ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

3
2024

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

1.1.6. Computational Mathematics (physical and mathematical sciences)

2.3.6. Information security methods and systems, information security (technical science)

2.3.8. Informatics and information processes (technical science)

Objectives and areas of research

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047
e-mail: grnat@rambler.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

1.1.6. Вычислительная математика (физико-математические науки)

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

2.3.8. Информатика и информационные процессы (технические науки)

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика», публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

Электронный адрес: grnat@rambler.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

Н.В. Гришина, кандидат технических наук, доцент,
Российский государственный гуманитарный университет (РГГУ)

CONTENTS

СОДЕРЖАНИЕ

УДК 629.7:004
DOI: 10.28995/ 2686-679X-2024-3-8-23

Повышение устойчивости системы управления роем беспилотных летательных аппаратов

Иван А. Глазырин
Российский государственный гуманитарный университет, Москва, Россия, ivan@helimed.ru

Аннотация. В статье рассматривается проблема обеспечения устойчивости процесса управления роем беспилотных летательных аппаратов в условиях воздействия комплекса дестабилизирующих факторов. В современном мире наблюдается переход к групповому использованию роботов – беспилотных летательных аппаратов. Указанная тенденция имеет место в различных сферах: поиск туристов в труднодоступных районах, мониторинг технического состояния нефтепроводов, разведка местности и обнаружение лесных пожаров, поражение военных объектов вероятного противника и др. В ходе исследования установлено, что современным требованиям к вероятности выполнения полетного задания в наибольшей степени отвечают системы управления роем летательных аппаратов, построенные по принципу децентрализации управления. При этом с ростом сложности решаемых задач возрастает потребность в разработке прикладных методов и средств, направленных на стабилизацию характеристик системы управления. Одним из перспективных направлений повышения устойчивости децентрализованной системы управления роем роботов является реализация технологии блокчейн, которая позволяет обеспечить надежный информационный обмен между отдельными летательными аппаратами в составе роя. В статье проведен анализ потенциальных возможностей и технических особенностей применения блокчейн-технологии при разработке современных систем управления роем роботов. Определены технические трудности использования блокчейн-технологии, и показаны возможные пути их преодоления.

Ключевые слова: беспилотный летательный аппарат, рой летательных аппаратов, децентрализованное управление, информационное взаимодействие, деструктивные воздействия, устойчивость управления, технология блокчейн

Для цитирования: Глазырин И.А. Повышение устойчивости системы управления роем беспилотных летательных аппаратов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 8–23. DOI: 10.28995/ 2686-679X-2024-3-8-23

Increasing the stability of the swarm control system for unmanned aerial vehicles

Ivan A. Glazyrin
Russian State University for the Humanities, Moscow, Russia,
ivan@helimed.ru

Abstract. The article considers an issue of ensuring the stability of the process of controlling a swarm of unmanned aerial vehicles under the impact of the destabilizing factors complex. In the modern world, there is a transition to the group use of robots – unmanned aerial vehicles. Such a trend takes place in various areas: searching for tourists in hard-to-reach areas, monitoring the technical condition of oil pipelines, reconnaissance of terrain and detection of forest fires, defeating military targets of a potential enemy, etc. The study found that it is the swarm control systems built on the principle of decentralized control that to the greatest extent meet modern requirements for the probability of completing a flight mission. At the same time, with the increasing complexity of the problems being solved, the need for the development of applied methods and tools aimed at stabilizing the characteristics of the control system increases. One of the promising areas for increasing the stability of a decentralized system for controlling a swarm of robots is the use of blockchain technology, which allows for reliable information exchange between individual aircraft in the swarm. The article analyzes the potential capabilities and technical features of using blockchain technology in the development of modern robot swarm control systems. The technical difficulties of using blockchain technology are identified and possible ways to overcome them are shown.

Keywords: unmanned aerial vehicle, swarm of aircraft, decentralized control, information interaction, destructive influences, stability control, blockchain technology

For citation: Glazyrin, I.A. (2024), "Increasing the stability of the control system for a swarm of unmanned aerial vehicles", *RSUH/RGGU Bulletin. "Computer science. Information security. Mathematics" Series,* no. 3, pp. 8–23, DOI: 10.28995/ 2686-679X-2024-3-8-23

Введение

В последние годы беспилотные летательные аппараты (БПЛА) стали незаменимым средством во многих предметных областях, включая аграрный сектор, промышленность, военное применение и использование при ликвидации последствий чрезвычайных ситуаций. По мере расширения функциональности и увеличения количества задействованных дронов возрастают требования к надежности, безопасности и устойчивости автоматизированных систем управления [Доброквашина 2024]. Традиционные технические решения в рамках концепции централизованного подхода к обработке траекторных данных и к управлению роем БПЛА становятся малоэффективными из-за проблем, связанных с задержками в передаче данных и низкой защищенностью радиолиний командного управления от средств радиоэлектронного подавления [Иванов, Афонин, Макаренко 2022]. Групповое применение БПЛА для решения специальных тактических задач (разведка местности, выявление и поражение объектов противника и др.) накладывает дополнительные требования на характеристики системы управления, которая в реальных условиях подвергается воздействию дестабилизирующих факторов различной физической природы [Гордиенко, Полянин, 2018]. В частности, система управления роем БПЛА для гарантированного выполнения полетного задания должна обладать необходимой устойчивостью к радиоэлектронному противодействию со стороны вероятного противника. Среди существующих технических направлений обеспечения устойчивости процесса управления особый интерес представляет технология блокчейн [Носиров, Фомичев 2021], которая способна обеспечивать децентрализацию управления БПЛА, а также повышенную безопасность и надежность обмена данными.

Целью статьи является анализ сущности и потенциала технологии блокчейн и особенностей ее интеграции в состав децентрализованной системы управления роем БПЛА в интересах повышения ее устойчивости к воздействию окружающей среды.

Дадим характеристику понятия «устойчивость управления». В современной теории управления понятие «устойчивость» имеет строгую математическую интерпретацию и зависит от типа системы управления и режима ее функционирования [Попов, Бесекерский 2003]. В общем случае устойчивость понимается как комплексное свойство некоторой динамической системы сохранять в условиях воздействия неблагоприятных факторов на приемлемом уровне свои системные характеристики. Для

анализа устойчивости нелинейных систем управления динамическими объектами используют специальные аналитические и вычислительные методы[1]. Проблема устойчивости управления роем БПЛА непрерывно актуализируется в силу непрерывного диалектического развития средств поражения на базе БПЛА и средств радиоэлектронной защиты критически важных наземных объектов [Иванов, Афонин, Макаренко 2022].

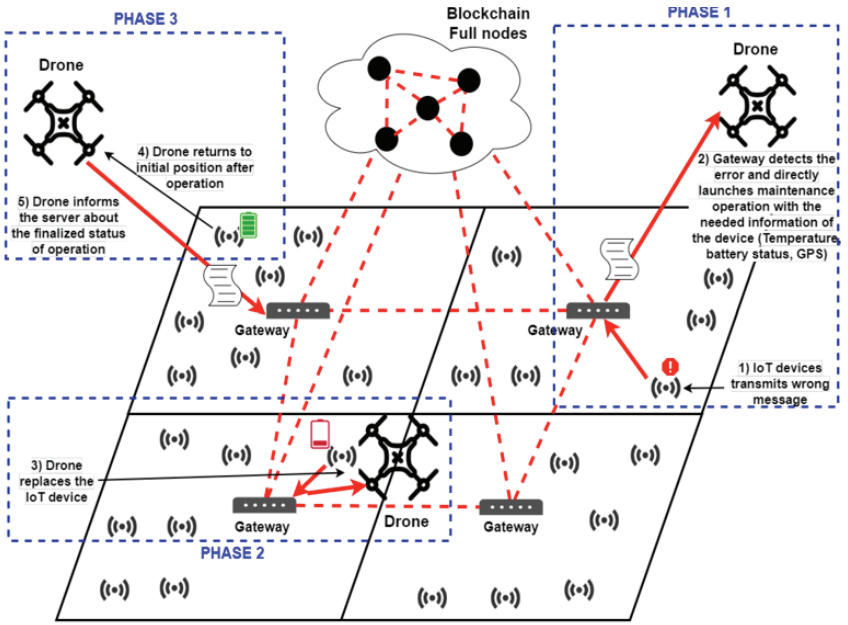

Рис. 1. Схема децентрализованной системы управления группой БПЛА (вариант)

На рис. 1 показана схема, отражающая один из вариантов реализации принципа децентрализованного управления роем БПЛА [Евдокименков, Красильщиков, Себряков 2016].

[1] *Толмачев А.А., Прохоров М.А., Андрианов А.С.* Определение категории устойчивости для распределенных автоматизированных систем управления // Космические аппараты и технологии. 2018. № 1 (23). URL: https://cyberleninka.ru/article/n/opredelenie-kategorii-ustoychivosti-dlya-raspredelennyh-avtomatizirovannyh-sistem-upravleniya (дата обращения 31.05.2024).

В условиях радиоэлектронного противодействия наиболее уязвимыми элементами в децентрализованной системе управления (ДСУ) являются компоненты бортовых систем дронов, участвующих в процессе обмена данными. Покажем, что применение блокчейн-технологии позволяет принципиально изменить механизм и условия протекания этого информационного процесса. Рассмотрим также теоретические и практические аспекты интеграции блокчейна в ДСУ роем БПЛА. Основное внимание уделим анализу таких ключевых аспектов, как устойчивость блокчейн-систем к внешним атакам, возможности автоматизации процессов управления с использованием смарт-контрактов, а также вопросам масштабируемости и производительности технологии в контексте ее применения в беспилотной авиации.

1. Обзор блокчейн-технологии

Блокчейн (от англ. *blockchain* – «цепочка блоков») в классическом варианте представляет собой технологию шифрования и хранения данных (реестра), которая позволяет сохранять и передавать данные в виде последовательности связанных блоков. При этом каждый блок содержит информацию и ссылку на предыдущий – вместе они образуют цепочку. Так данные в блокчейне защищены от изменений и фальсификации. В сети блокчейн множество участников, которые сотрудничают между собой для обработки и подтверждения операций. Каждый узел активно участвует в проверке и добавлении новых блоков с этими операциями.

Техническую реализацию принципов блокчейн можно рассматривать как распределенную информационную сеть, в которой участники информационного процесса получают возможность контролировать и верифицировать транзакции без использования центрального регулирующего органа. Защита данных с помощью криптографии и привязка каждой транзакции к предыдущей обеспечивают высокую степень информационной защиты и поддерживают устойчивость данных к изменениям и взломам.

Блокчейн, первоначально разработанный как технологическая основа для криптовалют, таких как Bitcoin, сегодня находит применение в областях, где требуется надежная регистрация и верификация транзакций без участия центральных посредников. Как показали прикладные исследования, применение блокчейн-технологии в системах управления БПЛА может значительно переформатировать эту область, предоставляя методы и инструментальные средства для повышения устойчивости, управления

данными и выполнения оперативных задач с высокой степенью автономности и безопасности[2].

Выделим основные свойства блокчейн-технологии, полезные для управления БПЛА:

– децентрализация: управление объектами не зависит от централизованного контрольного центра, что существенно уменьшает риски, связанные с единой точкой отказа;
– безопасность данных: блокчейн предлагает расширенные возможности для защиты данных, включая надежные процедуры шифрования и комплексные протоколы аутентификации;
– прозрачность и отслеживаемость: все операции документируются и могут быть проверены любым участником сети, что обеспечивает прозрачность всех действий;
– создание защищенного канала связи на основе блокчейн-технологии “Ethereum”.

“Ethereum” представляет собой платформу для создания децентрализованных онлайн-сервисов на базе блокчейна, используя смарт-контракты; эти контракты автоматически выполняются в блокчейн-сети, обеспечивая высокий уровень безопасности и исполнения условий контракта без участия третьих сторон.

Дополнительно отметим, что применение “Ethereum” в контуре управления роем БПЛА может значительно повысить безопасность данных, так как все команды управления и данные с датчиков БПЛА могут быть записаны в блокчейн в зашифрованном виде, обеспечивая их надежное хранение и защиту от несанкционированного доступа.

По данным проведенных исследований, введение технологии блокчейн в архитектуру ДСУ БПЛА не только позволяет повысить ее устойчивость к внешним и внутренним возмущениям, но и открывает новые возможности для улучшения таких системных характеристик, как наблюдаемость и управляемость.

2. Технологические основы блокчейн-технологии

В общем случае блокчейн можно представить как распределенный цифровой реестр, который сохраняет все транзакции или данные в виде последовательных блоков. К основным принципам

[2] *Бурлаков Д.О.* Блокчейн для децентрализованных дронов, структура и предлагаемые решения для борьбы с COVID-19 // Современные научные исследования и инновации. 2023. № 2. URL: https://web.snauka.ru/issues/2023/02/99421 (дата обращения 21.05.2024).

работы блокчейн-технологии следует отнести: криптографию, консенсус и децентрализацию.

Криптография. Блокчейн использует криптографию для защиты. Каждый блок данных содержит уникальный хеш предыдущего блока, создавая цепочку, которую невозможно изменить без изменения всех последующих блоков, что требует значительных вычислительных ресурсов и согласия сети. Эта технология также использует криптографические подписи для подтверждения подлинности транзакций[3].

Консенсус. Для поддержания согласованности данных между всеми участниками сети, блокчейн использует механизмы консенсуса. Примерами реализации могут служить Proof of Work (PoW) в Bitcoin и Proof of Stake (PoS) в "Ethereum". Эти механизмы обеспечивают единство данных в децентрализованной сети и предотвращают двойные затраты[4].

Децентрализация. Блокчейн-технология не предусматривает введение центрального управляющего органа – сеть полностью децентрализована. Это делает систему более устойчивой к атакам и сбоям, поскольку не существует единой точки отказа. Управление и обслуживание сети осуществляется через автоматизированные алгоритмы и совместное участие всех узлов сети[5].

В процессе анализа выявлены сильные и слабые стороны блокчейн-технологии в контексте управления БПЛА.

Достоинства блокчейн проявляются в следующем [Носиров, Фомичев 2021]:

- улучшенная безопасность: благодаря использованию криптографии и технологии хеш блокчейн обеспечивает высокую степень защиты данных; неизменность механизма блокчейна помогает предотвратить мошенничество и несанкционированный доступ[6];
- прозрачность и аудит: все транзакции записываются в блокчейн, доступный для проверки всем участникам сети, что обеспечивает прозрачность и возможность проведения аудита.

---

[3] Bitcoin – Open source P2P money. URL: https://bitcoin.org/bitcoin.pdf (дата обращения 21.05.2024).

[4] *Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S.* Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton, NJ: Princeton University Press, 2016.

[5] *Swan M.* Blockchain: Blueprint for a New Economy. Sebastopol: O'Reilly Media, Inc., 2015.

[6] *Antonopoulos A.M., Wood G.* Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol: O'Reilly Media, Inc. 2018.

Это особенно важно для БПЛА, используемых в критических приложениях, где требуется точная отслеживаемость операций[7].

Выделим основные недостатки:

– одной из главных проблем блокчейна является его ограниченная масштабируемость, особенно в публичных блокчейнах, таких как Bitcoin; проблемы с пропускной способностью и время обработки транзакций могут быть значительными, что ставит под вопрос применимость этой технологии для управления большим количеством БПЛА[8];
– технологии консенсуса (например: Proof of Work), используемые во многих блокчейнах, требуют значительных вычислительных ресурсов, что приводит к большому энергопотреблению. Это вызывает опасения с точки зрения увеличения стоимости.

3. Применение блокчейна в управлении БПЛА

Возможны различные варианты применения блокчейна в управлении БПЛА, в том числе: координация действий группы дронов, обеспечение безопасности данных при информационном обмене, аутентификация команд целеуказания и управления.

Переход к использованию блокчейн-технологии может радикально изменить подходы к управлению БПЛА, обеспечивая при этом высокую степень безопасности, автономности и надежности. Выделим несколько ключевых сценариев его применения.

Координация множественных аппаратов. В операциях с использованием нескольких БПЛА блокчейн может помочь автоматизировать процессы синхронизации и координации между аппаратами. Благодаря принципу децентрализации блокчейн позволяет дронам работать в единой сети без необходимости постоянного подключения к центральному серверу, что существенно уменьшает время реакции и повышает эффективность выполнения тактических задач.

---

[7] *Tapscott D., Tapscott A.* Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. New York: Penguin, 2016.

[8] *Croman K.* et al. On Scaling Decentralized Blockchains // 3rd Workshop on Bitcoin and Blockchain Research, Christ Church, Barbados. Berlin; New York: Springer, 2016. P. 106–125.

Обеспечение безопасности данных. Блокчейн обеспечивает высокую степень защиты данных, собираемых отдельными БПЛА, от несанкционированного доступа. Данные, записанные с помощью механизма блокчейн, защищены криптографией, и изменить их практически невозможно. Это критически важно для миссий наблюдения и разведки, где безопасность и целостность информации являются наибольшими приоритетами.

Аутентификация команд и управление доступом. Использование блокчейна может значительно повысить уровень безопасности управляющих команд, отправляемых ведущими (в группе) БПЛА. Смарт-контракты могут быть использованы для верификации и выполнения команд в реальном времени, обеспечивая следующую политику: только авторизованные пользователи могут управлять дронами или получать доступ к собранной информации.

Опираясь на доступные источники информации, приведем показательные примеры успешного использования блокчейн-технологии в системах управления БПЛА.

Логистика и доставка. Один из пилотных проектов, реализованный компанией Walmart в сотрудничестве с IBM, использует блокчейн для управления логистическими операциями. В этом проекте блокчейн применялся для отслеживания поставок, где каждый БПЛА выполнял роль независимого участника блокчейн-сети, что обеспечивало прозрачность и неизменность записей о перемещении грузов[9].

Мониторинг и обследование. В Австралии рассматривается использование БПЛА с блокчейном для мониторинга состояния инфраструктуры (например, дорог и мостов). БПЛА автоматически выполняют съемку, данные с которой записываются в блокчейн, гарантируя их подлинность и позволяя инженерам точно определять время и место выявления проблем[10].

---

[9] *McSweeney K.* Walmart's drone delivery plan includes blockchain tech // ZDNET, 30 May, 2017. URL: https://www.zdnet.com/article/walmarts-drone-delivery-plan-includes-blockchain-tech/#google_vignette (дата обращения 21.05.2024).

[10] Enhancing infrastructure monitoring in Australia: exploring drone-based autonomous inspection using AI // Infrastructure Magazine. URL: https://infrastructuremagazine.com.au/2023/09/05/enhancing-infrastructure-monitoring-in-australia-exploring-drone-based-autonomous-inspection-using-ai/ (дата обращения 24.05.2024).

4. Вызовы и ограничения

Интеграция блокчейн-технологий в системы управления БПЛА может столкнуться с рядом технических и операционных препятствий. Выделим некоторые из них.

Сложность интеграции. Внедрение блокчейна в существующие системы управления БПЛА требует значительных изменений в архитектуре и может вызвать проблемы совместимости. Процесс интеграции может быть сложным и дорогостоящим, особенно в системах, где уже используются устоявшиеся протоколы коммуникации и данные защищены по стандартам, не предусматривающим использование блокчейна[11].

Проблемы с обновлением данных. В системах управления БПЛА, где обновление данных происходит часто и требуется мгновенная реакция, блокчейн может вносить задержки из-за времени, необходимого для выполнения криптографических операций и достижения консенсуса. Это может быть критическим для миссий с высокими требованиями к скорости реагирования[12].

Потребление ресурсов. Блокчейн, особенно в реализациях с доказательством выполнения работы (Proof of Work), требует значительных вычислительных ресурсов, что может быть нецелесообразно для устройств с ограниченной вычислительной мощностью, таких как многие типовые БПЛА[13].

Масштабируемость и производительность. Масштабируемость является одной из основных технических проблем, с которой сталкиваются блокчейн-системы, особенно в контексте группового управления БПЛА.

Ограничения масштабируемости. Традиционные блокчейн-сети, такие как Bitcoin, страдают от ограниченной пропускной способности транзакций и высокой латентности. Для систем БПЛА, которые могут генерировать большое количество данных, такое ограничение может стать критическим. Решения, основан-

---

[11] Hyperledger Architecture. 2017. Volume 1. URL: https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/Hyperledger_Arch_WG_Paper_1_Consensus.pdf (дата обращения 21.05.2024).

[12] Blockchain-Enhanced UAV Networks for Post-Disaster Communication: A Decentralized Flocking Approach // arXiv. URL: https://ar5iv.labs.arxiv.org/html/2403.04796v1 (дата обращения 24.05.2024).

[13] *Gervais A. et al.* On the security and performance of proof of work blockchains // Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. New York: ACM, 2016. P. 3–16.

ные на блокчейне, должны быть способны обрабатывать тысячи транзакций в секунду для эффективного функционирования[14].

Производительность сети. Достижение необходимого уровня производительности сети, при котором время подтверждения транзакций минимально, является еще одной проблемой. Разработки, такие как блокчейн-технологии второго поколения (например, Ethereum) и предложения по масштабированию сети (например, Lightning Network), предлагают улучшения, но все еще требуют доработок для использования в критичных по времени системах[15].

Таким образом, необходимы дальнейшие исследования и разработки в области оптимизации блокчейн-технологий для их эффективного применения в системах управления группами БПЛА. Улучшение масштабируемости и производительности, а также минимизация задержек и ресурсоемкости – ключевые задачи, которые необходимо решить для широкого внедрения блокчейн-технологий в данной области.

5. Перспективные разработки

Новейшие исследования и разработки в области использования блокчейн-технологий для управления БПЛА открывают широкие возможности для повышения эффективности, безопасности и автономности этих систем[16]. Выделим наиболее перспективные инновации.

Создание защищенного канала связи на основе блокчейна "Ethereum". Этот инновационный подход объединяет преимущества децентрализованной блокчейн-технологии и автоматизированное управление дронами. Использование блокчейна "Ethereum" позволяет создать надежный и безопасный канал для передачи управляющих команд между оператором и БПЛА, обеспечивая целостность и неизменность передаваемых данных, а также высокий уровень защиты от несанкционированных вмешательств.

Децентрализованное управление полетами. Исследователи изучают возможности использования блокчейна для создания децен-

---

[14] *Croman K.* et al. On Scaling Decentralized Blockchains.

[15] *Poon J., Dryja T.* The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 2016. URL: https://lightning.network/lightning-network-paper.pdf (дата обращения 21.05.2024).

[16] *Бурлаков Д.О.* Блокчейн для децентрализованных дронов...

трализованных платформ управления полетами БПЛА, которые могут обеспечивать синхронизацию и координацию множества устройств без необходимости центрального контроля.

Усовершенствованные протоколы безопасности. Разработка блокчейн-базированных протоколов, которые могут автоматически обнаружить и нейтрализовать угрозы безопасности в реальном времени, является одним из наиболее перспективных направлений.

Интеграция с другими технологиями. Интеграция блокчейна с другими передовыми технологиями, такими как искусственный интеллект (ИИ), машинное обучение (ML) и Интернет вещей (IoT), открывает новые горизонты для создания умных и автономных систем управления БПЛА. Результатом развития и интеграции передовых технологий в составе системы управления БПЛА в ближайшей перспективе может стать создание высокоэффективной интеллектуальной системы управления роем БПЛА [Евдокименков, Красильщиков, Себряков 2016].

Блокчейн и ИИ/ML. Сочетание блокчейна с ИИ и машинным обучением позволяет создавать системы, которые могут самостоятельно анализировать собранные данные, оптимизировать маршруты полета и принимать решения на основе анализа больших объемов данных. ИИ может использоваться для анализа данных с БПЛА, записанных в блокчейн, для выявления аномалий или оптимизации параметров полета. Примером может служить система управления трафиком БПЛА, разработанная IBM, которая использует ИИ для обработки данных, получаемых от множества БПЛА и хранящихся в блокчейне IBM[17].

Блокчейн и IoT. Интеграция блокчейна с IoT-устройствами в БПЛА обеспечивает новый уровень безопасности и автономии. IoT-устройства, такие как датчики и камеры, могут автоматически регистрировать все события в блокчейне, что обеспечивает неизменность и проверяемость данных. Это особенно важно в приложениях, где требуется строгая отчетность и прозрачность, например в агросекторе или при мониторинге окружающей среды[18].

---

[17] How Blockchain and AI Can Work Together // Blockchain Council. URL: https://www.blockchain-council.org/blockchain/how-blockchain-and-ai-can-work-together/ (дата обращения 24.05.2024).

[18] *Reyna A.,* et al. On blockchain and its integration with IoT. Challenges and opportunities // Future Generation Computer Systems. 2018. Vol. 88 (3). P. 173–190.

6. Перспективные направления исследования

1. *Глубокое изучение интеграционных возможностей*: необходимо более детально исследовать технические аспекты интеграции блокчейна с существующими системами управления БПЛА, особенно в контексте совместимости с традиционными авиационными коммуникационными стандартами.

2. *Масштабируемость блокчейн-систем:* важным направлением исследований является разработка масштабируемых блокчейн-решений, способных эффективно обрабатывать большие объемы данных и транзакций, которые характерны для сетей БПЛА.

3. *Улучшение энергоэффективности:* требуются исследования по снижению энергопотребления блокчейн-алгоритмов, чтобы их можно было эффективно применять в портативных и мобильных устройствах, установленных на БПЛА, особенно в контексте использования методов консенсуса, менее требовательных к вычислительным ресурсам, чем Proof of Work.

4. *Безопасность и приватность данных:* необходимо продолжить работу над улучшением механизмов защиты данных в блокчейне, особенно в контексте обеспечения приватности данных при их обработке и хранении в децентрализованной сети.

5. *Практические испытания и демонстрационные проекты:* реализация пилотных проектов для тестирования блокчейн-управляемых БПЛА в различных условиях и сценариях, чтобы оценить их эффективность, устойчивость и возможные ограничения в реальных операционных условиях.

6. *Юридические и регуляторные аспекты:* важно учитывать регуляторные требования и стандарты, которые необходимо разработать и утвердить для обеспечения законности и безопасности эксплуатации блокчейн-интегрированных систем БПЛА.

Заключение

Анализ состояния и особенностей применения блокчейн-технологий в системах группового управления БПЛА выявил значительный потенциал этой инновации для повышения безопасности, устойчивости и автономности операций. Блокчейн способствует децентрализации процессов управления, улучшает защиту данных и оптимизирует координацию действий множества БПЛА. Эти преимущества особенно актуальны в контексте растущего использования БПЛА в коммерческих, гражданских и военных приложениях. Принципы криптографии и консенсуса,

лежащие в основе блокчейна, обеспечивают высокую степень защиты и надежности сетей БПЛА, делая их устойчивыми к внешним вмешательствам и техническим сбоям. Интеграция блокчейна с передовыми технологиями (ИИ, машинное обучение и IoT) открывает новые горизонты для создания интеллектуальных систем управления, которые могут самостоятельно адаптироваться к изменяющимся условиям и оптимизировать свою работу в реальном времени.

Исследования и разработки в области внедрения блокчейн-технологий в сферу управления БПЛА могут значительно повысить эффективность и безопасность использования БПЛА, сделав их незаменимым инструментом во многих отраслях и направлениях деятельности. Блокчейн обладает значительным технологическим потенциалом, позволяющим не только улучшить качество и обеспечить устойчивость процесса группового управления БПЛА, но и радикально трансформировать традиционные методы их применения.

Благодарности

Работа выполнена в рамках проекта РГГУ «Информационно-аналитическая система для автоматизированного управления роем беспилотных летательных аппаратов специального назначения» (конкурс «Студенческие проектные научные коллективы РГГУ»).

Acknowledgements

The work is carried out under the RSUH project “Information analytic system for automated swarm control of special purpose unmanned aerial vehicles” (competition “Student design research teams of RSUH”).

Литература

Гордиенко, Полянин 2018 – *Гордиенко В.С., Полянин К.С.* Система управления группой беспилотных летательных аппаратов // Наука без границ. 2018. № 1 (18). С. 44-47.

Доброквашина 2024 – *Доброквашина А.С.* К вопросу разработки графических интерфейсов для управления БЛА // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 8–20. DOI: 10.28995/2686-679X-2024-1-8-20.

Евдокименков, Красильщиков, Себряков 2016 – *Евдокименков В.Н., Красильщиков М.Н., Себряков Г.Г.* Распределенная интеллектуальная система управления группой беспилотных летательных аппаратов: архитектура и программно-математическое обеспечение // Известия ЮФУ. Технические науки. 2016. № 1 (174). С. 29–44.

Иванов 2019 – *Иванов Д.Я.* Исследование полимодельного комплекса системы планирования движения гетерогенной группы автономных роботов в условиях пространственно-ситуационной неопределенности // Робототехника и техническая кибернетика. Т. 7. № 4. СПб.: ЦНИИ РТК, 2019. С. 300–305.

Носиров, Фомичев 2021 – *Носиров З.А., Фомичев В.М.* Анализ блокчейн-технологии: основы архитектуры, Примеры использования, перспективы развития, проблемы и недостатки // Системы управления, связи и безопасности. 2021. № 2. С. 37–75. DOI: 10.24412/2410-9916-2021-2-37-75.

Иванов, Афонин, Макаренко 2022 – *Иванов М.С., Афонин И.Е., Макаренко С.И.* Повышение устойчивости автоматизированной системы управления комплекса с беспилотными летательными аппаратами в условиях воздействия средств физического поражения и радиоэлектронного подавления // Системы управления, связи и безопасности. 2022. № 2. С. 92–134. DOI: 10.24412/2410-9916-2022-2-92-134.

Попов, Бесекерский 2003 – *Попов Е.П., Бесекерский В.А.* Теория систем автоматического управления. СПб.: Профессия, 2003. 752 с.

References

Gordienko, V.S. and Polyanin, K.S. (2018), “Control system for a group of unmanned aerial vehicles”, *Science without borders*, vol. 1 (18), pp. 44–47.

Dobrokvashina, A.S. (2024), “On the issue of developing graphical interfaces for controlling UAVs”, *Bulletin of the Russian State University for the Humanities. Series “Informatics. Information Security. Mathematics”,* vol. 1, pp. 8–20.

Evdokimenkov, V.N., Krasilshchikov, M.N. and Sebryakov, G.G. (2016), “Distributed intelligent control system for a group of unmanned aerial vehicles. Architecture and software”, *Izvestia of the Southern Federal University. Technical science*, vol. 1 (174), pp. 29–44.

Ivanov, D.Ya. (2019), “Study of a polymodel complex of a motion planning system for a heterogeneous group of autonomous robots in conditions of spatial and situational uncertainty”, *Robotics and technical cybernetics*, vol. 7, no. 4., RTC, St. Petersburg, Russia, pp. 300–305.

Nosirov, Z.A. and Fomichev, V.M. (2021), “Analysis of blockchain technology. Fundamentals of architecture, examples of use, development prospects, challenges and shortcomings”, *Control, communication and security systems*, no. 2, pp. 37–75.

Ivanov, M.S., Afonin, I.E. and Makarenko, S.I. (2022), “Increasing the stability of the automated control system of a complex with unmanned aerial vehicles under the

influence of means of physical damage and radio-electronic suppression", *Control systems, communications and safety*, no. 2, pp. 92–134.

Popov, E.P. and Besekerskii, V.A. (2003), *Teoriya sistem avtomaticheskogo upravleniya* [Theory of automatic control systems], Professiya, St. Petersburg, Russia.

Информация об авторе

Иван А. Глазырин, магистрант, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; ivan@helimed.ru

Information about the author

Ivan A. Glazyrin, master student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, 125047, Russia; ivan@helimed.ru

УДК 005:517
DOI: 10.28995/ 2686-679X-2024-3-24-38

Решение задачи прогнозирования объема продаж на маркетплейсах на основе применения методов и инструментов анализа временных рядов

Людмила Ю. Савельева
Московский государственный институт международных отношений (университет) МИД Российской Федерации, Москва, Россия, saveleva@odin.mgimo.ru

Дарья Н. Стоева
Московский государственный институт международных отношений (университет) МИД Российской Федерации, Москва, Россия, decestoeva@gmail.com

Аннотация. Статья посвящена решению задачи прогнозирования объема продаж на маркетплейсах на основе применения методов и инструментов анализа временных рядов. Представлен подробный анализ методов и инструментов анализа временных рядов в контексте прогнозирования объема продаж. Рассмотрены различные подходы к анализу временных рядов, включая статистические методы, машинное обучение и глубокое обучение. В статье подробно описывается применение таких методов, как ARIMA, GARCH для прогнозирования объема продаж на маркетплейсах. Обсуждаются особенности данных маркетплейсов и их влияние на выбор методов анализа временных рядов. Особое внимание уделяется выбору признаков и оценке качества моделей прогнозирования. Статья содержит результаты экспериментов, проведенных на реальных данных маркетплейса, а также сравнение различных методов анализа временных рядов в контексте прогнозирования объема продаж. В заключение авторы делают выводы о преимуществах и недостатках различных подходов и предлагают рекомендации по выбору методов анализа временных рядов для решения задачи прогнозирования объема продаж на маркетплейсах. В контексте маркетплейсов рассматривается множественная регрессия для анализа и прогнозирования различных экономических показателей, связанных с их деятельностью. Исследована взаимосвязь между объемом продаж, ценами на товары, рекламными расходами и другими факторами, влияющими на доходность. Выявлены основные факторы, влияющие на успешность бизнеса на электронной площадке, и определены, какие из

них имеют наибольшее значение. При анализе данных о маркетинговых активностях, ценах на товары и лояльности клиентов с помощью множественной регрессии можно определить, какие факторы наиболее сильно влияют на доходность, и на основе полученных данных разработать эффективные стратегии для повышения прибыльности. При анализе данных с маркетплейса могут существовать внешние переменные, такие как экономические условия или изменения в законодательстве, которые могут влиять на доходность, но не связаны напрямую с рассматриваемыми независимыми переменными. Методы и инструменты анализа временных рядов позволяют учесть эти факторы и определить истинное влияние независимых переменных на зависимые переменные.

Ключевые слова: временные ряды, анализ экономических показателей, прогнозирование экономических показателей, независимых переменных, зависимые переменные

Для цитирования: Савельева Л.Ю., Стоева Д.Н. Решение задачи прогнозирования объема продаж на маркетплейсах на основе применения методов и инструментов анализа временных рядов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 24–38. DOI: 10.28995/ 2686-679X-2024-3-24-38

Solving the issue of forecasting sales volume on marketplaces based on the use of time series analysis methods and tools

Lyudmila Yu. Savel'eva
MGIMO University, Moscow, Russia, saveleva@odin.mgimo.ru

Dar'ya N. Stoeva
MGIMO University, Moscow, Russia, decestoeva@gmail.com

Abstract. The article deals with solving the problem of forecasting sales volume on marketplaces based on the use of time series analysis methods and tools. It presents a detailed analysis of time series analysis methods and tools in the context of sales volume forecasting. and considers various approaches to time series analysis, including statistical methods, machine learning and deep learning. The article also describes in detail the use of methods such as ARIMA, GARCH to predict sales volume on marketplaces. The features of these marketplaces and their impact on the choice of time series analysis methods are discussed. Special attention is paid to the selection of features and assessment of the quality of forecasting models. The article reports the results of experiments conducted on real marketplace data, as well as a comparison of various time

series analysis methods in the context of sales volume forecasting. Summarizing, the authors draw conclusions about the advantages and disadvantages of various approaches and offer recommendations on the choice of time series analysis methods to solve the problem of forecasting sales volume on marketplaces. In the context of marketplaces, multiple regression is considered to analyze and predict various economic indicators related to their activities. The relationship between sales volume, product prices, advertising costs and other factors affecting profitability is studied. The main factors influencing the success of a business on an electronic platform are identified and which of them are of the greatest importance. When analyzing data on marketing activities, product prices and customer loyalty, using multiple regression, it is possible to determine which factors most strongly affect profitability and, based on the data obtained, develop effective strategies to increase its yield. When analyzing data from the marketplace, there may be external variables, such as economic conditions or changes in legislation, that may affect profitability, but are not directly related to the independent variables under consideration. Time series analysis methods and tools allow for those factors to be taken into account and thus to determine the true impact of independent variables on dependent variables.

Keywords: time series, analysis of economic indicators, forecasting of economic indicators, independent variables, dependent variables

For citation: Savel'eva, L.Yu. and Stoeva, D.N. (2024), "Solving the issue of forecasting sales volume on marketplaces based on the use of time series analysis methods and tools", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 24–38, DOI: 10.28995/2686-679X-2024-3-24-38

Введение

Множественная регрессия является мощным и широко используемым статистическим методом, который находит свое применение в различных областях, включая экономику и производство. Этот метод позволяет анализировать взаимосвязь между одной зависимой переменной и несколькими независимыми переменными, исследуя их влияние на зависимую переменную и предсказывая значения этой переменной на основе значений независимых переменных.

В экономике множественная регрессия является неотъемлемым инструментом для анализа и прогнозирования процессов, связанных с производством, распределением ресурсов и принятием экономических решений. Этот метод позволяет исследовать взаимосвязь между различными экономическими переменными и

выявлять основные факторы, влияющие на успешность бизнеса, эффективность производственных процессов или динамику экономического роста [Althoff 2021].

В статье [Armstrong 1992] рассматриваются методы моделирования временных рядов ARIMA (Autoregressive Integrated Moving Average) и GARCH (Generalized Autoregressive Conditional Heteroskedasticity). Временные ряды широко используются в финансовых и экономических прогнозах, а также в других областях, где требуется анализ и прогнозирование последовательностей данных.

В работе [Bhargava 2016] приведен обзор основных концепций и методов ARIMA и GARCH. Рассмотрены шаги и процедуры для подготовки данных, оценки параметров моделей и обучения моделей на исходных временных рядах. Также проведено моделирование методов прогнозирования с использованием ARIMA и GARCH моделей.

Проведено сравнение эффективности и точности прогнозирования ARIMA и GARCH моделей на реальных временных рядах. В работе [Gardner 1990] рассмотрены различные метрики для оценки качества прогнозов.

Статья представляет полезный обзор методов моделей ARIMA и GARCH и их применение в анализе и прогнозировании временных рядов.

Полученные результаты и выводы могут быть полезны для исследователей и практиков, занимающихся анализом временных рядов и финансовым прогнозированием. Важным новшеством является, что эти методы применяются для экономического анализа различных показателей при торговле на маркетплейсах.

Программная реализация моделей множественной регрессии

ARIMA – это модель, которая учитывает автокорреляцию (зависимость от предыдущих значений) и скользящую среднюю (сглаживание шума) во временных рядах. Она широко применяется для моделирования различных типов временных рядов, включая как стационарные, так и нестационарные.

GARCH – это модель, которая специально разработана для моделирования условной гетероскедастичности во временных рядах. Условная гетероскедастичность предполагает изменяющуюся с течением времени дисперсию ошибок. Модель GARCH особенно полезна для анализа финансовых временных рядов, которые часто характеризуются высокой волатильностью.

ARIMA и GARCH – это две из наиболее распространенных временных рядов моделей, используемых для анализа и прогнозирования финансовых временных рядов, представленные в работе [Heineman 2021]. Они оба имеют свои достоинства и точность в прогнозировании, которые приведены в табл. 1.

Таблица 1

Достоинства и точность в прогнозировании моделей

	Модель ARIMA	**Модель GARCH**
Достоинства	Относительно простая модель, которая не требует сложных математических или статистических знаний для понимания и применения	Модель разработана специально для моделирования условной гетероскедастичности во временных рядах, то есть изменяющейся с течением времени дисперсии ошибок
	Модель может быть применена к широкому спектру временных рядов, включая как стационарные, так и нестационарные временные ряды; она может быть адаптирована к различным типам данных, включая ежедневные, еженедельные или ежемесячные данные	Модель предоставляет информацию о будущей волатильности и оценке риска для данного временного ряда; такая информация может быть ценной для принятия решений, связанных с портфелем, управлением рисками и другими задачами, требующими оценки неопределенности
	Модель учитывает как автокорреляцию (зависимость от предыдущих значений), так и скользящую среднюю (сглаживание шума); это позволяет модели учесть взаимосвязи между прошлыми значениями ряда и будущими значениями	Позволяет моделировать различные варианты условной гетероскедастичности, что делает ее гибкой для адаптации к особенностям конкретного временного ряда

Важно отметить, что прогнозирование финансовых временных рядов является сложной задачей, и определение наиболее точной модели может требовать экспериментов и анализа различных моделей и подходов. Рекомендуется проводить тщательный анализ данных и использовать совокупность разных моделей для достижения наилучших результатов прогнозирования. Кроме того, у этих методов имеются и недостатки, которые сведены в табл. 2

Таблица 2

Недостатки моделей

	Модель ARIMA	**Модель GARCH**
Недостатки	Временной ряд должен быть стационарным или стационарно сделанным; если ряд не является стационарным, требуется выполнить преобразования, такие как разности, чтобы сделать его стационарным; это может усложнить процесс моделирования и прогнозирования	Модель моделирует условную гетероскедастичность, т. е. изменяющуюся с течением времени дисперсию ошибок; однако она ограничена в своей способности улавливать стохастическую волатильность, которая является основным элементом реальных финансовых временных рядов
	Модель имеет несколько параметров, таких как порядки авторегрессии (p), разностей (d) и скользящей средней (q); выбор оптимальных значений этих параметров может быть сложным и требует экспертного анализа или использования алгоритмов оптимизации	Модель имеет несколько параметров, таких как порядки авторегрессии (p) и скользящей средней (q) для условной дисперсии; выбор оптимальных значений этих параметров может быть сложным и требует экспериментов или использования алгоритмов оптимизации
	Модель учитывает только зависимость от предыдущих значений ряда, игнорируя другие важные факторы или внешние воздействия; это может быть недостатком в случае, если влияние других переменных на ряд является значимым	Модель предполагает линейную зависимость между условной дисперсией и предыдущими ошибками; это может быть недостатком в случае, если во временном ряде имеются нелинейные зависимости или асимметрия волатильности

В целом модели ARIMA и GARCH имеют ряд ограничений и предположений, которые могут ограничить их применимость в некоторых случаях. Поэтому перед выбором модели необходимо тщательно проанализировать данные и учесть их особенности.

В работе [Lutz 2019] для программной реализации модели, основанной на множественной регрессии при реализации товаров через маркетплейсы, требуется выполнить следующие шаги.

1. Собрать данные, необходимые для построения модели. Набор данных должен включать зависимую переменную (объем продаж) и независимые переменные (цены на товары, рекламные расходы и другое).

2. Провести предварительный анализ данных для их проверки на наличие пропущенных значений, выбросов, а также других аномалий [Hyndman 2006].

3. Разделить данные на обучающую и тестовую выборки. Это позволит проверить эффективность модели на независимых данных. Если независимые переменные имеют разные диапазоны значений, может потребоваться их масштабирование для более стабильной работы модели [Smith 1989].

4. Для построения модели множественной регрессии используем функции и библиотеки машинного обучения, задаем зависимую переменную и независимые переменные, а проводим обучение модели.

5. Оцениванием качество модели после обучения. Рассчитываем метрики оценки, такие как среднеквадратичная ошибка (MSE) или коэффициент детерминации, для определения точности модели на тестовых данных [Thompson 1990].

6. Сравнение прогнозных значений с реальными значениями в тестовых данных позволит оценить точность модели и ее пригодность для дальнейшего использования. Если модель не удовлетворяет требованиям или не дает достаточно точных прогнозов, можно произвести доработку модели. Это может включать в себя добавление новых независимых переменных.

После достижения удовлетворительных результатов можно использовать модель для прогнозирования продаж товаров через маркетплейсы. Модель поможет определить оптимальные цены, эффективные маркетинговые стратегии и другие факторы, которые могут повлиять на доходность маркетплейса.

Первой моделью, которую реализовали, была модель авторегрессии скользящего среднего (ARIMA). Модель Бокса–Дженкинса предполагает, что временной ряд содержит три составляющие: авторегресионную, интегрированную и скользящее среднее, которые в модели обозначены p, d и q [Wang 2010]:

– величина p называется порядком авторегрессии. Она позволяет ответить на вопрос, будет ли очередной элемент ряда близок к значению X, если к нему были близки p предыдущих значений;
– величину d называют порядком интегрирования. Она показывает, насколько элемент ряда близок по значению к d предыдущим значениям, если разность между ними минимальна;
– параметр q – порядок скользящего среднего. Позволяет установить погрешность модели как линейную комбинацию наблюдавшихся ранее значений ошибок.

Модель ARIMA (*p, d, q*), где *p*, *d* и *q* – целые неотрицательные числа, характеризующие порядок для частей модели.

Для временного ряда *X(t)* модель может быть записана в виде:

$$(\Delta^d X_t) = \sum_{t=1}^{p} a_t \left(\Delta^d X_{t-1}\right) + \varepsilon_t + \sum_{j=1}^{q} b_j \left(\Delta^d \varepsilon_{t-j}\right),$$

где Δ^d – оператор разности порядка *d* (последовательное взятие *d* раз разностей первого порядка – сначала от самого ряда, затем от полученных разностей первого порядка, затем от второго порядка и т. д.);

$a(t)$ – коэффициенты авторегрессионной части модели, $\varepsilon(t)$ – значения ошибки (полагаются независимыми одинаково распределенными случайными величинами из нормального распределения с нулевым средним);

b_j – коэффициенты скользящего среднего.

Ниже приведен фрагмент кода для построения модели ARIMA для прогноза продаж на маркетплейсах.

```
    import pandas as pd
    import numpy as np
    import statsmodels.api as sm
# Загрузка данных о продажах
    sales_data = pd.read_csv('sales_data.csv')
# Преобразование данных во временной ряд
    date_index = pd.to_datetime(sales_data['date'])
    sales_ts = pd.Series(sales_data['sales'], index=date_index)
# Разделение на обучающий и тестовый наборы
    train_data = sales_ts[:'2021-01-20']
    test_data = sales_ts['2022-02-20':]
# Построение модели ARIMA
    model = sm.tsa.ARIMA(train_data, order=(1, 0, 1))
    model_fit = model.fit(disp=0)
# Прогнозирование на тестовом наборе
    forecast = model_fit.get_forecast(steps=len(test_data))
    forecast_mean = forecast.predicted_mean
    forecast_conf_int = forecast.conf_int()
# Визуализация прогнозов
    plt.figure(figsize=(10, 6))
    plt.plot(train_data, label='Обучающий набор')
    plt.plot(test_data, label='Фактические значения')
    plt.plot(forecast_mean, label='Прогноз')
    plt.fill_between(forecast_conf_int.index,
        forecast_conf_int.iloc[:, 0],
        forecast_conf_int.iloc[:, 1], color='gray', alpha=0.2)
```

```
plt.xlabel('Дата')
plt.ylabel('Продажи')
plt.title('Прогноз продаж с помощью модели ARIMA')
plt.legend()
plt.show()
```

Используем библиотеку statsmodels для построения модели ARIMA. Сначала загружаем данные о продажах из файла sales_data.csv и преобразуем их во временной ряд с помощью индекса даты. Затем разделяем данные на обучающий и тестовый наборы.

Строим модель ARIMA с параметрами order = (1, 0, 1), означает, что используем авторегрессионную компоненту порядка 1 без разностей и скользящего среднего порядка 1. Затем обучаем модель на обучающем наборе данных.

После обучения модели прогнозируем значения на тестовом наборе с помощью метода get_forecast. Получаем прогнозируемые значения (forecast_mean) и интервалы прогноза (forecast_conf_int), которые позволяют нам оценить неопределенность прогноза. Далее визуализируем обучающий набор, фактические значения и прогнозы на графике (рис. 1).

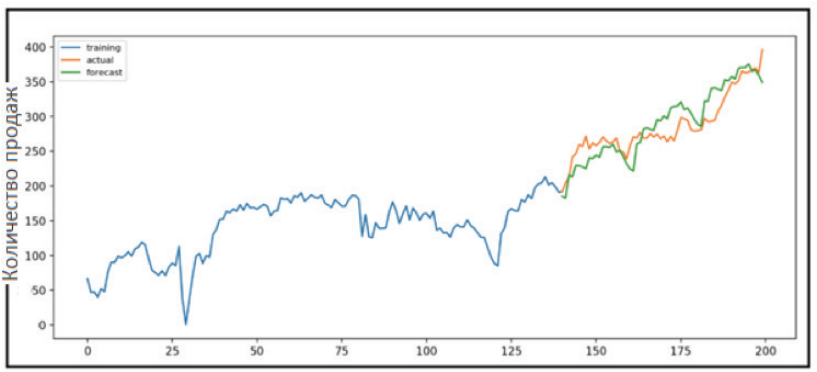

Рис. 1. Модель авторегрессионного интегрированного скользящего среднего (ARIMA)

Вторая реализованная модель используется для прогнозирования ситуации на финансовых рынках в условиях волатильности. Когда ситуация на финансовых рынках нестабильна и характеризуется высокой изменчивостью значений различных показателей (курсов валют, комиссии за продажу на маркетплейсах, базовые

тарифы на хранение товаров, стоимость логистики по складам и т. д.), имеет место изменчивость дисперсии на различных интервалах наблюдения, т. е. гетероскедастичность. В таких условиях обычные линейные регрессионные модели оказываются слишком грубыми [Xie 2015].

В основе ARCH-модели (Autoregressive Conditional Heteroscedastic model) используется условная, зависимая от времени дисперсия, выражаемая через квадрат значений показателей прошлых периодов:

$$\sigma^2(t) = a + \sum_{i=1}^{a} b_i \, r_{t-1}^2,$$

где a – коэффициент задержки (лага), или базовая волатильность. ARCH-модель моделирует волатильность в виде суммы константной базовой волатильности и линейной функции абсолютных значений нескольких последних изменений цен [Пономарёв 2023].

В ходе эволюции появилась GARCH-модель (Generalized Auto-regressive Conditional Heteroscedastic model) – обобщенная авторегрессионная модель гетероскедастичности, которая предполагает, что на текущую изменчивость дисперсии влияют как предыдущие изменения показателей, так и предыдущие оценки дисперсии (так называемые старые новости). Согласно данной модели (GARCH(p, q)), расчет дисперсии производится по следующей формуле:

$$\sigma^2(t) = a + \sum_{i=1}^{a} b_i \, r_{t-1}^2 + \sum_{i=1}^{p} c_i \, \sigma_{t-1}^2,$$

где p – количество предшествующих оценок, влияющих на текущее значение, c – весовые коэффициенты, отражающие степень влияния предыдущих оценок на текущие значения.

Рассмотрим реализацию авторегрессионной модели GARCH для прогнозирования продаж товаров через маркетплейсы на алгоритмическом языке Python:

```
    import pandas as pd
    import numpy as np
    import arch
# Загрузка данных о продажах
    sales_data = pd.read_csv('sales_data.csv')
```

```
# Преобразование данных во временной ряд
    date_index = pd.to_datetime(sales_data['date'])
    sales_ts = pd.Series(sales_data['sales'], index=date_index)
# Разделение на обучающий и тестовый наборы
    train_data = sales_ts[:'2023-12-31']
    test_data = sales_ts['2024-01-01':]
# Построение модели GARCH
    model = arch.arch_model(train_data, vol='Garch', p=1, q=1)
    model_fit = model.fit()
# Прогнозирование на тестовом наборе
    forecast = model_fit.forecast(start='2024-01-01', horizon=len(test_data))
# Визуализация прогнозов
    plt.figure(figsize=(10, 6))
    plt.plot(train_data, label='Обучающий набор')
    plt.plot(test_data, label='Фактические значения')
    plt.plot(forecast.mean['2024-01-01':], label='Прогноз среднего')
    plt.fill_between(forecast.mean['2024-01-01':].index,
        forecast.mean['h.1']['2024-01-01':],
        forecast.mean['h.1']['2024-01-01':], color='gray', alpha=0.2)
    plt.xlabel('Дата')
    plt.ylabel('Продажи')
    plt.title('Прогноз продаж с помощью авторегрессионной модели
    GARCH')
    plt.legend()
    plt.show()
```

Используем библиотеку arch для построения модели GARCH. Сначала загружаем данные о продажах из файла sales_data.csv и преобразуем их во временной ряд с помощью индекса даты. Затем разделяем данные на обучающий и тестовый наборы.

Строим модель GARCH с параметрами vol = 'Garch', p = 1, q = 1, что означает, что используем модель GARCH с одним авторегрессионным и одним скользящим средним параметром. Затем обучаем модель на обучающем наборе данных.

После обучения модели прогнозируем значения на тестовом наборе с помощью метода forecast. Получаем прогноз среднего значения, а также доверительный интервал. Затем визуализируем прогнозы на графике с фактическими значениями продаж.

Для сравнения двух моделей произвели наложение графиков прогнозов и получили следующий результат, который представлен на рис. 2.

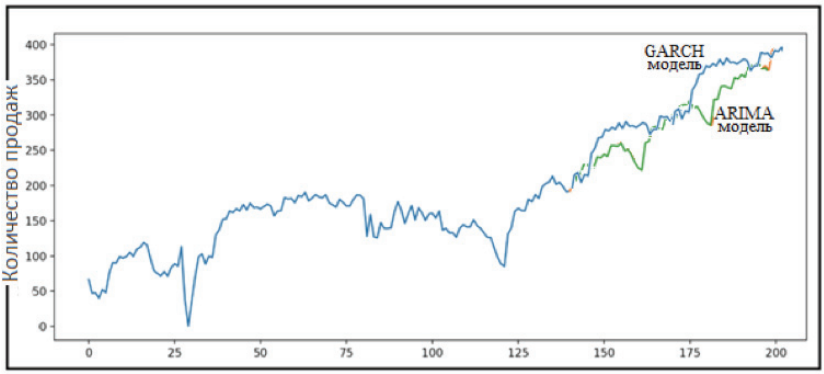

Рис. 2. Сравнение моделей ARIMA и GARCH на тестовой модели

Из сравнения двух моделей ARIMA и GARCH при прогнозировании количества продаж на маркетплейсах видно, что точность расчета прогноза лежит в пределах 7% от среднего количества продаж. Точность сильно зависит от количества внешних факторов, которые закладываются в модели при расчете. Чем больше параметров удается привлечь для прогнозирования, тем выше точность моделирования. Однако реальная экономическая ситуация имеет свойство постоянно меняться. К примеру, обновления на торговой площадке Wildberries происходят по несколько раз в день, а смена внутренних алгоритмов в различных областях платформы (рекламная, витринная, кластерная и т. д.) корректирует внешние условия и переменные со стороны платформы.

Заключение

Методы ARIMA и GARCH являются широко применяемыми инструментами в задачах прогнозирования торговли на маркетплейсах. Известные методы основаны на анализе временных рядов и могут быть эффективны при обоснованном их применении.

ARIMA-модель состоит из трех компонентов: авторегрессионной (AR), интегрированной (I) и скользящего среднего (MA). Она может быть полезна для прогнозирования ценовых изменений на маркетплейсах, особенно в случае, когда прошлые значения ряда могут влиять на будущие значения.

С другой стороны, метод GARCH широко используется для моделирования условной волатильности во временных рядах. Он позволяет учесть наличие гетероскедастичности, то есть изменяющейся во времени вариации, в данных. GARCH-модель подходит для прогнозирования краткосрочной волатильности торговых активов, что позволяет оценивать уровень риска и принимать соответствующие решения на маркетплейсах.

Каждый из этих методов имеет свои преимущества и ограничения. ARIMA моделирует тренды и сезонность, но может недооценивать условную волатильность. GARCH учитывает условную волатильность, но может не улавливать нелинейности и тренды. Поэтому эффективность применения ARIMA и GARCH может зависеть от конкретных данных и целей прогнозирования.

Указанные методы не являются единственными возможными для прогнозирования торговли на маркетплейсах. Существуют и другие альтернативы, включая машинное обучение и нейронные сети. Поэтому выбор конкретного метода должен быть основан на анализе конкретной задачи и доступных данных.

В целом ARIMA и GARCH могут быть полезными инструментами для прогнозирования торговли на маркетплейсах. Они позволяют учесть статистические свойства временных рядов и помогают прогнозировать будущие ценовые изменения и волатильность. Для достижения наилучших результатов необходимо тщательно настраивать параметры моделей и учитывать особенности конкретного рынка.

Литература

Пономарёв 2023 – *Пономарёв Д.С., Горохов М.М., Пономарёв С.Б.* Обработка форм статистической отчетности Федеральной службы исполнения наказаний на основе методов разведочного анализа данных библиотек языков “Python” и “R” // Вестник Воронежского института ФСИН России. 2023. № 2. С. 106–112.

Althoff 2021 – *Althoff C.* The Self-Taught Computer Scientist: The Beginner’s Guide to Data Structures & Algorithms. Chichester: John Wiley & Sons, 2021. 224 p.

Armstrong 1992 – *Armstrong J.S., Collopy F.* Error measures for generalizing about forecasting methods: empirical comparisons // International Journal of Forecasting. 1992. Vol. 8. P. 69–80.

Bhargava 2016 – *Bhargava A.* Grokking Algorithms: An illustrated guide for programmers and other curious people. Shelter Island, NY: Manning, 2016. 258 p.

Gardner 1990 – *Gardner E.* Evaluating forecast performance in an inventory control system // Management Science. 1990. Vol. 36. P. 490–499.

Heineman 2021 – *Heineman G.* Learning Algorithms: A Programmer's Guide to Writing Better Code. Sebastopol: O'Reilly Media, 2021. 278 p.

Hyndman 2006 – *Hyndman R., Koehler A.* Another look at measures forecast accuracy // International Journal of Forecasting. 2006. Vol. 22 (4). P. 679–688.

Lutz 2019 – *Lutz M.* Learning Python, 5th ed. Vol. 1 Sebastopol: O'Reilly, 2019. 832 p.

Smith 1989 – *Smith D.* Combination of forecasts in electricity demand prediction // International Journal of Forecasting. 1989. Vol. 8. P. 349–356.

Thompson 1990 – *Thompson P.A.* An MSE statistic for comparing forecast accuracy across series // International Journal of Forecasting. 1990. Vol. 6. P. 219–227.

Wang 2010 – *Wang J., Zhu S., Zhang W., Lu H.* Combined modeling for electric load forecasting with adaptive particle swarm optimization // Energy. 2010. Vol. 35. No. 4. P. 1671–1678.

Xie 2015 – *Xie J., Hong T., Stroud J.* Long-term Retail Energy Forecasting with Consideration of Residential Customer Attrition // IEEE Transactions on Smart Grid. 2015. Vol. 6 (5). P. 2245–2252.

References

Althoff, C. (2021), *The Self-Taught Computer Scientist: The Beginner's Guide to Data Structures & Algorithms*, John Wiley & Sons, Chichester, UK.

Armstrong, J.S. and Collopy, F. (1992), "Error measures for generalizing about forecasting methods: empirical comparisons", *International Journal of Forecasting*, vol. 8, pp. 69–80.

Bhargava, A. (2016), *Grokking Algorithms: An illustrated guide for programmers and other curious people*, Manning, Shelter Island, NY, USA.

Gardner, E. (1990), "Evaluating forecast performance in an inventory control system", *Management Science*, vol. 36, pp. 490–499.

Heineman, G. (2021), *Learning Algorithms: A Programmer's Guide to Writing Better Code*, O'Reilly Media, Sebastopol, USA.

Hyndman, R. and Koehler, A. (2006), "Another look at measures forecast accuracy", *International Journal of Forecasting*, vol. 22 (4), pp. 679–688.

Lutz, M. (2019), *Learning Python*, 5th ed., vol. 1, O'Reilly, Sebastopol, USA, 832 p.

Ponomarev, D.S., Gorokhov, M.M. and Ponomarev, S.B. (2023), "Processing the statistical reporting forms of the Federal Penitentiary Service based on methods of exploratory analysis in data from libraries of languages 'Python' and 'R' ", *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*, no. 2, pp. 106–112.

Smith, D. (1989), "Combination of forecasts in electricity demand prediction", *International Journal of Forecasting*, vol. 8, pp. 349–356.

Thompson, P.A. (1990), "An MSE statistic for comparing forecast accuracy across series", *International Journal of Forecasting*, vol. 6, pp. 219–227.

Wang, J., Zhu, S., Zhang, W. and Lu, H. (2010), "Combined modeling for electric load forecasting with adaptive particle swarm optimization", *Energy*, vol. 35, no. 4, 1671–1678.

Xie, J., Hong, T. and Stroud J. (2015), "Long-term Retail Energy Forecasting with Consideration of Residential Customer Attrition", *IEEE Transactions on Smart Grid,* vol. 6 (5), pp. 2245–2252.

Информация об авторах

Людмила Ю. Савельева, Московский государственный институт международных отношений (университет) МИД Российской Федерации (МГИМО), Одинцово, Московская обл., Россия; 143007, Россия, Московская обл., Одинцово, ул. Ново-Спортивная, д. 3; l.saveleva@odin.mgimo.ru

Дарья Н. Стоева, студент, Московский государственный институт международных отношений (университет) МИД Российской Федерации (МГИМО), Одинцово, Московская обл., Россия; 143007, Россия, Московская обл., Одинцово, ул. Ново-Спортивная, д. 3; decestoeva@gmail.com

Information about the authors

Lyudmila Yu. Savel'eva, MGIMO University, Odintsovo, Moscow region, Russia; 3, Novo-Sportivnaya St., Odintsovo, Moscow region, 143007, Russia; l.saveleva@odin.mgimo.ru

Dar'ya N. Stoeva, student, MGIMO University, Odintsovo, Moscow region, Russia; 3, Novo-Sportivnaya St., Odintsovo, Moscow region, 143007, Russia; decestoeva@gmail.com

УДК 336.71:004.56
DOI: 10.28995/ 2686-679X-2024-3-39-55

Проверка соответствия банковской системы требованиям к защите информации в платежной системе

Полина С. Александрова
Финансовый университет при Правительстве Российской Федерации, Москва, Россия, alekspolya2003@gmail.com

Александра С. Червинчук
Финансовый университет при Правительстве Российской Федерации, Москва, Россия, nuxela@gmail.com

Сергей А. Резниченко
Финансовый университет при Правительстве Российской Федерации, Москва, Россия;
Национальный исследовательский ядерный университет «МИФИ», Москва, Россия;
Российский государственный гуманитарный университет, Москва, Россия, rsa_5@bk.ru

Аннотация. В современном цифровом мире, где информационные технологии становятся все более важными во всех сферах деятельности, обеспечение безопасности информации выходит на передний план. Статья рассматривает особенности проверки соответствия банков и других организаций банковской сферы требованиям к защите информации в платежной системе. Проведение аудита в соответствии с этими требованиями поможет банкам эффективно защитить конфиденциальные данные клиентов, предотвратить кибератаки и обеспечить надежное функционирование своих систем. Целью работы является анализ особенностей проведения аудита информационной безопасности в банковской сфере с учетом требований к защите информации в платежной системе. В статье рассматриваются основные аспекты, такие как применение средств защиты информации, аутентификация, шифрование данных, а также требования к организационным и техническим мерам безопасности. Дается обзор основных положений и рекомендаций по эффективному проведению аудита информационной безопасности с учетом этих требований. Особое

внимание уделяется вопросам безопасности при обработке платежных транзакций, защиты персональных данных клиентов и предотвращения мошеннических операций. Представлен подход к систематизации и классификации мероприятий аудита информационной безопасности, ориентированный на соответствие требованиям проведения аудита в банковской сфере.

Ключевые слова: аудит, информационная безопасность, защита информации, аутентификация, шифрование данных, проверка соответствия, платежная система

Для цитирования: Александрова П.С., Червинчук А.С., Резниченко С.А. Проверка соответствия банковской системы требованиям к защите информации в платежной системе // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 39–55. DOI: 10.28995/ 2686-679X-2024-3-39-55

Checking the compliance of the banking system with the requirements for the protection of information in the payment system

Polina S. Aleksandrova
Financial University under the Government of the Russian Federation, Moscow, Russia; alekspolya2003@gmail.com

Aleksandra S. Chervinchuk
Financial University under the Government of the Russian Federation, Moscow, Russia; nuxela@gmail.com

Sergei A. Reznichenko
Financial University under the Government of the Russian Federation, Moscow, Russia;
National Research Nuclear University "MIFI", Moscow, Russia;
Russian State University for the Humanities, Moscow, Russia, rsa_5@bk.ru

Abstract. In today's digital world, where information technology is becoming increasingly important in all areas of activity, information security is coming to the fore. The article considers the specifics of checking the compliance of banks and other banking organizations with the requirements for information protection in the payment system. Conducting an audit in accordance with these requirements will help banks effectively protect confidential customer data, prevent cyber-attacks and ensure the reliable functioning of their systems. The purpose of the work is to analyze the specifics of conduct-

ing an information security audit in the banking sector, taking into account the requirements for information protection in the payment system. The article reviews the main aspects such as the use of information security tools, authentication, data encryption, as well as requirements for organizational and technical security measures. There is an outline of the main provisions and recommendations for the effective conduct of an information security audit, taking into account these requirements. Special attention is paid to security issues in the processing of payment transactions, the protection of personal data of customers and the prevention of fraudulent transactions. Focusing on compliance with the requirements of auditing in the banking sector the authors present an approach to the systematization and classification of information security audit activities.

Keywords: information security, auditing, authentication, data encryption, verification of compliance, payment system

For citation: Alexandrova, P.S., Chervinchuk, A.S. and Reznichenko, S.A. (2024), "Checking the compliance of the banking system with the requirements for the protection of information in the payment system", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 39–55, DOI: 10.28995/ 2686-679X-2024-3-39-55

Введение

В современном мире, где технологические инновации развиваются с невероятной скоростью, информационная безопасность становится ключевым элементом устойчивости и надежности любой финансовой организации. Электронные платежи стали неотъемлемой частью повседневной жизни. Люди используют банковские карты для покупок в магазинах, интернет-банкинг для оплаты счетов и перевода денег, мобильные приложения для пополнения счета телефона. При этом мы ожидаем, что все эти операции будут выполнены быстро, удобно и, самое главное, безопасно. Банковский сектор, который небезосновательно считается одним из наиболее значимых составляющих экономики любой страны, особенно уязвим перед угрозами информационной безопасности. Это обусловлено не только большим объемом обрабатываемых персональных данных и финансовой информации, но и высоким уровнем доверия, которое должно поддерживаться между банком и его клиентами. Нарушение информационной безопасности в банковской сфере может привести не только к финансовым потерям, но и к утрате репутации, что куда более разрушительно в долгосрочной перспективе [Кочаева, Йоллыев 2024; Гришина 2022].

Высокий риск угроз обусловливает необходимость проведения аудита для заблаговременного предотвращения возможных угроз. Для защиты от этих угроз необходимо, чтобы банковская система соответствовала требованиям к защите информации в платежной системе. Проверка соответствия банковской системы этим требованиям является важной задачей как для банковских специалистов, так и для аудиторов. Эта проверка позволяет выявить слабые места в системе безопасности и принять меры для их устранения, а также подтвердить, что банк соответствует международным и национальным стандартам в области безопасности платежей. В данной работе будет рассмотрено проведение проверки соответствия банковской системы требованиям к защите информации в платежной системе с точки зрения обеспечения защиты конфиденциальной информации и предотвращения угроз для финансовой системы, а также проверка выполнения данных требований в ходе аудита информационной безопасности.

Основная часть

Платежная система представляет собой комплекс организационных и технических средств, предназначенных для осуществления платежных операций. Она включает в себя банки, платежные терминалы, платежные карты, мобильные приложения и другие средства платежей. Платежная система обеспечивает безопасность и надежность платежей, а также предотвращает мошенничество и отмывание денег. Банковская система представляет собой систему кредитно-финансовых учреждений, которые предоставляют различные финансовые услуги, такие как прием вкладов, выдача кредитов, обмен валюты и т. д. Банки являются ключевыми участниками платежной системы, так как они обеспечивают обработку и передачу денежных средств между клиентами. Платежные и банковские системы тесно связаны друг с другом и взаимодействуют на различных уровнях. Например, банки используют платежные системы для обработки транзакций своих клиентов, а платежные системы используют банковские счета для хранения и передачи денежных средств. Обеспечение безопасности платежных и банковских систем является важной задачей, так как они подвержены различным угрозам, таким как мошенничество, кража персональных данных, хакерские атаки и т. д. Для защиты от этих угроз необходимо, чтобы платежные и банковские системы соответствовали требованиям к защите информации и использовали современные средства и технологии защиты. Для обеспечения

полноценного и безопасного функционирования банковских организаций им необходимо проводить аудит информационной безопасности, который будет оценивать соответствие требованиям основных нормативных правовых документов, регулирующих защиту информации в банковском секторе[1].

Анализ нормативной базы аудита на соответствие банковской системы требованиям к защите информации показал, что существует множество международных и национальных стандартов. Основными из них являются PCI DSS[2], ISO 27001[3], PA-DSS[4]. PCI DSS (Payment Card Industry Data Security Standard) – это международный стандарт безопасности, разработанный для защиты данных платежных карт. Он содержит 12 требований, которые должны выполняться всеми участниками платежного процесса. ISO 27001 (Information technology – Security techniques – Information security management systems – Requirements) – это международный стандарт, который определяет требования к системам управления безопасностью информации. PA-DSS (Payment Application Data Security Standard) – это международный стандарт безопасности, разработанный для защиты данных платежных приложений. Он содержит требования, которые должны выполняться разработчиками и поставщиками платежных приложений. В Российской Федерации помимо международных практик широко внедряются национальные стандарты и Положения Банка России. К наиболее известным можно отнести ГОСТ Р ИСО/МЭК 27001-2021[5], ПНСТ 799-2022[6], Положение № 802-П Банка России[7] и др. Ежегодно появляются все

---

[1] *Кобец Д.А., Музалевский Ф.А.* Что делать Банкам по информационной безопасности в 2022 году // RTM GROUP. URL: https://rtmtech.ru/wp-content/uploads/2021/11/CHto-delat-bankam-v-2022-godu-prezentatsiya-RTM-Group.pdf (дата обращения 23.05.2024).

[2] PCI DSS Версия 3.2.1. URL: https://www.pacifica.kz/upload/PCI_DSS_v3-2-1_RU.pdf (дата обращения 23.05.2024).

[3] ISO/IEC 27001:2022 // ISO. URL: https://www.iso.org/standard/27001 (дата обращения 23.05.2024).

[4] PA-DSS– URL: https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf (дата обращения 23.05.2024).

[5] ГОСТ Р ИСО/МЭК 27001-2021. URL: https://docs.cntd.ru/document/1200181890?ysclid=lwm8a219mt415519241 (дата обращения 23.05.2024).

[6] ПНСТ 799-2022. URL: https://docs.cntd.ru/document/1200194122?ysclid=lwm8d85f9r760763124 (дата обращения 23.05.2024).

[7] Положение № 802-П ЦБ РФ // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/405728183.

новые документы, так как информационные технологии постоянно совершенствуются, а значит, необходимы требования, соответствие которым обеспечит их безопасное использование. Национальный стандарт ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» – это национальный стандарт, который соответствует международному стандарту ISO 27001. Предварительный национальный стандарт ПНСТ 799-2022 «Информационные технологии. Криптографическая защита информации. Требования и определения» – это национальный стандарт, который определяет требования к организации и обеспечению безопасности криптографических средств, используемых для защиты информации[8]. Также участники банковской системы вправе устанавливать различные внутренние документы, соответствие которым они также обеспечивают.

Для проверки соответствия организации всем необходимым документам по обеспечению безопасности платежей и защиты информации необходимо проведение аудита информационной безопасности. Аудит информационной безопасности представляет способ контроля уровня защищенности информационных систем организации[9]. Он может быть проведен как внутренними специалистами банка, так и внешними аудиторами. Проверка соответствия состоит из следующих этапов [Синявская, Синявский 2022]:

1. *Подготовка к проверке*. На этом этапе определяется объем и цели проверки, а также разрабатывается план проверки.

2. *Сбор и анализ данных*. На этом этапе проводится сбор и анализ данных о системе защиты информации банка. Для этого могут быть использованы различные методы, такие как интервью с сотрудниками, проверка документации, тестирование системы и т. д.

3. *Оценка соответствия*. На этом этапе проводится аудит по проверке соответствия системы защиты информации банка требованиям к защите информации в платежной системе. Оценка может быть проведена на основе результатов анализа данных, а также на основе международных и национальных стандартов в области безопасности платежей и защиты информации.

---

[8] *Бочкарева Е.А., Вороненко Е.В.* Трансформация финансово-контрольных правоотношений в условиях цифровизации // Право и практика. 2022. URL: https://cyberleninka.ru/article/n/transformatsiya-finansovo-kontrolnyh-pravootnosheniy-v-usloviyah-tsifrovizatsii (дата обращения 23.05.2024).

[9] *Сердюк В.Д.* Аудит информационной безопасности (ИБ) // «ИТ Аналитика». URL: https://bytemag.ru/aydiit-iinformaciionnoji-bezopasnostii-1089//2008 (дата обращения 15.03.2024).

4. *Выводы и рекомендации*. На этом этапе формулируются выводы о соответствии системы защиты информации банка требованиям к защите информации в платежной системе, а также даются рекомендации по устранению выявленных недостатков.

Виды проверок соответствия.

1. Внутренние проверки соответствия – это проверки, которые проводятся специалистами банка для оценки соответствия системы защиты информации внутренним требованиям и стандартам.

2. Внешние проверки соответствия – это проверки, которые проводятся внешними аудиторами для оценки соответствия системы защиты информации банка внешним требованиям и стандартам, таким как законодательство, нормативные акты Центрального банка или международные стандарты.

3. Обязательные проверки соответствия – это проверки, которые проводятся в соответствии с законодательством или нормативными актами Центрального банка.

4. Добровольные проверки соответствия – это проверки, которые проводятся по инициативе банка для оценки соответствия системы защиты информации лучшим практикам и стандартам отрасли.

Большинство документов сходятся в наличии общих требований к защите информации, которые включают в себя:

1. Защита конфиденциальности информации: платежная система должна обеспечивать защиту персональных данных клиентов, информации о счетах, транзакциях и других конфиденциальных данных от несанкционированного доступа, раскрытия, изменения или уничтожения.

2. Целостность информации: платежная система должна обеспечивать целостность информации, то есть гарантировать, что информация не будет изменена или повреждена во время передачи, хранения или обработки.

3. Доступность информации: платежная система должна обеспечивать доступность информации, то есть гарантировать, что информация будет доступна клиентам и сотрудникам банка в любое время, когда это необходимо.

4. Аутентификация и авторизация: платежная система должна обеспечивать аутентификацию и авторизацию клиентов и сотрудников банка, то есть проверять их личность и права доступа к информации и операциям.

5. Защита от мошенничества: платежная система должна обеспечивать защиту от мошенничества, то есть предотвращать несанкционированные или фальшивые транзакции, кражу денег или персональных данных клиентов.

6. Контроль и мониторинг: платежная система должна обеспечивать контроль и мониторинг операций и событий, то есть регистрировать и анализировать все действия, связанные с обработкой платежей, для выявления и предотвращения возможных угроз.

Эти общие требования к безопасности платежей являются основой для разработки и внедрения систем защиты информации в платежной системе. Они также служат критерием для проверки соответствия банковской системы требованиям к защите информации в платежной системе.

В ходе исследования требований нормативной базы было рассмотрено Положение № 802-П Банка России «О требованиях к защите информации в платежной системе Банка России»[10]. Оно содержит требования к тому, как должна быть организована система защиты информации участников платежной системы Банка России. В соответствии с требованиями данного документа аудит информационной безопасности предполагает проверку соблюдения мер защиты информации, предусмотренных уровнем 2 для участников системы быстрых платежей (СБП), включая Организации Управления Информационной Опасностью Системы Быстрых Платежей (ОУИО СБП) и Операторов Платежных Каналов (ОПЦК). Аудитор должен гарантировать соблюдение организациями требований ГОСТ Р 57580.1-2017[11] и эффективное осуществление установленных организационно-технических мер безопасности. В частности, аудит должен включать проверку размещения объектов информационной инфраструктуры в отдельных сегментах сети, применение усиленных мер защиты информации.

Анализ позволил выявить общую структуру аудита информационной безопасности [Симакова 2024]. Аудиторская деятельность начинается с формирования команды аудита. Этот этап критичен, поскольку от компетенций и опыта участников команды напрямую зависит качество и объективность проведения аудита. Команда обычно включает в себя специалистов разного профиля: аудиторов информационной безопасности, IT-специалистов, юристов, специалистов по управлению рисками и, при необходимости, внешних консультантов. Важно, чтобы каждый член команды обладал глубокими знаниями в своей области и понимал специфику работы банковской системы. Подбор команды должен учитывать не только

[10] Положение № 802-П ЦБ РФ // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/405728183 (дата обращения 15.03.2024).

[11] ГОСТ Р 57580.1-2017. URL: https://docs.cntd.ru/document/1200146534 (дата обращения 15.03.2024).

профессиональные качества, но и способность к командной работе и аналитическому мышлению. На следующем этапе команда определяет область и объект аудита. Этот процесс включает в себя установление границ аудита, которыми в рамках данного Положения являются сервисы переводов денежных средств и соответствующая информационная инфраструктура. Разработка плана аудита является заключительным этапом подготовки и одним из наиболее значимых моментов в процессе аудита. План аудита должен быть максимально детализирован и включать в себя цели аудита, перечень проверяемых объектов и процессов, методологию проведения проверок, критерии оценки, а также график работы. Каждый пункт плана должен быть согласован с требованиями рассматриваемого документа. Заключительным этапом разработки плана аудита является его утверждение высшим руководством организации. После утверждения плана проверки команда аудита приступает к работе. В начале аудита информационной безопасности проводится предварительный анализ для общего представления о состоянии информационной безопасности в организации. Далее следует оценка систем управления информационной безопасностью на удовлетворение требованиям соответствующего документа, которые утверждены планом[12]. Информация, собранная на предыдущем этапе, используется для идентификации рисков и возможных угроз и для определения их величины. Завершается аудит проверкой эффективности мер по обеспечению информационной безопасности в организации.

Аудит информационной безопасности включает анализ соответствия внутренних документов участников ССНП, СБП, ОПКЦ и ОУИО СБП в разрезе следующих областей защиты информации, определенных в соответствии с требованиями ГОСТ Р 57580.1-2017[13]:

1. Гарантирование безопасности доступа к информации.
2. Обеспечение защиты компьютерных сетей.
3. Контроль за целостностью и безопасностью информационной инфраструктуры.

---

[12] *Гильманова Э.А., Ахметшина Р.И.* Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры // Форум молодых ученых. 2022. № 2 (66). URL: https://cyberleninka.ru/article/n/rol-audita-informatsionnoy-bezopasnosti-v-zhiznennom-tsikle-sistemy-obespecheniya-informatsionnoy-bezopasnosti-obektov-kriticheskoy DOI: 10.46566/2500-4050_2022_66_34. (дата обращения 15.03.2024).

[13] ГОСТ Р 57580.1-2017. URL: https://docs.cntd.ru/document/1200146534 (дата обращения 15.03.2024).

4. Защита от вредоносного программного обеспечения.
5. Предотвращение утечки информации.
6. Управление инцидентами информационной безопасности.
7. Обеспечение безопасности виртуальной среды.
8. Гарантирование безопасности информации при удаленном доступе[14].

Рассмотрение требований положений Банка России показало, что проверка информационной безопасности включает в себя анализ использования технологических мер безопасности, необходимых для обеспечения целостности и подлинности электронных сообщений на всех этапах их жизненного цикла, включая создание, обработку, передачу и хранение. Также затрагиваются процедуры регулирования в сфере использования криптографической защиты информации (СКЗИ) и управления ключевой информацией в этих средствах[15]. Операторы платежных каналов и организации по управлению информационными рисками быстрых платежных систем обязаны включить в свои внутренние документы описание состава и принципов применения технологических мер безопасности информации. Данные меры необходимы для контроля целостности и подтверждение подлинности передающихся данных, которые нужны для формирования электронных сообщений в процессе осуществления денежных операций с помощью СБП.

Исследование показало, что в процессе обмена электронными сообщениями при осуществлении денежных переводов организационные и технические меры защиты информации должны удовлетворять следующим требованиям:

1. Участники Системы быстрых платежей обязаны предоставлять электронные сообщения от клиентов участников СПС с электронной подписью в момент передачи.

2. Участники СБП и ОПЦК должны обеспечить защиту электронных коммуникаций между ними путем:
- использования усиленной электронной подписи в соответствии с условиями договора оказания услуг между участником СБП и ОПЦК;
- шифрования электронных сообщений на уровне приложений с использованием сертифицированных средств крипто-

[14] Положение № 802-П ЦБ РФ // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/405728183 (дата обращения 15.03.2024).

[15] ВЕСТНИК БАНКА РОССИИ. URL: https://www.cbr.ru/Queries/XsltBlock/File/131643/-1/2344-2345 (дата обращения 15.03.2024).

графической защиты информации в соответствии с ГОСТ Р ИСО/МЭК 7498-1-99[16].

В ходе анализа выявлено, что участники Национальной системы платежных стандартов обязаны обезопасить электронные сообщения при их транспортировке в Банк России в соответствии со следующими шагами:

– создание электронных сообщений и проверка соответствующих реквизитов должны осуществляться в информационной среде участника ССНП в соответствии с установленными нормами;

– применение двойной усиленной подписи, обусловленное необходимостью обеспечения целостности и аутентификации электронных сообщений. Одна подпись применяется при формировании сообщения, а другая – при проверке реквизитов электронного сообщения;

– для дополнительной защиты используется третий метод, предусматривающий применение Электронного Альбома, доступного на официальном веб-сайте Банка России;

– электронные сообщения шифруются на прикладном уровне с применением сертифицированных СКЗИ, успешно прошедших оценку соответствия[17].

Анализируя требования к аудиту банковских систем особое внимание следует уделить использованию средств информационной безопасности, обеспечивающих двустороннюю аутентификацию и шифрование данных на уровне представления или ниже. Средства, используемые на данных уровнях, должны соответствовать эталонной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99[18], и пройти процедуру оценки соответствия установленным требованиям, утвержденным федеральным органом исполнительной власти в области безопасности. Оператор платежного канала (ОПКЦ) в рамках проверки должен выполнить следующие процедуры:

1. ОПКЦ должен идентифицировать транзакции, которые можно считать переводом средств без согласия клиента. Для этого используются модели оценки транзакционного риска, установленные Банком России, а также показатели уровня транзакционного

[16] ГОСТ Р ИСО/МЭК 7498-1-99. URL: https://docs.cntd.ru/document/1200028699 (дата обращения 15.03.2024).

[17] Положение № 802-П ЦБ РФ // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/405728183 (дата обращения 15.03.2024).

[18] ГОСТ Р ИСО/МЭК 7498-1-99. URL: https://docs.cntd.ru/document/1200028699 (дата обращения 15.03.2024).

риска при осуществлении переводов с использованием сервиса быстрых платежей, предоставляемого участниками системы быстрых платежей (СБП).

2. В случае выявления подозрительного перевода денежных средств без согласия клиента ОПЦК незамедлительно приостановит прием к исполнению данного перевода и следующие за этим процедуры.

3. Участники СБП должны быть немедленно уведомлены о выявлении подозрительных операций.

4. Банк России также должен быть проинформирован о подозрительных операциях, связанных с переводом денежных средств без согласия клиента, в соответствии с соглашением о взаимодействии Банка России и ОПЦК.

5. ОПЦК должна определить показатель уровня риска данного перевода, основываясь на модели оценки риска операций Банка России. Данный показатель должен быть направлен банку плательщика и банку получателя в электронном сообщении по формату, установленному в договоре оказания услуг между участником СБП и ОПЦК[19].

Аудиторы обязаны проверить, применяют ли участники ССНП альтернативный способ взаимодействия с Банком России в случае сбоя основной системы и следуют ли правильному порядку направления запросов. Кроме того, аудиторы должны гарантировать предоставление участниками системы достоверной информации о своих уполномоченных лицах и корректное соблюдение процедур направления копий запросов о приостановлении или отмене обмена электронными сообщениями. Такие проверки направлены на обеспечение соблюдения установленных стандартов и требований участниками, а также на обеспечение надежной защиты информации при взаимодействии с Банком России. После получения запросов через автоматизированную систему Банк России обязан осуществить контроль за целостностью и подтверждением достоверности содержащейся в них информации. При получении запросов через альтернативный канал связи Банк России должен проверить соответствие реквизитов запроса информации, предоставленной участником ССНП. В случае если контроль целостности и подлинности запросов через автоматизированную систему Банка России дал отрицательный результат либо реквизиты запросов через метод взаимодействия резервирования не соответствуют сведениям, указанным участником ССНП, Банк России не должен принимать запросы к исполнению. При этом

[19] Там же.

уведомление участника ССНП должно осуществляться через автоматизированную систему Банка России.

По результатам оценки с 1 января 2023 г. уровень соответствия должен составлять не менее 0,85. Оценка уровня соответствия должна проводиться не реже одного раза в два года. Кроме того, организациям было выгодно достичь уровня 0,85 до 2023 г., так как необходимость в оценке начинается с 1 июля 2021 г. Это обусловлено тем, что при более низких результатах частота повторной оценки будет ниже, чем раз в два года [Ильясов 2024].

В ходе аудитов информационной безопасности часто выявляются типичные проблемы и уязвимости, которые могут существенно снизить уровень защиты информационных активов организации. К наиболее частым нарушениям относятся недостатки в управлении доступом, отсутствие регулярного обновления программного обеспечения и систем безопасности, слабости в обучении персонала по вопросам информационной безопасности, а также недостаточный контроль за физической безопасностью и защитой данных. В аудите информационной безопасности, согласно требованиям Положения Банка России № 802-П, могут возникнуть различные ограничения и проблемы. Вот некоторые из них:

1. Аудитор может столкнуться с ограничениями в доступе к необходимым данным, особенно если организация считает их конфиденциальными или чувствительными. Это может затруднить анализ текущего состояния системы безопасности.

2. В некоторых случаях персонал организации может недостаточно понимать требования Положения № 802-П, что приводит к неправильной интерпретации и реализации мер безопасности. Это может усложнить процесс аудита, поскольку необходимо будет разъяснить требования и рекомендации.

3. Системы информационной безопасности могут быть сложными и разнообразными, что создает технические ограничения для аудитора. Например, доступ к определенным журналам аудита или настройкам систем мониторинга может быть ограничен из-за технических особенностей.

4. Организация может столкнуться с проблемой недостаточных ресурсов для проведения аудита информационной безопасности. Это может включать ограниченный бюджет, нехватку специалистов или временные ограничения.

5. Проведение аудита может вызвать сопротивление со стороны сотрудников или руководства организации, особенно если они считают, что это создаст лишние неудобства или приведет к негативным последствиям для бизнеса.

6. Выявление и анализ уязвимостей в системе безопасности может быть сложной задачей, особенно если они скрыты или неочевидны. Аудитор должен иметь достаточные знания и опыт, чтобы эффективно выявлять и анализировать потенциальные угрозы [Минаков, Эриашвили 2024].

Главным из требований 802-П является внедрение электронных подписей для аутентификации и защиты сообщений, проходящих через платежную систему Банка России. Также 802-П ограничивает возможность по изготовлению криптоключей для обмена сообщениями конкретными операторами.

Исследование стандартов и положений Банка России на соответствие требованиям к защите информации в платежной системе показали, что можно выделить следующие особенности аудита информационной безопасности:

1. Проведение аудита информационной безопасности на соответствие данному Положению затрагивает преимущественно пределы выделенных сегментов вычислительных сетей, которые используются платежной системой при обработке защищаемой информации (п. 19).

2. Национальный стандарт ГОСТ Р 57580.2-2018[20] «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» лежит в основе проведения оценки соответствия (п. 19).

3. Уровень соответствия для выделенных сегментов вычислительных сетей должен быть не ниже 4-го уровня по ГОСТ Р 57580.2-2018 (п. 19).

4. Не реже, чем один раз в два года, должна быть проведена оценка соответствия (п. 19).

5. Необходимо оценивать выполнение требований по таким процессам, как управление доступом, защита сетей, контроль целостности, защита от вредоносного кода, предотвращение утечек и др. в соответствии с ГОСТ Р 57580.1-2017[21] (п. 7.1).

6. Особое внимание должно уделяться оценке применения криптографических средств защиты информации, в том числе электронной подписи, шифрования и порядку работы с ключами (п. 8, п. 12–14).

---

[20] ГОСТ Р 57580.2-2018. URL: https://docs.cntd.ru/document/1200158801?ysclid=lwm8uxxq6i193596260 (дата обращения 15.03.2024).

[21] ГОСТ Р 57580.1-2017. URL: https://docs.cntd.ru/document/1200166534 (дата обращения 15.03.2024).

Заключение

Таким образом, исследование показало, что проверка соответствия банковской системы требованиям к защите информации в платежной системе является важной задачей для обеспечения безопасности платежей и защиты информации клиентов. Соответствие системы защиты информации банка требованиям к защите информации в платежной системе позволяет снизить риски мошенничества, кражи персональных данных и других угроз безопасности. Аудит данного рода выделяется своей спецификой, требующей глубокого знания нормативных актов и правил, установленных Центральным банком России. В процессе аудиторской деятельности осуществляется комплексное изучение соблюдения участниками банковской системы установленных стандартов информационной безопасности, что включает в себя анализ применяемых технологических мер защиты информации, контроль целостности и аутентичности электронных сообщений, а также проверку соблюдения процедур отправки и приема данных.

В контексте представленных особенностей аудита информационной безопасности подчеркивается его ключевая роль в поддержании стабильности и надежности банковской системы, в повышении доверия участников и клиентов к финансовым операциям. Однако, несмотря на все усилия по обеспечению безопасности платежей, риски всегда существуют. Поэтому необходимо постоянно мониторить и совершенствовать систему защиты информации, проводить регулярные проверки соответствия и применять лучшие практики и стандарты отрасли. В качестве перспективных направлений исследования выделим следующие:

1. Исследования, направленные на оценку эффективности применения аудиторских методик и технологий в области информационной безопасности.
2. Исследования, направленные на анализ и прогнозирование тенденций в области угроз информационной безопасности.
3. Исследование влияния новых нормативных актов на процессы аудита информационной безопасности.
4. Изучение международного опыта в области аудита информационной безопасности и сравнительный анализ с практикой в России.

Литература

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской

Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Ильясов 2024 – *Ильясов И.* Перспективы развития электронных валют и платежных систем // Всемирный ученый. 2024. Т. 1. № 16. С. 240–245.

Кочаева, Йоллыев 2024 – *Кочаева А.Р., Йоллыев А.Б.* Безопасность в банковской сфере: ключевые аспекты и роль кибербезопасности в эпоху цифровой экономики // Вестник науки. 2024. № 1 (70). URL: https://cyberleninka.ru/article/n/bezopasnost-v-bankovskoy-sfere-klyuchevye-aspekty-i-rol-kiberbezopasnosti-v-epohu-tsifrovoy-ekonomiki (дата обращения 15.03.2024).

Минаков, Эриашвили 2024 – *Минаков А.В., Эриашвили Н.Д.* Анализ рисков и безопасности системы электронных средств платежа // Образование. Наука. Научные кадры. 2024. № 1. С. 274–281.

Симакова 2024 – *Симакова В.С.* Современные технологии проведения аудита // Экономика и бизнес: теория и практика. 2024. № 2-2. С. 80–83.

Синявская, Синявский 2022 – *Синявская Е.Е., Синявский В.Д.* Цифровая трансформация банковского сектора // Транспортное дело России. 2022. № 2. С. 34–36. URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-bankovskogo-sektora-2 (дата обращения 23.05.2024).

References

Grishina, N.V. (2022), “Analysis of the dynamics of personal data leakage in the context of the implementation of the program ‘Digital Economy of the Russian Federation’ ”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series*, no. 4, pp. 34–43.

Il’yasov, I. (2024), “Prospects for the development of electronic currencies and payment systems”, *A world scientist*, vol. 1, no. 16, pp. 240–245.

Kochaeva, A.R. and Iollyev, A.B. (2024), “Security in the banking sector. Key aspects and the role of cybersecurity in the era of the digital economy”, *Bulletin of Science*, no. 1 (70), available at: https://cyberleninka.ru/article/n/bezopasnost-v-bankovskoy-sfere-klyuchevye-aspekty-i-rol-kiberbezopasnosti-v-epohu-tsifrovoy-ekonomiki (Accessed 15 March 2024).

Minakov, A.V. and Eriashvili, N.D. (2024), “Risk and security analysis of the electronic payment system”, *Education. Science. Scientific staff*, vol. 1, pp. 274–281.

Simakova, V.S. (2024), “Modern audit technologies”, *Economics and Business: theory and practice*, no. 2-2. pp. 80–83.

Sinyavskaya, E.E. and Sinyavskii, V.D. (2022), “Digital transformation of the banking sector”, *Transport business of Russia*, vol. 2, pp. 34–36, available at: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-bankovskogo-sektora-2 (Accessed 15 May 2024).

Информация об авторах

Полина С. Александрова, студент, Финансовый университет при Правительстве Российской Федерации, Москва, Россия; 125993, Россия, Москва, Ленинградский пр-кт, д. 49; alekspolya2003@gmail.com

Александра С. Червинчук, студент, Финансовый университет при Правительстве Российской Федерации, Москва, Россия; 125993, Россия, Москва, Ленинградский пр-кт, д. 49; nuxela@gmail.com

Сергей А. Резниченко, кандидат технических наук, доцент, Финансовый университет при Правительстве Российской Федерации, Москва, Россия; 125993, Россия, Москва, Ленинградский пр-кт, д. 49;

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; 115409, Россия, Москва, Каширское ш., д. 31;

Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская площадь, д. 6; rsa_5@bk.ru

Information about the authors

Polina S. Aleksandrova, student, Financial University under the Government of the Russian Federation, Moscow, Russia; 49, Leningradskii Av., Moscow, 125993, Russia; alekspolya2003@gmail.com

Aleksandra S. Chervinchuk, student, Financial University under the Government of the Russian Federation, Moscow, Russia; 49, Leningradskii Av., Moscow, 125993, Russia; nuxela@gmail.com

Sergei A. Reznichenko, Cand. Of Sci. (Computer Science), associate professor, Financial University under the Government of the Russian Federation, Moscow, Russia; 49, Leningradskii Av., Moscow, 125993, Russia;

National Research Nuclear University “MIFI” (Moscow Engineering Physics Institute), Moscow, Russia; 31, Kashirskoe Highway, Moscow, 115409, Russia;

Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; rsa_5@bk.ru

УДК 004.56:55
DOI: 10.28995/ 2686-679X-2024-3-56-70

Обеспечение информационной безопасности геоинформационных систем при использовании суперкомпьютерных технологий

Дмитрий Н. Баранников
Российский государственный гуманитарный университет, Москва, Россия, d.2006@mail.ru

Ирина А. Русецкая
Российский государственный гуманитарный университет, Москва, Россия, irkom@mail.ru

Аннотация. Геоинформационные системы в настоящее время находят применение в различных сферах деятельности, науки и производства. С помощью современных геоинформационных систем реализуются сбор, хранение, обновление и представление большого количества обрабатываемой информации, а также пространственный анализ данных в картографических, фотограмметрических, кадастровых системах и т. д. Использование технологий мультимедиа позволяет предоставить наглядно обрабатываемые данные, подбирать удобный масштаб и получать справочную информацию в виде таблиц и графиков. Для решения задач обработки, хранения и анализа большого объема таких данных могут эффективно использоваться суперкомпьютерные технологии. При использовании возможностей суперкомпьютеров необходимо уделять внимание проблемам информационной безопасности и защите конфиденциальности, доступности и целостности используемых данных. В работе проводится изучение проблем обеспечения информационной безопасности геоинформационных систем при использовании суперкомпьютеров. В статье уделяется внимание анализу значения геоинформационных технологий для различных областей деятельности, исследование применения геоинформационных систем в рамках суперкомпьютерных технологий. Особое внимание уделяется анализу проблем обеспечения информационной безопасности систем при использовании суперкомпьютерных технологий и мер обеспечения безопасности суперкомпьютеров в работе геоинформационных систем.

Ключевые слова: суперкомпьютер, геоинформационные системы, информационная безопасность, защита информации, картографические данные, суперкомпьютерные технологии

Для цитирования: Баранников Д.Н., Русецкая И.А. Обеспечение информационной безопасности геоинформационных систем при использовании суперкомпьютерных технологий // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 56–70. DOI: 10.28995/ 2686-679X-2024-3-56-70

Ensuring information security of geographic information systems using supercomputer technologies

Dmitrii N. Barannikov
Russian State University for the Humanities, Moscow, Russia, d.2006@mail.ru

Irina A. Rusetskaya
Russian State University for the Humanities, Moscow, Russia, irkom@mail.ru

Abstract. Geographic information systems are currently used in various fields of activity, science and production. With the help of modern geographic information systems, the collection, storage, updating and presentation of a large amount of processed information, as well as spatial analysis of data in cartographic information systems, automated mapping systems, automated photogrammetric systems, land information systems, automated cadastral systems, etc. are realized. The use of multimedia technologies allows providing visually processed data, selecting a convenient scale and obtaining background information in the form of tables and graphs. To solve problems of processing, storing and analyzing large volumes of such data, supercomputer technologies can be effectively used. When using the capabilities of supercomputers, it is necessary to pay attention to information security issues and protecting the confidentiality, availability and integrity of the data used. The article studies the issues of ensuring information security of geographic information systems when using supercomputers. It also analyzes the importance of geographic information technologies for various fields of activity, and studies the use of geographic information systems within the framework of supercomputer technologies. Particular attention is paid to analyzing the issues of ensuring information security of systems when using supercomputer technologies and measures to ensure the security of supercomputers in the operation of geographic information systems.

Keywords: supercomputer, geographic information systems, information security, information protection, cartographic data, supercomputer technologies

For citation: Barannikov, D.N. and Rusetskaya, I.A. (2024), “Ensuring information security of geographic information systems using supercomputer technologies”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series,* no. 3, pp. 56–70, DOI: 10.28995/ 2686-679X-2024-3-56-70

Введение

В настоящее время в большинстве областей деятельности человека находят применение геоинформационные системы (далее – ГИС). Данные системы эффективно решают ряд важных задач: от подбора наилучшего маршрута до исследования проблематики в сфере экологии и перенаселения.

Во всех используемых программах присутствует большая степень визуализации, что приводит к использованию значительного ресурса и увеличенному потреблению мощности. В связи с этим существуют ограничения по использованию имеющихся возможностей. Интеграция ресурсов суперкомпьютера позволяет свести к минимуму энергетические затраты при использовании ГИС и увеличить их производительность.

Однако рост обрабатываемых данных, увеличение количества пользователей способствуют проявлению угроз нарушения целостности, достоверности данных и влиянию вредоносных воздействий, поступающих от внешних и внутренних источников, а также увеличению вероятности получения информации третьими лицами. Поэтому проблема анализа и обеспечения информационной безопасности (далее – ИБ) технологий геоинформационных систем на мощностях, обеспечивающих качественное повышение производительности, обоснованно занимает ведущую роль.

Целью данного исследования является анализ проблем обеспечения безопасности ГИС при использовании суперкомпьютерных технологий.

В соответствии с данной целью исследование решает следующий ряд задач:

- анализ значения ГИС для различных областей деятельности;
- изучение возможностей суперкомпьютерных технологий для ГИС;
- исследование проблем обеспечения ИБ систем при использовании суперкомпьютерных технологий;
- анализ мер обеспечения ИБ ГИС при применении суперкомпьютерных технологий.

I. Значение геоинформационных систем в различных областях

Каждый этап эволюционного развития человека характеризуется уникальными прорывными идеями, которые находят свое воплощение и дальнейшую практическую реализацию. Пространственная ориентация была актуальной во все времена, однако точность расчетов требовала больших усилий и часто имела погрешности. Возможность вычисления расчетных показателей с помощью применения технологий автоматизации существенно упростила процедуру получения данных, а также повысила точность и универсальность полученных показателей.

Появление в профессиональной деятельности человека первых электронных вычислительных машин упростило многие трудоемкие операции, связанные с получением данных. На зарекомендовавшей себя с положительной стороны электронно-вычислительной платформе стали создаваться системы, позволяющие визуализировать расчетные показатели с целью создания карт, а также размещать различные объекты и оценивать информацию, ориентированную на обработку пространственных данных.

Исторической точкой отсчета создания геоинформационной системы считается 1960 год, когда в Канаде была запущена первая программа управления землепользованием. Практическое использование ГИС показало свою результативность, и началось стремительное расширение применения положительной практики для транспортных систем.

Затем был период переоценки, уточнения и доработки. Но уже с 1980 года, когда потребитель оценил преимущества использования ГИС, отмечается всплеск технологических разработок и практического применения как в гражданском секторе, так и на благо обороноспособности стран. В гражданском секторе особая роль отводилась природоохранным вопросам, а также картографированию лесных массивов. Для данных функций отлично подходила воздушная и космическая съемка со специализированных бортов.

Российские разработки в указанный период были направлены на обеспечение и укрепление военного потенциала, поэтому имели специализированную направленность. И только в девяностых годах прошлого века коммерческие ГИС стали завоевывать рынок, конкурируя с обилием импортных разработок.

В современном понимании ГИС – это многофункциональная автоматизированная система, позволяющая собирать, анализировать, хранить, распространять и отображать пространственно-кодированные данные с использованием программно-аппаратных

комплексов, а также осуществлять различные манипуляции с пространственными объектами, визуализируя географические координаты.

В инновационных геоинформационных системах реализуется сбор, хранение, обновление и представление обрабатываемой информации. Отличительной чертой ГИС в сравнении с применяемыми автоматизированными системами управления является то, что в ГИС присутствуют технологии пространственного анализа данных, что позволяет преобразовывать информацию и осуществлять синтез используемых данных в картографических, фотограмметрических, кадастровых системах и т. д. Использование технологий мультимедиа позволяет предоставить наглядно обрабатываемые данные, подбирать удобный масштаб и получать справочную информацию в виде таблиц и графиков.

Компьютерные технологии позволяют пользователю решать необходимые задачи с использованием цифровых карт, анализировать полученные результаты, редактировать цифровые карты, а также получать дополнительную информацию о размещаемых на карте объектах, сравнивать и обобщать разнородную информацию, своевременно вносить изменения и добавлять данные. Кликнув на необходимом объекте, можно получить краткую информацию о нем. Например, если выбрать какой-либо административный объект, то можно получить информацию не только о внешнем виде, месте расположения объекта, но и о количестве сотрудников, графике работы организации и т. д.

Данные, размещенные в геоинформационных системах, визуализируются на картографическом изображении и накладываются слоями, позволяя добавлять слой или удалять, что делает удобнее процесс обновления. Например, для лиц, занимающихся исследовательской деятельностью в арктическом регионе, можно с использованием данных спутниковых систем изучать изменение ледяного покрова в зависимости от времени года, активности промышленных выбросов и других факторов, влияющих на климатические изменения [Булатов 2019].

Возможности ГИС позволяют покадрово фиксировать необходимую информацию в проекциях с заданным масштабом на различных площадях в необходимый период времени. Данные технологии позволяют как исследователям акцентировать свое внимание при поиске нужных объектов, так и пользователям изучать необходимые сведения.

Области применения ГИС многообразны [Воронин 2019]. В частности, не обходится без ГИС изучение климатических изменений на планете, водных ресурсов и влияния воздействий чело-

века на природу. Получаемая информация помогает осуществлять прогноз последствий в случае техногенных аварий. Сфера поддержания обороноспособности страны требует оснащения высокоинтеллектуальных систем геоинформационными технологиями. Так, в 2021 г. АО «Концерн Радиоэлектронные технологии» вывел на рынок систему, позволяющую БПЛА преодолевать большие расстояния над водной и земной поверхностью без привязки к каким-либо ориентирам, при этом исключив использование при полете GPS или «Глонасс». В сельскохозяйственной деятельности геоинформационные системы используют не только для навигации машин и анализа погодных условий, но и для оценки плодородия почв и пригодности их для посадки тех или иных сельскохозяйственных культур.

Государственные лесные инспекторы с помощью ГИС более эффективно осуществляют мониторинг вырубки деревьев и проводят инвентаризацию и управление особо охраняемыми природными территориями.

Бизнес также прекрасно адаптировал ГИС под свои цели. Крупные компании с помощью инструмента геоанализа получают и анализируют данные о местах массового пребывания людей, потребительском спросе; в дальнейшем эти данные используют для определения желательных локаций магазинов и мерчендайзинга товаров.

Нельзя не сказать и о ГИС, которые позволяют оперативно реагировать на природные катастрофы, координировать действия спасательных служб, выявлять проблемы с медобслуживанием, а также осуществлять прогноз распространения эпидемий. Органы государственного и муниципального управления осуществляют контроль за дорожной обстановкой, рациональным использованием муниципальной собственности, эксплуатацией инфраструктуры и принятием мер повышения инвестиционной привлекательности территорий.

Большой объем данных, которые получает пользователь, собирается и адаптируется для различных систем, поступает из разных источников и обрабатывается с помощью компьютерных технологий и вычислительных систем [Вагизов 2017]. Приложения, которые использует ГИС, включают в себя оцифрованные картографические данные, аэрофотоснимки, информацию, получаемую от спутников, аналитическую информацию из сети Интернет и т. д. Аппаратные и программные системы организуют информационные процессы независимо от источника информации, объединяя различные переменные слоями на одной карте. Информация о местности или объекте, если находится в цифровом формате, за-

гружается в систему, или предварительно перед загрузкой производится процесс преобразования в цифровой формат [Горбунов 2015]. Полученные данные ГИС хранит в виде слоев, а справочная информация находится в виде таблиц.

Отдельно стоит сказать о технологической составляющей. Используемые в ГИС форматы отображения, обработки и хранения данных, которые запускает аппаратный компонент, требуют для своей работы мощные серверы [Хыдыров 2022]. В качестве основных проблем при использовании ГИС можно назвать следующие: сложность в эксплуатации, слабая многоплатформенность, недостаточный набор средств для работы с пространственной информацией, сложная интеграция с другими программными пакетами [Семченко 2021].

Одним из направлений расширения возможностей для пользователей ГИС является использование технологии создания распределенных ГИС, когда в работе используются не мощности персонального компьютера, а удаленный сервер. Все это несколько облегчает пользователю получение необходимой информации, но требует увеличения мощностей серверов. Для решения отдельно взятых задач данные подходы могут являться эффективными. Однако увеличивающийся рост информационных потоков приводит к тому, что не вся информация будет предоставлена пользователю без существенных временных задержек. Также остается высокая вероятность потери необходимой информации или предоставления неполной информации. Стоит отметить, что перспективным направлением развития пространственной обработки данных является применение технологий больших данных, требующее огромных ресурсов.

В этом вопросе могут прийти на помощь суперкомпьютерные инфраструктуры.

II. Суперкомпьютеры в решении энергозатратных объемных задач

С начала 90-х годов в Российской Федерации вопрос увеличения вычислительной мощности, а следовательно, производительности и продуктивности решаемых задач, вышел на активный уровень поиска решений. Разрабатываемая Национальная исследовательская компьютерная сеть должна быть интегрирована в мировое научно-образовательное сообщество, что способствовало бы достижению цели по развитию инструментов суперкомпьютерной инфраструктуры. Использование такой инфраструктуры

позволит каждому пользователю эффективно и оперативно решать возникающие задачи за оптимальное время.

Практическая реализация суперкомпьютером задач в интересах Министерства обороны Российской Федерации позволила обрабатывать сообщения различных систем, объединяя данные в единый сервис. Используя положительный опыт, накопленный Минобороны России, и другие наработки, в России продолжается построение Национальной исследовательской компьютерной сети. В данную сеть объединяются, в частности, имеющиеся суперкомпьютеры Санкт-Петербургского политехнического университета Петра Великого, Межведомственного суперкомпьютерного центра РАН и Объединенного института ядерных исследований. На данных мощностях существует возможность обработки больших данных, сервисного обучения, использования глобальной аналитики и применения накопленных ресурсов при решении мегарасчетных задач. В связи с этим ректор СПбПУ отметил, что развитие вычислительных ресурсов – задача сверхважная не только для науки, но и для промышленности, вузов и научно-исследовательских организаций, которыми проводится целый ряд фундаментальных и прикладных исследований.

Увеличение производительности обработки данных не осуществляется в интересах решения одной, пусть и наиболее важной, задачи. Суперкомпьютеры охватывают многочисленные области применения, включая такие, как медицина, кинематограф, промышленность, добыча полезных ресурсов, исследовательская деятельность. Оптимизация имеющихся возможностей происходит путем решения параллельных задач. Поэтому наряду с решением уже имеющихся проблем, производительность суперкомпьютеров позволяет использовать возможности в интересах геоинформационных систем.

III. Безопасность информации при использовании высокотехнологичных устройств суперкомпьютерных технологий

Взаимосвязь суперкомпьютерных технологий и ИБ определяется тем, что такие технологии могут как служить инструментом защиты информации, так и ставить новые проблемы при обеспечении ИБ в различных системах, в том числе ГИС.

Так, прогнозируемое специалистами в ближайшем будущем использование квантовых компьютеров ставит новые требования перед разработкой методов так называемой «квантово-безопасной»

криптографической защиты информации, так как применение таких компьютеров предполагает сведение к возможному минимуму времени, которое требуется для взлома существующих алгоритмов шифрования. Для предупреждения проявления подобного рода угроз исследователями разных стран ведется работа над созданием постквантовых криптографических алгоритмов. В этом процессе активно применяются суперкомпьютерные технологии, которые используются для создания и тестирования постквантовых алгоритмов шифрования [Русецкая 2021].

Суперкомпьютерные технологии также могут применяться в целях обеспечения информационной безопасности при помощи создания моделей кибератак, при поиске и анализе уязвимостей, тестировании устойчивости к кибератакам и т. д. Подобное моделирование позволяет выявлять реальные и потенциальные угрозы информационным системам, в том числе ГИС.

Кроме того, суперкомпьютерные технологии могут применяться в информационно-аналитической работе по обеспечению ИБ при анализе больших разнородных массивов данных, в частности интегрируемых в ГИС, для анализа закономерностей, факторов и тенденций, определяющих возникновение и проявление угроз ИБ.

Особенно хорошие результаты при этом может дать использование суперкомпьютеров, в которых решена проблема преодоления так называемой «стены памяти». Подобные суперкомпьютеры разрабатываются в США и КНР, как правило, имеют массово-мультитредовую архитектуру и обеспечивают многоуровневую аппаратную защиту используемых данных и программных средств [Моляков 2019 б].

Таким образом, является неоспоримой эффективность использования суперкомпьютерных технологий для решения проблем безопасности информационных систем.

Однако использование суперкомпьютеров ставит и новые проблемы в области обеспечения защиты используемых информационных технологий и массивов данных, которые будут рассмотрены ниже.

Важность проблем обеспечения безопасности при использовании суперкомпьютерных технологий определяет и наличие нормативно-правовых требований по обеспечению защиты информационных систем.

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ требует соблюдения мер по обеспечению информационной безопасности объектов КИИ, составной частью которых являются суперкомпьютерные устройства и технологии, используемые для организации функционирования таких объектов.

Обеспечение комплексной защиты объектов КИИ напрямую связано, в частности, и с безопасностью геоинформационных систем критического применения, которые обеспечивают работу объектов КИИ.

Таким образом, обеспечение ИБ ГИС при использовании суперкомпьютеров является важной составляющей при решении задач национальной безопасности.

Необходимость эффективного обеспечения ИБ государства при использовании суперкомпьютерных технологий подчеркивает тот факт, что с 2012 г. полномочия ФСБ России и ФСТЭК России были расширены в связи с подписанием Указа Президента РФ от 8 февраля 2012 г. № 146 «О федеральных органах исполнительной власти, уполномоченных в области обеспечения безопасности информации в информационных системах, созданных с использованием суперкомпьютерных и грид-технологий».

Выделим основные проблемы, существующие при обеспечении безопасности использования суперкомпьютерных технологий.

Информация, обрабатываемая суперкомпьютерами, имеет значительную ценность, что определяет серьезность и подготовленность неправомерных действий потенциальных внутренних и внешних злоумышленников с целью нарушения целостности, доступности и конфиденциальности информации и возможность использования для этого высокотехнологичного оборудования.

Серьезную проблему российским суперкомпьютерным технологиям могут создавать элементы импортной базы: серверных плат, программного обеспечения и т. п.

Можно выделить также проблемы безопасности суперкомпьютеров, обусловленные технологическими особенностями их построения:

– отсутствие оптимизации и адаптации применяемых программно-аппаратных решений к объемам входных данных, архитектуре, набору конфигураций серверов суперкомпьютеров, которое определяет снижение быстродействия систем при применении межсетевых экранов, антивирусов, DLP-систем и др. средств защиты;
– использование сложной элементной базы, включающей большое количество компонентов, что повышает вероятность использования закладных устройств, а также определяет сложность их поиска и выявления;
– трудность обнаружения инцидентов в области ИБ и мониторинга событий в условиях большого количества одновременно выполняемых процессов (сотни тысяч – до миллиона) [Моляков 2019а].

Проблемы обеспечения безопасности суперкомпьютеров, в частности в используемых ГИС, определяются также факторами организационного характера. С учетом того, что сложная система осуществляет решение большого количества разноплановых задач, возрастает количество персонала, эти задачи решающего, что сказывается на увеличении риска утечки информации через внутренних нарушителей. Таким образом, организационные меры не теряют своей актуальности независимо от сложности системы и надежности используемых средств защиты. Также не исключается внешнее воздействие злоумышленников, направленное на несанкционированное получение, искажение или блокирование информации.

Актуальные меры, необходимые для обеспечения безопасного использования суперкомпьютеров, могут включать в себя следующие:

- совершенствование нормативно-правовой базы обеспечения защиты суперкомпьютерных технологий;
- принятие организационных мер по обеспечению безопасного функционирования объектов, использующих суперкомпьютерные технологии в ГИС, в частности работу с персоналом, работающим в этой сфере;
- внедрение подсистемы многофункциональной поддержки виртуализации оборудования;
- ведение информационно-аналитической работы по изучению угроз безопасности суперкомпьютерам, которая включает в себя, например, изучение и классификацию аппаратных закладных устройств, способов их выявления и нейтрализации и т. д.;
- поддержка отечественных исследований и научно-практических разработок в сфере создания защищенной информационной среды при использовании суперкомпьютерных технологий.

Заключение

Усложняющиеся информационные процессы и увеличение объемов данных требуют все больших ресурсов, которых в настоящее время бывает недостаточно для решения многоуровневых задач. Возможности суперкомпьютеров позволяют осуществлять решение сложных вычислительных, аналитических и других задач обработки и хранения геоинформационных данных, недоступных отдельным высокопроизводительным компьютерным системам.

Суперкомпьютеры позволяют продуктивнее создавать конкурентоспособную продукцию. Многообразие выполняемых задач в интересах различных отраслей создает предпосылку для стимулирования различных уязвимостей, направленных на утечку информации, подлежащей защите. Сложные программные продукты уже сами по себе содержат внутренние ошибки и уязвимости без какого-либо воздействия, что тоже необходимо учитывать при разработке системы безопасности.

Все перечисленное требует ужесточения подходов к технологии обработки информации. При этом избыточное регулирование системы обеспечения ИБ может привести к нехватке используемой мощности и бюрократическим барьерам.

В этих условиях перед специалистами, занимающимися вопросами обеспечения ИБ, стоит сложная задача оптимальной загрузки прикладного программного обеспечения обрабатываемыми данными и предотвращения угроз высокопроизводительным компьютерным системам.

Возможности суперкомпьютеров выходят далеко за рамки возможностей промышленных компьютеров, обеспечивая вычислительную мощность в несколько сот петафлопс. Такой сверхвысокой производительности позволяет достичь параллельная работа микропроцессоров, которые выполняют разнообразные операции. Увеличивая возможности систем обработки данных, которые представляют коммерческий, научный и государственный интерес, а также сохраняя эти данные в электронном виде, необходимо не только защищать информацию, но и обеспечивать системы защиты на уровне, позволяющем своевременно обнаружить, устранить и предупредить проявление уязвимостей. Целью злоумышленников может быть не только находящаяся в суперкомпьютере информация, но и непосредственно электроника различных блоков и устройств [Грызунов 2022].

В суперкомпьютерных системах защита геоинформационных ресурсов должна осуществляться не фиксированным набором методов и средств, предотвращающих угрозы безопасности, а происходить непрерывно, с учетом результатов тестирования подстраиваясь под выявленные угрозы. Суперкомпьютер при решении задач ИБ ГИС должен осуществлять анализ создавшейся обстановки при каждом воздействии внутри системы и выбирать оптимальный вариант защиты.

Таким образом, применение возможностей суперкомпьютеров, например в рамках Национальной исследовательской компьютерной сети, позволит повысить быстродействие обработки данных, решая задачи в интересах геоинформационных систем, при этом

обеспечивая защиту данных. Использование ресурсов суперкомпьютеров для анализа возможных или потенциальных угроз и выбора средств защиты позволит оптимизировать процесс устранения уязвимостей.

Литература

Булатов 2019 – *Булатов А.М.* Корпоративная система управления проектами как инструмент повышения эффективности реализации проектов по созданию геоинформационных систем // Россия – Азия – Африка – Латинская Америка: экономика взаимного доверия. Материалы X Евразийского экономического форума молодежи, Екатеринбург, 16–19 апреля 2019 года. Т. 1. Екатеринбург: Уральский государственный экономический университет, 2019. С. 138–141.

Воронин 2019 – *Воронин А.В., Зацаринный А.А.* Геоинформационная система как важнейший компонент системы принятия управленческих решений // Системы высокой доступности. 2019. Т. 15. № 3. С. 27–33.

Вагизов 2017 – *Вагизов М.Р.* Разработка интерактивных геоинформационных систем: принципы построения и конструирования системы // Информационные системы и технологии: теория и практика: Сб. научных трудов научно-технической конференции института леса и природопользования, Санкт-Петербург, 1 февраля 2017 года. Т. 1. Вып. 9. СПб.: Санкт-Петербургский государственный лесотехнический университет им. С.М. Кирова, 2017. С. 21–27.

Горбунов 2015 – *Горбунов А.А., Пономорчук А.Ю., Иванов В.Г.* Использование геоинформационных систем при принятии управленческих решений в единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2015. № 2. С. 71–76.

Хыдыров 2022 – *Хыдыров Р.Б.* Оценка внедрения геоинформационных систем в организационно-управленческих вопросах транзитных систем // Техника и технология транспорта. 2022. № 3 (26).

Семченко 2021 – *Семченко А.С., Линкина А.В.* Этап инфологического проектирования сложных систем (в контексте геоинформационных систем) // Вестник Воронежского института высоких технологий. 2021. № 4 (39). С. 75–77.

Русецкая 2021 – *Русецкая И.А.* Криптография: от прошлого к будущему // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 47–57.

Моляков 2019а – *Моляков А.С.* Аксиоматика и принципы обеспечения информационной безопасности суперкомпьютеров: Учеб.-метод. пособие по дисциплине «Безопасность операционных систем». М.: Спутник+, 2019. 134 с.

Моляков 2019б – *Моляков А.С.* Модель угроз и теоретические основы метода реактивной защиты суперкомпьютеров // Естественные и технические науки. 2019. № 7 (133). С. 197–201.

Грызунов 2022 – *Грызунов В.В.* Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 101–116.

References

Bulatov, A.M. (2019), "Corporate project management system as a tool to improve the effectiveness of the geoinformation systems projects", *Russia – Asia – Africa – Latin America: the economy of mutual trust: Proceedings of the 10th Eurasian Economic Youth Forum, Yekaterinburg, April 16–19, 2019*, vol. 1, Ural State University of Economics, Yekaterinburg, Russia, pp. 138–141.

Gorbunov A.A., Ponomorchuk A.Yu. and Ivanov, V.G. (2015), "The use of geoinformation systems in making managerial decisions in the unified state system of emergency prevention and response", *Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia*, no. 2, pp. 71–76.

Gryzunov, V.V. (2022), "Adaptive resource availability management methods for geographic information systems under destructive impacts", *Proceedings of educational institutions of communication*, vol. 8, no. 3, pp. 101–116.

Khydyrov, R.B. (2022), "Evaluation of the introduction of geoinformation systems in organizational and managerial issues of transit systems", *Technique and technology of transport*, no. 3 (26).

Molyakov, A.S. (2019a), *Aksiomatika i printsipy obespecheniya informatsionnoi bezopasnosti superkomp'yuterov: uchebno-metodicheskoe posobie po distsipline "Bezopasnost' operatsionnykh system"* [Axiomatics and principles of ensuring information security of supercomputers. Educational manual for the discipline "Security of Operating Systems"], Sputnik+, Moscow, Russia, 134 p.

Molyakov, A.S. (2019b), "Threat model and theoretical foundations for the method of reactive protection of supercomputers", *Natural and technical sciences*, no. 7 (133), pp. 197–201.

Rusetskaya, I.A. (2021), "Cryptography. From past to future", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 47–57.

Semchenko, A.S. and Linkina, A.V. (2021), "The stage of infological design of complex systems (in the context of geoinformation systems)", *Bulletin of the Voronezh Institute of High Technologies*, no. 4 (39), pp. 75–77.

Vagizov, M.R. (2017), "Development of interactive geoinformation systems. Principles of system construction and design", *Information systems and technologies: theory and practice: Collection of scientific papers of the scientific and Technical conference of the Institute of Forest and Nature Management*, St. Petersburg, February 1, vol. 1, is. 9, St. Petersburg State Forestry Engineering University named after S.M. Kirov, St. Petersburg, Russia, 2017, pp. 21–27.

Voronin, A.V. and Zatsarinniy, A.A. (2019), "Geoinformation system as the most important component of the management decision-making system", *High availability systems*, vol. 15, no. 3, pp. 27–33.

Информация об авторах

Дмитрий Н. Баранников, кандидат военных наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; d.2006@mail.ru

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; irkom@mail.ru

Information about the authors

Dmitrii N. Barannikov, Cand. of Sci. (Military Sciences), associate professor, Russian State University of Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, 125047, Russia; d.2006@mail.ru

Irina A. Rusetskaya, Cand. of Sci. (History), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, 125047, Russia; irkom@mail.ru

УДК 004.7
DOI: 10.28995/ 2686-679X-2024-3-71-86

Претекстинг в социальных сетях: актуальность проблемы и пути ее решения

Валерий К. Маркелов
Ивановский государственный университет, Шуйский филиал, Шуя, Ивановская область, Россия, v.a.l.e.m.a.r.k@yandex.ru

Александр Н. Привалов
Тульский государственный педагогический университет им. Л.Н. Толстого, Тула, Россия;
Ивановский государственный университет, Шуйский филиал, Шуя, Ивановская область, Россия, privalov.61@mail.ru

Аннотация. В эпоху цифровой трансформации и активного развития информационных технологий социальные сети – это основное средство для общения между пользователями в Интернете. В работе рассматривается феномен популярности социальных сетей, который обращает на себя внимание киберпреступников, считающих социальные сети наиболее привлекательной средой для использования методов социальной инженерии с целью выманивания персональных данных и денежных средств ее пользователей.

Проведенный качественный анализ публикаций в базах научных публикаций eLibrary и Google Scholar позволил определить наиболее актуальные направления исследований по проблемам информационной безопасности в социальных сетях. Одним из таких направлений является проблема защищенности пользователей от атак с применением методов фишинга и претекстинга.

Полученные результаты анализа публикаций в базах научных публикаций eLibrary, Scopus, Google Scholar за последние 10 лет по проблемам противодействия методам социальной инженерии в социальных сетях демонстрируют возрастающий интерес ученых к данной области исследований.

Вместе с этим в последние годы наблюдается рост числа исследований, посвященных изучению претекстинга как метода социальной инженерии, однако количество исследований, посвященных этой проблеме, остается недостаточным, что свидетельствует о необходимости разработки эффективных мер по повышению уровня защищенности пользователей социальных сетей от атак претекстинга.

Ключевые слова: социальные сети, социальная инженерия, претекстинг, фишинг, защита информации, пользователи социальных сетей, информационная безопасность

Для цитирования: Маркелов В.К., Привалов А.Н. Претекстинг в социальных сетях: актуальность проблемы и пути ее решения // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 71–86. DOI: 10.28995/ 2686-679X-2024-3-71-86

Pretexting in social networks. Relevance of the issue and ways of its solution

Valerii K. Markelov
Ivanovo State University, Shuya branch,
Shuya, Ivanovo region, Russia, v.a.l.e.m.a.r.k@yandex.ru

Aleksandr N. Privalov
Tula State Lev Tolstoy Pedagogical University, Tula, Russia;
Ivanovo State University, Shuya branch,
Shuya, Ivanovo region, Russia, privalov.61@mail.ru

Abstract. In the era of digital transformation and active development of information technologies, social networks are the main means for communication between users on the Internet. The article considers the phenomenon of the social networks popularity, which draws an attention of cybercriminals who consider social networks to be the most attractive environment for using social engineering techniques to lure personal data and money from its users.

A qualitative analysis of publications in the databases of scientific publications eLibrary and Google Scholar helped to identify the most relevant areas of research on issues of information security in social networks. One such area is the issue of protecting users from phishing and pretexting attacks. Results of analyzing publications in the databases of scientific publications eLibrary, Scopus, Google Scholar over the past 10 years on the issues of countering social engineering methods in social networks demonstrate the growing interest of scientists in this area of research.

At the same time, in recent years there has been an increase in the number of studies concerning the research of pretexting as a method of social engineering, however, the number of studies addressing the issue remains insufficient, which suggests that there is a need to develop effective measures to improve the level of protection for social network users from pretexting attacks.

Keywords: social networks, social engineering, pretexting, phishing, information protection, social network users, information security

For citation: Markelov, V.K. and Privalov, A.N. (2024), "Pretexting in social networks. Relevance of the issue and ways of its solution", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 71–86, DOI: 10.28995/ 2686-679X-2024-3-71-86

Введение

В современном обществе социальные сети – это один из основных инструментов для общения и обмена информацией между пользователями в сети Интернет. Понятие «социальная сеть» прежде всего обозначало «социальную структуру, состоящую из множества субъектов (индивидов, социальных групп, организаций) и связей между ними, возникающими по поводу обмена ресурсами» [Ветцель 2020, с. 139]. В современном понимании «социальная сеть – это онлайн-платформа, предназначенная для общения, поиска единомышленников и объединения людей в группы по интересам» [Брославский, Полянский 2020, с. 230].

Таким образом, «социальная сеть – это платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений» [Абдуллаева 2015, с. 543].

Социальные сети выполняют ряд следующих функций:

– коммуникативную (предоставляют возможности для поддержания связи и общения между пользователями сети Интернет);
– развлекательную (предоставляют своим пользователям доступ к разнообразным формам развлекательного контента: фотографиям, музыке, видео, сообществам, онлайн-играм и т. д., при этом пользователи могут принимать участие в развлекательных сообществах, слушать музыку, просматривать фотографии и видео других пользователей социальной сети и т. п.);
– информационную (позволяют осуществлять обмен информацией с другими пользователями, «причем такая информация может относиться как к элементам персонального (личные достижения, фотографии), так и к элементам познавательного, новостного и обучающего характера» [Иванько и др. 2020, с. 4]);
– коммерческую («предоставляют своим пользователям площадку для продвижения бизнеса, а также для рекламы товаров и услуг» [Табашникова, Яговцева 2023, с. 436]).

Причиной появления феномена социальных сетей является повышенная потребность в общении, которая свойственна людям. Популярность социальных сетей стремительно растет: согласно отчету Digital 2024: Global Overview Report, по состоянию на январь 2024 г. «число активных пользователей социальных сетей составляет 5,04 млрд человек (январь 2023 г. – 4,76 млрд человек)»[1]. Данные отчета статистического портала Statista показывают, что по состоянию на январь 2024 г. «самые популярные социальные сети посещают более 3 млрд активных пользователей в месяц»[2]. Самыми популярными социальными сетями в России, согласно отчету аналитической компании MediaScope[3], являются ВКонтакте (месячный охват: 90 млн пользователей в месяц, 74,0% от населения страны) и Telegram (месячный охват: 84 млн пользователей в месяц, 69,1% от населения страны).

Феномен популярности социальных сетей не только привлекает миллионы пользователей по всему миру, но и обращает на себя внимание киберпреступников [Гришина 2022], которые считают социальные сети привлекательной средой для использования методов социальной инженерии с целью выманивания персональных данных и денежных средств пользователей.

Социальные сети – это одно из основных средств для осуществления атак с применением методов социальной инженерии (фишинг, претекстинг и т. д.). Кевин Митник, известный специалист по информационной безопасности, определяет социальную инженерию как «совокупность подходов прикладных социальных наук, приемов и технологий, ориентированных на создание организационных структур для регулирования и управления действиями человека» [Митник, Саймон 2004, с. 26]. Кристофер Хаднеги, один из ведущих специалистов в области социальной инженерии, под социальной инженерией понимает «любые действия, подталкивающие другого человека сделать то, что может как пойти ему на пользу, так и навредить» [Хэднеги 2020, с. 16].

---

[1] Digital 2024 – Digital 2024: Global Overview Report // DataReportal. Global Digital Insights. URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения 02.04.2024).

[2] Biggest social media platforms 2024 // Statista. The Statistics Portal for Market Data, Market Research and Market Studies. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (дата обращения 28.03.2024).

[3] MediaScope – Рейтинги // Исследовательская компания Mediascope. URL: https://mediascope.net/data/ (дата обращения 03.04.2024).

Анализ публикаций по проблемам информационной безопасности в социальных сетях

Проведенный качественный анализ публикаций в базах научных публикаций eLibrary и Google Scholar позволил определить наиболее актуальные направления исследований по проблемам информационной безопасности в социальных сетях. В табл. 1 представлены результаты анализа актуальных направлений исследований по проблемам информационной безопасности в социальных сетях.

Таблица 1

Исследования по проблемам информационной безопасности в социальных сетях

Проблемы информационной безопасности в социальных сетях	Авторы публикаций
Проблема защищенности персональных данных в социальных сетях	«Лосяков А.В., Слесарев Ю.В.» [Лосяков, Слесарев 2016], «Апатова Н.В., Минабилева М.Н.» [Апатова, Минабилева, 2021], «Филиппов П.Б.» [Филиппов 2012]
Проблема защищенности пользователей социальных сетей от атак социальной инженерии	«Фомина Н.А.» [Фомина 2015], «Дьяков, Н.В.» [Дьяков 2020], «Замолоцких В.С., Сидоренко В.Г.» [Замолоцких, Сидоренко 2020]
Проблема фишинга в социальных сетях	«Кудрявцев О.А., Щекочихин О.В.» [Кудрявцев, Щекочихин 2018], «Аникина Н.А., Соколов Н.А.» [Аникина, Соколов 2024], «Нилин П.А., Чугунова О.В.» [Нилин, Чугунова 2020]

Проблема защищенности персональных данных в социальных сетях

В исследовании А.В. Лосякова и Ю.В. Слесарева [Лосяков, Слесарев 2016] рассматриваются вопросы правового регулирования размещения и защиты персональных данных в социальных сетях. В частности, авторы выделяют следующие «правовые проблемы в сфере защиты персональных данных: отсутствие четких формулировок понятия “персональные данные”; отсутствие выстроенного правового механизма применения законодательства

к нарушителям; неопределенность в методах и пределах правового регулирования в сфере использования социальных сетей» [Лосяков, Слесарев 2016, с. 4].

Н.В. Апатова и М.Н. Минабилева в своем исследовании [Апатова, Минабилева, 2021] выделяют различные риски безопасности персональных данных в социальных сетях, которые могут привести к краже пароля от учетной записи. К таким рискам прежде всего относятся: атаки с использованием вредоносных программ (программы-вымогатели); атаки с применением методов социальной инженерии (фишинг); атаки с применением сторонних приложений для социальных сетей.

В своей работе Б.П. Филиппов [Филиппов 2012] также рассматривает вопросы использования и реализации защиты персональных данных в социальных сетях. Автор исследования подчеркивает, что «персональные данные, размещенные по воле пользователей, могут нести опасность, так как являются объектами для атак с целью кражи конфиденциальных данных или их отправки киберпреступникам» [Филиппов 2012, с. 73].

Автор исследования указывает на существующие программные решения проблем информационной безопасности в социальных сетях, которые помогают «задать уровень открытости для коммуникации, а также на возможности агентской организации безопасности в социальных сетях средствами родительского контроля» [Филиппов 2012, с. 75].

Проблема обеспечения информационной безопасности в социальных сетях от атак социальной инженерии

В работе [Фомина 2015] показана проблема использования методов социальной инженерии при мошенничестве в социальных сетях. В частности, она указывает на то, что «мошенничество в социальных сетях нацелено на взлом страницы в социальной сети и отправку сообщений от его имени с просьбой о помощи, сбор денег на помощь “близким” и т. п.» [Фомина 2015, с. 446].

Н.А. Дьяков в своей работе [Дьяков 2020] рассматривает виды и формы социальной инженерии, различные способы мошенничества в социальных сетях. Автор исследования выделяет следующие правила, которые направлены на противодействие мошенническим действиям: «не оставлять свои персональные данные на открытых ресурсах; при получении сообщения о блокировке аккаунта не

вводить данные во вложенные формы; если вы стали получать подозрительные письма и сообщения от ваших друзей, постараться связаться с ними другим способом» [Дьяков 2020, с. 127].

В своем исследовании В.С. Замолоцких и В.Г. Сидоренко [Замолоцких, Сидоренко 2020] рассматривают киберугрозы в социальных сетях. В качестве таких угроз авторы выделяют спам-атаки, а также атаки с применением методов социальной инженерии, в частности фишинговые атаки, направленные на получение доступа к учетной записи пользователя социальной сети, и выделяют следующие стратегии проведения подобных атак: «уязвимость протокола WEP, метод полного перебора, метод подмены» [Замолоцких, Сидоренко 2020, с. 68].

Проблема фишинга в социальных сетях

О.А. Кудрявцев и О.В. Щекочихин в своей работе [Кудрявцев, Щекочихин 2018] рассматривают особенности фишинговых атак в различных сервисах, в том числе в социальных сетях. При этом авторы подчеркивают, что для реализации фишинговых атак могут применяться различные средства, такие как социальные сети, электронная почта, мессенджеры, SMS-сообщения и т. д.

Н.А. Аникина и Н.А. Соколов в своем исследовании [Аникина, Соколов 2024] описывают фишинг как один из самых распространенных и опасных видов онлайн-мошенничества. Успешные фишинговые атаки могут иметь серьезные последствия для жертв. Пользователи социальных сетей могут потерять доступ к своим аккаунтам, стать жертвами финансового мошенничества, а их личные данные могут быть использованы для преступных целей.

П.А. Нилин и О.В. Чугунова в своем исследовании [Нилин, Чугунова 2020] описывают способы борьбы с фишинг-атаками. Для защиты от фишинга они предлагают программные решения для автоматического обнаружения и предотвращения фишинговых атак. В частности, «чтобы предотвратить фишинговые атаки, вводится дополнительный уровень безопасности при входе пользователя на веб-сайт, который обеспечивается посредством двухфакторной аутентификации» [Нилин, Чугунова 2020, с. 91].

Проблема претекстинга в социальных сетях

Претекстинг является важным элементом атак социальной инженерии с использованием фишинга. «Претекстинг – это метод

социальной инженерии, при котором злоумышленник по заранее подготовленному сценарию (претекст) подводит потенциальную жертву к тому, чтобы она совершила требуемые действия или выдала необходимую конфиденциальную информацию (как правило, это осуществляется через социальные сети, телефон, электронную почту и требует предварительной обработки информации о жертве)» [Захлевная 2023, с. 411].

Как правило, данный метод социальной инженерии чаще всего реализуется посредством телефонной связи. Согласно опросу Всероссийского центра изучения общественного мнения (ВЦИОМ)[4], проведенного в феврале 2024 г., 67% россиян за последние полгода-год получали звонки от телефонных мошенников. Согласно результатам исследования Е.В. Зотиной, «материалы следственно-судебной практики, сведения из интернет-источников содержат такие примеры реализации претекстинга в рамках телефонного мошенничества, как “Банковская карта заблокирована”, “Родственник попал в ДТП”, “Получение компенсации за БАД”, “Выигрыш в лотерее”, “Банковский счет заблокирован в связи с попыткой нелегального перевода в недружественную страну”» [Зотина 2023, с. 33].

Помимо телефонного мошенничества претекстинг получил широкое распространение при проведении атак социальной инженерии в социальных сетях. Сравнительная характеристика атак социальной инженерии показана на рис. 1.

Отчет Verizon 2023 Data Breach Investigations Report, представленный компанией Verizon Business, показал, что «атаки с использованием претекстинга в 2023 г. составляли более 50% всех атак с использованием методов социальной инженерии»[5]. Исследование, проведенное компанией Positive Technologies, показывает, что «социальные сети являются одним из самых распространенных каналов для атак социальной инженерии, ключевым элементом которых являются техники фишинга и претекстинга»[6].

---

[4] Телефонное мошенничество 2024 // ВЦИОМ. Новости. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения 26.03.2024).

[5] Verizon 2023 – Verizon 2023 Data Breach Investigations Report // Verizon. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения 24.03.2024).

[6] Cybersecurity threatscape 2023 – Cybersecurity threatscape: Q3 2023 // Positive Technologies. URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/ (дата обращения 23.03.2024).

Критерий	Претекстинг по телефону	Претекстинг в социальной сети
Вредоносное воздействие	Атака социальной инженерии с использованием техники претекстинга по телефону	Атака социальной инженерии с использованием претекстинга в социальной сети
Источник угрозы	Мобильный телефон, смартфон	Социальная сеть
Уязвимость	Телефонный звонок злоумышленника потенциальной жертве	Отправка сообщения в социальной сети злоумышленником потенциальной жертве
Объект воздействия	Пользователь мобильного телефона	Пользователь социальной сети
Способ реализации угрозы	Техника претекстинга	

Рис. 1. Сравнительная характеристика атак

Анализ публикаций по проблемам противодействия методам социальной инженерии в социальных сетях демонстрирует возрастающий интерес ученых к данной области исследований. В рамках контент-анализа публикаций в базах научных публикаций eLibrary, Scopus, Google Scholar за последние 10 лет были подобраны ключевые слова, которые описывают тематику публикаций по соответствующей области исследований.

На рис. 2 представлены количественные результаты публикационной активности по теме исследования за последние 10 лет (с 2014 по 2023 г.), которые показывают рост публикаций по проблемам противодействия методам социальной инженерии в социальных сетях.

В качестве основы комбинаций для поисковых запросов использовались комбинации ключевого слова «социальные сети/social networks» со следующим набором ключевых слов: «социальная инженерия/social engineering», «социоинженерные атаки/social engineering attacks», «защита информации/data protection/information protection», «информационная безопасность/information security».

Рис. 2. Результаты публикационной активности eLibrary, Scopus, Google Scholar за последние 10 лет (с 2014 по 2023 г.)

Рис. 3. Результаты публикационной активности по ключевому слову «претекстинг/pretexting» в базах публикаций eLibrary, Scopus, Google Scholar за последние 10 лет (с 2014 по 2023 г.)

Проведенный анализ публикаций по проблеме претекстинга как метода социальной инженерии также демонстрирует возрастающий интерес ученых к данной области исследований. На рис. 3 представлены количественные результаты публикационной активности по ключевому слову «претекстинг» за последние 10 лет (с 2014 по 2023 г.), которые показывают рост публикаций по проблеме претекстинга.

Отметим, что исследований, посвященных проблеме претекстинга в социальных сетях (публикации, содержащие ключевые слова «претекстинг/pretexting», «социальные сети / social media»), выявлено недостаточно (рис. 4).

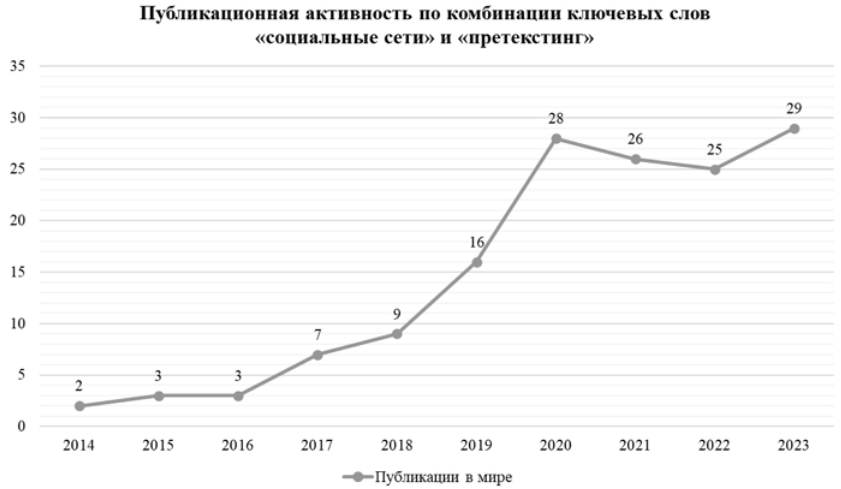

Рис. 4. Результаты публикационной активности по комбинации ключевых слов «социальные сети/social media» и «претекстинг/pretexting» в базах публикаций eLibrary, Scopus, Google Scholar за последние 10 лет (с 2014 по 2023 г.)

Заключение

Таким образом, исследования, посвященные проблемам информационной безопасности в социальных сетях, становятся более актуальными. Следует отметить, что социальные сети являются одной из основных площадок для обмена информацией как в Российской Федерации, так и во всем мире. Месячный охват самых популярных социальных сетей в России (ВКонтакте, Telegram и т. д.)

составляет более 80 млн пользователей в месяц, что делает их более привлекательными для злоумышленников.

Одной из актуальных проблем, с которыми сталкиваются пользователи социальных сетей, является проблема защищенности пользователей от атак социальной инженерии с использованием техники фишинга и претекстинга. При этом отметим, что в последние годы наблюдается рост числа исследований, посвященных изучению претекстинга как метода социальной инженерии, однако количество исследований, посвященных проблеме претекстинга в социальных сетях, остается недостаточным.

Опасность претекстинга как метода социальной инженерии неоспорима. С использованием техники претекстинга злоумышленники могут получить доступ к персональным данным, конфиденциальной информации, а также к денежным средствам своих жертв. Кроме того, претекстинг может быть комбинирован с другими методами социальной инженерии, в частности с фишингом, что делает такие атаки еще более опасными.

Следовательно, в целях противодействия атакам претекстинга в социальных сетях необходимо разработать модели и методики противодействия соответствующим атакам. При этом одним из возможных подходов является обучение пользователей социальных сетей основам безопасности в социальных сетях и выявлению атак социальной инженерии с использованием претекстинга. Это может быть достигнуто путем проведения информационных кампаний, разработки обучающих материалов и тренировочных сценариев, которые помогут пользователям социальных сетей распознавать атаки социальной инженерии с использованием претекстинга и принимать соответствующие меры для предотвращения подобных атак.

Таким образом, проблема социоинженерных атак с использованием претекстинга чрезвычайно важна. Работы по обеспечению информационной безопасности в социальных сетях можно развивать в следующих направлениях:

1) разработка эффективных алгоритмов, направленных на обнаружение социоинженерных атак в социальных сетях;
2) разработка и внедрение методики противодействия социоинженерным атакам с использованием претекстинга, которая обеспечивает повышение уровня осведомленности пользователей социальных сетей о реализации подобных атак.

Литература

Абдуллаева 2015 – *Абдуллаева Р.А.* Анализ влияния социальных сетей на жизнь современного общества // Международный журнал прикладных и фундаментальных исследований. 2015. № 9–3. С. 542–546.

Аникина, Соколов 2024 – *Аникина Н.А., Соколов Н.А.* Фишинг и мошенничество в настоящее время // Территория науки и образования. 2024. № 1. С. 85–87.

Апатова, Минабилева, 2021 – *Апатова Н.В., Минабилева М.Н.* Проблемы безопасности данных в социальных сетях // Проблемы информационной безопасности социально-экономических систем: VII Всероссийская научно-практическая конференция с международным участием, Гурзуф, 18–20 февраля 2021 г. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2021. С. 100–101.

Брославский, Полянский 2020 – *Брославский П.В., Полянский С.С.* Роль социальных сетей в формировании информационного общества // Высокие технологии, наука и образование: актуальные вопросы, достижения и инновации: Сборник статей VII Всероссийской научно-практической конференции, Пенза, 27 июня 2020 г. Пенза: Наука и Просвещение, 2020. С. 229–231.

Ветцель 2020 – *Ветцель К.Я.* Социальные медиа и социальные сети: проблемы терминологии и модели взаимодействия пользователей // Международный научно-исследовательский журнал. 2020. № 9-1 (99). С. 139–141.

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Дьяков 2020 – *Дьяков Н.В.* Применение методов социальной инженерии в социальных сетях // Общество. 2020. № 2 (17). С. 126–128.

Замолоцких, Сидоренко 2020 – *Замолоцких В.С., Сидоренко В.Г.* Киберугрозы в социальных сетях // Информатизация образования и науки. 2020. № 4 (48). С. 66–75.

Захлевная 2023 – *Захлевная И.И.* Социальная инженерия: актуальная угроза и меры защиты // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова: Сборник докладов Международной научно-технической конференции молодых ученых БГТУ им. В.Г. Шухова, Белгород, 16–17 мая 2023 года. Часть 17. Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. С. 409–412.

Зотина 2023 – *Зотина Е.В.* Антропология телефонного мошенничества с использованием претекстинга: криминологическое исследование // Мониторинг правоприменения. 2023. № 2 (47). С. 32–38. DOI: 10.21681/2226-0692-2023-2-32-38.

Иванько и др. 2020 – *Иванько А.Ф., Иванько М.А., Лихтина Е.К.* Социальные сети, как элемент информационных технологий // Научное обозрение. Фундаментальные и прикладные исследования. 2020. № 1. URL: https://scientificreview.ru/ru/article/view?id=77 (дата обращения 18.03.2024).

Кудрявцев, Щекочихин 2018 – *Кудрявцев О.А., Щекочихин О.В.* Фишинг в электронной почте, sms-сообщениях, мессенджерах и социальных сетях // Поведение молодежи в современном интернет-пространстве: стратегии, риски, защита: Сборник статей Всероссийской студенческой научно-практической конференции, Орехово-Зуево, 15 мая 2018 года. Орехово-Зуево: Государственный гуманитарно-технологический университет, 2018. С. 22–26.

Лосяков, Слесарев 2016 – *Лосяков А.В., Слесарев Ю.В.* Правовое регулирование размещения и защиты персональных данных в социальных сетях // XXI век: итоги прошлого и проблемы настоящего плюс. 2016. № 4 (32). С. 143–147.

Митник, Саймон 2004 – *Митник К.Д., Саймон В.Л.* Искусство обмана. М.: Компания АйТи, 2004. 359 с.

Нилин, Чугунова 2020 – *Нилин П.А., Чугунова О.В.* Исследование способов борьбы с фишинг-атаками // Инновации в информационных технологиях, машиностроении и автотранспорте (ИИТМА-2020): Сборник материалов IV Международной научно-практической конференции с онлайн-участием, Кемерово, 7–10 декабря 2020 года. Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2020. С. 89–91.

Табашникова, Яговцева 2023 – *Табашникова К.С., Яговцева А.А.* Социальные сети как инструмент продвижения бизнеса на территории Российской Федерации в реалиях 2023 года // Молодой ученый. 2023. № 4 (451). С. 436–438.

Филиппов 2012 – *Филиппов П.Б.* Использование и реализация защиты персональных данных в социальных сетях Интернета // Прикладная информатика. 2012. № 2 (38). С. 71–77.

Фомина 2015 – *Фомина Н.А.* Использование методов социальной инженерии при мошенничестве в социальных сетях // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: Материалы внутривузовской конференции, Магнитогорск, 9–12 октября 2015 г. Магнитогорск: Магнитогорский государственный технический университет, 2015. С. 443–453.

Хэднеги 2020 – *Хэднеги К.* Искусство обмана: Социальная инженерия в мошеннических схемах. М.: Альпина Паблишер, 2020. 282 с.

References

Abdullaeva, R.A. (2015), “Analysis of social networks influence on the life of modern society”, *International Journal of Applied and Fundamental Research*, no. 9-3, pp. 542–546.

Anikina, N.A. and Sokolov, N.A. (2024), “Phishing and fraud at the present time”, *Territory of science and education*, no. 1, pp. 85–87.

Apatova, N.V. and Minabileva, M.N. (2021) “Issues of data security in social networks“, Issues *of information security of socio-economic systems: VII All-Russian scientific and practical conference with international participation*, Gurzuf, 18–20 February 2021, V.I. Vernadsky Crimean Federal University, Simferopol, Russia, pp. 100–101.

Broslavskii, P.V. and Polyanskii, S.S. (2020), "The role of social networks in the formation of the information society", *High technologies, science and education: current issues, achievements and innovations: Collection of articles of the VII All-Russian Scientific and Practical Conference*, Penza, June 27, 2020, Nauka i Prosveshchenie, Penza, Russia, pp. 229–231.

Dyakov, N.V. (2020), "Application of social engineering methods in social networks", *Society*, no. 2 (17), pp. 126–128.

Filippov, P.B. (2012) "Use and implementation of personal data protection in social networks of the Internet", *Applied informatics*, no. 2 (38), pp. 71–77.

Fomina, N.A. (2015), "The use of social engineering methods in fraud on social networks", *Information security and issues of preventing cyber extremism among youth: Proceedings of the intra-university conference*, Magnitogorsk, 9–12 October 2015, Magnitogorsk State Technical University, Magnitogorsk, Russia, pp. 443–453.

Grishina, N.V. (2022), "Analysis of the dynamics of personal data leakage in the context of the implementation of the program 'Digital Economy of the Russian Federation' ", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 34–43.

Hadnegy, K. (2020), *The art of deception: Social engineering in fraudulent schemes*, Alpina Publisher, Moscow, Russia. 282 p.

Ivanko, A.F., Ivanko, M.A. and Likhtina, E.K. (2020), "Social networks as an element of information technology", *Scientific Review. Basic and applied research*, no. 1.

Kudryavtsev, O.A. and Shchekochikhin, O.V. (2018) "Phishing in email, SMS messages, instant messengers and social networks", *Youth behavior in the modern Internet space. Strategies, risks, protection. Collection of articles of the All-Russian Student Scientific and Practical Conference*, Orekhovo-Zuyevo, 15 May 2018, State University of Humanities and Technology, Orekhovo-Zuyevo, Russia, pp. 22–26.

Losyakov, A.V. and Slesarev, Yu.V. (2016) "Legal regulation of placement and protection of personal data in social networks", *21st century. Results of the past and issues of the present plus*, no. 4 (32), pp. 143–147.

Mitnik, K.D. and Simon, V.L. (2004) *The art of deception*, IT Company, Moscow, Russia, 359 p.

Nilin, P.A. and Chugunova, O.V. (2020) Research on ways to combat phishing attacks, *Innovations in information technologies, mechanical engineering and motor transport (IITMA-2020): collection of materials of the IV International scientific and practical conference with online participation*, Kemerovo, 7–10 December 2020, T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia, pp. 89–91.

Tabashnikova, K.S. and Yagovtseva, A.A. (2023), "Social networks as a tool for promoting business on the territory of the Russian Federation in the realities of 2023", *Young scientist*, no. 4 (451), pp. 436–438.

Wetzel, K.Y. (2020) "Social media and social networks. Issues of terminology and models of user interaction", *International scientific research journal*, no. 9-1 (99), pp. 139–141.

Zakhlevnaya, I.I. (2023) "Social engineering: current threat and protective measures", *International scientific and technical conference of young scientists of Belgorod Shukhov State Technological University: Collection of reports of the International Scientific and Technical Conference of Young Scientists of Belgorod Shukhov State Technological University*, Belgorod, 16–17 May 2023. Part 17, Belgorod Shukhov State Technological University, Belgorod, Russia, pp. 409–412.

Zamolotskikh, V.S. and Sidorenko, V.G. (2020) "Cyber threats in social networks", *Informatization of education and science*, no. 4 (48), pp. 66–75.

Zotina, E.V. (2023) "Anthropology of telephone fraud using pretexting: criminological research", *Law Enforcement Monitoring*, no. 2 (47), pp. 32–38.

Информация об авторах

Валерий К. Маркелов, аспирант, Ивановский государственный университет, Шуйский филиал, Шуя, Россия; 155908, Россия, Ивановская область, Шуя, ул. Кооперативная, д. 24; v.a.l.e.m.a.r.k@yandex.ru

Александр Н. Привалов, доктор технических наук, профессор, Тульский государственный педагогический университет им. Л.Н. Толстого, Тула, Россия; 300026, Тульская область, Тула, проспект Ленина, д. 125;

Ивановский государственный университет, Шуйский филиал, Шуя, Россия; 155908, Россия, Ивановская область, Шуя, ул. Кооперативная, д. 24; privalov.61@mail.ru

Information about the authors

Valerii K. Markelov, postgraduate student, Ivanovo State University, Shuya branch, Shuya, Russia; 24, Kooperativnaya St., Shuya, Ivanovo region, 155908, Russia; v.a.l.e.m.a.r.k@yandex.ru

Aleksandr N. Privalov, Dr. of Sci. (Mechanical Engineering), associate professor, Tula State Lev Tolstoy Pedagogical University, Tula, Russia; 125, Lenin Av., Tula, 300026, Russia;

Ivanovo State University, Shuya branch, Shuya, Russia; 24, Kooperativnaya Str., Shuya, Ivanovo region, 155908, Russia; privalov.61@mail.ru

УДК 004.56:027
DOI: 10.28995/ 2686-679X-2024-3-87-103

Информационная безопасность библиотечных систем предприятий

Вероника С. Назаровская
Российский государственный гуманитарный университет, Москва, Россия, nazarovskaya2380@mail.ru

Дмитрий Н. Баранников
Российский государственный гуманитарный университет, Москва, Россия, d.2006@mail.ru

Ирина А. Русецкая
Российский государственный гуманитарный университет, Москва, Россия, irkom@mail.ru

Аннотация. В статье раскрывается проблематика использования электронных ресурсов, находящихся в библиотечных системах предприятий и их защита от различных негативных воздействий. Рассматриваются вопросы обеспечения безопасности цифровых и физических носителей информации, находящихся в библиотеках, а также обосновывается важность сохранения традиционных функций библиотек в условиях перехода библиотечных подразделений на цифровые технологии. Подчеркивая удобство использования современных технологий, включая системы искусственного интеллекта и технологии больших данных, авторы обращают внимание на модифицирующиеся внутренние и внешние источники угроз информационной безопасности, влияющие на библиотечные системы. Внимание уделяется вопросам информационной безопасности, классификации угроз и методам их предотвращения. В статье также затрагиваются вопросы обучения и повышения квалификации библиотечных сотрудников. Рассматриваются мероприятия, которые позволяют повысить уровень знаний сотрудников по оценке рисков воздействия на информацию и принимать меры, снижающие (исключающие) случаи утечки или утраты информации в библиотечных системах. В статье уделяется внимание особенностям защиты информационных ресурсов электронных библиотек; выделяются основные объекты защиты; рассматриваются вопросы разграничения доступа к электронным библиотечным ресурсам пользователей различных категорий.

Ключевые слова: информационная безопасность, защита информации, библиотека, библиотечные системы

Для цитирования: Назаровская В.С., Баранников Д.Н., Русецкая И.А. Информационная безопасность библиотечных систем предприятий // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 87–103. DOI: 10.28995/ 2686-679X-2024-3-87-103

Information security of enterprise library systems

Veronika S. Nazarovskaya
Russian State University for the Humanities, Moscow, Russia, nazarovskaya2380@mail.ru

Dmitrii N. Barannikov
Russian State University for the Humanities, Moscow, Russia, d.2006@mail.ru

Irina A. Rusetskaya
Russian State University for the Humanities, Moscow, Russia, irkom@mail.ru

Abstract. The article reveals the problematics of using electronic resources located in the library systems of enterprises and their protection from various negative influences. It considers the issues of ensuring the security of digital and physical information media located in libraries, and substantiates the importance of preserving the traditional functions of libraries in the context of the transition of library departments to digital technologies. Emphasizing the ease of use of modern technologies, including artificial intelligence systems and Big Data technologies, the authors draw attention to the modifying internal and external sources of information security threats affecting library systems. Attention is paid to information security issues, classification of threats and methods of their prevention. The article also touches on the issues of training and advanced training of library staff. Activities are being considered that increase staff knowledge of information exposure risk assessments and take actions that reduce (eliminate) cases of information breaches or loss in library systems. The article pays attention to the features of protecting information resources of digital libraries; the main objects of protection are highlighted; the issues of delimiting access to electronic library resources of users of various categories are considered.

Keywords: information security, information protection, library, library systems

For citation: Nazarovskaya, V.S., Barannikov, D.N. and Rusetskaya, I.A. (2024), "Information security of enterprise library systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 87–103, DOI: 10.28995/ 2686-679X-2024-3-87-103

Введение

Библиотека в широком смысле представляет собой значимое для различных слоев населения общественное учреждение с давними традициями, уверенно закрепившее свое влияние в разнообразных аспектах жизни людей.

Библиотечный фонд нашел и продолжает занимать достойное место в общественной жизни людей, учебных заведений, научно-исследовательских институтов, предприятий.

До недавнего времени библиотечные фонды успешно справлялись с хранением, передачей и использованием физических информационных ресурсов. Однако цифровая обработка информации эволюционно вошла в библиотечную сферу, и технический прогресс привнес инновационные подходы: изменилась нормативно-правовая база, автоматизировались процессы, были введены новые средства хранения и передачи информации.

Процессы модернизации, происходящие в промышленности, в первую очередь ориентированные на получение экономического эффекта и конкурентных преимуществ, привели к естественной эволюции существующих взглядов в библиотечной сфере, что предопределило линию развития используемых технологий. Массовое использование программно-аппаратных ресурсов библиотечных систем обеспечило упрощение ручного труда сотрудников библиотек, а рутинные процессы переместило в сферу информационных технологий.

Удобство использования информационных технологий (далее – ИТ) актуализируется переводом библиотечных коллекций в цифровой формат, что расширяет возможности изучения фондов, также упрощает пользование имеющимися интеллектуальными ресурсами. Прогресс в области ИТ делает цифровизацию фондов библиотек крайне важной. Например, шаги, предпринятые московским правительством, позволили в пилотном режиме интегрировать инновационные технологии в жизнь: через портал мэра Москвы жители города могут быстро заказывать и бронировать необходимую литературу в любой библиотеке. Во всех московских библиотеках функционирует унифицированная цифровая система, которая позволяет посетителям, оформившим читательский билет, использовать его в различных филиалах. Эта эффективная система упрощает работу библиотечных сотрудников и обеспечивает пользователям возможность быстро находить необходимые печатные и цифровые издания[1].

[1] Библиотеки нового поколения: как Москва стала одним из самых читающих городов страны // Официальный сайт мэра Москвы. URL: https://www.mos.ru/news/item/115323073/ (дата обращения 06.10.2023).

Согласно действующему в России Федеральному закону «О библиотечном деле» от 29.12.1994 № 78-ФЗ, библиотеки выполняют информационные, культурные и образовательные функции, для реализации которых требуются специфические ресурсы и инструменты. В частности, образовательная роль библиотеки подразумевает наличие образовательных материалов. В условиях оборота больших объемов информационных потоков особую актуальность приобретает использование технологий для цифровизации этих образовательных ресурсов; примеры таких технологий демонстрируются на рис. 1.

Рис. 1. Технологии цифровизации образовательных ресурсов библиотек

С развитием ИТ и запуском процессов цифровизации различных областей жизни общества библиотеки как институты испытывают значительные трансформации. В качестве наглядного примера можно рассмотреть изменения, происходящие в сфере высшего образования. Дополнительные учебные материалы, практические и лабораторные задания все чаще предоставляются студентам исключительно в электронном формате, поскольку именно так они позволяют студентам продолжать учебный процесс, не только находясь в стенах учебных аудиторий, но и используя возможности обучения в любом удобном пространстве. Однако библиотечный ресурс продолжает выполнять свою традиционную функцию хранения знаний, предоставляя доступ к интеллектуальным базам не только в электронном виде. Несмотря на активную цифровизацию библиотечных фондов, многие библиотеки сохраняют практику предоставления читальных залов для индивидуальной и групповой работы, что остается важным и актуальным, так как работа с книгой, отпечатанной типографским способом, не во всех случаях может быть заменена на процедуру использования цифровых технологий. Однако электронный ресурс имеет ряд достоинств по объему

обрабатываемой информации, скорости получения данных, следовательно, процесс цифровизации активно используется в сферах, где необходимо обработать большой объем информации в короткие сроки. Учитывая особенности современного обучения, можно уверенно сказать, что имеющиеся потребности как студентов, так и преподавательского состава необходимо удовлетворять с помощью использования технологий цифрового формата. Для проведения различных занятий используются такие ключевые атрибуты, как Wi-Fi роутер, проводное интернет-соединение, а также оборудование для печати. Кроме того, читальный зал следует оснастить персональными компьютерами, на которых будут установлены разнообразные прикладные программы. Все перечисленное техническое оборудование может являться источником дестабилизирующего воздействия на информационные ресурсы. Тем самым в настоящее время вопрос информационной безопасности (далее – ИБ) библиотечных систем остается по-прежнему весьма актуальным.

Целью данной работы является анализ современных проблем обеспечения ИБ библиотечных ресурсов предприятий как традиционного, так и цифрового форматов.

Библиотечные системы предприятий

Предприятия содержат библиотеки для хранения книжных и научных фондов. Наличие данных структурных подразделений необходимо для приобретения, циркуляции и хранения знаний. В пример можно привести Объединенную промышленную корпорацию «Обонпром», одну из самых значительных ассоциаций предприятий машиностроительной отрасли в России[2], в библиотеке которой в общедоступном режиме представлены различные цифровые издания, классифицированные по нескольким рубрикам:

- Обычные вооружения;
- Авиационная промышленность;
- Ракетно-космическая промышленность;
- Судостроительная промышленность;
- Радиоэлектронная промышленность;
- Атомная промышленность;
- Общая оборонная промышленность;
- Архивы;
- Справочники.

[2] Библиотека // Obon-prom. URL: https://oboron-prom.ru/biblioteka.html (дата обращения 09.12.2023).

Часть материалов электронной библиотеки находится полностью в открытом доступе, поэтому обратиться к ним может любой пользователь сети Интернет.

Однако большинство предприятий имеют также закрытые информационные ресурсы и библиотеки, предназначенные для внутреннего использования сотрудниками, занимающимися исследованиями и разработками. Так, на предприятиях имеются технические библиотеки, в которых хранится документация на продукцию, чертежи изделий и т. д. Данные ресурсы могут иметь ограниченный доступ различных категорий, например, относиться к служебной информации ограниченного распространения, на носители которой наносится пометка «Для служебного пользования»[3]. В соответствии с пунктом 2.1 Положения № 1233, решение о проставлении пометки «Для служебного пользования» на документах, содержащих конфиденциальную информацию, принимается исполнителем и должностным лицом, ответственным за подписание или утверждение данного документа. Как указано в пункте 1.6 того же Положения, должностные лица, уполномоченные руководством государственного органа или государственной корпорации для отнесения служебной информации к ограниченной по использованию, несут персональную ответственность за обоснованность принятого решения. Согласно статье 13.14 Кодекса Российской Федерации об административных правонарушениях, лицо, получившее доступ к информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), и разгласившее эту информацию в связи с исполнением служебных или профессиональных обязанностей, подлежит наложению административного штрафа в размере от пятисот до одной тысячи рублей для граждан и от четырех тысяч до пяти тысяч рублей для должностных лиц.

Важность обеспечения ИБ библиотечных систем предприятий определяется следующими факторами:

– возрастание объема данных, хранящихся в библиотечных системах;

[3] Постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» от 03.11.1994 № 1233 1994 г. Ст. 1 с изм. и допол. в ред. от 06.08.2020 // Информационно-правовой портал ГАРАНТ.РУ. URL: https://base.garant.ru/188429/ (дата обращения 09.12.2023).

– важность результатов исследований и технических разработок, проводимых для нужд предприятий для экономики и безопасности страны;
– возможность роста ценности определенной информации;
– совершенствование современных информационных и телекоммуникационных технологий, используемых как для обработки, хранения и предоставления пользователям информации, так и для несанкционированного доступа к контенту библиотечных систем;
– невнимание руководителей и сотрудников библиотек к вопросам ИБ и недостаточная подготовка в этой сфере [Рахматуллаев 2019].

Таким образом, задача защиты информационных ресурсов библиотек предприятий является актуальной. Для повышения эффективности систем защиты информации необходимы дополнительные исследования по вопросам выявления и нейтрализации уязвимостей в существующих системах обеспечения безопасности данных в библиотеках.

Теоретические аспекты защиты информации в библиотеках

Защита информационных ресурсов производственных библиотек обладает определенной спецификой. В частности, библиотекам необходимо предоставлять ресурсы посетителям и пользователям библиотечной системы и при этом проводить мероприятия, направленные на защиту этих ресурсов от, например, потери и различных других отрицательных воздействий, которые являются факторами угроз безопасности библиотечных систем[4].

Исходя из классического подхода, источники угроз разделяют на внутренние и внешние.

Внутренние угрозы могут проявляться в следующих формах:
– непреднамеренные ошибки сотрудников библиотеки и администраторов библиотечных систем;
– неквалифицированное выполнение сотрудниками обязанностей, приводящее к утечке и утрате информации;
– ошибки в работе автоматизированных библиотечных систем; программно-аппаратные сбои и пр.

[4] Сервер – под замок, или Как минимизировать риски // Журнал «Библиотечное дело». URL: http://www.bibliograf.ru/issues/2007/2/66/0/655/ (дата обращения 02.11.2023).

К формам проявления внешних угроз, например, относятся:
– вирусные и другие вредоносные программные атаки;
– доступ несанкционированных пользователей;
– аварии, пожары, техногенные происшествия;
– информационный мониторинг и вмешательство со стороны конкурентов и недоброжелателей и др.

Исследователь А.С. Карауш выделяет причины возникновения повреждения данных, которые представлены на рис. 2. К ним относятся:
– неумышленные ошибки человека, составляющие до 52% от общего числа причин возникновения повреждения данных;
– отказ техники – до 10% случаев;
– повреждения водой – до 10% случаев;
– умышленные действия человека – до 10% случаев;
– повреждения в результате пожара – до 15% случаев;
– другое – до 3% случаев [Алешин 2005].

Рис. 2. Диаграмма «Причины повреждения данных»

По данным статистики, случайные или неосознанные действия человека составляют большую часть всех причин, приводящих к повреждению данных или потере информации. Также можно сделать вывод о том, что современная система устройства библиотеки обладает определенными недостатками. Для обеспечения эффек-

тивной защиты информации в библиотеках авторы статьи акцентируют внимание на двух необходимых аспектах защиты данных, на которые важно обратить внимание. К ним относятся:

1. Использование современных цифровых технологий.

2. Проведение обучения для работников библиотек по основам взаимодействия с информационными системами и изучению принципов обеспечения ИБ.

Использование в библиотеках современных цифровых технологий

В силу того, что библиотечные системы проходят этап модернизации и внедрения современных достижений, естественным шагом является переход к созданию полноценных электронных библиотек и многие бизнес-процессы библиотечных организаций автоматизируются и подвергаются активной цифровизации. В связи с этим информационный ресурс должен быть защищен с помощью технологий, направленных на защиту информации как от внешних воздействий, так и от внутренних нарушений [Егорова 2022].

Защита ресурсов электронных библиотек требует особого внимания для предприятий, выполняющих работы в сфере обеспечения обороноспособности страны в рамках промышленных объектов, имеющих стратегическое значение для национальной безопасности государства. Научно-исследовательские, учебные, справочные и др. материалы, составляющие ресурсы таких цифровых библиотек, нуждаются в обеспечении доступности, целостности и конфиденциальности информации [Крюкова 2020].

Нормативно-методическое обеспечение деятельности по защите цифровых библиотечных ресурсов составляют, в частности, Федеральный закон «Об информации, информационных технологиях и о защите информации», устанавливающий правила использования информации, права и обязанности ее обладателей, порядок доступа к информации и ее распространения; национальный стандарт ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», в котором описывается создание и поддерживание эффективной системы управления информационной безопасностью; ГОСТ Р ИСО/МЭК 27000 – 2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности», который устанавливает основные понятия, принципы и требования к ИБ информационных систем и др. документы.

В настоящее время особую актуальность приобретает Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». Искусственный интеллект (далее – ИИ) находит свое применение в различных областях деятельности человека, включая библиотечные учреждения. Так, в Российской государственной библиотеке в подразделении R&D[5] технологии ИИ уже применяются для того, чтобы разделять газетные полосы на отдельные статьи[6].

В качестве примера применения технологий ИИ можно отметить, что Электронно-библиотечная система «Лань» в сотрудничестве со специалистами из Томского государственного университета работает над созданием сервиса для каталогизации, который базируется на применении технологий ИИ. Процесс каталогизации достаточно трудоемок, но без него не обходится ни одна отрасль. Поэтому благодаря этой инновации удастся значительно ускорить процесс работы с продукцией как на этапе разработки, так и в процессе ее эксплуатации. Разработчики отмечают, что новая система сможет автоматизировать процесс распределения изданий по тематическим категориям и областям знаний. Данную задачу ранее приходилось выполнять вручную[7].

В электронной библиотеке к основным объектам, подлежащим защите, относятся: базы данных (публикаций, читателей, инцидентов и т. д.), веб-сайты, оборудование (серверное, сетевое, служебное), программное обеспечение [Федякова 2016]. Все эти объекты необходимо защищать на каждом этапе функционирования библиотечной системы.

Одним из важнейших факторов при обеспечении безопасности библиотечных ресурсов является разграничение прав доступа различных категорий пользователей. При этом возможны, например, следующие формы доступа:

– открытый;
– ограниченный по времени;

---

[5] Research and Development – исследование и развитие

[6] Потребуется 2 тысячи лет, чтобы оцифровать весь фонд «Ленинки»: гендиректор РГБ Вадим Дуда – о цифровой трансформации библиотеки // TAdviser. URL: https://www.tadviser.ru/index.php/Потребуется_2_тысячи_лет,_чтобы_оцифровать_весь_фонд_Ленинки:_гендиректор_РГБ_Вадим_Дуда_-_о_цифровой_трансформации_библиотеки. (дата обращения 02.11.2023).

[7] Экосистемное решение для смешанного обучения // АККРЕДИТАЦИЯ В ОБРАЗОВАНИИ: информационно-аналитический журнал. URL: https://akvobr.ru/new/publications/267 (дата обращения 15.10.2023).

– удостоверяемый электронной подписью;
– предоставляемый только с определенных IP-адресов;
– предоставляемый только для читателей, имеющих право допуска к информации ограниченного распространения, и т. п. [Койнов 2016].

Объекты защиты, в том числе ресурсы библиотечных систем, нуждаются в оценке угроз безопасности, построении модели угроз и определении мер реагирования на происходящие инциденты ИБ, а также их предупреждение и нейтрализацию.

Обучение сотрудников библиотеки требованиям обеспечения информационной безопасности

Наряду с обеспечением безопасности автоматизированных информационных библиотечных систем не менее важными являются организационно-технические меры обеспечения безопасности библиотек [Рубчинская 2019].

Одним из направлений организационной работы в этой сфере является работа с персоналом библиотек по обучению ИБ.

В стремительно развивающемся мире для того, чтобы быть востребованным сотрудником, необходимо обладать навыками использования современной техники, знать принципы работы программного обеспечения, установленного на устройствах, и многое другое.

Можно выделить следующие виды обязанностей сотрудников библиотеки:

1. Работа с автоматизированной информационно-библиотечной системой, компонентами которой, например, являются:
   - знание функциональных возможностей системы;
   - навыки пользования компьютерной техникой;
   - умение решить нестандартные ситуации в процессе обслуживания посетителей и др.
2. Работа с аппаратурой в читальных залах и на пунктах книговыдачи:
   - подключение периферийных устройств;
   - выполнение услуг печати для посетителей библиотеки;
   - определение проблем и починка вышедших из строя устройств, таких как Wi-Fi-роутер;
   - выявление проблем при работе с персональным компьютером и/или удаленным рабочим столом и др.
3. Выдача литературы посетителям.

4. Регистрация посетителей в библиотечной системе.
5. Оформление сдачи литературы в пунктах книговыдачи.
6. Помощь посетителям читальных залов с работой в персональных компьютерах:
   - помощь с включением ПК;
   - помощь с входом в учетную запись;
   - помощь в скачивании файлов;
   - помощь в освоении предоставляемых библиотекой ресурсов закрытого и открытого доступа;
   - помощь в работе с сайтом библиотеки и др.

Количество пунктов в данном списке дает понять, что библиотекарь сейчас – это не только сотрудник, с помощью которого можно получить доступ к библиотечному фонду. Библиотекарь должен владеть множеством различных навыков. Многие исследователи утверждают, что сейчас библиотекарям важно знать не только особенности процесса комплектования книг, но и владеть компьютером, знать принцип работы баз данных, которые лежат в основе библиотечных систем, и множество других важных составляющих библиотечных бизнес-процессов.

Высокие темпы развития технологий иногда вызывают сложности для их восприятия обычными людьми. Для сотрудников библиотек становится обязательным постоянное обучение. Это объясняется тем, что библиотекам необходимо регулярно обновлять свои функции в соответствии с изменениями в области информационных технологий и приспосабливаться к потребностям современных посетителей библиотеки. Сохранение актуальности этих учреждений требует постоянного учета текущих тенденций развития цифровой среды.

ИБ организации напрямую зависит от квалифицированности сотрудников библиотеки.

В качестве примера можно рассмотреть такую форму проявления уязвимости библиотечных ресурсов, как кража. Кража литературы в библиотечных организациях происходит двумя различными способами. Во-первых, остается актуальной кража книжных изданий из читальных залов, несмотря на использование различных технологических меток, таких как RFID. Данные метки, предназначенные для срабатывания при выносе книжных изданий за пределы читального зала, подвержены возможному умышленному извлечению посетителями библиотеки, что позволяет им успешно уносить литературу без обнаружения. Во-вторых, реальную угрозу представляет собой кража документов из электронных каталогов. Доступ к определенным каталогам зависит от наличия привилегий. Например, обучающиеся бакалавриата ограничены

в доступе к выпускным квалификационным работам предыдущих лет. Однако с применением взлома систем злоумышленники могут получить доступ к данным файлам, даже если эта литература не предназначена для них.

Соответственно, сотрудники библиотеки должны быть осведомлены о возможных утечках и делать все возможное для их предотвращения. Рано или поздно современные цифровые технологии будут использованы в системах безопасности, поэтому так важно, чтобы сотрудники библиотеки были готовы к этому уже сейчас, так как в ином случае переход на новые системы будет слишком резким и повлечет за собой потерю производительности, ведь сотрудники не будут знать, как их использовать. Для этого необходимо повышать цифровую грамотность кадров. Для помощи в этом деле могут быть привлечены сотрудники молодого поколения, лучше разбирающиеся в технологиях новых тенденциях. Эти сотрудники будут отличными помощниками для старшего поколения. Сотрудник с многолетним опытом и стажем может обучать молодого сотрудника основным принципам работы с библиотечным фондом, а тот, в свою очередь, может быть полезен при обучении навыкам пользования современной техникой и программами [Адамьянц 2020].

Полноценно автоматизировать выполнение функциональных задач сотрудников библиотеки невозможно, однако технологии, основанные на ИИ, открывают новые возможности. Такие технологии должны не только активно внедряться в бизнес-процессы библиотечных систем различного уровня, но и применяться в целях защиты безопасности данных. Так, Елена Новикова, директор департамента по обеспечению эксплуатации и безопасности Российской государственной библиотеки, в своей статье отмечает неизбежность интеграции технологий Больших данных и искусственного интеллекта для повышения безопасности библиотечной среды[8]. По словам автора, использование данных технологий, например, позволит расширить возможности применения видеонаблюдения не только в целях безопасности, но и для выявлений трендов, востребованных тем или популярных книжных изданий среди посетителей и пользователей библиотечных услуг.

[8] Технологии искусственного интеллекта для безопасности и сохранности фондов Российской государственной библиотеки // Системы безопасности. URL: https://www.secuteck.ru/articles/tekhnologii-iskusstvennogo-intellekta-dlya-bezopasnosti-i-sohrannosti-fondov-rossijskoj-gosudarstvennoj-biblioteki (дата обращения 02.11.2023).

Технологии ИИ весьма эффективны для защиты данных, в том числе конфиденциальных. Применение ИИ при управлении хранилищем данных содействует увеличению производительности системы. Ограничение доступа пользователей в рамках алгоритма функционирования системы способствует усилению ИБ. ИИ, оборудованный встроенными алгоритмами машинного обучения, обеспечивает быструю реакцию на различные ситуации, воздействующие на состояние системы. Снижение влияния человеческого фактора на работу системы способствует ее более эффективному функционированию и глубокому анализу запросов пользователей. Кроме того, мониторинг информации о возможных атаках обеспечивает поддержание высокого уровня безопасности различных систем, в том числе и библиотечных[9]. Таким образом, существуют различные векторы развития ИИ в рамках библиотечных систем.

Заключение

Для защищенности информации на предприятиях и производственных объектах необходимо рассматривать способы обеспечения ИБ структурных подразделений, обеспечивающих хранение и обработку различных документов. Авторы статьи заключили, что местом интеграции знаний является техническая библиотека, содержащая важные информационные ресурсы, включающие как открытую, так и конфиденциальную информацию.

В статье рассмотрены теоретические аспекты защиты информации в библиотечных системах. Затем был проведен анализ применения современных цифровых технологий в целях защиты данных. Как было выяснено, такие технологии, как ИИ и большие данные, уже используются для обеспечения ИБ в библиотеках. Применение систем ИИ может способствовать усилению ИБ за счет ограничения доступа пользователей и быстрого реагирования на изменения в системе благодаря алгоритмам машинного обучения. Также ИИ помогает предотвращать аппаратные и программные неисправности и снижает влияние человеческого фактора на систему, обеспечивая более глубокий анализ пользовательских

[9] *Жилин В.В., Сафарьян О.А.* Искусственный интеллект в системах хранения данных // Advanced Engineering Research (Rostov-on-Don). 2020. № 2. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-sistemah-hraneniya-dannyh (дата обращения 17.11.2023).

запросов и высокий уровень безопасности. Все это открывает новые направления для развития ИИ в библиотечной организации предприятий.

Еще одним важным аспектом обеспечения ИБ предприятий является обучение сотрудников основам работы с информационными системами и принципам ИБ. Сотрудники должны быть в состоянии оценивать риски ИБ и быть готовыми предотвратить возможность утечки или утраты информации и ее носителей.

Литература

Адамьянц 2020 – *Адамьянц А.О.* Математические знания библиотекарей – основа получения профессиональных компетенций // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 3. С. 20–34. DOI: 0.28995/2686-679X-2020-3-20-34.

Алешин 2005 – *Алешин Л.И.* Безопасность в библиотеке. Учеб.-метод. пособие. М.: ЛИБЕРЕЯ-БИБИНФОРМ, 2005. 248 с.

Егорова 2022 – *Егорова Е.А.* Библиотека vs интернет: конкуренты или партнеры? // Вестник Тюменского государственного института культуры. 2022. № 3 (25). С. 94–97.

Койнов 2016 – *Койнов Р.С., Добрынин А.С.* Модель управления доступом типовой библиотечной информационной системы // Вестник Астраханского государственного технического университета. Серия «Управление, вычислительная техника и информатика». 2016. № 4. С. 46–54.

Крюкова 2020 – *Крюкова Е.С.* Модель функционирования электронной библиотеки для анализа ее качества и информационной безопасности // Вопросы оборонной техники. Серия 16 «Технические средства противодействия терроризму». 2020. № 9-10 (147–148). С. 16–22.

Рахматуллаев 2019 – *Рахматуллаев М.А., Норматов Ш.Б.* Защита научно-образовательных ресурсов в информационно-библиотечных системах // Наука и научная информация. 2019. Т. 2. № 2. С. 121–128.

Рубчинская 2019 – *Рубчинская О.В.* Информационная безопасность библиотеки в электронной среде // XLVII Огарёвские чтения: Материалы научной конференции: В 3 ч. Саранск, 6–13 декабря 2018 г. / Сост. А.В. Столяров; отв. за вып. П.В. Сенин. Ч. 3. Саранск: Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва. 2019. С. 224–228.

Федякова 2016 – *Федякова Н.Н., Ивойлов Э.М., Табачников Р.А.* Обеспечение информационной безопасности Электронной библиотеки // Контентус. 2016. № 6 (47). С. 283–291.

References

Adamyants, A.O. (2020) "Librarians' mathematical knowledge as the foundation for building up professional skills", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 20–34, DOI: 10.28995/2686-679X-2020-3-20-34.

Aleshin, L.I. (2005), *Bezopasnost' v biblioteke. Ucheb.-metod. posob* [Security in the library. Study guide manual], LIBEREA-BIBINFORM, Moscow, Russia, 248 p.

Egorova, E.A. (2022), "Library vs Internet. Competitors or partners?", *Bulletin of the Tyumen State Institute of Culture*, no. 3 (25), pp. 94–97.

Fedyakova, N.N. Ivoilov, E.M. and Tabachnikov, R.A. (2016), "Ensuring information security of the Electronic Library", *Contentus,* no. 6 (47), pp. 283–291.

Koynov, R.S. (2016), "Access control model for a typical library information system", *Bulletin of the Astrakhan State Technical University. Series: Management, computer technology and information science*, no. 4, pp. 46–54.

Kryukova, E.S. (2020), "Model of the functioning of an electronic library for analyzing its quality and information security", *Issues of defense technology. Episode 16: Technical means of countering terrorism*, no. 9–10 (147–148), pp. 16–22.

Rakhmatullaev, M.A. and Normatov, Sh.B. (2019), "Protection of scientific and educational resources in information and library systems", *Science and scientific information*, vol. 2, no. 2, pp. 121–128.

Rubchinskaya, O.V. (2019), "Information security of the library in the electronic environment", in Stolyarov, A.V. (compl.) and Senin, P.V. (issuing editor), *XLVII Ogarevskie chteniya: Materialy nauchnoi konferentsii. V 3-kh chastyakh, Saransk, 6–13 dekabrya 2018 g.* [Proceedings of 67th Ogarev scientific conference. In 3 parts, Saransk, December 6–13, 2018, part 3], National Research Mordovian State University named after N.P. Ogarev, Saransk, Russia, pp. 224–228.

Информация об авторах

Вероника С. Назаровская, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; nazarovskaya2380@mail.ru

Дмитрий Н. Баранников, кандидат военных наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; d.2006@mail.ru

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; irkom@mail.ru

Information about the authors

Veronika S. Nazarovskaya, student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; nazarovskaya2380@mail.ru

Dmitrii N. Barannikov, Cand. of Sci. (Military Sciences), associate professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; d.2006@mail.ru

Irina A. Rusetskaya, Cand. of Sci. (History), associate professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; irkom@mail.ru

УДК 004
DOI: 10.28995/2686-679X-2024-3-104-122

Метод определения степени визуального сходства web-страниц для обнаружения фейковых сайтов организаций

Вадим А. Смирнов
Ивановский государственный университет, Ивановская обл., Шуя, Россия, v.a.d.i.m@bk.ru

Аннотация. В статье обосновывается актуальность разработки метода определения степени визуального сходства web-страниц с учетом выделения областей, характеризующих основные блоки сайта, в отображаемом в окне браузера содержимом гипертекстовых документов. Проведен анализ сайтов с целью сбора статистики наличия семантических тегов HTML5 в коде страниц, которая показала недостаточное их распространение для использования при однозначной идентификации верхней и нижней частей сайта, боковых меню и других элементов интерфейса Интернет-ресурса средствами парсинга. Предложен метод, позволяющий определить основные блоки сайта с использованием попиксельного сравнения уменьшенных копий скриншотов различных web-страниц. Проведен анализ существующих методов сравнения изображений, в числе которых: aHash, dHash, pHash, сравнение гистограмм цветов и другие методы. Описана процедура создания снимков отображаемого в окне браузера содержимого гипертекстовых документов, примененная в вычислительном эксперименте, и приведен перечень программных средств, которые были использованы для этой цели. Проверена эффективность существующих методов определения степени сходства изображений для оценки принадлежности web-страницы сайту организации при анализе скриншота проверяемой страницы и изображений подлинного интернет-ресурса. Показана более высокая эффективность разработанного метода для решения той же задачи. Разработанный метод может применяться в дальнейших исследованиях в сфере информационной безопасности при создании программного комплекса для обнаружения фейковой активности.

Ключевые слова: сравнение сайтов, фейковый сайт, сравнение изображений, перцептивный хэш, информационная безопасность

Для цитирования: *Смирнов В.А.* Метод определения степени визуального сходства web-страниц для обнаружения фейковых сайтов организаций // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 104–122. DOI: 10.28995/2686-679X-2024-3-104-122

The method for determining the degree of visual similarity of web pages for detecting fake websites of organizations

Vadim A. Smirnov
Ivanovo State University, Ivanovo region, Shuya, Russia,
v.a.d.i.m@bk.ru

Abstract. The article substantiates the relevance of developing a method for determining the degree of visual similarity of web pages, taking into account the allocation of areas characterizing the main blocks of the site in the contents of hypertext documents displayed in the browser window. The analysis of sites was carried out in order to collect statistics on the presence of HTML5 semantic tags in the page code, which showed their insufficient distribution for use in unambiguous identification of the upper and lower parts of the site, side menus and other interface elements of the Internet resource by parsing. A method is proposed to determine the main blocks of the site using pixel-by-pixel comparison of reduced copies of screenshots of various web pages. The author analyzed existing image comparison methods, including: aHash, dHash, pHash, and compared the color histograms and other methods. There's a description of procedure for creating snapshots of the contents of hypertext documents displayed in the browser window, used in a computational experiment and a list of software tools that were used for the purpose. The effectiveness of existing methods for determining the degree of similarity of images to assess the belonging of a web page to an organization's site was tested when analyzing a screenshot of the page being checked and images of a genuine Internet resource. The higher efficiency of the developed method for solving the same problem is shown. The developed method can be used in further research in the field of information security when creating a software package for detecting fake activity.

Keywords: site comparison, fake site, image comparison, perceptual hash, information security

For citation: Smirnov, V.A. (2024), "The method for determining the degree of visual similarity of web pages for detecting fake websites of organizations", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 104–122, DOI: 10.28995/2686-679X-2024-3-104-122

Введение

Последние годы характеризуются существенным ростом объема фейковой активности в сети Интернет. Экспертами ГК «Солар» был отмечен рост более чем в два раза количества под-

дельных сайтов, маскирующихся под сервисы Google[1]. Исследователи компании BI.ZONE отмечают рост количества сайтов с фейковыми розыгрышами призов[2]. В то же время в исследованиях в области информационной безопасности указывается на необходимость защиты пользователей сети Интернет от «деструктивного воздействия информации, не являющейся нейтральной, то есть имеющей целью получения какого-либо нежелательного для субъекта, к которому она обращена, результата» [Баранников, Русецкая 2024, с. 67]. Подобные инциденты обуславливают необходимость разработки новых методов противодействия распространению фейковой информации, а также поиска существующих методов, уже применяемых в других задачах, которые могут быть использованы и в области обеспечения защиты от угроз со стороны фейковой активности.

В числе методов, модификация и использование которых необходимы в данной области, могут выступать общеизвестные методы, применяемые для анализа различных характеристик интернет-ресурсов. Перечень возможных подходов к проведению подобного анализа приведен в публикации [Тюрин 2020], где автор исследует возможность создания информационной системы для поиска функциональных изменений на web-странице. Автор обосновывает необходимость применения подобной системы тем, что именно новый функционал сайта наиболее вероятно содержит какие-либо уязвимости, еще не обнаруженные пентестерами. В числе прочих вариантов анализа (анализ исходного кода, размера ответа сервера, анализ карты сайта) он предлагает также использовать методы визуального анализа сайта. При этом И.С. Тюрин указывает на возможность анализа не только сайта целиком, но и отдельных его блоков: header, footer, боковые блоки и др. В то же время описание способов, позволяющих однозначно определить подобные блоки на сайте, в статье отсутствует.

Существующий стандарт HTML5[3], разработанный консорциумом W3C, предполагает использование в разметке сайта таких тегов, как header, footer, article и др., которые могут быть использованы для

[1] Число фейковых сайтов Google выросло за полгода в два раза // Известия. URL: https://iz.ru/1613788/2023-12-01/chislo-feikovykh-saitov-google-vyroslo-za-polgoda-v-dva-raza (дата обращения 02.04.2024).

[2] В Сети выросло число сайтов с фейковыми розыгрышами // Известия. URL: https://iz.ru/1588092/2023-10-12/v-seti-vyroslo-chislo-saitov-s-feikovymi-rozygryshami (дата обращения 02.04.2024).

[3] W3C HTML 5.2. URL: https://html.spec.whatwg.org/multipage/ (дата обращения 02.04.2024).

выделения основных блоков сайта. В публикации W3Techs показано, что HTML5 используется на 93% сайтов, проанализированных исследователями[4]. В то же время, с одной стороны, тег header может присутствовать на сайте неоднократно, так как им принято выделять не только верхнюю часть сайта, но и верхнюю часть публикации. С другой стороны, не исключена ситуация, когда упомянутые теги на web-странице будут отсутствовать.

При этом именно упомянутые основные блоки сайта позволяют однозначно идентифицировать принадлежность ему конкретной страницы, поскольку все остальные области на скриншоте могут быть отображением динамически изменяемого контента web-страницы. Аналогично при создании фейкового сайта злоумышленник будет сохранять в верстке web-страницы основные блоки такими же, как у оригинального сайта, а центральная часть фейкового сайта будет содержать форму для сбора персональных данных, ссылку для скачивания вредоносного программного средства или др., в связи с чем она будет отличаться от подлинного сайта. Таким образом, именно основные блоки сайта могут позволить программному средству защиты распознать факт заимствования интерфейса оригинального сайта.

Вышеуказанные ограничения в разметке сайтов на языке HTML, расположенных в сети Интернет, не позволяют создать универсального способа обнаружения таких блоков на основе кода страницы и вызывают необходимость поиска других методов выделения содержимого основных блоков сайта при анализе его визуального отображения. В связи с этим возникает необходимость решения **научной задачи** – разработать метод определения степени визуального сходства web-страниц для обнаружения фейковых сайтов организаций с учетом выделения в изображении web-страницы областей, характеризующих основные блоки сайта.

После открытия web-страницы в браузере и создания ее скриншота отображенный контент может быть обработан как растровое изображение. В связи с этим задача определения степени визуального сходства web-страниц может быть сведена к задаче определения схожести изображений. Это обусловливает необходимость анализа в рамках этой работы существующих алгоритмов, обеспечивающих определение меры сходства изображений.

---

[4] Usage statistics of HTML5 for websites. URL: https://w3techs.com/technologies/details/ml-html5 (дата обращения 02.04.2024).

Обзор существующих методов определения сходства изображений

В исследовании [Рудаков, Васютович 2015] сравнение изображений производится путем сравнения их перцептивных хешей. В рамках статьи для вычисления хеша предложено использовать методы: низкочастотный фильтр (путем уменьшения изображения до размера 8 × 8) и хеш по среднему (в других публикациях данный алгоритм именуется как aHash), хеш на основе гистограммы цветов, хеш на основе дискретного косинусного преобразования (в других публикациях данный алгоритм именуется как pHash). В статье показано, что хеш-функция на основе дискретного косинусного преобразования обладает лучшими способностями по различению изображений из перечисленных хеш-функций. Из отрицательных характеристик данного метода выделена неустойчивость к повороту изображений и их горизонтальному отражению. Сходные выводы представлены и в публикации [Ахрамеева, Трескин 2017]. Отметим, что в предметной области сравнения скриншотов web-страниц сайтов такие искажения стоит считать маловероятными, поэтому данный метод может быть применен в рамках данной работы.

Как и в предыдущих публикациях, в публикации [Петифорова, Штепа 2021] рассмотрена возможность использования алгоритмов aHash и pHash для определения сходства изображений. Кроме того, в работе использован алгоритм dHash, основанный на низкочастотной фильтрации (путем уменьшения изображения до размера 9 × 8) и функции определения расстояния как разницы оттенков серого между каждой парой пикселей, стоящей рядом друг с другом в каждой строке. В работе сравнивались данные методы с целью выбора наиболее оптимального метода с учетом скорости обработки фотографии. Наилучшей скоростью работы, согласно исследованию [Петифорова, Штепа 2021], из вышеперечисленных методов обладает dHash.

В исследованиях [Мягких, Ядута 2023; Гибкин 2019] подтверждена работоспособность алгоритма aHash в том виде, в каком он описан в исследованиях [Рудаков, Васютович 2015; Ахрамеева, Трескин 2017; Петифорова, Штепа 2021]. В публикации [Скиба, Размочаева 2019] исследуется возможность применения данного алгоритма в социальной сети художников с целью поиска неправомерных заимствований. Авторы, как и в других описаниях данного алгоритма, предлагают использовать низкочастотный фильтр, но уменьшают изображение не до размера 8 x 8, а до размера 64 × 64.

В исследовании [Олисеенко, Абрамов, Тулупьев 2021] в качестве алгоритма сравнения изображений, публикуемых в аккаунтах

пользователей социальной сети, применяется pHash. Сравнение производится с целью выявления аккаунтов в социальной сети, принадлежащих одному человеку. Предложенный подход рекомендуется авторами для дальнейшего исследования в задаче поиска фейковых аккаунтов в социальной сети. В публикации [Корепанова, Абрамов, Тулупьев 2021] данная тема развивается путем добавления в метод этапа выделения изображений, на которых присутствует лицо человека. С этой целью авторами используется библиотека face_recognition[5] для языка Python. Представленные исследования подтверждают применимость метода вычисления перцептивного хэша в прикладных задачах при сравнении изображений.

Популярность и востребованность описанных алгоритмов стала причиной появления отраслевых решений, которые используют данные алгоритмы. В частности, для Python разработана библиотека ImageHash[6], содержащая готовые функции вычисления aHash, dHash и pHash.

Общим свойством перечисленных методов сравнения изображений является наличие в них этапа преобразования цветного изображения в черно-белое с оттенками серого. Такой подход оправдан в ряде случаев, поскольку большое количество объектов реального мира могут быть определены именно их формой, а не цветом. В то же время для каждого юридического лица характерен свой бренд и принятые в нем цветовые решения. Например, для телекоммуникационной компании МТС характерен красный цвет, компании Мегафон – зеленый, IT-компания 1С использует желтый цвет в качестве основного в сочетании с красным. Этот факт отмечен также в публикации [Харченко, Качалов 2022], которые описывают, что Google идентифицируется как сочетание синего цвета с красным, зеленым и желтым. Таким образом, в сравнении скриншотов сайтов организаций стоит опираться на тот подход, который будет учитывать каждую цветовую координату как отдельный анализируемый признак.

Решение этого вопроса может быть связано с применением метода сравнения изображений на основе сравнения гистограмм цветов, построенных при анализе пикселей каждого из изображений [Кирпичников, Ляшева, Шлеймович 2014]. В некоторых вариантах реа-

[5] Проект “Face Recognition” в репозитории пользователя ageitgey // GitHub. URL: https://github.com/ageitgey/face_recognition (дата обращения 02.04.2024).

[6] Проект “ImageHash” в хранилище пакетов PyPI для Python // Python. URL: https://pypi.org/project/ImageHash/ (дата обращения 02.04.2024).

лизации этого метода оба изображения переводятся в черно-белый формат с оттенками серого и строятся гистограммы, отражающие количество пикселей на изображении в цветовом диапазоне от 0 до 255. После этого между гистограммами находится расстояние по одной из метрик, представленных в публикации [Кирпичников, Лящева, Шлеймович 2014], на основе которого делаются дальнейшие выводы. В другом варианте реализации могут быть представлены отдельные гистограммы для каждого цветового канала. По итогам попарного сравнения по указанному алгоритму гистограмм для каждого цветового канала анализируемых изображений будут получены три величины, из которых может быть найдено среднее значение – итоговая степень сходства этих изображений.

Описание перечисленных выше общеизвестных алгоритмов хеширования приведено в работе [Fei, Ju, Zhen, Li 2017]. Кроме того, в статье [Fei, Ju, Zhen, Li 2017] предложен новый метод построения хеш-строки laplaceHash, который является модификацией алгоритма aHash. Подсчет среднего значения цветовой координаты всех пикселей изображения предваряет преобразование Лапласа, которое усиливает контрастность изображения. Результаты представленного в цитируемой статье вычислительного эксперимента показывают, что данное действие повышает точность сравнения.

Стоит учитывать, что многие web-ресурсы состоят из нескольких страниц, в связи с чем возникает необходимость попарного сравнения изображений всех страниц подлинного сайта и проверяемой web-страницы. Данный процесс является время- и трудозатратным, что делает востребованной разработку иных методов оценки визуального сходства.

Материалы и методы

При разработке метода в этой работе были использованы технические средства: язык программирования Java, библиотека алгоритмов компьютерного зрения OpenCV (с модулем для интеграции в Java-программы), библиотека Jsoup для анализа, извлечения и управления данными, хранящимися в документах HTML, Selenium WebDriver для автоматизированного открытия web-страниц в браузере и создания скриншотов.

Сам процесс создания скриншота web-страницы для последующего сравнения нуждается в более подробном рассмотрении. Скриншот страницы сайта не может быть выполнен так, чтобы захватывать только верхнюю часть сайта (header), поскольку нижняя часть (footer) часто обладает существенным набором свойств, поз-

воляющих отличить один сайт от другого. В то же время создание полного скриншота web-страницы может привести к тому, что в процессе работы программы для разных страниц сайта будут получены изображения различных размеров. Например, высота страницы об использовании приложения «Госключ» примерно в 2 раза выше высоты главной страницы сервиса Госуслуги. При масштабировании изображения до квадратных размеров, в соответствии с рядом упомянутых в статье алгоритмов, в разной степени будут искажены пропорции одних и тех же элементов на скриншотах различных web-страниц. В связи с этим в данной работе для оценки степени сходства web-страниц предлагается сравнивать два изображения, сделанных путем склейки скриншотов верхней части и нижней части проверяемого и подлинного сайтов соответственно.

Для загрузки Интернет-ресурсов в работе был использован браузер Mozilla Firefox, установленный на операционной системе Windows 7. Открытие web-страницы в браузере делает возможным запуск нежелательных скриптов на компьютере, где производится тестирование программы. Для повышения степени защищенности компьютера в браузер были установлены расширения NoScript и uBlock Origin.

Разработку метода определения степени визуального сходства web-страниц предварял процесс парсинга интернет-ресурсов, целью которого была проверка наличия на сайтах организаций семантических тегов HTML5. Список сайтов российских юридических лиц в момент проведения исследования был получен с портала государственных услуг Российской Федерации. На web-странице о сертификатах безопасности от Минцифры был ранее опубликован список доменных имен, в отношении которых выпущены российские сертификаты. В различных источниках[7] можно найти подтверждение тому, что данный список ранее был общедоступен.

Результаты анализа присутствия на сайтах тегов HTML5

Анализ 4824 сайтов организаций, в отношении доменных имен которых выпущен сертификат безопасности от Минцифры, подтвердил, что существует большое количество сайтов, не применяющих для разметки семантические теги HTML5. С помощью

[7] Минцифры: 7 тысяч доменов установили российские TLS-сертификаты. URL: https://searchengines.guru/ru/news/2055801 (дата обращения 02.04.2024).

парсинга была предпринята попытка проверить наличие тегов header, footer, main, nav, section, article, aside. Результаты анализа представлены в форме гистограммы на рис. 1.

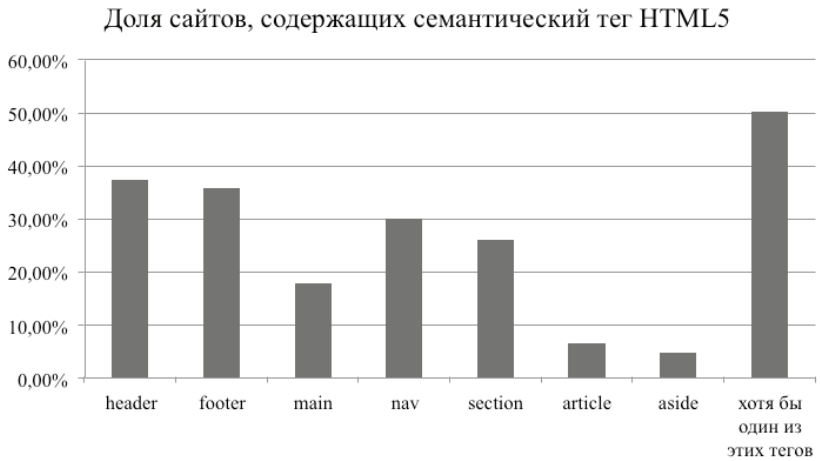

Рис. 1. Результаты анализа исходного кода сайтов на наличие семантических тегов HTML5

Анализ показал, что в исходном коде менее 51% исследованных сайтов присутствовали указанные теги HTML5. Проведенное исследование показало актуальность разработки метода, позволяющего оценить степень сходства web-страниц сайтов, опираясь на их визуальное отображение, а не особенности разметки элементов страницы и построенную браузером DOM-модель.

Предлагаемое решение научной задачи

Для решения задачи определения степени визуального сходства web-страницы проверяемого сайта с web-страницами подлинного сайта предлагается использовать следующий алгоритм:

Шаг 1. Получить URL-адреса страниц подлинного сайта. Далее обозначим за N количество обнаруженных страниц на сайте.

Шаг 2. Создать массив S, содержащий N элементов-изображений, представляющих собой склейки скриншотов верхней и нижней части страниц сайта, открывающихся по URL, полученным на шаге 1.

Шаг 3. Создать массив изображений R, отмасштабировав каждое из изображений массива S до размера 32 × 64, из которых извлечено значение красного цветового канала. Аналогично создать массивы G, B со значениями зеленого и синего цветовых каналов соответственно.

Шаг 4. Создать трехмерный массив MO, где:

$$MO[1][j][k] = \frac{\sum_N^{i=1} R[i][j][k]}{N},$$

$$\text{при условиях} \begin{cases} 1 \le j \le 64, \\ 1 \le k \le 32, \end{cases}$$

где $R[i][j][k]$ – цветовая координата пикселя i-го изображения в массиве R, расположенного в j-ой строке и в k-ом столбце.

Аналогично:

$$MO[2][j][k] = \frac{\sum_N^{i=1} G[i][j][k]}{N},$$

$$MO[3][j][k] = \frac{\sum_N^{i=1} B[i][j][k]}{N},$$

где $G[i][j][k]$, $B[i][j][k]$ – цветовая координата пикселя i-го изображения в массивах G и B соответственно, расположенного в j-ой строке и в k-ом столбце.

Математический смысл элемента трехмерного массива $MO[i][j][k]$ заключается в определении среднеарифметического значения i-го цветового канала пикселя скриншота сайта, расположенного в j-ой строке и в k-ом столбце.

Шаг 5. Определить трехмерный массив MD как:

$$MD[1][j][k] = \sqrt{\frac{1}{N}\sum_N^{i=1}(R[i][j][k] - MO[1][j][k])^2},$$

$$MD[2][j][k] = \sqrt{\frac{1}{N}\sum_N^{i=1}(G[i][j][k] - MO[2][j][k])^2},$$

$$MD[3][j][k] = \sqrt{\frac{1}{N}\sum_N^{i=1}(B[i][j][k] - MO[3][j][k])^2}.$$

Математический смысл элемента трехмерного массива $MD[i][j][k]$ заключается в определении среднеквадратичного отклонения значения i-го цветового канала пикселя скриншота сайта, расположенного в j-ой строке и в k-ом столбце.

Шаг 6. Получить изображение $V_{полн.}$ проверяемого сайта, представляющее собой склейку скриншотов верхней и нижней части страницы сайта.

Шаг 7. Получить изображение $V_{умен.}$, отмасштабировав изображение $V_{полн.}$ до размера 32 x 64. Получить из $V_{умен.}$ отдельно красный, зеленый и синий цветовые каналы как V_R, V_G и V_B соответственно.

Шаг 8. Вычислить количество совпадающих пикселей C следующим образом:

$$C = \sum_{64}^{j=1}\sum_{32}^{k=1}\begin{cases} 1, & \text{если} \begin{cases} MO[1][j][k] - \dfrac{MD[1][j][k]}{\sqrt{N}} < V_R[j][k] \\ MO[1][j][k] + \dfrac{MD[1][j][k]}{\sqrt{N}} > V_R[j][k] \\ MO[2][j][k] - \dfrac{MD[2][j][k]}{\sqrt{N}} < V_G[j][k] \\ MO[2][j][k] + \dfrac{MD[2][j][k]}{\sqrt{N}} > V_G[j][k] \\ MO[3][j][k] - \dfrac{MD[3][j][k]}{\sqrt{N}} < V_B[j][k] \\ MO[3][j][k] + \dfrac{MD[3][j][k]}{\sqrt{N}} > V_B[j][k] \end{cases} \\ 0, & \text{в противном случае} \end{cases}.$$

Математический смысл данных проверок заключается в том, что любой цветовой канал каждого пикселя проверяемого изображения должен совпадать с вычисленным математическим ожиданием цветовой координаты с учетом стандартного отклонения среднего значения [Вьонг, Ушакова 2017, с. 152].

Шаг 9. Итоговая степень сходства проверяемой страницы сайта со страницами подлинного сайта будет определяться как $Similatory = \frac{C}{64*32}$.

Данный алгоритм сводится к сравнению всех пикселей изображения. В то же время на любом скриншоте есть конкретные области, которые содержат повторяющиеся на каждой странице элементы (header, footer) и динамически изменяющиеся элементы (фотографии в статьях, реклама и т. д.).

С этой целью предлагается помимо трехмерных массивов MD и MO вычислять для набора изображений маску, где 1 (белый цвет) будет означать пиксель, отражающий элементы дизайна (существенный признак внешнего вида страницы сайта), а 0 (черный цвет) – элемент содержимого конкретной страницы, рекламу и т. д., которые не влияют на идентификацию страницы сайта.

«В статистике принято считать, что если коэффициент вариации менее 33%, то совокупность данных является однородной, если более 33%, то неоднородной» [Шатырко 2013, с. 203]. В соответствии с этим до шага 6 необходимо сформировать матрицу mask по следующему правилу:

$$mask[j][k] = \begin{cases} 1, & \text{если } \begin{cases} \frac{MD[1][j][k]}{MO[1][j][k]} * 100\% \le 33\% \\ \frac{MD[2][j][k]}{MO[2][j][k]} * 100\% \le 33\% \\ \frac{MD[3][j][k]}{MO[3][j][k]} * 100\% \le 33\% \end{cases} \\ 0, & \text{в противном случае} \end{cases}$$

$$\text{при условиях } \begin{cases} 1 \le j \le 64, \\ 1 \le k \le 32. \end{cases}$$

Тогда значение C на шаге 8 будет вычисляться так:

$$C = \sum_{64}^{j=1} \sum_{32}^{k=1} \begin{cases} 1, & \text{если } \begin{cases} mask[j][k] = 1 \\ MO[1][j][k] - \frac{MD[1][j][k]}{\sqrt{N}} < V_R[j][k] \\ MO[1][j][k] + \frac{MD[1][j][k]}{\sqrt{N}} > V_R[j][k] \\ MO[2][j][k] - \frac{MD[2][j][k]}{\sqrt{N}} < V_G[j][k] \\ MO[2][j][k] + \frac{MD[2][j][k]}{\sqrt{N}} > V_G[j][k] \\ MO[3][j][k] - \frac{MD[3][j][k]}{\sqrt{N}} < V_B[j][k] \\ MO[3][j][k] + \frac{MD[3][j][k]}{\sqrt{N}} > V_B[j][k] \end{cases} \\ 0, & \text{в противном случае} \end{cases}.$$

Итоговая степень сходства проверяемой страницы сайта со страницами подлинного сайта будет определяться как:

$$Similatory = \frac{c}{\sum_{64}^{j=1}\sum_{32}^{k=1}\begin{cases}1, & \text{если } mask[j][k]=1\\ 0, & \text{в противном случае}\end{cases}}.$$

Предложенный метод нуждается в тестировании как в варианте реализации с использованием маски, так и без нее.

Результаты оценки качества работы метода

С целью оценки работоспособности разработанных методов для тестируемых сайтов были найдены следующие меры сходства:

а) между разными страницами одного и того же сайта;

б) между страницами различных сайтов.

Для тестирования были выбраны сайт Steam (steamcommunity.com), портал государственных услуг Российской Федерации (gosuslugi.ru), сайт Шуйского филиала ИвГУ (sspu.ru). Результаты тестирования представлены в табл. 1. В таблице отражены усредненные результаты эксперимента по сравнению скриншотов страниц сайтов описанными методами.

Таблица 1

Тестирование методов определения визуального сходства web-страниц

Используемый метод	aHash	dHash	pHash	laplaceHash
Сходство двух различных страниц сайта Steam	53,65%	59,11%	64,33%	57,06%
Сходство страницы сайта Steam со страницей другого сайта	49,97%	51,66%	51,28%	50,18%
Сходство двух страниц портала Госуслуги	64,84%	66,46%	66,75%	65,19%
Сходство страницы портала Госуслуги со страницей другого сайта	55,97%	57,32%	50,16%	50,55%
Сходство двух различных страниц сайта Шуйского филиала ИвГУ	86,72%	75,00%	81,50%	82,76%
Сходство страницы сайта Шуйского филиала ИвГУ со страницей другого сайта	52,20%	50,20%	51,02%	49,52%

Окончание табл. 1

Используемый метод	Сравнение гистограмм (черно-белое изображение)	Сравнение гистограмм (цветное изображение)	**Предложенный алгоритм прямого сравнения**	**Предложенный алгоритм сравнения по маске**
Сходство двух различных страниц сайта Steam	21,58%	21,51%	**27,84%**	**85,39%**
Сходство страницы сайта Steam со страницей другого сайта	11,41%	12,17%	**0,75%**	**0,09%**
Сходство двух страниц портала Госуслуги	23,06%	26,20%	**29,43%**	**40,07%**
Сходство страницы портала Госуслуги со страницей другого сайта	18,92%	19,17%	**4,57%**	**4,39%**
Сходство двух различных страниц сайта Шуйского филиала ИвГУ	60,21%	61,13%	**48,60%**	**54,90%**
Сходство страницы сайта Шуйского филиала ИвГУ со страницей другого сайта	28,61%	29,41%	**3,28%**	**3,15%**

Результаты проведенного эксперимента позволили установить, что все протестированные методы в среднем оценивают степень сходство одной страницы сайта с другой страницей этого же сайта выше, чем степень сходства страниц двух различных сайтов. Это подтверждает корректность применения любого из вышеперечисленных методов в данной задаче.

В то же время именно в предложенных методах степень сходства в первой ситуации (страницы одного сайта) более чем в 5 раз выше, чем степень сходства во второй ситуации (страницы

различных сайтов). В связи с этим применение данных методов позволит получить более точный результат. При этом во всех протестированных случаях работа метода прямого сравнения (без использования маски) оказалась менее качественной, чем работа метода с применением маски.

Выводы

Вычислительный эксперимент показал, что в рамках предложенного метода определения визуального сходства web-страниц оказалось возможным выделить существенные свойства дизайна web-страниц, указывающие на их принадлежность сайту определенной организации. Идентификация таких свойств в данной работе основана на вычислении статистических характеристик цветовых координат каждого пикселя уменьшенного изображения, получаемого из скриншота отображаемого в окне браузера содержимого гипертекстовых документов. На основе вычисленных характеристик предлагается строить черно-белую маску, где пиксели, отражающие существенные свойства дизайна страницы, отмечены белым цветом, а пиксели, не влияющие на идентификацию страницы, – черным цветом.

Дальнейшая работа должна предполагать включение предложенного метода в программное средство, которое будет извлекать из реестра доменных имен данные о последних зарегистрированных интернет-ресурсах и проверять факт эксплуатации ими дизайна сайта защищаемой организации. Высокая степень сходства web-страниц двух различных сайтов (подлинного и проверяемого) будет указывать на необходимость исследования проверяемого сайта на наличие фейковой активности.

Литература

Ахрамеева, Трескин 2017 – *Ахрамеева К.А., Трескин Н.Л.* Использование перцептивных хэш-функций для обеспечения информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции: В 4 т. Санкт-Петербург, 1–2 марта 2017 года / Под ред. С.В. Бачевского. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. Т. 2. С. 71–4.

Баранников, Русецкая 2024 – *Баранников Д.Н., Русецкая И.А.* Современные подходы к обеспечению информационной безопасности детей // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 65–79. DOI: 10.28995/2686-679X-2024-1-65-79.

Вьюнг, Ушакова 2017 – *Вьюнг Т.Т.З., Ушакова Н.В.* Стандартное отклонение или стандартная ошибка // Современные технологии в науке и образовании – СТНО–2017: Сб. тр. II Международной научно-технической и научно-методической конференции: В 8 т. Рязань, 1–3 марта 2017 г. Рязань: Рязанский государственный радиотехнический университет, 2017. Т. 2. С. 149–153.

Гибкин 2019 – *Гибкин Ю.С.* Разработка алгоритма оценки сходства изображений без предварительного обучения методом перцептивного хеширования // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, Белгород, 1–20 мая 2019 г. Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2019. С. 2900–2904.

Кирпичников, Ляшева, Шлеймович 2014 – *Кирпичников А.П., Ляшева С.А., Шлеймович М.П.* Контекстный поиск изображений // Вестник Казанского технологического университета. 2014. Т. 17. № 18. С. 244–251.

Корепанова, Абрамов, Тулупьев 2021 – *Корепанова А.А., Абрамов М.В., Тулупьев А.Л.* Идентификация аккаунтов пользователей социальных сетей при помощи сравнения графического контента // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 6. С. 942–950. DOI: 10.17586/2226-1494-2021-21-6-942-950.

Мягких, Ядута 2023 – *Мягких П.А., Ядута А.З.* Сравнение изображений с использованием перцептивных хешей // Фундаментальные и прикладные исследования в науке и образовании: Сб. статей международной научной конференции, Санкт-Петербург, 15 мая 2023 г. СПб.: Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2023. С. 72–76.

Олисеенко, Абрамов, Тулупьев 2021 – *Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л.* Идентификация аккаунтов пользователей при помощи сравнения изображений: подход на основе pHash // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 4. С. 562–570. DOI: 10.17586/2226-1494-2021-21-4-562-570.

Петифорова, Штепа 2021 – *Петифорова, Д.Е., Штепа К.А.* Анализ использования перцептивного хеширования в процессе идентификации изображений // Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем: Материалы Всероссийской конференции с международным участием, Москва, 19–23 апреля 2021 г. М.: Российский университет дружбы народов, 2021. С. 274–277.

Рудаков, Васютович 2015 – *Рудаков И.В., Васютович И.М.* Исследование перцептивных хеш-функций изображений // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2015. № 8. С. 269–280. DOI: 10.7463/0815.0800596.

Скиба, Размочаева 2019 – *Скиба А.С., Размочаева Н.В.* Разработка социальной сети для художников с возможностью проверки на плагиат // Наука настоящего и будущего. 2019. Т. 1. С. 109–113.

Тюрин 2020 – *Тюрин И.С.* Система поиска структурных и функциональных изменений веб-ресурса // Региональная информатика (РИ-2020): Материалы XVII Санкт-Петербургской международной конференции. Санкт-Петербург, 28–30 октября 2020 г. Часть 2. СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2020. С. 194–195.

Харченко, Качалов 2022 – *Харченко С.С., Качалов К.А.* Проблемы распознавания схожих изображений // Электронные средства и системы управления: Материалы докладов Международной научно-практической конференции. 2022. № 1-2. С. 189–191.

Шатырко 2013 – *Шатырко А.В.* Перспективы применения «отрицательного трансферта» для сглаживания уровня регионального неравенства // Региональная экономика. Юг России. 2013. № 2 (2). С. 203–209.

Fei, Ju, Zhen, Li 2017 – *Fei M., Ju Zh., Zhen X., Li J.* Real-time visual tracking based on improved perceptual hashing // Multimedia Tools and Applications. 2017. Vol. 76. Iss. 3. P. 4617–4634. DOI: 10.1007/s11042-016-3723-5.

References

Ahrameeva, K.A. and Treskin, N.L. (2017), “Using perceptual hash-functions in information security”, *Current issues of infotelecommunications in science and education (St. Petersburg, March, 2017): 6th International Scientific-technical and Scientific-methodical Conference,* Coll. of articles in 4 vols., SPbGUT, St. Petersburg, Russia, vol. 2, pp. 71–74.

Barannikov, D.N. and Rusetskaya, I.A. (2024), “Modern approaches to ensuring children’s information security”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series*, no. 1. pp. 65–79, DOI: 10.28995/2686-679X-2024-1-65-79.

Vuong, T.T.D. and Ushakova, N.V. (2017), “Standard deviation or standard error”, *Modern technologies in science and education – STNO–2023 (Ryazan, March, 2017): Proceedings of the 2nd International Scientific-technical and Scientific-methodical Conference in 8 vols*, Ryazan State Radio Engineering University, Ryazan, Russia, vol. 2, pp. 149–153.

Gibkin, Yu.S. (2019), “Development of an algorithm for evaluating the similarity of images without prior training by the method of perceptual hashing”, *International Scientific and Technical Conference of Young Scientists BSTU IM. V.G. Shukhova* (Belgorod, May, 2019), Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia, pp. 2900–2904.

Kirpichnikov, A.P., Lyasheva, S.A. and Shleymovich, M.P. (2014), "Content-based image retrieval", *Bulletin of the Technological University, Kazan National Research Technological University*, vol. 17, no. 18, pp. 244–251.

Korepanova, A.A., Abramov, M.V. and Tulupyev, A.L. (2021), "Identification of social media user accounts by comparing graphical content", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, vol. 21, no. 6, pp. 942–950, DOI: 10.17586/2226-1494-2021-21-6-942-950.

Myagkikh, P.A. and Yaduta, A.Z. (2023), "Comparison of images using perceptive hashes. Fundamental and applied research in science and education", *Collection of articles from the international scientific conference "Fundamental and applied research in science and education"* (St. Petersburg, May 15, 2023), Humanitarian National Research Institute "National Development", Saint Petersburg, Russia, 2023, pp. 72–76.

Oliseenko, V.D., Abramov, M.V. and Tulupyev, A.L. (2021), "Identification of user accounts by image comparison. The pHash-based approach", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, vol. 21, no. 4, pp. 562–570, DOI: 10.17586/2226-1494-2021-21-4-562-570.

Petiforova, D.E. and Shtepa, K.A. (2021), "Analysis of the use of perceptual hashing in the process of image identification", *Information and Telecommunication Technologies and Mathematical Modeling of High-Tech Systems. Proceedings of the All-Russian Conference with International Participation* (Moscow, April 19–23, 2021), Peoples' Friendship University of Russia, Moscow, Russia, pp. 274–277.

Rudakov, I.V. and Vasiutovich, I.M. (2015), "Analysis of Perceptual Image Hash Functions", *Science and Education. Scientific publication of Bauman MSTU*, no. 8. pp. 269–280, DOI: 10.7463/0815.0800596.

Skiba, A.S. and Razmochaeva, N.V. (2019), "Development of a social network for artists with the ability to check for plagiarism", *Science of the Present and Future*, vol. 1, pp. 109–113.

Tyurin, I.S. (2020), "System for searching structural and functional changes of web resource" // Regional Informatics (RI-2020). *17th St. Petersburg Internatonal Conference. Proceedings of the Conference. Part 2* (St. Petersburg, October 28–30, 2020), St. Petersburg Society of Informatics, Computer Technology, Communication and Management Systems, St. Petersburg, Russia, pp. 194–195.

Harchenko, S.S. and Kachalov, K.A. (2022), "Issues of recognizing similar images", *Electronic Devices and Control Systems. Proceedings of the reports of the International Scientific and Practical Conference*, no. 1-2. pp. 189–191.

Shatyrko, A.V. (2013), "Prospects for the use of the "negative transfer" for the mitigating the level of the regional inequality", *Regional Economy. South of Russia*, no. 2 (2), pp. 203–209.

Fei, M., Ju, Zh., Zhen, X. and Li, J. (2017), "Real-time visual tracking based on improved perceptual hashing", *Multimedia Tools and Applications*, vol. 76, issue 3, pp. 4617–4634. DOI: 10.1007/s11042-016-3723-5.

Информация об авторе

Вадим А. Смирнов, аспирант, Ивановский государственный университет, Ивановская область, Шуя, Россия; 155908, Россия, Ивановская область, Шуя, ул. Кооперативная, д. 24; v.a.d.i.m@bk.ru

Information about the author

Vadim A. Smirnov, postgraduate student, Ivanovo State University, Ivanovo region, Shuya, Russia; 24, Cooperative St., Ivanovo region, Shuya, 155908, Russia; v.a.d.i.m@bk.ru

УДК 519
DOI: 10.28995/ 2686-679X-2024-3-123-136

О стабильных состояниях малой группы субъектов, взаимодействующих с общим полем возбуждения

Надежда Б. Викторова
Российский государственный гуманитарный университет, Москва, Россия, nbvictorova@list.ru

Денис А. Морозов
Российский государственный гуманитарный университет, Москва, Россия, morozovd170@gmail.com

Алексей В. Казанский
Российский государственный гуманитарный университет, Москва, Россия, kazanskij02@mail.ru

Алехандро А. Никитин
Российский государственный гуманитарный университет, Москва, Россия, alejandro.nikitin@gmail.com

Владислав Д. Волков
Российский государственный гуманитарный университет, Москва, Россия, volkov99vlad@gmail.com

Аннотация. В статье рассматривается задача математического моделирования социальных явлений по аналогии с физической моделью Тависа–Каммингса в рамках социального лазера А. Хренникова. Данная парадигма предполагает подобие социального возбуждения и электромагнитного поля. В контексте этой парадигмы осуществляется аналогия эмоционального возбуждения с электромагнитным полем фиксированной моды. В статье вводится особый базис в пространстве квантовых состояний системы. Необходимо исходить из равенства интенсивности взаимодействия с полем для всех социальных индивидов. Такое предположение позволяет ввести базис, который резко сокращает размерность гамильтониана системы. Подпространство квантовых состояний, порожденное векторами нового базиса с ограниченной энергией, оказывается инвари-

антным относительно гамильтониана. Имея оператор Тависа–Каммингса, в статье находится явный вид гамильтониана и стационарные состояния данной системы и их собственные энергии. Полученные стационарные состояния не зависят ни от энергии возбуждения поля (константа hw), ни от энергии взаимодействия индивидов с полем (константа g). Результаты статьи будут полезны для исследования эмоциональных процессов в малых группах населения, например внутри семьи. Социальный лазер А. Хренникова – это модель взаимодействия группы людей разного состава и количества с социальным возбуждением. Физической природой этого возбуждения является электромагнитное поле. Однако механизмы такого взаимодействия можно понять, используя резко упрощенную по сравнению с реальностью абстракцию, в которой поведение людей и поле психического возбуждения сводится к взаимодействию двухуровневых атомов, представляющих индивиды, и одномодового поля внутри оптической полости. Достоинство этой модели заключается в простоте ее математического описания, а также в наличие физических прототипов, возможностью создания программных комплексов по моделированию.

Ключевые слова: математическое моделирование, модель Тависа–Каммингса, кубит, полевые операторы, матрица линейного оператора, гамильтониан системы, собственные вектора и собственные значения эрмитовой матрицы

Для цитирования: Викторова Н.Б., Морозов Д.А., Казанский А.В., Никитин А.А., Волков В.А. О стабильных состояниях малой группы субъектов, взаимодействующих с общим полем возбуждения // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 123–136. DOI: 10.28995/ 2686-679X-2024-3-123-136

On stable states of a small group of subjects interacting with a common field of excitation

Nadezda B. Victorova
Russian State University for the Humanities, Moscow, Russia, nbvictorova@list.ru

Denis A. Morozov
Russian State University for the Humanities, Moscow, Russia, morozovd170@gmail.com

Aleksei V. Kazanskii
Russian State University for the Humanities, Moscow, Russia, kazanskij02@mail.ru

Alekhandro A. Nikitin
Russian State University for the Humanities, Moscow, Russia, alejandro.nikitin@gmail.com

Vladislav D. Volkov
Russian State University for the Humanities, Moscow, Russia, volkov99vlad@gmail.com

Abstract. The article considers the task of mathematical modeling of social phenomena by analogy with the physical model of the Tavis–Cummings system within the framework of A. Khrennikov's social laser paradigm. The paradigm assumes a similarity between social excitation and an electromagnetic field. Within that paradigm, there is an analogy between emotional excitement and a fixed-mode electromagnetic field. The article introduces a special basis in the space of quantum states of the system. It is necessary to assume equality of interaction intensity with the field for all social individuals. Such an assumption allows introducing a basis that sharply reduces the dimensionality of the system's Hamiltonian. The subspace of quantum states generated by the vectors of the new basis with limited energy turns out to be invariant with respect to the Hamiltonian. Having the Tavis–Cummings operative, the article finds the explicit form of the Hamiltonian and the stationary states of the system and their eigenenergies. The resulting stationary states do not depend on either the field excitation energy (constant hw) or the interaction energy of individuals with the field (constant g). Outcomes of the article will be useful for investigating emotional processes in small population groups, such as within a family. A. Khrennikov's social laser is a model of interaction of a population group of different composition and size with social excitation. The physical nature of that excitation is an electromagnetic field. However, the mechanisms of such interaction can be understood using a sharply simplified abstraction, in which the behavior of people and the field of psychic excitement is reduced to the

interaction of two-level atoms representing individuals and a single-mode field within an optical cavity. The advantage of that model lies in its simplicity of mathematical description, as well as in the availability of physical prototypes and the possibility of creating software complexes for modeling.

Keywords: Mathematical modeling, Tavis–Cummings model, qubit, field operators, linear operator matrix, system Hamiltonian, eigenvectors and eigenvalues of a Hermitian matrix

For citation: Victorova, N.B., Morozov, D.A, Kazanskii, A.V., Nikitin, A.A. and Volkov, V.D. (2024), "On stable states of a small group of subjects interacting with a common field of excitation", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 123–136, DOI: 10.28995/ 2686-679X-2024-3-123-136

Введение

Исследуется эмоциональное состояние трех субъектов с учетом общего поля психического возбуждения, рассматриваемого в парадигме социального лазера А. Хренникова[1].

Возбуждение моделируется в виде одномодового электромагнитного поля в оптической полости с размещенными в ней атомами, которые представляют собой субъекты. Для упрощения вычислений мы будем рассматривать только 4 уровня возбуждения поля, которые обозначаются символами 0, 1, 2, 3.

Цель работы

Целью работы является подбор базиса, составление гамильтониана и нахождение стационарных состояний рассматриваемой системы с использованием стандартных приемов линейной алгебры.

На основе концепции социального лазера взаимодействие индивидов с полем возбуждения представляется в виде взаимодействия атомов с одномодовым электромагнитным полем. Это позволяет применить к данному социальному процессу математический аппарат конечномерных моделей квантовой электродинамики. В рамках этого подхода открывается возможность нахождения стабильных состояний.

[1] *Khrennikov A.* Social Laser Model for the Bandwagon Effect: Generation of Coherent Information Waves // *Entropy*. 2020. Vol. *22* (5). P. 559. URL: https://doi.org/10.3390/e22050559 (дата обращения 15.01.2024).

Модель Тависа–Каммингса

Модель Тависа–Каммингса [Jaynes, Cummings 1963; Ожигов 2020; Викторова 2023][2] – это конечномерная модель, которая описывает взаимодействие ансамбля двухуровневых атомов, помещенных в оптический резонатор с одномодовым полем частоты, близкой к собственной частоте резонатора. Для связи атомов с полем справедливо приближение RWA. Рассмотрим 3 двухуровневых атома, взаимодействующих с модой электромагнитного поля в идеальном резонаторе. Атомы взаимодействуют с электромагнитным полем полости, испуская или поглощая фотон. При поглощении фотонов атом возбуждается, или переходит в возбужденное состояние (excited state), при испускании переходит в исходное состояние (ground state). Через обозначаем основное состояние, через возбужденное состояние.

Данная модель описывает трех атомную систему с одной резонансной модой электромагнитного поля внутри оптической полости. Поскольку константа g взаимодействия атомов с полем одинакова для всех трех атомов, мы считаем всех трех участников группы равноценными по отношению к полю. Поэтому энергия их взаимодействия с полем одинакова. Мы можем сгруппировать возбуждение по общему уровню энергии: 0, 1, 2, 3 в единицах hw. И из этого следует возможность выбора нового базиса в пространстве состояний в подпространстве, где m – число атомов в системе (m = 3).

Переход от естественного базиса системы, к новому

Рассмотрим естественный базис системы

$$|n\rangle\,|at_1, at_2, at_3\rangle, \tag{1}$$

где $ph = \{0, 1, 2, 3\}$, $at_i = \{0, 1\}$. В такой системе у нас 32 возможных состояния.

Введем состояние

$$\{k\rangle = \frac{1}{\sqrt{C_m^k}} \sum_{x(j)=k} |j\rangle_{at}, \tag{2}$$

[2] *Cummings F.W.* Reminiscing about thesis work with E T Jaynes at Stanford in the 1950s // *IOP Publishing*. URL: https://iopscience.iop.org/article/10.1088/0953-4075/46/22/220202 (дата обращения 01.01.2024).

где через $x(j)$ обозначим вес Хэмминга двоичного набора $|j\rangle_{at}$. Поэтому

$$\{0\rangle = |000\rangle_{at}$$

$$\{1\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)_{at}$$

$$\{2\rangle = \frac{1}{\sqrt{3}}(|101\rangle + |011\rangle + |110\rangle)_{at}$$

$$\{3\rangle = |111\rangle_{at}.$$

Тогда базис

$$|\Phi_K\rangle = |m-k\rangle_{ph}\ \{k\rangle \tag{3}$$

ортонормирован в C^4.

Имеем

$$|\phi_0\rangle = |3\rangle_{ph}\{0\rangle,$$

$$|\phi_1\rangle = |2\rangle_{ph}\{1\rangle = \frac{1}{\sqrt{3}}|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle)_{at},$$

$$|\phi_2\rangle = |1\rangle_{ph}\{2\rangle = \frac{1}{\sqrt{3}}|1\rangle_{ph}(|101\rangle + |011\rangle + |110\rangle)_{at},$$

$$|\phi_3\rangle = |0\rangle_{ph}\{3\rangle.$$

В представлении взаимодействия такая система описывается гамильтонианом Тависа–Каммингса [Jaynes, Cummings 1963]/[Ожигов 2020]/[Ожигов, Викторова, Сковорода 2016]/[Викторова 2023].

$$H_{Tc} = \hbar w a^+ a + \hbar w\,(\sigma_1^+\sigma_1 + \sigma_2^+\sigma_2 + \sigma_3^+\sigma_3) + \\ + g(a^+(\sigma_1 + \sigma_2 + \sigma_3) + a^-(\sigma_1^+ + \sigma_2^+ + \sigma_3^+), \tag{4}$$

где $\hbar w a^+ a$ – энергия поля,

$\hbar w\,(\sigma_1^+\sigma_1 + \sigma_2^+\sigma_2 + \sigma_3^+\sigma_3)$ – энергия атомов,

$g(a^+(\sigma_1 + \sigma_2 + \sigma_3) + a^-(\sigma_1^+ + \sigma_2^+ + \sigma_3^+)$ – энергия взаимодействия поля с атомом;

$\hbar$ – постоянная Планка, w – частота фотона в полости, g – константа взаимодействия атома с полем.

Операторы уничтожения (5) и рождения (6) фотона определяются формулами

$$a^-|n\rangle = \sqrt{n}\,|n-1\rangle, \tag{5}$$

$$a^+|n\rangle = \sqrt{n+1}\,|n+1\rangle. \tag{6}$$

Поэтому

$$a^-|0\rangle = 0, \quad a^-|1\rangle = |0\rangle. \quad a^-|2\rangle = \sqrt{2}\,|1\rangle,$$

$$a^-|3\rangle = \sqrt{3}\,|2\rangle.$$

$$a^+|0\rangle = |1\rangle, \; a^+|1\rangle = \sqrt{2}\,|2\rangle, \; a^+|2\rangle = \sqrt{3}\,|3\rangle, \; a^+|3\rangle = 0.$$

Применив композицию операторов рождения и уничтожения к |n⟩, получим

$$a^+a^-|n\rangle = n\,|n\rangle, \tag{7}$$

что означает, что число n есть собственное значение оператора количества фотонов a^+a^-. Тогда

$$a^+a^-|0\rangle = 0\,|0\rangle = 0$$
$$a^+a^-|1\rangle = 1\,|1\rangle$$
$$a^+a^-|2\rangle = 2\,|2\rangle$$
$$a^+a^-|3\rangle = 3\,|3\rangle$$

Оператор возбуждения атома σ^+ действует на соответствующий кубит по правилу

$$\sigma^+|0\rangle = |1\rangle, \; \sigma^+|1\rangle = 0. \tag{8}$$

Оператор уничтожения возбуждения атома σ^- аналогичен первому

$$\sigma^-|0\rangle = 0, \; \sigma^-|1\rangle = |0\rangle. \tag{9}$$

Тогда очевидно, что

$$\sigma_i^+\,\sigma_i|000\rangle_{at} = 0, \text{ где i = 1, 2, 3,}$$

$$\left(a^+(\sigma_1 + \sigma_2 + \sigma_3)\right)|3\rangle_{ph}\,|000\rangle = 0,$$

$$\left(a^-(\sigma_1^+ + \sigma_2^+ + \sigma_3^+)\right)|3\rangle_{ph}\,|000\rangle = = 3|2\rangle_{ph}\,\frac{|100\rangle + |010\rangle\,|001\rangle}{\sqrt{3}}.$$

Применяем оператор H к первому базисному вектору.

$$H|\phi_0\rangle = H\,|3\rangle_{ph}\,|000\rangle_{at} = hw\;a^{+}a^{-}\;|3\rangle_{ph}\,|000\rangle +$$
$$+hw(\sigma_1^{+}\sigma_1 + \sigma_2^{+}\sigma_2 + \sigma_3^{+}\sigma_3)\,|3\rangle_{ph}\,|000\rangle +$$
$$+g\big(a^{+}(\sigma_1 + \sigma_2 + \sigma_3)\big)\,|3\rangle_{ph}\,|000\rangle +$$
$$+g\big(a^{-}(\sigma_1^{+} + \sigma_2^{+} + \sigma_3^{+})\big)\,|3\rangle_{ph}\,|000\rangle =$$
$$= 3hw|3\rangle_{ph}\,|000\rangle +$$
$$g\sqrt{3}|2\rangle_{ph}(\,|100\rangle + \,|010\rangle + \,|001\rangle) =$$
$$= 3hw|3\rangle_{ph}\,|000\rangle + 3g(|2\rangle_{ph}\{1\rangle.$$

Аналогично найдем образ второго базисного вектора

$$H|\phi_1\rangle = \mathrm{H}\tfrac{1}{\sqrt{3}}|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle)_{at} =$$
$$= hw\;a^{+}a^{-}\;\tfrac{1}{\sqrt{3}}|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle) +$$
$$+\frac{hw}{\sqrt{3}}(\sigma_1^{+}\sigma_1 + \sigma_2^{+}\sigma_2 + \sigma_3^{+}\sigma_3)\,|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle) +$$
$$+\frac{ga^{+}}{\sqrt{3}}(\sigma_1 + \sigma_2 + \sigma_3)|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle) +$$
$$+\frac{ga^{-}}{\sqrt{3}}(\sigma_1^{+} + \sigma_2^{+} + \sigma_3^{+})|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle) =$$
$$= \frac{2hw}{\sqrt{3}}\,|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle) +$$
$$+\frac{hw}{\sqrt{3}}\,|2\rangle_{ph}(|001\rangle + |010\rangle + |100\rangle) +$$
$$+3g\,|3\rangle_{ph}(|000\rangle) +$$
$$+\tfrac{\sqrt{2}g}{\sqrt{3}}\,|1\rangle_{ph}(|101\rangle + |101\rangle + |110\rangle + |110\rangle + |011\rangle + |011\rangle\,) =$$
$$= 3g|3\rangle_{ph}(|000\rangle) +$$
$$+3hw\;\frac{|2\rangle_{ph}(|001\rangle + |001\rangle + |100\rangle)}{\sqrt{3}} +$$
$$+2\frac{\sqrt{2}}{\sqrt{3}}g|1\rangle_{ph}(|101\rangle + |110\rangle + |011\rangle) =$$
$$= 3g|3\rangle_{ph}(|000\rangle) + 3hw|2\rangle_{ph}\{1\rangle + 2\sqrt{2}\,g|1\rangle_{ph}\{2\rangle$$

Находим образ третьего базисного вектора

$$H|\phi_2\rangle = \mathrm{H}\frac{1}{\sqrt{3}}|1\rangle_{ph}(|110\rangle + |101\rangle + |011\rangle)_{at} =$$

$$= hw\ a^+a^-\ \frac{1}{\sqrt{3}}|1\rangle_{ph}(|110\rangle + |101\rangle + |011\rangle) +$$

$$+\frac{hw}{\sqrt{3}}(\sigma_1^+\sigma_1 + \sigma_2^+\sigma_2 + \sigma_3^+\sigma_3)\,|1\rangle_{ph}(|110\rangle + |101\rangle + |011\rangle) +$$

$$+\frac{ga^+}{\sqrt{3}}(\sigma_1 + \sigma_2 + \sigma_3)|1\rangle_{ph}(|110\rangle + |101\rangle + |011\rangle) +$$

$$+\frac{ga^-}{\sqrt{3}}(\sigma_1^+ + \sigma_2^+ + \sigma_3^+)|1\rangle_{ph}(|110\rangle + |101\rangle + |011\rangle) =$$

$$= \frac{hw}{\sqrt{3}}\,|1\rangle_{ph}(|110\rangle + |101\rangle + |011\rangle) +$$

$$+\frac{hw}{\sqrt{3}}\,|1\rangle_{ph}2(|110\rangle + |101\rangle + |011\rangle) +$$

$$+\frac{\sqrt{2}g}{\sqrt{3}}\,|2\rangle_{ph}2(|010\rangle + |001\rangle + |100\rangle\,)$$

$$+\frac{1}{\sqrt{3}}g\,|0\rangle_{ph}(3|111\rangle) +$$

$$= 2\frac{\sqrt{2}}{\sqrt{3}}g|2\rangle_{ph}(|010\rangle + |001\rangle + |100\rangle) +$$

$$+3hw\ \frac{|1\rangle_{ph}(|110\rangle+|011\rangle+|101\rangle)}{\sqrt{3}} +$$

$$\sqrt{3}g|0\rangle_{ph}(|111\rangle) =$$

$$= \ 2\sqrt{2}\,g\,\left(|2\rangle_{\,ph}\{1\}\right) + 3hw(|1\rangle_{\,ph}\{2\})\ +\ \sqrt{3}\,g|0\rangle_{\,ph}\{3\}.$$

Находим образ последнего базисного вектора

$$H|\phi_3\rangle = H\,|0\rangle_{ph}\,|111\rangle_{at} = hw\ a^+a^-\ |0\rangle_{ph}\,|111\rangle +$$

$$+hw(\sigma_1^+\sigma_1 + \sigma_2^+\sigma_2 + \sigma_3^+\sigma_3)\,|0\rangle_{ph}\,|111\rangle +$$

$$+g\big(a^+(\sigma_1 + \sigma_2 + \sigma_3)\big)\,|0\rangle_{ph}\,|111\rangle +$$

$$+g\big(a^-(\sigma_1^+ + \sigma_2^+ + \sigma_3^+)\big)\,|0\rangle_{ph}\,|111\rangle =$$

$$= hw|0\rangle_{ph}\,3|111\rangle + g|1\rangle_{ph}(\,|011\rangle + \,|101\rangle + \,|110\rangle) =$$

$$= \sqrt{3}g(|1\rangle_{ph}\,\{2\rangle + 3hw|0\rangle_{ph}\,|111\rangle.$$

Поэтому гамильтониан рассматриваемой системы имеет вид

$$H = \begin{pmatrix} 3hw & 3g & 0 & 0 \\ 3g & 3hw & 2\sqrt{2}g & 0 \\ 0 & 2\sqrt{2}g & 3hw & \sqrt{3}g \\ 0 & 0 & \sqrt{3}g & 3hw \end{pmatrix}. \qquad (10)$$

Поиск собственных значений и собственных векторов оператора

Найдем собственные значения оператора. Для этого составим и решим характеристическое уравнение

$$\begin{vmatrix} 3hw-\lambda & 3g & 0 & 0 \\ 3g & 3hw-\lambda & 2\sqrt{2}g & 0 \\ 0 & 2\sqrt{2}g & 3hw-\lambda & \sqrt{3}g \\ 0 & 0 & \sqrt{3}g & 3hw-\lambda \end{vmatrix} = 0.$$

Получаем биквадратное уравнение

$$(3hw- \ )^4 - 20\ ^2(3hw- \ )^2 + 27\ ^4 = 0$$

и находим собственные значения

$$\lambda_0 = 3hw - g\sqrt{10+\sqrt{73}}$$

$$\lambda_1 = 3hw + g\sqrt{10+\sqrt{73}}$$

$$\lambda_2 = 3hw - g\sqrt{10-\sqrt{73}}$$

$$\lambda_3 = 3hw + g\sqrt{10-\sqrt{73}}$$

гамильтониана (10).

Отметим, что λ_0 – основной (минимальный) уровень энергии. Найдем собственные вектора и нормируем их, используя Wolfram Mathematica 12.3

$$|V_0\rangle = \frac{1}{d_0}\begin{pmatrix} \frac{(1-\sqrt{73})\sqrt{10+\sqrt{73}}}{6\sqrt{6}} \\ \frac{7+\sqrt{73}}{2\sqrt{6}} \\ \frac{-\sqrt{10+\sqrt{73}}}{\sqrt{3}} \\ 1 \end{pmatrix}$$

$$|V_1\rangle = \frac{1}{d_1}\begin{pmatrix} \frac{(-1+\sqrt{73})\sqrt{10+\sqrt{73}}}{6\sqrt{6}} \\ \frac{7+\sqrt{73}}{2\sqrt{6}} \\ \frac{\sqrt{10+\sqrt{73}}}{\sqrt{3}} \\ 1 \end{pmatrix}$$

$$|V_2\rangle = \frac{1}{d_2}\begin{pmatrix} \frac{(1+\sqrt{73})\sqrt{10-\sqrt{73}}}{6\sqrt{6}} \\ \frac{7-\sqrt{73}}{2\sqrt{6}} \\ \frac{-\sqrt{10-\sqrt{73}}}{\sqrt{3}} \\ 1 \end{pmatrix}$$

$$|V_3\rangle = \frac{1}{d_3}\begin{pmatrix} \frac{(-1-\sqrt{73})\sqrt{10-\sqrt{73}}}{6\sqrt{6}} \\ \frac{7-\sqrt{73}}{2\sqrt{6}} \\ \frac{\sqrt{10-\sqrt{73}}}{\sqrt{3}} \\ 1 \end{pmatrix}$$

Длины векторов, найденные с помощью Wolfram Mathematica 12.3

$$d_0 = d_1 = \sqrt{\frac{1}{6}(73+7\sqrt{73})}$$

$$d_2 = d_3 = \sqrt{\frac{1}{6}(73-7\sqrt{73})}$$

Отметим, что полученные вектора образуют ортонормированный базис.

Заключение

Главным результатом работы является составление базиса системы, гамильтониана и нахождение четырех независимых стабильных состояний трех индивидов и поля возбуждения. Под полем возбуждения подразумевается некоторое социальное возбуждение или психическое возбуждение малой группы индивидов, с которым они взаимодействуют. Заметим при этом, что состояния $|V_0\rangle$, соответствующее минимальной собственной энергии λ_0, является наиболее устойчивым в том смысле, что в этом состоянии рассматриваемый ансамбль уже не может испустить во внешнее пространство дополнительную энергию. В социальном плане это состояние с минимальной энергией характеризует условие наибольшей устойчивости группы из 3 индивидов. Предложенный подход позволяет использовать математическую модель Тависа–Каммингса из теоретической физики для определения психологического состояния в малых коллективах. Кроме того математический язык, используемый в социальный психологии, позволяет прояснить ее модели и методы.

Литература

Викторова 2023 – *Викторова Н.Б.* Основы математического моделирования квантовых вычислительных процессов. М.: Лань, 2023. 120 с.

Ожигов 2020 – *Ожигов Ю.И* Квантовый компьютер. М.: МАКС Пресс, 2020. 172 с.

Ожигов, Викторова, Сковорода 2016 – *Ожигов Ю.И., Викторова Н.Б., Сковорода Н.А.* Quantum revivals of a non-rabi type in a Jaynes-Cummings model // Theoretical and Mathematical Physics. 2016. Vol. 189 (2). С. 1673–1679.

Jaynes, Cummings 1963 – *Jaynes E.T., Cummings F.W.* Comparison of quantum and semiclassical radiation theories with application to the beam maser // Proc. IEEE. 1963. Vol. 51 (1). P. 89–109.

References

Jaynes, E.T. and Cummings, F.W. (1963), "Comparison of quantum and semiclassical radiation theories with application to the beam maser", *Proceedings of the IEEE,* vol. 51, no. 1, pp. 89–109.

Ozhigov, Yu. (2020), *Kvantovyi komp'yuter*, [A quantum computer], Max Press, Moscow, Russia.

Ozhigov, Yu., Victorova, N. and Skovoroda, N. (2016), "Quantum revivals of a non-rabi type in a Jaynes-Cummings model", *Theoretical and Mathematical Physics,* vol. 189, pp. 1673–1679.

Victorova, N.B. (2023), *Osnovy matematicheskogo modelirovaniya kvantovykh vychislitel'nykh protsessov* [Fundamentals of mathematical modeling of quantum computing processes], Lan', Moscow, Russia.

Информация об авторах

Надежда Б. Викторова, кандидат физико-математических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; nbvictorova@list.ru

Денис А. Морозов, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; morozovd170@gmail.com

Алексей В. Казанский, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; kazanskij02@mail.ru

Алехандро А. Никитин, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; alejandro.nikitin@gmail.com

Владислав D. Волков, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; volkov99vlad@gmail.com

Information about the authors

Nadezhda B. Victorova, Cand. of Sci (Physics and Mathematics), associate professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; nbvictorova@list.ru

Denis A. Morozov, student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; morozovd170@gmail.com

Alexei V. Kazanskii, student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; kazanskij02@mail.ru

Alekhandro A. Nikitin, student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; alejandro.nikitin@gmail.com

Vladislav D. Volkov, student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; volkov99vlad@gmail.com

Научный журнал
Вестник РГГУ
Серия «Информатика.
Информационная безопасность. Математика»
№ 3
2024

Дизайн обложки
Е.В. Амосова

Корректор
А.А. Леонтьева

Компьютерная верстка
Н.В. Москвина

Учредитель и издатель
Российский государственный гуманитарный университет
125047, Москва, Миусская пл., 6

Свидетельство о регистрации СМИ
ПИ № ФС77-72977 от 25.05.2018 г.
Периодичность 4 раза в год

Подписано в печать 15.08.2024
Выход в свет 22.08.2024
Формат 60×90 1/16
Уч.-изд. л. 8,5. Усл. печ. л. 8,6
Тираж 1050 экз. Свободная цена
Заказ № 2033

Отпечатано в типографии Издательского центра
Российского государственного гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru