВА СУБЪЕКТОВ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В ВУЗЕ
Васильева Е.Ю., Минин А.А. Экология человека. 2006. № 11. С. 32-38. [Электронный ресурс]. URL: <https://elibrary.ru/item.asp?id=9232354>. (дата обращения: 29.09.2024.)
4. InCites.Объективный анализ людей, программ и коллег [Электронный ресурс]. URL: <https://clarivate.com/cis/solutions/incites/>. (дата обращения: 30.09.2024.)

Юданов Р.С.

Основные методы и применение стеганографии в различных областях

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-414

Аннотация

В статье рассматриваются основные принципы и методы стеганографии, такие как безопасность, незаметность и вместимость, и их роль в защите информации. Приведены различные области применения стеганографии, включая информационную безопасность, военные и разведывательные операции, защиту авторских прав и коммерческие задачи.

Ключевые слова: стеганография, безопасность данных, встраивание информации, цифровые водяные знаки, информационная безопасность, кибербезопасность.

Abstract

The article discusses the basic principles and methods of steganography, such as security, invisibility and capacity, and their role in protecting information. Various fields of application of steganography are presented, including information security, military and intelligence operations, copyright protection and commercial tasks.

Keywords: steganography, data security, information embedding, digital watermarks, information security, cybersecurity.

В стеганографии для сокрытия секретных данных необходимы три ключевых принципа, представленных на рисунке 1: безопасность, незаметность и вместимость. Эти принципы являются основными факторами, определяющими эффективность стеганографической системы. В зависимости от применения, существуют специфические требования для различных стеганографических методов [1].

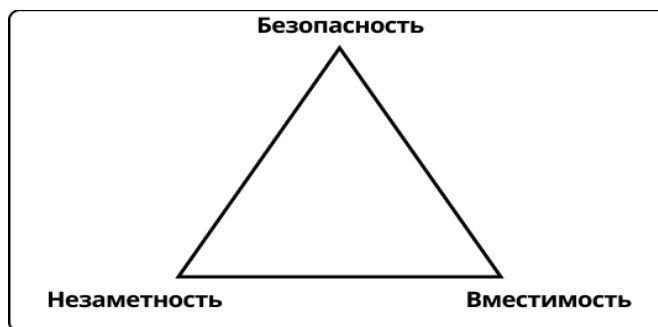


Рисунок 1. Основные принципы стеганографии.

Однако существует компромисс между размером скрытых данных и качеством стеганографических файлов. Если необходимо встроить большой объем секретных данных, то изменение стеганографических файлов становится сложнее, так как сложнее обеспечить незаметность из-за возможных искажений. Поэтому основная задача заключается в оптимальном поддержании этих принципов. Устойчивость не всегда является обязательной, однако безопасность, незаметность и вместимость всегда необходимы. В отношении цифровых водяных знаков большая вместимость и незаметность не являются столь обязательными.

Незаметность является приоритетом в стеганографии и направлена на сокрытие секретных данных внутри других медиа файлов. Человеческий глаз не может обнаружить их даже при применении статистических методов. Статистические методы являются эффективным средством для злоумышленников, чтобы определить, передаются ли секретные данные между двумя сторонами. Поэтому медиаданные не должны заметно изменяться по статистическим показателям из-за встраивания секретных данных. Если статистические данные в исходных и стеганографических файлах схожи, то можно считать, что безопасность достаточно высокая для передачи данных. Качество медиаданных должно сохраняться при передаче через незащищенные сети, несмотря на шум, возникающий в процессе встраивания.

Термин "безопасность" в стеганографии относится к "необнаруживаемости" или "незаметности". Стеганографический метод считается безопасным, если скрытые данные не могут быть обнаружены с помощью статистических техник третьими лицами. Безопасность является основным требованием для предотвращения доступа незаконных лиц или компьютеров при коммуникации через незащищенный канал, обеспечивая сохранность данных [2].

Эффективная стеганографическая система, как правило, стремится передать максимальное количество информации с использованием минимального количества покрывающих медиаданных. Это снижает вероятность перехвата при передаче через незащищенный канал и, таким образом, обычно требует высокой вместимости встраивания. Основной задачей в стеганографии является поддержание высокой вместимости при сохранении безопасности и незаметности [3].

Устойчивость означает способность методов встраивания и извлечения выдерживать любые искажения, вызванные третьими лицами с помощью различных методов обработки. В случае стеганографии, если стеганографические файлы не пострадали или остались неизменны при передаче через Интернет, это не считается атакой, и человек получает файл в исходном виде. В противном случае возможны атаки, такие как сжатие, изменение формата файла и преобразование между цифровым и аналоговым форматами во время процесса передачи. Однако для систем распознавания по отпечаткам пальцев устойчивость необходима при преднамеренном изменении или модификации файлов.

Существуют различные методы стеганографии, каждый из которых имеет свои сильные и слабые стороны в зависимости от применения. Основные методы включают стеганографию в изображениях, аудио, видео, а также в текстах и сетевых протоколах. Эти подходы можно сравнить по таким критериям, как безопасность, незаметность, вместимость и устойчивость к атакам.

Стеганография в изображениях является одним из наиболее популярных методов, так как изображения имеют большой объем данных, что позволяет скрывать информацию с минимальными изменениями визуального контента. Метод наименее значимого бита (LSB) является наиболее распространённым, так как обеспечивает высокую вместимость, однако данный метод менее устойчив к стеганализу — специальным техникам обнаружения скрытых данных.

Аудиостеганография предоставляет аналогичные преимущества, однако её устойчивость к изменениям в формате данных выше. Например, фазовое кодирование и эхо-сигналы позволяют скрывать информацию таким образом, что её трудно обнаружить даже при сжатии аудиофайла, но вместимость информации ниже по сравнению с изображениями.

Видеостеганография, как расширение методов стеганографии для изображений, предоставляет возможность скрывать информацию в видеокдрах, что делает её более гибкой

для сокрытия больших объемов данных. Однако сложность обработки видеофайлов и больших объемов данных делает данный метод более ресурсоёмким.

Лингвистическая стеганография использует тексты для сокрытия данных, внедряя их в грамматические конструкции или заменяя слова синонимами. Хотя этот метод обладает высокой степенью незаметности, он имеет ограниченную вместимость и требует значительной вычислительной мощности для обработки больших текстов.

Сетевая стеганография использует протоколы и сетевой трафик для сокрытия данных на уровне различных уровней модели OSI. Этот метод предоставляет высокую гибкость, так как может скрывать информацию на разных уровнях, от транспортного до прикладного, но его устойчивость к обнаружению и сложности реализации зависят от выбранного уровня и протокола.

Различные области применения стеганографии демонстрируют её универсальность и эффективность в решении задач, связанных с защитой информации. От обеспечения безопасности конфиденциальных данных в информационных системах до защиты авторских прав в цифровых медиафайлах, стеганография нашла своё место в самых разных сферах [4]. Её способность скрывать данные внутри других, кажущихся безобидными объектов, делает её незаменимым инструментом в условиях растущих угроз кибербезопасности.

Рассмотрим более подробно на конкретных примерах, что отображено в таблице 1, где и с какой целью может быть использована стеганография.

Таблица 1

Основные области применения стеганографии и их описание.

<i>Область применения</i>	<i>Описание</i>
<i>Информационная безопасность</i>	<i>Используется для защиты конфиденциальных данных от несанкционированного доступа и кибератак, скрывая информацию в медиафайлах.</i>
<i>Военные и разведывательные цели</i>	<i>Обеспечивает безопасную передачу секретных данных, скрывая сообщения в аудио, изображениях и других файлах.</i>
<i>Защита авторских прав (цифровые водяные знаки)</i>	<i>Внедрение водяных знаков в цифровые медиафайлы для защиты от пиратства и несанкционированного использования.</i>
<i>Коммерческие приложения</i>	<i>Защита деловой информации и коммуникаций, скрывая данные в изображениях и документах для предотвращения утечек.</i>
<i>Медицинские приложения</i>	<i>Обеспечение безопасности медицинских записей, скрывая данные о пациентах в медицинских изображениях.</i>

Понимание различных примеров и областей применения стеганографии позволяет лучше оценить её потенциал и значимость в современном мире. Стеганография используется для надежной передачи сообщений, что критически важно для поддержания безопасности и защиты информации. Она играет ключевую роль в создании комплексных систем защиты информации, способствуя повышению общей безопасности в цифровом пространстве.

1. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
2. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 560-564.
3. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография. СПб.: Изд-во СПбГУТ, 2016.
4. Герлинг Е.Ю., Ахрамеева К.А., ВЫЯВЛЕНИЕ СКРЫТОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ С ШУМОМ // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 3. С. 21-26.

Юданов Р.С.

Современные методы проведения тестирования на проникновение

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)

doi: 10.18411/trnio-10-2024-415

Аннотация

В статье рассматриваются современные методы проведения тестирования на проникновение, включая традиционные подходы черного, белого и серого ящика, а также использование больших языковых моделей (LLM). Описаны ключевые особенности каждого метода, их преимущества и недостатки, а также возможности применения LLM для автоматизации процессов тестирования, включая генерацию атак, анализ уязвимостей и создание эксплойтов.

Ключевые слова: тестирование на проникновение, черный ящик, белый ящик, серый ящик, большие языковые модели (LLM), кибербезопасность.

Abstract

The article discusses modern methods of conducting penetration testing, including traditional black, white and gray box approaches, as well as the use of large language models (LLM). The key features of each method, their advantages and disadvantages, as well as the possibilities of using LLM to automate testing processes, including attack generation, vulnerability analysis and exploit creation, are described.

Keywords: penetration testing, black box, white box, gray box, large language models (LLM), cybersecurity.

Тестирование на проникновение — это процесс оценки безопасности компьютерных систем или сетей путем имитации атаки злоумышленника. Цель тестирования на проникновение - выявить уязвимости и устранить их, чтобы повысить уровень защищенности. В процессе тестирования на проникновение используются различные методологии, стратегии, инструменты.

С каждым годом появляются все новые методы атак и уязвимости, из-за которых специалистам бывает сложно проводить ручные тесты. Поэтому все чаще компании стараются внедрить новые методы тестирования. Такие как тестирования с использованием больших языковых моделей.

В проведении тестирования на проникновения, ключевым аспектом является оценка степени защищенности системы от различных видов атак. Языковые модели могут быть задействованы в различных этапах, включая сбор информации о целевой системе, анализ уязвимостей, написание эксплойтов и оценку эффективности защитных механизмов.

Согласно исследованиям, учёных из Иллинойского университета в Урбане-Шампейне. LLM становятся все более эффективными, как в доброкачественном, так и в вредоносном использовании. С расширением возможностей, исследователи все больше интересуются их способностью использовать уязвимости в области кибербезопасности. В частности, в недавней работе были проведены предварительные исследования способности LLM самостоятельно взламывать веб-сайты. Однако эти исследования ограничены простыми уязвимостями [1].

LLM могут автономно использовать однодневные уязвимости в реальных системах. Чтобы показать это, они собрали данные о 15 однодневных уязвимостях, включая те, которые в описании CVE отнесены к категории критических по степени серьезности. Согласно описанию CVE, GPT-4 способен использовать 87% этих уязвимостей по сравнению с 0% для любой другой тестируемой нами модели или сканеров уязвимостей с открытым исходным кодом (ZAP

и Metasploit). К счастью, для обеспечения высокой производительности нашему агенту GPT-4 требуется описание CVE: без описания GPT-4 может использовать только 7% уязвимостей [2].

Данное исследование особенно подчеркивает, что использование языковых моделей в тестировании на проникновение представляет собой перспективный подход, который позволяет улучшить эффективность и точность проводимых тестов.

Ручное тестирование на проникновение выполняется вручную тестировщиками, которые используют свои знания и опыт для поиска уязвимостей. Это может включать в себя такие действия, как:

- Сканирование сети: Тестировщики используют инструменты сканирования сети для поиска открытых портов, служб и уязвимых систем.
- Анализ уязвимостей: Тестировщики используют инструменты анализа уязвимостей для поиска известных уязвимостей в системе.
- Эксплуатация уязвимостей: Тестировщики используют свои навыки и опыт для эксплуатации уязвимостей и получения доступа к системе.
- Постэксплуатация: Тестировщики используют свой доступ к системе для выполнения дальнейших действий, таких как кража данных или повышение привилегий.

Тестирование на проникновение с использованием LLM представляет собой новый подход, который использует возможности языковых моделей на базе искусственного интеллекта для выявления уязвимостей в системах и сетях. LLM (Large Language Models) — это модели ИИ, обученные на огромных объемах текстовых данных, которые способны создавать связные и естественно звучащие тексты. Они могут быть обучены на данных, содержащих информацию об уязвимостях, эксплоитах и методах тестирования на проникновение. Схема использования данного метода в тестировании на проникновение представлена на рисунке 1.

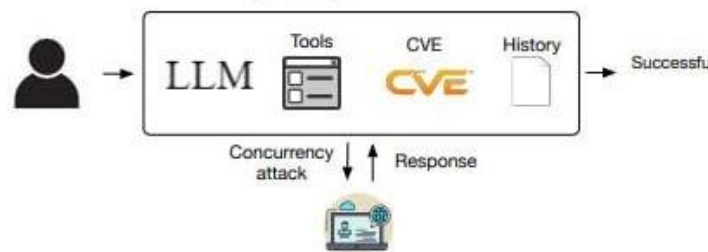


Рисунок 1. Схема работы.

Существует несколько подходов к проведению тестирования на проникновение, которые различаются уровнем знаний о тестируемой системе и способом доступа к ней. Один из таких подходов — "черный ящик", при котором тестировщики не обладают знаниями о структуре компании и используют внешние данные для проведения атак. Этот метод приближен к реальным условиям, позволяя выявлять реальные угрозы и проверять эффективность средств защиты, однако он имеет такие недостатки, как неполное покрытие и возможность пропуска скрытых уязвимостей, а также высокую стоимость тестирования [3].

Другой подход — "белый ящик", при котором тестировщики обладают полными знаниями о системе, включая исходный код, архитектуру и документацию. Этот метод позволяет провести более глубокий анализ и выявить скрытые уязвимости, которые могут быть упущены при тестировании "черного ящика". Преимущества включают полную покрытие и низкую стоимость тестирования, но недостатками являются низкая реалистичность, медленная скорость и риск утечки конфиденциальной информации.

Третий подход — "серый ящик", представляющий собой комбинацию первых двух методов. В этом случае тестировщики имеют частичные знания о системе и учетные записи

непривилегированных пользователей в различных сервисах, что делает тестирование более эффективным [4]. Этот метод объединяет реалистичность и выявление уязвимостей разного уровня, обеспечивая оптимальную скорость и стоимость тестирования, однако при этом возможны пропуски уязвимостей и требуется доступ к системе.

Для более наглядного понимания различий между основными методами тестирования на проникновение, ниже представлена таблица 1, которая сравнивает три подхода: черный ящик, белый ящик и серый ящик. В таблице отражены ключевые параметры каждого метода, их преимущества и недостатки, что поможет лучше оценить их применимость в различных сценариях тестирования безопасности.

Таблица 1

Сравнение основных методов тестирования на проникновение.

Подход	Уровень знаний	Преимущества	Недостатки
Черный ящик	Нет знаний о системе	Реалистичность, выявление реальных угроз	Неполнота покрытия, высокая стоимость
Белый ящик	Полные знания о системе	Полнота покрытия, низкая стоимость	Отсутствие реалистичности, риск утечки данных
Серый ящик	Частичные знания о системе	Оптимальный баланс между реалистичностью и полнотой покрытия	Возможные пропуски уязвимостей, доступ к системе обязателен

Тестирование на проникновение является важным этапом обеспечения безопасности ИТ-систем, а выбор методологии напрямую зависит от целей компании и требуемой глубины анализа. Черный ящик обеспечивает реалистичность, но имеет ограничения в покрытии. Белый ящик позволяет глубже проанализировать систему, но менее реалистичен. Серый ящик — это сбалансированный подход, объединяющий достоинства обоих методов.

1. University of Illinois Urbana-Champaign. LLM Agents can Autonomously Exploit One-day Vulnerabilities. [Электронный ресурс]. 2024. URL: <https://arxiv.org/abs/2404.08144>.
2. SecurityLab. Методы тестирования на проникновение и анализ защищенности. [Электронный ресурс]. 2023. URL: <https://www.securitylab.ru/news/548003.php>.
3. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
4. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.

Яблоков Д.С.

Методы анализа сетевого трафика

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)

doi: 10.18411/trnio-10-2024-416

Аннотация

В статье исследуются методы анализа сетевого трафика, включая активные и пассивные подходы, анализ временных рядов и статический анализ. Рассматриваются ключевые принципы мониторинга сетевой активности, выявления аномалий и реагирования на угрозы безопасности, такие как DDoS-атаки и несанкционированный доступ.

Ключевые слова: анализ сетевого трафика, кибербезопасность, пассивный мониторинг, активный мониторинг, визуализация данных, временные ряды.

Abstract

The article explores methods of network traffic analysis, including active and passive approaches, time series analysis and static analysis. The key principles of monitoring network activity, detecting anomalies and responding to security threats such as DDoS attacks and unauthorized access are considered.

Keywords: network traffic analysis, cybersecurity, passive monitoring, active monitoring, data visualization, time series.

Анализ сетевого трафика (Network Traffic Analysis) можно описать как процесс изучения сетевого трафика для характеристики общих портов и протоколов, используемых в сети, мониторинга и реагирования на угрозы, а также обеспечения максимально полного представления о сети организации. Данный процесс (NTA) помогает специалистам по информационной безопасности выявлять аномалии, в том числе угрозы безопасности в сети, а также своевременно и эффективно реагировать на них. Анализ сетевого трафика также может облегчить процесс соблюдения правил информационной безопасности. Злоумышленники все чаще находят уязвимости, которые большинство компаний допускают в своих сетях, что усложняет обнаружение и, как следствие, реагирование на угрозы. В таких случаях анализ сетевого трафика снова может оказаться полезным [1]. В таблице 1, показаны и перечислены повседневные случаи использования анализа сетевого трафика (NTA):

Таблица 1

Случаи использования анализа сетевого трафика (NTA).

<i>Использование NTA</i>	<i>Описание</i>	<i>Цели и Преимущества</i>
<i>Сбор трафика в реальном времени (Collecting)</i>	<i>Мониторинг всех сетевых взаимодействий для наблюдения за потоками данных и быстрой реакции на аномалии.</i>	<i>Быстрое выявление потенциальных угроз, таких как DDoS-атаки или несанкционированный доступ.</i>
<i>Установка базового уровня (Setting)</i>	<i>Анализ типичных паттернов трафика, частоты передачи данных, используемых портов и протоколов для определения "нормы".</i>	<i>Облегчение точного определения отклонений, которые могут указывать на кибератаки или технические сбои.</i>
<i>Анализ подозрительных портов и хостов (Identifying)</i>	<i>Анализ активности через необычные порты и мониторинг</i>	<i>Идентификация попыток эксплуатации уязвимостей и несанкционированной деятельности.</i>
<i>Обнаружение вредоносного ПО (Detecting)</i>	<i>Выявление сигнатур вредоносного ПО и аномальных паттернов поведения, указывающих на наличие вирусов, троянов, программ-вымогателей.</i>	<i>Защита сети и данных от разрушительного программного обеспечения и улучшение сетевой безопасности.</i>

Также стоит отметить, что анализ сетевого трафика помогает не только обнаружить текущие угрозы, но и спрогнозировать потенциальные уязвимости. Например, если обнаружить множество SYN-пакетов на портах, которые никогда (или редко) использовались в сети, то можно сделать вывод что злоумышленник пытается определить, какие порты открыты на хостах. Подобные действия являются типичными маркерами «portscan». Проведение данного сетевого анализа трафика и приход к таким выводам требует определённого теоретического минимума.

Мониторинг сети включает в себя постоянное наблюдение и анализ сетевой инфраструктуры, устройств и моделей трафика для обеспечения оптимальной производительности, доступности и безопасности. Отслеживая ключевые показатели, такие как задержка, потеря пакетов и состояние устройства, сетевые администраторы получают ценную информацию о поведении сети, что позволяет им оперативно выявлять и устранять проблемы. Методы анализа сетевого трафика могут быть различными и зависят от целей мониторинга, типов сетей и используемых инструментов. Рассмотрим их более подробно:

Активный анализ сетевого трафика – данный метод предполагает активную генерацию и отправку трафика в сеть для тестирования и измерения ее производительности. Данный метод обычно основан на синтетических транзакциях, таких как проверка связи с устройством или выполнение скриптовых тестов, для оценки производительности сети и обнаружения потенциальных проблем. Он предоставляет в режиме реального времени информацию о доступности сети, времени отклика и пропускной способности.

Пассивный анализ сетевого трафика - подразумевает мониторинг и запись сетевого трафика без влияния на его ход. Вместо этого он захватывает и анализирует существующий сетевой трафик, часто с помощью сетевых перехватов или зеркалирования портов. Пассивный мониторинг обеспечивает комплексное представление о фактическом поведении сети, позволяя проводить детальный анализ моделей трафика, угроз безопасности и производительности приложений с течением времени. Инструменты для пассивного анализа включают снифферы, такие как Wireshark, которые могут захватывать и анализировать копии пакетов, проходящих через сеть [2].

Анализ временных рядов в контексте сетевого трафика включает изучение трафика, который записывается и анализируется в течение определённого периода времени. Этот метод позволяет выявить закономерности, тренды и возможные аномалии в данных, которые проходят через сеть. Основная цель анализа временных рядов — обеспечение возможности проследить динамику изменения сетевого трафика, что критически важно для ряда задач. Например, с его помощью можно определить, когда именно происходят пики загрузки сети, что может указывать на необходимость увеличения сетевых ресурсов или наличие нестандартной или вредоносной активности, такой как DDoS-атаки. Анализ также помогает определить периоды сниженной активности, что может быть полезно для планирования технического обслуживания или апгрейдов систем. Для выполнения анализа временных рядов данные собираются в регулярные интервалы времени. Эти данные могут включать различные параметры, такие как объем переданных данных, скорость передачи, количество активных соединений и другие метрики. После сбора данных применяются статистические методы для выявления общих тенденций и отклонений от нормы.

Статический анализ сетевого трафика представляет собой метод исследования, при котором данные анализируются без учёта изменений во времени. Это означает, что анализируются отдельные моменты или выборки данных без привязки к их динамике. В отличие от анализа временных рядов, статический анализ не фокусируется на изменении данных со временем и не требует длительного наблюдения за трафиком для выявления тенденций или закономерностей. Также характерной чертой данного метода анализа сетевого трафика является использование математических моделей и алгоритмов для исследования собранных данных о сети. Статический анализ часто используется для проверки соответствия трафика определенным стандартам или правилам безопасности, для выявления вредоносного кода или других аномалий, которые могут быть встроены в сами данные. При статическом анализе большое внимание уделяется детальному изучению содержимого трафика, что позволяет глубоко понять его природу и потенциальные угрозы [3].

Диаграммы и визуализации – данные методы анализа сетевого трафика, наглядно представляют данные, которые помогают быстрее и эффективнее понимать сложные паттерны и аномалии в сетевой активности. Инструменты визуализации, такие как Splunk или Grafana, могут использоваться для создания комплексных дашбордов, отображающих ключевые метрики производительности и безопасности. Визуализация данных трафика позволяет отслеживать в реальном времени такие параметры, как объем трафика, скорость передачи, источники и маршруты трафика, а также выявлять необычные или подозрительные активности, которые могут указывать на нарушения безопасности. Она также полезна для оптимизации сетевых ресурсов, позволяя анализировать использование пропускной способности и эффективность сетевой инфраструктуры.

Каждый из рассмотренных методов играет важную роль в комплексном подходе к управлению сетевыми ресурсами и обеспечению кибербезопасности. Пассивный и активный анализы обеспечивают фундаментальное понимание текущего состояния сети и её поведения под нагрузкой, предоставляя важные данные для мониторинга и оптимизации. Анализ временных рядов раскрывает динамические изменения в трафике, помогая выявлять тенденции и предсказывать потенциальные проблемы. Статистический анализ применяется для глубокого понимания характеристик трафика и обнаружения аномалий, что критически важно для предотвращения атак и сбоев [4]. Наконец, диаграммы и визуализации предоставляют интуитивно понятные и легко усваиваемые способы представления данных, что существенно упрощает анализ и принятие решений.

Комбинирование этих методов позволяет организациям не только реагировать на текущие события в сети, но и стратегически планировать улучшения безопасности и эффективности своих сетевых инфраструктур. Это подчеркивает необходимость интегрированного подхода к анализу сетевого трафика, где каждый метод дополняет другие, обеспечивая всеобъемлющий контроль и управление сетевыми операциями.

1. Беккель Л.С., Максименко М.Э., Анализ сетевой активности как инструмент повышения безопасности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). Санкт-Петербург, 2022. С. 137-142.
2. Сокол В.Е., Ушаков И.А., Красов А.В., Черепанов С.В., Основы сетевых технологий//Учебник / Том Часть 1. Санкт-Петербург, 2023.
3. Стародубова Д.Д., Стародубов Р.Д., Ушаков И.А., Модель обнаружения аномалий сетевого трафика//Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. С. 661-665.
4. Красов А.И., Миняев А.А., Пешков А.И., Ушаков И.А., Оценка систем защиты информации // Свидетельство о регистрации программы для ЭВМ RU 2020664343, 11.11.2020. Заявка № 2020663630 от 03.11.2020.

Яблоков Д.С.

Традиционные методы классификации сетевого трафика

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-417

Аннотация

В статье описаны традиционные методы классификации сетевого трафика, такие как классификация по протоколам, портам и содержимому. Рассматриваются подходы с использованием машинного обучения, включая SVM и нейронные сети, для повышения безопасности и оптимизации сети.

Ключевые слова: классификация сетевого трафика, протоколы, порты, машинное обучение, SVM, нейронные сети.

Abstract

The article describes traditional methods of classifying network traffic, such as classification by protocols, ports and content. Machine learning approaches, including SVM and neural networks, are considered to improve network security and optimization.

Keywords: classification of network traffic, protocols, ports, machine learning, SVM, neural networks.

Традиционная классификация сетевого трафика представляет собой метод классификации и идентификации трафика путем анализа свойств пакетов сетевого трафика. В этой области было проведено множество исследований, как итог данных работ, были сформированы основные методы классификаций.

Метод классификации на основе протокола. Это один из самых ранних методов классификации сетевого трафика, который классифицирует трафик в зависимости от используемого сетевого протокола, что позволяет точно определять типы данных, передаваемых через сеть, и соответствующим образом реагировать на них [1]. Принцип работы данного метода начинается с анализа пакетов данных, которые передаются в сети. Каждый пакет содержит заголовки, которые указывают, какой протокол используется для передачи данных. Наиболее часто используемые протоколы включают TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), а также протоколы более высокого уровня, такие как HTTP, HTTPS, FTP, и SMTP.

Применение классификации сетевого трафика на основе протокола охватывает множество аспектов управления сетью и безопасности. Этот метод позволяет глубже понять, как трафик взаимодействует с сетевой инфраструктурой, и обеспечивает основу для множества операционных и стратегических решений. Классифицировать трафик по протоколам особенно важно для обеспечения безопасности сети. Зная, какие протоколы должны использоваться в нормальных условиях, специалисты могут быстро выявлять аномалии, которые могут указывать на вредоносные действия или технические нарушения. Например, необычно высокое количество трафика по определённому протоколу может сигнализировать о попытке атаки или наличии вредоносного ПО. Также классификация трафика помогает в оптимизации работы сети. Понимание того, какие протоколы потребляют больше всего ресурсов, позволяет администраторам сети настроить приоритеты и обеспечить достаточный уровень производительности для критически важных приложений, в то время как менее важные задачи могут быть ограничены в ресурсах. Это также способствует более эффективному распределению пропускной способности и может предотвратить перегрузки сети.

Метод классификации на основе портов. Данный метод основан на анализе номеров портов, используемых в сетевых соединениях. Эти порты являются частью транспортного слоя в стеке TCP/IP, и каждый порт обычно ассоциируется с определённым типом службы или протокола. Классификация по портам позволяет определить тип передаваемых данных, оценить их приоритет и определить соответствующие меры безопасности. Для наглядного представления информации о методе классификации сетевого трафика на основе портов, разделим ключевые плюсы и минусы этого метода и отразим их в таблице 1:

Таблица 1

Ключевые преимущества и недостатки метода классификации сетевого трафика на основе портов.

Преимущества	Недостатки
<i>Контроль доступа и фильтрация. Позволяет настроить фаерволы и другие механизмы фильтрации для разрешения или блокирования трафика на основе номеров портов.</i>	<i>Динамическое портовое присвоение. Современные приложения могут использовать динамические порты, что усложняет идентификацию и фильтрацию постоянного порта.</i>
<i>Приоритизация трафика. Классификация по портам облегчает настройку качества обслуживания (QoS) для критически важных приложений.</i>	<i>Шифрование трафика. Шифрованный трафик, такой как HTTPS, скрывает детали портов, делая классификацию менее эффективной.</i>
<i>Мониторинг и аналитика. Помогает в мониторинге и анализе сетевого трафика для выявления аномалий и нарушений безопасности.</i>	<i>Обход сетевых фильтров. Приложения могут маскировать свою деятельность под стандартные порты, чтобы обойти сетевые фильтры.</i>
<i>Соответствие нормам безопасности. Управление портами способствует соблюдению требований к безопасности и политик доступа.</i>	<i>Требование дополнительных методов. Часто требует комбинирования с другими методами классификации для увеличения точности и эффективности.</i>

Данная таблица подчеркивает, как метод классификации сетевого трафика на основе портов может быть полезен для различных аспектов управления сетью, но также подчеркивает ограничения, с которыми могут столкнуться организации при его использовании. Эффективное применение этого метода часто требует его интеграции с другими технологиями и подходами к анализу сетевого трафика.

Классификация сетевого трафика по содержанию является одним из методов анализа, позволяющим глубоко понимать и управлять передаваемыми через сеть данными. Этот метод основан на изучении конкретных данных внутри пакетов трафика, что позволяет не только определить тип трафика, но и выявить потенциальные угрозы безопасности, такие как вредоносные программы или неавторизованный доступ к конфиденциальной информации. Классификация по содержанию требует анализа данных на уровне приложений, включая текст, изображения, аудио и видео [2]. Это может включать инспекцию глубоких пакетов (Deep Packet Inspection, DPI), которая позволяет просматривать и управлять данными, идентифицируя конкретные признаки или сигнатуры в трафике. DPI является мощным инструментом для обеспечения безопасности, соблюдения политик и оптимизации сети.

Традиционный метод машинного обучения в контексте классификации и идентификации сетевого трафика включает использование алгоритмов, таких как машины опорных векторов (SVM) и нейронные сети. Эти методы обеспечивают возможность анализировать большие объемы данных и автоматически выявлять сложные шаблоны и аномалии в трафике, что особенно полезно для обеспечения безопасности сетей и управления трафиком [3]. На рисунке 1 отображены два основных подхода в традиционных методах машинного обучения (SVM и нейронные сети), их основные функции.

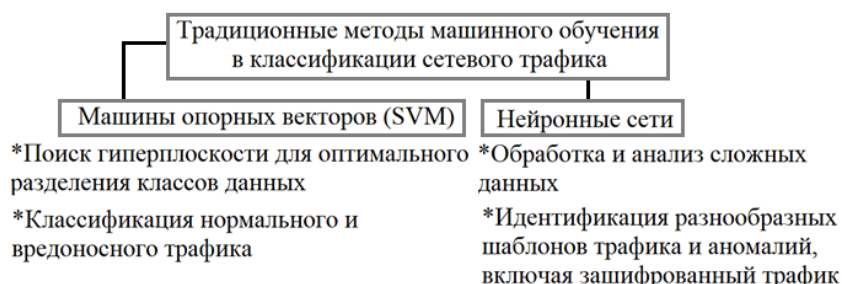


Рисунок 1. Основные подходы в традиционных методах машинного обучения и их функции.

Использование традиционных методов машинного обучения для классификации сетевого трафика позволяет повысить точность идентификации различных видов трафика и аномалий. Эти методы способны обрабатывать и анализировать данные в режиме реального времени, предоставляя сетевым администраторам мощные инструменты для мониторинга, предотвращения и реагирования на сетевые угрозы.

Использование метода классификации сетевого трафика на основе глубокого обучения представляет ряд вызовов, которые необходимо учитывать при интеграции этого подхода в сетевую инфраструктуру. Одной из ключевых проблем является необходимость в больших объемах размеченных обучающих данных [4]. В сетевом контексте, где трафик постоянно эволюционирует и часто содержит чувствительную информацию, сбор и поддержка актуальности таких данных может быть как трудоемким, так и потенциально небезопасным.

Кроме того, глубокое обучение требует значительных вычислительных ресурсов, особенно во время тренировки моделей. Это может стать серьезным барьером для организаций с ограниченными техническими ресурсами или теми, кто нуждается в быстрой обработке данных в реальном времени. Реализация эффективных и масштабируемых вычислительных

систем для поддержки глубокого обучения может потребовать значительных инвестиций в инфраструктуру.

Дополнительной сложностью является интерпретация результатов. Модели глубокого обучения, как правило, действуют как "черные ящики", что затрудняет понимание того, как были получены конкретные выводы. Это может усложнить диагностику проблем и разработку стратегий ответа на инциденты, так как администраторам сетей может быть сложно точно определить, почему модель классифицировала трафик определенным образом.

1. Билятдинов К.З., Красов А.В., Меняйло В.В., Пешков А.И., Карпов А.Н., Теория информационных процессов и систем//Санкт-Петербург, 2019.
2. Сокол В.Е., Ушаков И.А., Красов А.В., Черепанов С.В., Основы сетевых технологий//Учебник / Том Часть 1. Санкт-Петербург, 2023.
3. Казаков Д.Б., Красов А.В., Лоханько Н.О., Подоляк Р.С., Методика защиты сети связи от DDoS атак с помощью BGP Flowspec//Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 386-390.
4. Беккель Л.С., Максименко М.Э., Анализ сетевой активности как инструмент повышения безопасности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). Санкт-Петербург, 2022. С. 137-142.

Яблоков Д.С.

Устройство фундаментальной концепции сетевых технологий TCP/IP

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi: 10.18411/trnio-10-2024-418

Аннотация

В статье рассматривается фундаментальная концепция сетевых технологий на основе модели TCP/IP. Описаны ключевые уровни модели — прикладной, транспортный, межсетевой и каналный, а также их функции в передаче данных. Приводятся преимущества модели, такие как масштабируемость, надёжность и гибкость, а также отмечены её недостатки, включая сложность настройки и уязвимость к атакам.

Ключевые слова: TCP/IP, сетевые технологии, протокол передачи данных, маршрутизация, уровни модели TCP/IP, инфокоммуникационные системы.

Abstract

The article discusses the fundamental concept of network technologies based on the TCP/IP model. The key levels of the model are described — application, transport, inter-network and channel, as well as their functions in data transmission. The advantages of the model, such as scalability, reliability and flexibility, are given, as well as its disadvantages, including complexity of configuration and vulnerability to attacks.

Keywords: TCP/IP, network technologies, data transfer protocol, routing, TCP/IP model layers, infocommunication systems.

Протокол TCP/IP, или Протокол управления передачей/Интернет-протокол, является фундаментом для интернета и значительной части современных сетевых взаимодействий. Эта технология представляет собой набор коммуникационных протоколов, используемых для соединения сетевых устройств в Интернете. TCP/IP позволяет различным сетям успешно обмениваться данными, независимо от их внутренней архитектуры или платформы. TCP (Transmission Control Protocol) задействован в передаче данных, контролируя отправку и гарантируя их доставку получателю в неизменном виде.

IP (Internet Protocol) отвечает за адресацию и связывание устройств в сети, а также за разделение данных на пакеты для их эффективной отправки. Для быстрого нахождения маршрута между компьютерами были разработаны IP-адреса — уникальные идентификаторы, присваиваемые каждому устройству в сети [1].

Функциональность модели TCP/IP разделена на четыре уровня, что наглядно отражено на рисунке 1, каждый из которых включает определенные протоколы. TCP/IP — это система многоуровневой серверной архитектуры, в которой каждый уровень определяется в соответствии с конкретной выполняемой функцией. Все эти четыре уровня TCP/IP работают совместно, передавая данные с одного уровня на другой.

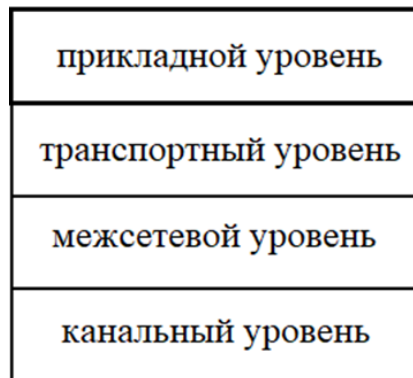


Рисунок 1. Структура модели TCP/IP.

Прикладной уровень — Это самый верхний уровень, который указывает приложения и программы, которые используют модель TCP/IP для связи с пользователем через приложения и различные задачи, выполняемые этим уровнем, включая представление данных для приложений, выполняемых пользователем, и пересылает их на транспортный уровень.

Уровень приложений поддерживает плавное соединение между приложением и пользователем для обмена данными и предлагает различные функции, такие как удаленное управление системой, услуги электронной почты и т. д.

Транспортный уровень - Этот уровень отвечает за установление соединения между отправителем и устройством-получателем, а также выполняет задачу разделения данных прикладного уровня на пакеты, которые затем используются для создания последовательностей. Он также выполняет задачу сохранения данных, т. е. их передачи без ошибок, и контролирует скорость потока данных по каналу связи для плавной передачи данных.

Межсетевой уровень - выполняет задачу управления передачей данных в сетевых режимах и применяет протоколы, связанные с различными этапами, связанными с передачей данных по каналу, который находится в форме пакетов, отправленных предыдущим уровнем. Простыми словами данный уровень строит маршруты между устройствами в сети интернет что в свою очередь называется процессом маршрутизации. Для того чтобы установить местоположение получателя и проложить маршрут к нему, IP использует систему DNS, которая содержит информацию об IP-адресах всех устройств в интернете [2]. После получения адреса передаваемый файл делится на маленькие части, известные как пакеты. Эти пакеты включают в себя части данных и служебную информацию, такую как IP-адреса отправителя и получателя. Затем начинается процесс передачи пакетов через маршрутизаторы и коммутаторы. Однако за процесс отправки отвечает уже транспортный уровень.

Канальный уровень – данный уровень устанавливает физическое соединение между устройствами в локальной сети с помощью радиоволн и проводов. Здесь используются всеми известные протоколы: Ethernet, Wi-Fi, Bluetooth [3]. На этом уровне информация разделяется на маленькие сегменты, называемые фреймами, которые затем передаются между устройствами. Каждый фрейм включает часть передаваемых данных и служебные сведения.

Для определения маршрута фреймов применяется адресация канального уровня, использующая MAC-адреса. Эти уникальные физические адреса устройств позволяют протоколам канального уровня идентифицировать отправителей и получателей [4]. Важной функцией канального уровня является также обеспечение безошибочной передачи данных, для чего используются различные средства проверки.

Модель TCP/IP является стандартной сетевой моделью, которая легла в основу интернета и сыграла ключевую роль в развитии современных сетевых технологий. Она имеет свои плюсы и минусы, которые отражены в таблице 1 ниже.

Таблица 1

Плюсы и минусы модели TCP/IP.

Преимущества модели TCP/IP	Недостатки модели TCP/IP
<i>Масштабируемость. Модель TCP/IP хорошо масштабируется и может работать как в небольших, так и в крупных сетях.</i>	<i>Сложность: модель довольно сложна и требует определенного уровня знаний для настройки и обслуживания.</i>
<i>Надежность: модель прочная и надежная, что делает ее подходящей для критически важных приложений.</i>	<i>Уязвимость: из-за своей сложности он уязвим для атак.</i>
<i>Гибкость: он очень гибок и обеспечивает совместимость между различными типами сетей.</i>	<i>Производительность. Производительность может снизиться из-за перегрузки сети и задержек.</i>

Модель TCP/IP на протяжении десятилетий является стандартом сетевых технологий и обеспечивает эффективную передачу данных между устройствами. Её структура, разделенная на уровни, позволяет гибко адаптироваться под различные сетевые архитектуры и условия эксплуатации. Несмотря на существующие недостатки, такие как сложность настройки и уязвимость к атакам, преимущества модели, включая масштабируемость, надежность и совместимость, делают её незаменимым элементом для построения современных сетей. Важным является дальнейшее изучение и развитие технологий, основанных на TCP/IP, что способствует устойчивому развитию инфокоммуникационных систем.

1. Сокол В.Е., Ушаков И.А., Красов А.В., Черепанов С.В., Основы сетевых технологий//Учебник / Том Часть 1. Санкт-Петербург, 2023.
2. Василишин Н.С., Дубровин Н.Д., Ушаков И.А., Чечулин А.А., Методы сбора и анализа сетевого трафика на основе технологий больших данных//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). - 2017. - С. 127-131.
3. Красов А.В., Лосин Е.П., Ушаков И.А., Проблема безопасности передачи групповых рассылок в IP-сетях// Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 295-301.
4. Билятдинов К.З., Красов А.В., Меняйло В.В., Пешков А.И., Карпов А.Н., Теория информационных процессов и систем//Санкт-Петербург, 2019.

РАЗДЕЛ XXII. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Абдразаков В.А., Харченко С.Н.

Роль участия искусственного интеллекта в образовании

ФГБОУ ВО "Кубанский Государственный Аграрный Университет им. Трубилина"

(Россия, Краснодар)

doi: 10.18411/trnio-10-2024-419

Аннотация

Статья рассматривает влияние искусственного интеллекта (ИИ) на образовательный процесс, подчеркивая его значимость для студентов и преподавателей. Основные аспекты включают персонализацию обучения, адаптивные технологии, автоматизацию административных задач и расширение доступа к образовательным ресурсам. ИИ позволяет создавать индивидуализированные учебные планы, подстраиваться под уровень знаний учащихся и облегчать рутинные задачи преподавателей. Также рассматривается роль ИИ в поддержке учителей и развитии навыков XXI века, таких как критическое мышление и креативность.

Ключевые слова: искусственный интеллект, образование, креативность, персонализация обучения, критическое мышление, эксклюзивное образование, автоматизация.

Abstract

The article examines the impact of artificial intelligence (AI) on the educational process, emphasizing its importance for students and teachers. The main aspects include the personalization of learning, adaptive technologies, automation of administrative tasks and increased access to educational resources. AI allows you to create individualized curricula, adjust to the level of knowledge of students and facilitate the routine tasks of teachers. The role of AI in supporting teachers and developing 21st century skills such as critical thinking and creativity is also considered.

Keywords: artificial intelligence, education, creativity, personalization of learning, critical thinking, exclusive education, automation.

В последние годы искусственный интеллект (ИИ) стал неотъемлемой частью различных секторов экономики, и образование не стало исключением. Внедрение ИИ в образовательный процесс открывает новые горизонты как для студентов, так и для преподавателей. Рассмотрим ключевые аспекты роли ИИ в образовании и его влияние на будущее учебного процесса.

Персонализация обучения

Одним из самых значительных преимуществ ИИ является возможность персонализации образовательного процесса. Системы на основе ИИ могут анализировать данные о каждом учащемся, включая его сильные и слабые стороны, стиль обучения и предпочтения. Это позволяет создавать индивидуализированные учебные планы и рекомендации, что способствует более эффективному усвоению материала. Например, платформы, такие как Coursera и Khan Academy, используют алгоритмы для адаптации курсов под конкретные нужды учащихся, что повышает их мотивацию и вовлеченность.

Адаптивные технологии

Адаптивные системы обучения, использующие ИИ, могут подстраиваться под уровень знаний студента в реальном времени. Если учащийся испытывает трудности с определенной темой, система может предложить дополнительные упражнения или объяснения. Это помогает избежать фрустрации и способствует более глубокому пониманию материала. Такие технологии уже активно применяются в онлайн-образовании, где студенты могут получать мгновенную обратную связь и адаптированные задания.

Автоматизация административных задач

ИИ способен существенно облегчить работу преподавателей, автоматизируя рутинные административные задачи, такие как оценка тестов, составление расписаний и управление учебными материалами. Это позволяет учителям сосредоточиться на более важных аспектах их работы — взаимодействии со студентами и разработке новых методик обучения. Например, системы автоматизированного тестирования могут не только оценивать работы, но и предоставлять статистику по общему уровню усвоения материала классом.

Доступ к образовательным ресурсам

Искусственный интеллект также расширяет доступ к образовательным ресурсам. Платформы на основе ИИ могут предоставлять студентам доступ к онлайн-курсам, библиотекам и другим учебным материалам, независимо от их местоположения. Это особенно актуально для студентов из удаленных или недостаточно обеспеченных регионов. ИИ может помочь в переводе материалов на разные языки, что делает образование более доступным для международной аудитории.

Поддержка преподавателей

ИИ может служить мощным инструментом для поддержки преподавателей системы анализа данных могут предоставлять информацию о том, какие методики обучения работают лучше всего, а также помогать в выявлении студентов, нуждающихся в дополнительной помощи. Это позволяет учителям более эффективно планировать свои занятия и адаптировать подходы к обучению. Например, использование аналитики больших данных может помочь выявить закономерности в успеваемости студентов и предсказать их дальнейшие успехи.

Развитие навыков XXI века

Современные образовательные программы все чаще ориентируются на развитие навыков критического мышления, креативности и сотрудничества. ИИ может помочь в этом, предлагая интерактивные задания и симуляции, которые способствуют развитию этих навыков в процессе обучения. Например, виртуальные лаборатории и симуляторы позволяют студентам проводить эксперименты в безопасной среде, развивая практические навыки.

Будущее образования с ИИ

С развитием технологий можно ожидать появления новых форматов обучения, таких как смешанное обучение (blended learning), где традиционные методы сочетаются с онлайн-обучением и использованием ИИ. Важно продолжать исследовать возможности ИИ в образовании, чтобы максимально эффективно использовать его потенциал для улучшения учебного процесса и подготовки студентов к вызовам современного мира.

Поддержка студентов с особыми потребностями

ИИ может сыграть важную роль в поддержке студентов с особыми потребностями. Технологии распознавания речи, текстовые преобразователи и другие инструменты могут помочь учащимся с ограниченными возможностями более эффективно участвовать в учебном процессе. Например, программы, использующие ИИ для перевода текста в речь, могут значительно облегчить обучение для студентов с нарушениями слуха или зрения.

Геймификация обучения

Геймификация — это использование игровых элементов в образовательном процессе для повышения мотивации и вовлеченности студентов. ИИ может помочь в создании адаптивных игровых сценариев, которые учитывают прогресс учащихся и предлагают соответствующие уровни сложности. Платформы, такие как Kahoot! и Quizizz, используют элементы геймификации для создания интерактивных викторин и опросов, что делает процесс обучения более увлекательным.

Подготовка к будущим профессиям

С учетом быстрого развития технологий и изменения рынка труда, образование должно готовить студентов к новым профессиям и навыкам. ИИ может помочь в разработке курсов, которые соответствуют требованиям современного рынка труда. Например, программы по программированию и анализу данных могут быть адаптированы с помощью ИИ для обеспечения актуальности содержания.

Вызовы и риски

Несмотря на множество преимуществ, использование ИИ в образовании также связано с определенными вызовами:

- **Этика и конфиденциальность:** Сбор и анализ данных о студентах могут вызывать опасения относительно конфиденциальности. Важно обеспечить защиту личной информации учащихся и использовать данные этично.
- **Неравенство доступа:** Не все студенты имеют равный доступ к технологиям и интернету. Это может усугубить существующие социальные и экономические различия в образовании.
- **Зависимость от технологий:** Слишком сильная зависимость от ИИ может привести к снижению критического мышления и навыков самостоятельного обучения у студентов.
- **Качество контента:** Не все образовательные ресурсы на основе ИИ могут быть высокого качества. Важно тщательно оценивать и выбирать платформы и материалы.

Заключение

ИИ имеет огромный потенциал для трансформации образования, делая его более доступным, персонализированным и эффективным. Однако необходимо учитывать как преимущества, так и вызовы, связанные с его внедрением. Чтобы обеспечить успешную интеграцию ИИ в образовательный процесс, важно развивать этические практики использования технологий, обеспечивать равный доступ ко всем ресурсам и поддерживать баланс между традиционными методами обучения и инновациями.

1. «Homo Roboticus? Люди и машины в поисках взаимопонимания» Джона Маркроффа.
2. «Искусственный интеллект. Современный подход» Стюарта Рассела и Питера Норвига.
3. «Как создать разум: секрет человеческого мышления раскрыт» Рэя Курцвейла.
4. «Глубокое обучение в картинках. Визуальный гид по искусственному интеллекту» Джона Крона, Гранта Бейлевельда и Аглаэ Бассенс.

РАЗДЕЛ XXIII. НАНОТЕХНОЛОГИИ

Мукминова И.Р.

Функциональная отделка текстиля с использованием полиэлектролитов

Уфимский государственный нефтяной технический университет

(Россия, Уфа)

doi: 10.18411/trnio-10-2024-420

Аннотация

Синтетические полиэлектролиты, благодаря своим уникальным свойствам, таким как растворимость в воде, электростатическое взаимодействие и высокая стабильность, находят широкое применение для функциональной отделки текстильных материалов. В статье также рассматриваются перспективы развития применения различных методов синтетических полиэлектролитов.

Ключевые слова: полиэлектролиты, текстильная отделка, послойная самосборка, функциональные свойства, водоотталкивающие покрытия, антибактериальные покрытия, текстильные материалы.

Abstract

Synthetic polyelectrolytes, due to their unique properties such as solubility in water, electrostatic interaction and high stability, are widely used for functional finishing of textile materials. The article also discusses the prospects for the development and application of various methods of synthetic polyelectrolytes.

Keywords: polyelectrolytes, textile finishing, layered self-assembly, functional properties, water-repellent coatings, antibacterial coatings, textile materials.

Синтетические полиэлектролиты — это полимеры, содержащие заряженные группы, которые могут диссоциировать в водных растворах, создавая заряженные макромолекулы. Эти материалы привлекают значительное внимание благодаря своим уникальным свойствам, включая способность к ионному обмену, адсорбции на поверхностях и взаимодействию с другими заряженными молекулами. В текстильной промышленности синтетические полиэлектролиты находят применение в процессах отделки текстильных материалов, улучшая их функциональные характеристики и повышая долговечность.

Полиэлектролиты делятся на два основных типа: катионные и анионные, в зависимости от заряда ионогенных групп. Каждый тип полиэлектролитов обладает специфическими свойствами, что определяет их возможное применение в различных процессах отделки текстиля. Синтетические полиэлектролиты представляют собой полимеры, в молекулах которых имеются ионогенные группы, способные диссоциировать на ионы в растворах. Эти полимеры включают в себя разнообразные группы веществ, как в природе (белки, пектины, полисахариды), так и в синтетическом виде. С их помощью можно влиять на различные физические и химические свойства материалов. Одним из важных свойств синтетических полиэлектролитов является их способность образовывать пленки на поверхности текстильных материалов, которые могут изменять их характеристики. Например, нанесение полиэлектролитных покрытий позволяет создать водоотталкивающие эффекты на текстиле, делая его устойчивым к воде. Также полиэлектролиты хорошо растворимы в воде и демонстрируют высокую ионную проводимость, что делает их полезными для процессов электропроводимости текстильных материалов. Это свойство особенно важно для антистатической обработки и разработки проводящих текстильных материалов.

Полиэлектролиты могут обмениваться ионами с окружающей средой, что делает их эффективными в процессах модификации поверхностных свойств текстиля. Этот аспект

полезен при нанесении антимикробных покрытий или улучшении гидрофобных свойств материалов. В растворах полиэлектролиты демонстрируют сложные реологические свойства, включая зависимость вязкости от концентрации и степени ионизации. Эти свойства позволяют их использовать для управления вязкостью растворов при нанесении отделочных составов на текстиль.

Итак, катионные полиэлектролиты используются для улучшения антистатических свойств текстильных материалов, что немаловажно для синтетических волокон, которые склонны накапливать статическое электричество. Их применение помогает снизить уровень статического заряда и предотвратить налипание пыли и мелких частиц на ткани. Синтетические полиэлектролиты, обладающие анионными группами, активно применяются для создания водоотталкивающих покрытий на текстильных материалах. Эти покрытия позволяют улучшить устойчивость тканей к воздействию влаги, что особенно важно для одежды и технических тканей.

Для применения синтетических полиэлектролитов в текстильной отделке необходимо разработать эффективные методы нанесения и модификации. Один из перспективных методов - метод послойной самосборки, который обеспечивает равномерное распределение полиэлектролитов на поверхности материала.

Метод послойной самосборки (Layer-by-Layer, LbL) основан на электростатическом взаимодействии между заряженными молекулами полиэлектролитов и поверхностью текстильного материала. Этот процесс использует последовательное нанесение слоев полиэлектролитов с противоположными зарядами, чтобы обеспечивать равномерное распределение и прочное закрепление на поверхности, при этом толщина наносимого слоя может быть точно контролируется, что позволяет регулировать свойства конечного продукта. Также послойная самосборка позволяет комбинировать различные полиэлектролиты, придавая текстильным материалам множество полезных свойств, таких как водоотталкивающие, антибактериальные и антистатические свойства.

Итак, данный метод используется для нанесения антибактериальных покрытий, которые предотвращают рост микроорганизмов на поверхности тканей, а также для создания водоотталкивающих и грязеотталкивающих покрытий.

Второй метод – это метод микрокапсулирование, позволяющий нанести активные ингредиенты, такие как косметические или фармацевтические вещества, на поверхность текстильных материалов с целью их контролируемого высвобождения при контакте с кожей. Этот процесс открывает широкие возможности для создания функциональных текстильных изделий, которые могут предоставлять различные полезные эффекты, включая увлажнение, антивозрастное воздействие, ароматерапию и другие терапевтические свойства.

Микрокапсулы представляют собой маленькие структуры, в которых активные ингредиенты заключены в оболочку. Механизм высвобождения этих веществ может регулироваться свойствами оболочки, а также внешними факторами, такими как трение, давление, изменение температуры, диффузия или растворение оболочки.

Метод коацервации является одним из наиболее популярных в текстильной промышленности. В его основе лежит взаимодействие катионных и анионных полимеров в водных растворах, которое приводит к образованию коацервата — материала, формирующего оболочку микрокапсул. В процессе коацервации активные ингредиенты заключаются в микрокапсулы, которые затем наносятся на текстильный материал.

Ключевое преимущество метода коацервации заключается в его универсальности — он позволяет эффективно контролировать размеры микрокапсул и скорость высвобождения активных веществ, что делает его подходящим для применения в различных областях, от медицины до косметики.

Современные исследования в области синтетических полиэлектролитов открывают новые возможности для их использования в текстильной промышленности. Увеличение экологической осведомленности и тенденции к устойчивому производству стимулируют разработку биоразлагаемых полиэлектролитов, которые могут быть использованы для создания

экологически чистых отделочных составов. Кроме того, продолжаются разработки полиэлектролитов с улучшенными свойствами, такими как усиленные антимикробные и гидрофобные эффекты, что расширяет спектр их применения в текстильной продукции.

Таким образом, синтетические полиэлектролиты обладают множеством уникальных свойств, которые делают их эффективными и универсальными материалами для отделки текстильных изделий. Их применение открывает перспективы для разработки высокофункциональных текстильных материалов с улучшенными эксплуатационными характеристиками. Интенсивные исследования в этой области позволяют надеяться на дальнейшее расширение их использования и совершенствование процессов обработки текстиля.

1. Бост Ф., Кросетто Г. Инновационный текстиль и активные материал.
2. Кирсанова Е.А. Материаловедение (дизайн костюма) [Текст] / Е.А. Кирсанова, Ю.С. Шустов, А.В. Куличенко [и др.]. - М.: ИНФРА-М 2013. - 395 с.
3. Киреев В.В. Высокомолекулярные соединения. М.: Высш. шк., 1992. 511 с.
4. Кукин Г.Н. Текстильное материаловедение (волокна и нити) Г.Н. Кукин, А.Н. Соловьев, А.И. Кобляков. - М.: Легпромбытиздат 1989. - 352 с.



LJournal

Научно-издательский центр

Рецензируемый научный журнал

**ТЕНДЕНЦИИ РАЗВИТИЯ НАУКИ И ОБРАЗОВАНИЯ
№114, Октябрь 2024**

Часть 9

Подписано в печать 25.10.2024. Тираж 400 экз.
Формат.60x841/16. Объем уч.-изд. л.10,36
Отпечатано в типографии Научный центр «LJournal»
Главный редактор: Иванов Владислав Вячеславович