НАУЧНЫЙ АСПЕКТ

na-journal.ru

2024

№3

ТОМ 27

УДК 001.8(082)

ББК 1
Н 34

Периодичность – 12 раз в год

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Свидетельство ПИ № ФС 77-84349

ISSN 2226-5694

Учредитель, главный редактор – Хасиятуллов Марат Габделахатович

Состав ред. коллегии представлен на сайте https://na-journal.ru

Адрес редакции:
420125, г. Казань, ул. Азата Аббасова, д. 21А, кв. 149

Издатель ООО «Аспект»

Адрес издательства:
443068, г. Самара, ул. Николая Панова, д. 16, оф. 34

Н 34 НАУЧНЫЙ АСПЕКТ № 3 2024. – Самара: Изд-во ООО «Аспект», 2024 . – Т27 . – 138 с.

Журнал «Научный аспект» является научным изданием и отражает результаты научной деятельности авторов по различным дисциплинам в области гуманитарных, естественных и технических наук.

УДК 001.8(082)
ББК 1

Почтовый адрес: 420100 г. Казань а/я 9
Официальный сайт: https://na-journal.ru
Электронная почта: public@na-journal.ru

Подписано к печати 16.04.2024
Дата выхода в свет 25.04.2024
Цена свободная

Бумага ксероксная. Печать оперативная. Заказ № .
Формат 60×84 /16. Объем 8,28 п.л. Тираж 100 экз.

Отпечатано в типографии «Куранты»
420029, г. Казань, Сибирский тракт, 34к14, оф. 317, тел. +7 (843) 216-12-71

Содержание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.8:004.056

Роль искусственного интеллекта в обеспечении информационной безопасности

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье рассматривается вклад искусственного интеллекта (ИИ) в развитие методов и технологий защиты информационных систем от киберугроз. В свете постоянно растущего объема данных и увеличения сложности кибератак, традиционные подходы к обеспечению безопасности становятся недостаточно эффективными. В этой связи искусственный интеллект представляется мощным инструментом, способным значительно повысить эффективность обнаружения и предотвращения кибератак. Подробно рассматриваются различные аспекты использования ИИ в кибербезопасности, включая машинное обучение для анализа аномалий в сетевом трафике, алгоритмы глубокого обучения для распознавания вредоносного ПО и системы искусственного интеллекта для автоматического реагирования на инциденты безопасности.*

***Abstract**: This paper discusses the contribution of artificial intelligence (AI) to the development of methods and technologies to protect information systems from cyber threats. In light of the ever-increasing volume of data and the complexity of cyberattacks, traditional security approaches are becoming insufficiently effective. In this regard, artificial intelligence appears to be a powerful tool that can significantly improve the efficiency of detecting and preventing cyberattacks. Various aspects of using AI in cybersecurity are discussed in detail. Those include machine learning for analyzing anomalies in network traffic, deep learning algorithms for malware recognition, and artificial intelligence systems for automatic response to security incidents.*

***Ключевые слова**: искусственный интеллект, информационная безопасность, киберугрозы, машинное обучение, распознавание вредоносного ПО, автоматическое реагирование на инциденты.*

***Keywords**: artificial intelligence, information security, cyber threats, machine learning, malware recognition, automatic incident response.*

1. Введение

В современном мире, где цифровая трансформация затрагивает все аспекты нашей жизни, вопросы информационной безопасности становятся все более актуальными и сложными. Увеличение объема цифровых данных, разнообразие электронных устройств и сложность сетевых инфраструктур создают фундамент для новых и более изощренных форм киберугроз. В этом контексте, традиционные подходы к обеспечению безопасности часто оказываются неэффективными, поскольку они не способны адаптироваться к динамически меняющейся киберсреде и выявлять сложные угрозы в реальном времени. В такой обстановке, применение искусственного интеллекта (ИИ) представляет собой перспективное направление для усиления мер по обеспечению информационной безопасности.

Искусственный интеллект, благодаря своим возможностям для обучения, анализа и принятия решений, открывает новые горизонты в борьбе с киберугрозами. ИИ может анализировать большие объемы данных на предмет выявления аномалий, обучаться на примерах предыдущих атак для лучшего распознавания угроз в будущем и автоматизировать процессы реагирования на инциденты безопасности. Таким образом, ИИ не только повышает эффективность обнаружения кибератак, но и способствует разработке более надежных и адаптируемых систем безопасности.

Искусственный интеллект (ИИ) играет ключевую роль в обеспечении информационной безопасности, предоставляя новые возможности для защиты цифровых систем и данных от киберугроз. Вот несколько основных аспектов, где ИИ вносит значительный вклад в кибербезопасность:

2. Обнаружение угроз и аномалий

Системы на основе ИИ способны анализировать огромные объемы данных значительно быстрее и эффективнее, чем это могли бы делать люди. Используя алгоритмы машинного обучения, они могут выявлять необычные паттерны поведения в сетевом трафике или системных журналах, которые могут указывать на наличие кибератаки. Это особенно важно

для обнаружения атак нулевого дня, когда угроза ещё не была идентифицирована и не существует сигнатур для её обнаружения.

3. Распознавание вредоносного ПО

Алгоритмы глубокого обучения, такие как нейронные сети, могут анализировать характеристики программного обеспечения и его поведение для определения, является ли оно вредоносным. Это включает в себя анализ поведенческих моделей, таких как необычные запросы к сети, попытки доступа к определённым файлам или изменения в системных настройках. Благодаря способности ИИ к обучению и адаптации, системы могут становиться всё более умелыми в распознавании новых и модифицированных вредоносных программ.

4. Автоматизация реагирования на инциденты

ИИ может автоматизировать ряд действий по реагированию на обнаруженные угрозы, ускоряя процесс нейтрализации атак и минимизируя их последствия. Это может включать в себя автоматическое отключение заражённых устройств от сети, блокировку подозрительного трафика или автоматическое применение обновлений безопасности. Такая автоматизация позволяет сократить время между обнаружением угрозы и её устранением, что критически важно для минимизации ущерба от кибератак.

5. Прогнозирование угроз

ИИ не только обеспечивает реактивные меры безопасности, но и может предсказывать будущие атаки на основе анализа текущих тенденций и данных о предыдущих инцидентах. Алгоритмы могут выявлять закономерности в кибератаках и использовать эту информацию для прогнозирования вероятных целей и методов следующих атак. Это позволяет организациям заранее укреплять защиту потенциально уязвимых систем и инфраструктур.

6. Повышение эффективности и снижение затрат

Внедрение ИИ в системы информационной безопасности позволяет автоматизировать рутинные задачи, такие как мониторинг сети и анализ логов, тем самым снижая нагрузку на специалистов по безопасности и позволяя им сосредоточиться на более сложных задачах. Это не только повышает общую эффективность системы безопасности, но и способствует оптимизации затрат.

7. Заключение

В заключение, статья подчеркивает критическую роль искусственного интеллекта (ИИ) в современной информационной безопасности, обрисовывая его как мощный инструмент, способный преобразовывать и укреплять защитные меры против киберугроз. Применение ИИ в области кибербезопасности открывает новые горизонты для обнаружения угроз, распознавания вредоносного ПО, автоматизации реагирования на инциденты и прогнозирования будущих атак, тем самым повышая эффективность защитных механизмов и снижая затраты на обеспечение информационной безопасности. Однако, внедрение ИИ также сопряжено с рядом вызовов и требует тщательного рассмотрения этических и практических аспектов. Важно стремиться к разработке и внедрению ИИ-систем с учетом принципов прозрачности, ответственности и защиты приватности, чтобы минимизировать потенциальные риски, связанные с автоматизацией и обработкой больших объемов данных. В заключение, интеграция искусственного интеллекта в стратегии информационной безопасности представляет собой не только технологическое новшество, но и вызов для организаций, стремящихся оставаться на шаг впереди киберугроз. Это требует непрерывного обучения, адаптации и сотрудничества между специалистами в области кибербезопасности, разработчиками ИИ и широкой общественностью. Перед лицом постоянно развивающихся угроз, искусственный интеллект остается ключевым инструментом в арсенале средств защиты, предлагая новые и эффективные способы обеспечения безопасности в цифровую эпоху.

Список литературы

1. Штеренберг С.И., Бударный Г.С., Чумаков И. В. Анализ безопасности доменных систем // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 587–588.
2. Штеренберг С.И., Бударный Г.С., Чумаков И. В. Методика обеспечения безопасности доменных систем доверенной зоны // Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. Санкт-Петербург, 2022. С. 621–625.
3. Альбовский И.А., Андреевский И.Л., Васильев М.Д., Васильева И.Н., Гатчин Ю.А., Гниденко И.Г., Егорова И.В., Иванченко А.С., Красильникова Е.В., Майорова Е.В., Сидоров Е.С., Соколовская С.А., Солодянников А.В., Стельмашонок В.Л., Стельмашонок Е.В., Сухостат В.В., Фоминцева А.П., Хуссамов Р.Р., Штеренберг С. И. Цифровая трансформация и проблемы информационной безопасности // Санкт-Петербург, 2023.
4. Штеренберг С. И. Моделирование интеллектуальной системы обнаружения вторжений на основе машинного и глубокого обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 935–940.
5. Штеренберг С. И. Разработка методологии защиты системы искусственного интеллекта в распределенных информационных системах // Вестник СибГУТИ. 2023. Т. 17. № 3. С. 78–86.

УДК 004.056

Будущее киберфизических систем: от теории к практике

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье рассматриваются перспективы и вызовы, связанные с развитием и внедрением киберфизических систем (КФС), которые интегрируют вычислительные процессы с физическими операциями в реальном времени. Уделено внимание обзору основных концепций и теоретических основ КФС, подчеркивая их важность для развития индустрии 4.0, умных городов, автоматизированного здравоохранения и экологически устойчивых систем управления. Подробно анализируется текущие достижения в области КФС, освещая прогресс в интеграции сенсорных технологий, машинного обучения, искусственного интеллекта и облачных вычислений для создания систем, способных к самооптимизации, самодиагностике и предиктивному управлению. Рассматриваются практические примеры успешного применения КФС в различных секторах, демонстрирующие их потенциал для повышения эффективности, безопасности и устойчивости операций.*

***Abstract**: This paper discusses the prospects and challenges associated with the development and deployment of cyber-physical systems (CPS) that integrate computational processes with real-time physical operations. Attention is given to an overview of the basic concepts and theoretical foundations of CPSs, emphasizing their importance for the development of Industry 4.0, smart cities, automated healthcare, and sustainable management systems. Current advances in the field of CPS are analyzed in detail, highlighting progress in integrating sensor technologies, machine learning, artificial intelligence, and cloud computing to create systems capable of self-optimization, self-diagnosis, and predictive control. Practical examples of successful applications of CPS in various sectors are discussed, demonstrating their potential to improve efficiency, safety, and sustainability of operations.*

***Ключевые слова**: киберфизические системы, умные города, машинное обучение, искусственный интеллект, облачные вычисления, кибербезопасность, конфиденциальность данных, предиктивное управление, самооптимизация систем.*

***Keywords**: cyber-physical systems, smart cities, machine learning, artificial intelligence, cloud computing, cybersecurity, data privacy, predictive control, self-optimisation of systems.*

1. Введение

Будущее киберфизических систем (КФС) представляется как эра, в которой глубокая интеграция между вычислительными процессами и физическими объектами станет не просто обыденностью, но и основой для новых технологических прорывов и социальных изменений. Этот переход от теории к практике ознаменуется рядом ключевых развитий и вызовов.

2. Теоретические основы

Киберфизические системы обладают уникальной способностью координировать, контролировать и интегрировать физические процессы с помощью компьютерных алгоритмов и сетей. В теоретическом плане, КФС строятся на принципах реального времени, автономности, эффективности и адаптивности. Разработка и изучение КФС требует мультидисциплинарного подхода, включающего элементы информатики, системного анализа, механики, электроники и робототехники.

3. Переход к практике

В практическом плане, будущее КФС связано с их внедрением в самые разные сферы жизни:

- Промышленность 4.0: КФС станут основой для создания полностью автоматизированных и оптимизированных производственных линий, способных к самостоятельному принятию решений на основе данных с сенсоров и из других источников.
- Умные города: Интеграция КФС в инфраструктуру городов приведет к повышению их эффективности, безопасности и устойчивости, от умного освещения и управления трафиком до мониторинга окружающей среды и энергопотребления.
- Здравоохранение: КФС обеспечат более высокий уровень медицинского обслуживания через автоматизированное мониторинговое оборудование, управление данными пациентов и даже роботизированную хирургию.

- Транспорт: Развитие автономных транспортных средств и интеллектуальных систем управления трафиком станет возможным благодаря прогрессу в области КФС.

4. Вызовы и перспективы

Вызовы и перспективы развития киберфизических систем (КФС) охватывают широкий спектр аспектов, начиная от технических и технологических проблем до этических, социальных и юридических вопросов. Давайте рассмотрим их более подробно.

1. Вызовы

Кибербезопасность: С ростом сложности и распространенности КФС увеличивается и риск кибератак. Защита критически важной инфраструктуры, такой как энергосистемы, транспорт и здравоохранение, от хакерских атак, требует новых подходов к безопасности и постоянного обновления защитных механизмов.

Конфиденциальность данных: Сбор и анализ больших объемов данных, необходимых для работы КФС, порождают вопросы приватности. Как обеспечить конфиденциальность личных данных при их обработке системами?

Этические и юридические вопросы: Внедрение КФС в повседневную жизнь поднимает вопросы ответственности за принимаемые системами решения, особенно в критически важных сферах, таких как медицина и транспорт. Кто будет нести ответственность за ошибки или сбои в работе КФС?

2. Перспективы

Инновации и экономический рост: КФС способны стимулировать развитие новых технологий и бизнес-моделей, открывая пути для инноваций и создания новых рабочих мест в высокотехнологичных отраслях.

Повышение качества жизни: КФС обещают существенные улучшения в управлении ресурсами, здравоохранении, образовании и транспорте,

делая эти и многие другие аспекты жизни более эффективными, безопасными и удобными.

Устойчивое развитие: Внедрение КФС может способствовать более рациональному использованию ресурсов, снижению вредных выбросов и оптимизации производственных процессов, что в свою очередь способствует достижению целей устойчивого развития.

Умные города и автономный транспорт: Развитие КФС является ключом к созданию умных городов с эффективным управлением городскими ресурсами и услугами, а также к развитию автономных транспортных систем, способных сократить число дорожно-транспортных происшествий и улучшить мобильность городских жителей.

5. Заключение

В заключение, статья подчеркивает значимость киберфизических систем как фундаментального элемента в следующей волне технологических инноваций и социальных изменений. Переход от теоретических основ к практическому внедрению КФС открывает безграничные возможности для развития промышленности, улучшения городской инфраструктуры, повышения качества медицинских услуг и оптимизации транспортных систем. Вместе с тем, он ставит перед обществом и специалистами серьезные вызовы, включая обеспечение кибербезопасности, защиту персональных данных, решение этических и юридических вопросов. Успешное преодоление этих препятствий потребует скоординированных усилий ученых, инженеров, политиков и общественности.

Список литературы

1. Красов А.В., Шакин Д.Н., Лансере Н.Н., Фадеев И.И., Гельфанд А. М. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии // Офтальмохирургия. 2022. № S4. С. 92–101.
2. Штеренберг С.И., Бударный Г.С., Чумаков И. В. Методика обеспечения безопасности доменных систем доверенной зоны // Региональная

информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. Санкт-Петербург, 2022. С. 621–625.
3. Гельфанд А.М., Сигачева В.В., Архипов А.В., Сиротина Л. К. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 21–27.
4. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д. В. Построение доверенной вычислительной среды. Санкт-Петербург, 2019.
5. Штеренберг С.И., Москальчук А.И., Коптелова В.А., Виноградова О. М. Разработка методов обеспечения безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 32–38.

УДК 004

Прогрессивные веб-приложения (PWA): будущее мобильных и веб-технологий

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье проводится анализ возможностей и перспектив прогрессивных веб-приложений как ключевого фактора эволюции цифровой экосистемы. Обозриваются основные характеристики PWA, включая их способность работать оффлайн, быструю загрузку и возможность добавления на главный экран устройства, что приближает их функциональность к нативным приложениям. Основное внимание уделяется техническим аспектам разработки PWA, в том числе использованию Service Workers, манифеста веб-приложения и API для кеширования. Статья подчеркива-*

ет преимущества PWA в контексте улучшения пользовательского опыта, повышения производительности и оптимизации поисковой оптимизации (SEO). Также отдельное внимание уделяется вызовам и ограничениям, с которыми разработчики могут столкнуться при создании PWA, включая вопросы совместимости и производительности на различных устройствах.

***Abstract**: This paper analyzes the opportunities and prospects of progressive web applications as a key driver of the digital ecosystem evolution. Key characteristics of PWAs are reviewed, including their ability to operate offline, fast loading, and the ability to be added to a device's home screen, bringing their functionality closer to native applications. The focus is on the technical aspects of PWA development, including the use of Service Workers, a web application manifest, and caching APIs. The paper highlights the benefits of PWAs in the context of improving user experience, performance, and search engine optimization (SEO). There is also a separate focus on the challenges and limitations developers may face when building PWAs, including compatibility and performance issues across devices.*

***Ключевые слова**: прогрессивные веб-приложения, мобильные технологии, веб-разработка, оффлайн функциональность, производительность веб-приложений, кеширование данных, кросс-платформенная совместимость, быстрая загрузка, будущее веб-технологий.*

***Keywords**: progressive web applications, mobile technology, web development, offline functionality, web application performance, data caching, cross-platform compatibility, fast loading, future of web technology.*

1. Введение

В последние годы цифровой мир испытывает значительные трансформации, особенно в сфере мобильных и веб-технологий. На передний план выходят прогрессивные веб-приложения (PWA), которые обещают революционизировать наше восприятие и использование мобильного и вебсофта. Эти приложения сочетают в себе лучшие качества традиционных веб-сайтов и мобильных приложений, предлагая пользователю улучшенный опыт благодаря их скорости, надежности и функциональности. В этом введении мы рассмотрим, что делает прогрессивные веб-приложения настолько перспективными и почему они могут считаться будущим мобильных и веб-технологий. Прогрессивные веб-приложения представляют собой веб-приложения, но с расширенными возможностями, такими как

работа в офлайн-режиме, получение push-уведомлений и доступ к аппаратным средствам устройства, которые традиционно были доступны только для нативных приложений. Это достигается благодаря современным веб-API и стратегиям кеширования, позволяющим PWA мгновенно загружаться, даже при слабом интернет-соединении или его отсутствии. Благодаря этим качествам, PWA обещают преобразить способы разработки, распространения и использования приложений в цифровой эпохе. В основе успеха PWA лежит стремление к улучшению пользовательского опыта на всех уровнях: от скорости загрузки и работоспособности в различных сетевых условиях до удобства установки и автоматических обновлений. При этом разработчики получают возможность создавать единое приложение, которое эффективно функционирует как на десктопах, так и на мобильных устройствах, минимизируя трудозатраты и сокращая время на разработку и поддержку. Таким образом, PWA не только улучшают взаимодействие с пользователем, но и предлагают значительные преимущества для бизнеса и разработчиков.

Прогрессивные веб-приложения (PWA) представляют собой следующий шаг в развитии веб-технологий, смешивая границы между веб-сайтами и мобильными приложениями. Они объединяют лучшее из обоих миров, предлагая пользователю высококачественный и согласованный опыт независимо от устройства и качества интернет-соединения. Вот ключевые аспекты, которые делают PWA будущим мобильных и веб-технологий:

2. Основные характеристики PWA

Надежность: благодаря использованию Service Workers, PWA могут загружаться и функционировать даже в условиях нестабильного или отсутствующего интернет-соединения.

Быстрота: PWA оптимизированы для мгновенной загрузки и плавного взаимодействия, что существенно улучшает пользовательский опыт.

Зацепление: Способность отправлять push-уведомления и возможность добавления иконки приложения на главный экран устройства повышают вовлеченность пользователя.

3. Технологические основы

Service Workers: Скрипты, работающие в фоновом режиме и отвечающие за кеширование контента для работы оффлайн, перехват запросов к сети, а также возможность отправки push-уведомлений.

Манифест веб-приложения: JSON-файл, который позволяет разработчикам устанавливать внешний вид приложения на главном экране, включая иконку, цвета и полноэкранный режим.

HTTPS: PWA требуют использования HTTPS для обеспечения безопасности данных пользователя.

4. Преимущества для бизнеса и разработчиков

Универсальность: Разработчики могут создавать единое приложение, которое работает на любом устройстве и в любом браузере, сокращая время и затраты на разработку и поддержку.

Улучшение SEO: поскольку PWA являются в основном веб-сайтами, они индексируются поисковыми системами, что способствует лучшей видимости в интернете.

Повышение конверсии: Быстрая загрузка и улучшенный пользовательский опыт приводят к снижению отказов и увеличению конверсии.

5. Вызовы разработки PWA

Совместимость: хотя большинство современных браузеров поддерживают ключевые функции PWA, существуют различия в реализации и поддержке функций между разными браузерами и операционными системами.

Взаимодействие с устройством: В то время как нативные приложения могут без ограничений использовать возможности устройства, PWA все еще сталкиваются с некоторыми ограничениями в доступе к аппаратному обеспечению.

6. Будущее PWA

PWA продолжают развиваться, и с каждым обновлением стандартов веба их возможности расширяются. С улучшением поддержки браузерами и операционными системами, а также с ростом внимания к вопросам производительности и пользовательского опыта, PWA обещают занять значительную нишу в мире мобильных и веб-технологий, предлагая более гибкие и эффективные решения для разработчиков и бизнеса.

7. Заключение

В заключение статьи «Прогрессивные веб-приложения (PWA): будущее мобильных и веб-технологий», можно подчеркнуть, что PWA представляют собой мощный инструмент в арсенале современных веб-разработчиков и бизнеса, способный значительно трансформировать способы взаимодействия пользователей с мобильным и веб-контентом. Благодаря их уникальным характеристикам, таким как способность работать оффлайн, быстрая загрузка, возможность получения push-уведомлений и простота установки на главный экран, прогрессивные веб-приложения не только улучшают пользовательский опыт, но и открывают новые возможности для повышения вовлеченности и удержания пользователей. С учетом текущих трендов и потенциала технологии, PWA обладают всеми необходимыми качествами, чтобы стать доминирующим форматом мобильных приложений в ближайшем будущем, предлагая пользователям и бизнесам новые возможности для взаимодействия, удовлетворения потребностей и достижения коммерческих целей. Прогрессивные веб-приложения не просто отражают будущее мобильных и веб-технологий — они активно формируют его, создавая новые стандарты для цифрового пространства.

Список литературы

1. Красов А.В., Гельфанд А.М., Фадеев И.И., Казанцев А. А. Программная реализация средств предотвращений вторжений и аномалий сете-

вой инфраструктуры // Свидетельство о регистрации программы для ЭВМ RU 2020617705, 10.07.2020. Заявка № 2020616731 от 29.06.2020.
2. Гельфанд А.М., Казанцев А.А., Красов А.В., Орлов Г. А. Оценка рисков и угроз безопасности в среде “Умный дом” // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 316–321.
3. Волкогонов В.Н., Казанцев А.А., Катасонов А.И., Орлов Г. А. Анализ безопасности wi-fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 270–275.
4. Майоров А.В., Красов А.В., Ушаков И. А. Модель представления больших данных о компьютерных атаках в формате nosql // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47–54.
5. Красов А. В. Методы выявления сетевой стеганографии // Методы и технические средства обеспечения безопасности информации. 2023. № 32. С. 52–54.

УДК 004.8

Использование машинного обучения для улучшения пользовательского опыта в мобильных приложениях

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья посвящена анализу различных методов и стратегий применения машинного обучения в процессе разработки мобильных приложений. Она начинается с обзора основных принципов машинного обучения и способов его интеграции в мобильные платформы, включая обработку естественного языка, компьютерное зрение и прогнозирование поведения пользователей. В статье также рассматриваются*

вызовы и ограничения, связанные с внедрением машинного обучения в мобильные приложения, включая вопросы конфиденциальности данных, требования к вычислительным ресурсам и необходимость обеспечения безопасности пользовательской информации.

***Abstract**: The article is devoted to analyzing various methods and strategies of applying machine learning in the process of mobile application development. It begins with an overview of the basic principles of machine learning and ways it can be integrated into mobile platforms, including natural language processing, computer vision, and predicting user behavior. The paper also discusses the challenges and limitations of implementing machine learning in mobile applications, including data privacy issues, computational resource requirements, and the need to secure user information.*

***Ключевые слова**: машинное обучение, мобильные приложения, обработка естественного языка, автоматизация взаимодействия, интерфейс пользователя, оптимизация производительности приложений, конфиденциальность данных, интеграция машинного обучения, инновационные технологии в мобильной разработке.*

***Keywords**: machine learning, mobile applications, natural language processing, NLP, interaction automation, user interface, UI, application performance optimisation, data privacy, machine learning integration, innovative technologies in mobile development.*

1. Введение

В эпоху цифровизации и постоянного технологического прогресса мобильные приложения стали неотъемлемой частью повседневной жизни миллионов пользователей по всему миру. Они предоставляют широкий спектр функциональности, начиная от общения и развлечений до образования, здоровья и финансов, делая технологии доступными и удобными для широкой аудитории. В таком контексте важность обеспечения высококачественного пользовательского опыта (UX) невозможно переоценить. UX становится ключевым дифференциатором, определяющим успех или неудачу мобильного приложения на рынке, где конкуренция продолжает усиливаться.

С развитием искусственного интеллекта (ИИ) и машинного обучения (ML) перед разработчиками мобильных приложений открываются новые возможности для улучшения пользовательского опыта. Машинное обучение предлагает мощные инструменты для анализа больших объемов данных о пользовательском поведении, позволяя создавать персонали-

зированные и адаптивные пользовательские интерфейсы, предсказывать предпочтения и потребности пользователей, а также автоматизировать рутинные процессы, повышая удобство и эффективность использования приложений.

2. Использование машинного обучения (ML)

Использование машинного обучения (ML) для улучшения пользовательского опыта (UX) в мобильных приложениях открывает впечатляющие возможности для разработчиков и дизайнеров. Оно позволяет создавать приложения, которые не только интуитивно понятны и удобны в использовании, но и способны предсказывать потребности пользователей, предлагать персонализированный контент и обеспечивать высокий уровень интерактивности. Рассмотрим ключевые аспекты использования машинного обучения для улучшения UX в мобильных приложениях.

3. Персонализация

Одним из наиболее значимых преимуществ машинного обучения является возможность персонализации пользовательского опыта. Алгоритмы ML анализируют данные о предпочтениях пользователя, истории взаимодействия с приложением и поведении в целом. Это позволяет приложениям адаптироваться к каждому пользователю, предлагая контент, продукты или услуги, которые наиболее актуальны и интересны именно ему. Например, музыкальные стриминговые сервисы используют машинное обучение для создания персонализированных плейлистов.

4. Улучшение поиска

Машинное обучение также может существенно улучшить поисковые механизмы внутри приложений. Благодаря обработке естественного языка (NLP) и алгоритмам глубокого обучения, приложения могут более точно понимать запросы пользователей и предлагать релевантные результаты, даже если запрос был введен с ошибками или опечатками.

5. Прогнозирование и предсказания

Алгоритмы машинного обучения могут анализировать большие объемы данных о поведении пользователей и на основе этого делать предсказания о их будущих действиях. Это может быть использовано для предсказания спроса на определенные продукты в электронной коммерции, для предложения статей или новостей, которые с большой вероятностью заинтересуют пользователя, или для предупреждения о потенциальных проблемах в использовании приложения.

6. Автоматизация обслуживания клиентов

Машинное обучение позволяет автоматизировать многие аспекты обслуживания клиентов, например, через использование чат-ботов. Эти интеллектуальные ассистенты могут обрабатывать запросы пользователей в реальном времени, предоставляя быстрые и релевантные ответы, что значительно повышает удовлетворенность пользователей и эффективность поддержки.

7. Улучшение интерфейса и взаимодействия

Использование машинного обучения также может способствовать оптимизации пользовательского интерфейса и процесса взаимодействия с приложением. Анализируя, как пользователи взаимодействуют с приложением, можно выявить слабые места в дизайне интерфейса и оптимизировать их для улучшения общего пользовательского опыта.

8. Вызовы и ограничения

Несмотря на многочисленные преимущества, использование машинного обучения в мобильных приложениях не лишено вызовов и ограничений. Одним из главных вызовов является необходимость обработки больших объемов данных, что требует значительных вычислительных ресурсов и может повлиять на производительность приложения, особенно в усло-

виях ограниченной вычислительной мощности мобильных устройств. Кроме того, важным аспектом является обеспечение конфиденциальности и защиты данных, поскольку приложения собирают и анализируют личную информацию пользователей.

9. Заключение

Использование машинного обучения для улучшения пользовательского опыта в мобильных приложениях открывает перед разработчиками новые возможности для создания инновационных, удобных и безопасных приложений. Оно позволяет не только значительно повысить уровень удовлетворенности пользователей, но и дает компаниям конкурентное преимущество на рынке. Однако для успешной интеграции машинного обучения в процесс разработки приложений необходим комплексный подход, учитывающий как технические аспекты, так и вопросы безопасности и конфиденциальности данных.

Список литературы

1. Абраменко Г. Т., Лансере Н. Н., Фадеев И. И. Анализ особенностей субъектов критической информационной инфраструктуры Российской Федерации, функционирующих в сфере науки //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 49–54.
2. Радынская В. Е., Поляничева А. В., Ахрамеева К. А. Разработка метода защиты ядра программных приложений с применением самомодифицирующегося кода //Региональная информатика и информационная безопасность.— 2019. — С. 136–141.
3. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022).— 2022. — С. 572–573.
4. Скорых М. А., Израилов К. Е., Башмаков А. В. Задача ориентированное сравнение средств анализа сетевого трафика // Теория и практика обеспечения информационной безопасности.— 2021. — С. 103–107.

5. Шестаков А. В. Начала деканаук и технологий СПбГУТ // Труды учебных заведений связи.— 2023. — Т. 8.— № . 4. — С. 4–11.

УДК 004

Влияние технологии блокчейн на разработку мобильных приложений

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье освещаются основные концепции блокчейна, включая архитектуру распределенного реестра, криптографическую безопасность, смарт-контракты и консенсусные механизмы. Детально анализируются, как эти особенности могут быть использованы для решения распространенных проблем в мобильной разработке, таких как безопасность данных, идентификация и аутентификация пользователей, а также управление цифровыми активами и транзакциями. Также в статье подробно рассматриваются технические и организационные аспекты внедрения блокчейн-технологий в процесс разработки мобильных приложений. Проводится анализ ключевых факторов, влияющих на выбор блокчейн-платформы для конкретного приложения, включая скорость транзакций, стоимость внедрения и эксплуатации, а также поддержку со стороны разработчиков и сообщества. Освещаются вопросы интеграции блокчейна с существующими мобильными платформами и операционными системами, а также рассматриваются потенциальные сложности и ограничения, связанные с этим процессом.*

***Abstract**: This paper highlights the basic concepts of blockchain, including distributed ledger architecture, cryptographic security, smart contracts, and consensus mechanisms. Ways these features can be used to solve common problems in mobile development such as data security, user identification and authentication, and digital asset and transaction management are analyzed in detail. The paper also elaborates on the technical and organizational aspects of implementing blockchain technologies in the mobile application development process. It analyzes the key factors that influence the choice of a blockchain platform for a particular application, including transaction speed, cost of implementation and operation, and developer and community support. The integration of blockchain with existing mobile platforms and operating systems is covered, and the potential complexities and limitations associated with this process are discussed.*

Ключевые слова: *блокчейн, разработка мобильных приложений, децентрализованные приложения, криптографическая безопасность, идентификация и аутентификация, защита данных, инновации в мобильной разработке, интеграция технологий.*

Keywords: *blockchain, mobile application development, decentralised applications (DApps), cryptographic security, identification and authentication, data protection, innovation in mobile development, technology integration.*

1. Введение

В последние годы технология блокчейн вызвала значительный интерес среди исследователей и практиков в различных областях, превращаясь из основы криптовалют в мощный инструмент для создания инновационных решений в финансовом секторе, цепочках поставок, государственном управлении и многих других сферах. Одним из наиболее перспективных направлений применения блокчейна является разработка мобильных приложений, где он обещает принести революцию в понимание безопасности, прозрачности и децентрализации.

Технология блокчейн представляет собой распределенный реестр данных, который обеспечивает высокий уровень безопасности и надежности за счет криптографии и механизмов консенсуса. Эти характеристики делают блокчейн идеальным для разработки мобильных приложений, которые требуют защиты личных данных, обеспечения транзакционной безопасности и создания доверительной среды для пользователей.

2. Блокчейн в разработке мобильных приложений

Технология блокчейн оказала значительное влияние на многие отрасли, и разработка мобильных приложений не исключение. Это влияние можно рассмотреть с нескольких ключевых аспектов:

1. Улучшение безопасности и приватности

Блокчейн применяет криптографические алгоритмы для защиты данных, делая почти невозможным несанкционированный доступ или фальсификацию информации. В мобильных приложениях это может повысить безопасность пользовательских данных, особенно в приложениях для об-

мена сообщениями, финансовых операций и личной информации. Также, за счет децентрализации, данные пользователя могут храниться в распределенной сети, уменьшая риски, связанные с централизованными базами данных.

2. Транзакции без посредников

Блокчейн позволяет проводить транзакции напрямую между пользователями без необходимости в посредниках, таких как банки или платежные системы. Это может сократить время и стоимость транзакций в мобильных приложениях, связанных с передачей ценностей, таких как платежи или переводы денег.

3. Применение смарт-контрактов

Смарт-контракты — это самоисполняющиеся контракты с условиями сделки, прямо встроенными в код. В мобильных приложениях это может использоваться для автоматизации выполнения сделок, управления доступом к услугам или контенту, без необходимости вмешательства третьих сторон.

4. Повышение прозрачности и доверия

Блокчейн предоставляет полную прозрачность проведения транзакций и изменений в данных, что может повысить доверие пользователей к мобильным приложениям. Это особенно важно для приложений, связанных с финансами, торговлей или любыми операциями, где требуется верификация истории транзакций.

5. Создание новых типов приложений

Технология блокчейн открывает путь для создания новых типов мобильных приложений, таких как децентрализованные приложения (DApps), которые работают на блокчейн-платформах и обладают всеми преимуществами блокчейна, включая безопасность, прозрачность и отсутствие централизованного контроля.

3. Вызовы

Несмотря на многочисленные преимущества, интеграция блокчейна в мобильные приложения также представляет определенные вызовы, включая сложности масштабирования, потребление ресурсов (напри-

мер, батареи на мобильных устройствах из-за интенсивных вычислений), а также необходимость в специализированных знаниях и навыках для разработки на блокчейн-платформах.

4. Заключение

Влияние технологии блокчейн на разработку мобильных приложений огромно и многообещающе. Оно открывает новые возможности для безопасности, прозрачности и эффективности, однако требует от разработчиков преодоления определенных технических и концептуальных вызовов. Разработка на блокчейне требует глубокого понимания криптографии, сетевых протоколов и принципов децентрализации, что может стать барьером для традиционных разработчиков мобильных приложений. К тому же, вопросы масштабируемости блокчейн-сетей и их способность обрабатывать большое количество транзакций без существенных задержек остаются актуальными для многих платформ.

Для реализации полного потенциала блокчейна в разработке мобильных приложений важно сосредоточить усилия на улучшении пользовательского опыта и интерфейсов, адаптированных под особенности блокчейн-технологий, упрощении взаимодействия с блокчейн-сетями и снижении порога входа для пользователей и разработчиков.

В будущем можно ожидать дальнейшее сближение мира блокчейна и мобильных технологий, поскольку исследования и разработки в области блокчейна продолжат предлагать новые решения для улучшения масштабируемости, производительности и доступности. Это будет способствовать созданию новых типов мобильных приложений, которые могут кардинально изменить многие отрасли, предлагая пользователям уровень безопасности, доверия и взаимодействия, недостижимый для традиционных технологий.

Список литературы

1. Кибирев М. П., Миняев А. А., Скорых М. А. Сравнительный анализ утилит для проведения атаки PTH //Актуальные проблемы инфо-

телекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 710–715.
2. Алехин Р. В. и др. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры // Офтальмохирургия.— 2022.— № . 4s. — С. 115–122.
3. Макарова А. Д. и др. Рассмотрение компонентов технологии доверительных отношений freeipa, а также вопрос о целесообразности перехода на данное решение // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 775–778.
4. Алехин Р. В. и др. Анализ защищенности облачной инфраструктуры openstack при эмуляции атаки вида ddos на узлах инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 52–55.
5. Бударный Г. С. и др. Исследование концепции ядра в различных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 411–417.

УДК 004

Сетевые функции виртуализации (NFV): преобразование архитектуры телекоммуникационных сетей

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная статья посвящена анализу принципов работы и основных преимуществ технологии NFV, а также ее влиянию на развитие и эволюцию архитектуры современных телекоммуникационных сетей. В статье рассматриваются ключевые аспекты NFV, включая виртуализацию сетевых функций, децентрализацию управления сетями и интеграцию с технологией программно-определяемых сетей (SDN). Особое внимание в статье уделено анализу того, как NFV способствует повышению гибкости и масштабируемости сетей, упрощению внедрения новых сервисов, а также*

значительному снижению операционных и капитальных затрат за счет эффективного использования ресурсов и централизованного управления. Приводятся примеры успешного применения NFV в телекоммуникационных сетях различных операторов, а также обсуждаются вызовы и перспективы дальнейшего развития этой технологии.

***Abstract**: This article is devoted to analyzing the operating principles and main advantages of NFV technology, as well as its impact on the development and evolution of the architecture of modern telecommunication networks. The article discusses key aspects of NFV, including virtualization of network functions, decentralization of network management, and integration with software-defined networking (SDN) technology. The paper focuses on how NFV can improve network flexibility and scalability, simplify the deployment of new services, and significantly reduce operating and capital costs through efficient resource utilization and centralized management. Examples of successful application of NFV in telecommunication networks of various operators are given, and challenges and prospects for further development of this technology are discussed.*

***Ключевые слова**: сетевые функции виртуализации, программно-определяемые сети, телекоммуникационные сети, масштабируемость сетей, интеграция сетевых сервисов, эволюция телекоммуникационных сетей, будущее телекоммуникаций, эффективность использования ресурсов, централизованное управление сетью, новые сервисы телекоммуникаций.*

***Keywords**: network function virtualisation, NFV, software-defined networking, SDN, telecommunications networks, network scalability, network service integration, telecommunications network evolution, future of telecommunications, resource efficiency, centralised network management, new telecommunications services.*

1. Введение

В последнее десятилетие индустрия телекоммуникаций столкнулась с беспрецедентным ростом спроса на свои услуги, что обусловлено стремительным развитием интернета вещей (IoT), мобильных технологий и облачных вычислений. Эти тенденции не только способствовали увеличению объема передаваемых данных, но и повысили требования к гибкости, масштабируемости и надежности сетевой инфраструктуры. В ответ на эти вызовы телекоммуникационная отрасль активно исследует и внедряет новые подходы к проектированию и управлению сетями, среди которых особое место занимает технология сетевых функций виртуализации (NFV).

Сетевые функции виртуализации (NFV) представляют собой инновационный подход к архитектуре телекоммуникационных сетей, который коренным образом меняет традиционное понимание сетевой инфраструктуры. Основная идея NFV заключается в отделении сетевых функций от физического оборудования, что позволяет реализовывать эти функции в виде виртуального программного обеспечения на стандартном коммерческом серверном оборудовании, в облаке или в виртуализированной среде. Это включает в себя такие сетевые функции, как брандмауэры, балансировщики нагрузки, шлюзы и даже целые виртуальные сети.

2. Преобразование архитектуры телекоммуникационных сетей

1. Гибкость и масштабируемость

NFV значительно повышает гибкость и масштабируемость телекоммуникационных сетей. Сетевые операторы могут быстро развертывать и масштабировать сетевые функции в зависимости от текущих потребностей без необходимости вложений в специализированное аппаратное обеспечение.

2. Снижение затрат

Одним из ключевых преимуществ NFV является снижение капитальных (CAPEX) и операционных (OPEX) затрат. Экономия достигается за счет использования стандартного аппаратного обеспечения и автоматизации процессов управления сетью, что уменьшает необходимость в физическом оборудовании и упрощает обслуживание.

3. Ускорение внедрения новых услуг

NFV позволяет телекоммуникационным компаниям быстрее внедрять новые сервисы и функциональность, поскольку разработка и тестирование виртуализированных сетевых функций может происходить в более короткие сроки.

3. Вызовы и решения

Внедрение NFV сопряжено с рядом вызовов, включая вопросы безопасности, управления многослойными виртуализированными сетями

и интеграции с существующей инфраструктурой. Однако эти проблемы активно решаются через разработку стандартов и протоколов, а также внедрение систем управления и оркестрации NFV, которые обеспечивают централизованное управление виртуализированными сетевыми функциями и ресурсами.

4. Интеграция с SDN

Интеграция NFV с технологией программно-определяемых сетей (SDN) открывает дополнительные возможности для создания гибких и автоматизированных сетевых архитектур. В то время как SDN позволяет централизованно управлять потоком данных в сети, NFV предоставляет инфраструктуру для развертывания и управления сетевыми функциями. Совместное использование NFV и SDN способствует созданию полностью виртуализированных сетей, которые легко адаптируются под меняющиеся бизнес-потребности и требования к трафику.

5. Перспективы и будущее развития

Сочетание NFV и SDN представляет собой будущее телекоммуникационных сетей, обещая революцию в способах построения, управления и эксплуатации сетевой инфраструктуры. По мере развития этих технологий можно ожидать появление новых бизнес-моделей и сервисов, которые будут полагаться на высокую гибкость, масштабируемость и экономическую эффективность виртуализированных сетей.

Инновации в сервисах: NFV облегчает внедрение новаторских сервисов, таких как виртуализированные сети для Интернета вещей (IoT), мобильные виртуальные сети операторов (MVNO) и облачные вычисления на краю сети (edge computing), которые требуют высокой степени гибкости и динамичности сетевой инфраструктуры.

Управление и оркестрация: Развитие инструментов управления и оркестрации является критически важным для масштабирования и эффективной эксплуатации виртуализированных сетевых функций. Продвинутые системы управления NFV позволяют автоматизировать развертывание,

мониторинг, масштабирование и лечение сетевых сервисов, снижая операционные затраты и упрощая управление сложными сетевыми конфигурациями.

Стандартизация и совместимость: Продолжающаяся работа над стандартизацией NFV и улучшение совместимости между различными вендорами и решениями являются ключевыми для обеспечения широкого внедрения и успешного функционирования виртуализированных сетевых сервисов. Международные организации и консорциумы, такие как ETSI, активно работают над разработкой и утверждением стандартов NFV.

6. Заключение

В заключение, технология сетевых функций виртуализации (NFV) открывает новые возможности для телекоммуникационной индустрии, позволяя создавать более гибкие, экономически эффективные и инновационные сетевые решения. Продолжающееся развитие NFV и его интеграция с другими передовыми технологиями, такими как SDN и облачные вычисления, будут способствовать трансформации телекоммуникационных сетей и способов предоставления сервисов в ближайшем будущем. Эта трансформация будет сопровождаться появлением новых сервисных моделей и возможностей для конечных пользователей, включая улучшенное качество связи, более широкий спектр сервисов на основе облачных технологий и персонализированные сетевые услуги, адаптированные под индивидуальные потребности. Виртуализация сетевых функций также способствует развитию глобальной мобильности и поддержке устройств Интернета вещей, обеспечивая бесшовную интеграцию и взаимодействие между различными устройствами и платформами.

Список литературы

1. Шариков П. И., Красов А. В. Исследование возможности вложения цифрового водяного знака в байт-код путем замены уязвимого байт-кода Java класса //Информационная безопасность регионов России (ИБРР-2017).— 2017. — С. 499–500.

2. Красов А. В., Шариков П. И. Метод использования самомодифицирующегося кода для защиты приложения с кодовым зашумлением //Телекоммуникационные и вычислительные системы.— 2016. — С. 118–121.
3. Шемякин С. Н. и др. Выяснение криптографических свойств булевых функций шифра «Магма» //Экономика и качество систем связи.— 2021.— № . 1 (19). — С. 67–73.
4. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 4. — С. 61–65.
5. Кушнир Д. В., Шемякин С. Н. Вестник Санкт-Петербургского государственного университета технологии и дизайна. серия 1: естественные и технические науки: Санкт-Петербургский государственный университет промышленных технологий и дизайна.— № . 4. — С. 63–67.

УДК 004

Квантовые сети: от теоретических основ до практического применения

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье представлен всесторонний обзор развития и текущего состояния технологии квантовых сетей, начиная с их теоретических основ и заканчивая реальными случаями использования и практическими реализациями. Подробно рассматриваются ключевые концепции и принципы, лежащие в основе квантовой коммуникации и квантовой криптографии, такие как квантовая запутанность и квантовое распределение ключей, которые обеспечивают безусловную безопасность передачи данных. Особое внимание уделяется рассмотрению успешных экспериментов и пилотных проектов в области квантовых сетей, проведенных в разных странах мира. Представлен анализ результатов этих проектов, демонстрирующих реальную возможность создания квантово-защищенных коммуникационных линий для передачи конфиденциальной информации в коммерческих и государственных сетях.*

***Abstract**: This paper provides a comprehensive overview of the development and current state of quantum network technology, starting from its theoretical foundations and ending with actual use cases and practical implementations. The key concepts and principles underlying quantum communication and quantum cryptography, such as quantum entanglement and quantum key distribution, which provide unconditional security for data transmission, are discussed in detail. Special attention is given to reviewing successful experiments and pilot projects in the field of quantum networks conducted around the world. An analysis of the results of these projects is presented, demonstrating the real possibility of creating quantum-secure communication links for the transmission of confidential information in commercial and government networks.*

***Ключевые слова**: квантовые сети, квантовая коммуникация, квантовая криптография, квантовое распределение ключей, интеграция квантовых и классических сетей, глобальная квантово-защищенная сеть, квантовый интернет, будущее квантовых технологий.*

***Keywords**: quantum networks, quantum communication, quantum cryptography, quantum key distribution, QKD, integration of quantum and classical networks, global quantum-secure network, quantum internet, future of quantum technologies.*

1. Введение

В последние годы квантовые технологии продемонстрировали значительные успехи, открывая новые горизонты для развития современных коммуникационных систем. Среди этих инноваций особое место занимают квантовые сети, представляющие собой передовое направление, способное радикально преобразовать понимание и функционирование телекоммуникационных инфраструктур. Статья «Квантовые сети: от теоретических основ до практического применения» призвана ознакомить читателя с основами квантовой коммуникации, её текущим состоянием и перспективами развития.

Квантовые сети базируются на принципах квантовой механики, включая явления квантовой запутанности и суперпозиции, что позволяет осуществлять передачу информации с непревзойденным уровнем безопасности. Введение в эксплуатацию квантового распределения ключей (QKD) и квантовой криптографии представляет собой переломный момент в защите информации, предлагая методы обеспечения конфиденциальности, которые теоретически невозможно взломать с использованием нынешних или будущих технологий.

Квантовые сети представляют собой передовое направление в области информационных технологий, где принципы квантовой механики применяются для передачи данных, обеспечивая новый уровень безопасности и эффективности. Они открывают двери к разработке квантового интернета, где информация передается с использованием квантовых состояний, таких как квантовая запутанность и суперпозиция, в отличие от классических битов в современных сетях.

2. Теоретические основы

Квантовые сети строятся на основе квантовой механики, раздела физики, изучающего поведение материи и энергии на микроскопическом уровне. В этом удивительном мире частицы, такие как фотоны или электроны, могут находиться в нескольких состояниях одновременно (суперпозиция), мгновенно взаимодействовать друг с другом на большие расстояния (запутанность), и их нельзя точно измерить без внесения возмущений в их состояние (принцип неопределенности Гейзенберга).

1. Квантовое распределение ключей (QKD)

QKD использует квантовую запутанность для создания абсолютно безопасного канала связи. При передаче квантового ключа любая попытка его перехвата приведет к изменению квантового состояния системы, что сразу станет заметно. Это делает QKD идеальным инструментом для распределения ключей шифрования, обеспечивая высокий уровень безопасности для конфиденциальной коммуникации.

3. Практическое применение

На практике реализация квантовых сетей сталкивается с рядом вызовов, включая трудности в поддержании квантовой запутанности на большие расстояния и интеграции с существующими телекоммуникационными инфраструктурами. Тем не менее, были достигнуты значительные успехи:

Квантовое распределение ключей (QKD): уже существуют коммерческие решения для QKD, которые обеспечивают безопасную передачу информации для государственных и финансовых учреждений.

Пилотные проекты: В разных странах мира проводятся пилотные проекты для тестирования квантовых сетей на практике. Например, в Китае запущена квантовая коммуникационная линия между Пекином и Шанхаем.

Исследования и разработки: Исследовательские институты и компании по всему миру активно работают над развитием технологий для квантовых сетей, включая усовершенствование квантовых повторителей, которые позволят преодолеть ограничения на дальность передачи квантовой информации.

4. Будущее квантовых сетей

Будущее квантовых сетей кажется многообещающим, с потенциалом радикально изменить способы, которыми мы передаем и защищаем информацию. Ожидается, что развитие квантовых сетей позволит создать глобальный квантовый интернет, где информация может передаваться между любыми точками мира с безусловной безопасностью, основанной на законах квантовой механики.

Это развитие также предполагает значительные улучшения в сфере квантовой криптографии, позволяя реализовать новые методы защиты данных от киберугроз, включая угрозы, связанные с развитием квантовых компьютеров, которые могут нарушить текущие стандарты шифрования.

Кроме того, квантовые сети обещают стимулировать развитие и внедрение квантовых вычислений, предоставляя платформу для создания распределенных квантовых вычислительных систем. Это может привести к прорывам в таких областях, как материаловедение, фармацевтика и искусственный интеллект, где квантовые вычисления могут предложить существенные преимущества перед классическими подходами.

Однако для достижения этих перспектив необходимы совместные усилия ученых, инженеров, отраслевых экспертов и политиков в разработке стандартов, нормативных баз и этических принципов использования квантовых технологий. Также важно обеспечить широкое понимание и принятие квантовых технологий обществом, чтобы максимально использовать их потенциал для блага человечества.

5. Заключение

В заключение, квантовые сети открывают новую эпоху в информационных технологиях, где безопасность, скорость и мощность передачи и обработки данных достигают совершенно нового уровня. Исследования и разработки в этой области продолжаются, и хотя до полного внедрения квантового интернета еще далеко, уже сейчас ясно, что квантовые сети станут ключевым компонентом технологического будущего.

Список литературы

1. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т.— 2021. — Т. 9. — С. 1–2.
2. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 2. — С. 50–56.
3. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом //СПб.: СПбГУТ.— 2014. — Т. 176.
4. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии //Телекоммуникации.— 2020.— № . 8. — С. 14–20.
5. Березина Е. О., Виткова Л. А., Ахрамеева К. А. Классификация угроз информационной безопасности в сетях IOT //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 2. — С. 11–18.

УДК 004.056

Информационная безопасность в Full-stack разработке

Губницын Лев Ильич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья начинается с обзора основных угроз информационной безопасности, с которыми сталкиваются full-stack разработчики, включая уязвимости на стороне клиента и сервера, атаки на веб-приложения, такие как кросс-сайтовое скриптование (XSS), подделка межсайтовых запросов (CSRF), SQL-инъекции и другие. Затем авторы переходят к детальному рассмотрению методик и инструментов, позволяющих минимизировать риски и повысить уровень защиты разрабатываемых систем. Особое внимание уделяется принципам безопасного программирования, включая обеспечение безопасности данных, аутентификации и авторизации пользователей, а также использование современных криптографических методов для защиты информации. Рассматриваются также вопросы тестирования безопасности, включая автоматизированное сканирование уязвимостей и пентестинг, как важные составляющие процесса разработки.*

***Abstract**: The paper begins with an overview of the main information security threats faced by full-stack developers, including client-side and server-side vulnerabilities, web application attacks such as cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, and others. Then the authors proceed to a detailed review of techniques and tools to minimize risks and increase the level of protection of developed systems. Special attention is paid to the principles of secure programming, including data security, user authentication and authorization, as well as the use of modern cryptographic methods to protect information. Security testing, including automated vulnerability scanning and penetration testing, are also addressed as important parts of the development process.*

***Ключевые слова**: информационная безопасность, Full-stack разработка, уязвимости веб-приложений, кросс-сайтовое скриптование (XSS), подделка межсайтовых запросов (CSRF), SQL-инъекции, безопасное программирование, тестирование безопасности, сессионное управление.*

***Keywords**: information security, Full-stack development, web application vulnerabilities, cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, secure programming, security testing, session management.*

1. Введение

В современном мире, где цифровые технологии проникают во все аспекты нашей жизни, безопасность веб-приложений становится критически важной задачей для разработчиков. В контексте full-stack разработки, охватывающей как фронтенд, так и бэкенд аспекты создания приложений, информационная безопасность представляет собой особенно сложный вызов. Это обусловлено необходимостью защиты данных на всех уровнях взаимодействия пользователя с системой, начиная от пользовательского интерфейса и заканчивая базой данных.

Информационная безопасность в контексте full-stack разработки охватывает комплекс мер, направленных на защиту всех аспектов веб-приложения, от пользовательского интерфейса до баз данных и серверной логики. Это включает в себя защиту от внешних атак, таких как SQL-инъекции, кросс-сайтовое скриптование (XSS), подделка межсайтовых запросов (CSRF) и других, а также обеспечение конфиденциальности, целостности и доступности данных пользователя.

2. Информационная безопасность в full-stack разработке

Информационная безопасность в full-stack разработке — это не просто набор технических решений и инструментов, это целая философия, пронизывающая процесс создания веб-приложений от начала и до конца. В мире, где угрозы информационной безопасности эволюционируют ежедневно, важность этой философии только усиливается. Разработчики, охватывающие как фронтенд, так и бэкенд, сталкиваются с задачей не только создать функциональное и удобное приложение, но и обеспечить его надежную защиту от множества потенциальных атак.

Основой безопасности является глубокое понимание того, как данные перемещаются и хранятся в приложении, как пользователи взаимодействуют с системой, и как могут быть использованы уязвимости. Безопасность не добавляется в последний момент или в качестве дополнения; она встроена в архитектуру и дизайн приложения с самого начала. Это озна-

чает, что каждая строка кода, каждый выбор технологии и каждое архитектурное решение должны быть сделаны с учетом потенциальных рисков для безопасности.

Реализация безопасности в full-stack разработке требует от разработчиков постоянного обучения и адаптации. Сфера информационной безопасности постоянно меняется, и методы, которые были эффективны вчера, могут оказаться недостаточными сегодня. Это означает, что разработчики должны быть на шаг впереди злоумышленников, предвидеть потенциальные атаки и знать современные методы защиты.

Однако информационная безопасность в full-stack разработке — это не только борьба с угрозами. Это также способ повысить доверие пользователей к вашему продукту. В эпоху, когда пользователи все более обеспокоены защитой своих данных, способность обеспечить высокий уровень безопасности становится конкурентным преимуществом. Пользователи выбирают те приложения и сервисы, которым они могут доверять, и отказываются от тех, кто не может гарантировать защиту их личной информации.

3. Основные угрозы и вызовы

Кросс-сайтовое скриптование (XSS): Эта угроза включает внедрение вредоносных скриптов в веб-страницы, просматриваемые другими пользователями, что может привести к несанкционированному доступу к данным пользователя или к сессиям.

SQL-инъекции: Атака, при которой злоумышленник может выполнять произвольные SQL-команды на сервере баз данных, часто с целью чтения или модификации данных, к которым у атакующего не должно быть доступа.

Подделка межсайтовых запросов (CSRF): Этот тип атак позволяет злоумышленнику выполнять действия от имени пользователя без его согласия, часто используя аутентификационные данные жертвы.

Небезопасное хранение данных: Неправильное управление и защита конфиденциальных данных пользователей может привести к их утечке.

4. Стратегии защиты

Санитизация ввода: Все данные, вводимые пользователем, должны проходить проверку и санитизацию на стороне сервера и клиента для предотвращения внедрения вредоносного кода.

Параметризованные запросы: Для защиты от SQL-инъекций следует использовать параметризованные запросы, которые помогают обеспечить, что ввод пользователя будет обработан как данные, а не как часть SQL-команды.

Токены аутентификации и сессии: Использование токенов и HTTP заголовков для защиты от CSRF, а также правильное управление сессиями и аутентификацией помогают предотвратить несанкционированный доступ.

Шифрование: Все конфиденциальные данные, передаваемые между клиентом и сервером, должны быть зашифрованы с использованием современных алгоритмов шифрования.

Регулярное обновление и патчинг: Постоянное обновление всех компонентов системы, включая библиотеки и фреймворки, критически важно для защиты от известных уязвимостей.

5. Заключение

Таким образом, информационная безопасность в full-stack разработке — это нечто большее, чем просто защита от атак. Это основополагающий принцип, который влияет на каждый аспект разработки приложения, от идеи до реализации. Он требует от разработчиков не только технических навыков, но и постоянного стремления к обучению, а также глубокого понимания потребностей и ожиданий пользователей. В конечном итоге, именно этот принцип позволяет создавать не просто функциональные, но и безопасные приложения, которые заслуживают доверия пользователей.

Список литературы

1. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 111–114.

2. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 107–110.
3. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия.— 2021. — Т. 1. — С. 68–75.
4. Алехин Р. В. и др. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры // Офтальмохирургия.— 2022.— № . 4s. — С. 115–122.
5. Шемякин С. Н. и др. Выяснение криптографических свойств булевых функций шифра «Магма» //Экономика и качество систем связи.— 2021.— № . 1 (19). — С. 67–73.

УДК 33

Основные угрозы безопасности IP и способы их предотвращения

Микков Александр Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч- Бруевича

***Аннотация**: Защита IP-адресов важна для безопасности данных. Рассмотрены угрозы, такие как DDoS, IP-спуфинг и утечка IP-адресов, и предложены способы их предотвращения. Используйте специализированные программы и аппаратные средства, аутентификацию, шифрование данных, VPN и прокси-серверы. Важен комплексный подход с защищенными протоколами, обновлением ПО, мониторингом и обучением пользователей. Это поможет минимизировать риски и обеспечить надежную защиту данных.*

***Abstract**: The IP address protection is important for data security. Threats such as DDoS, IP spoofing and IP address leakage are considered and ways to prevent them are suggested. Use specialized software and hardware, authentication, data encryption, VPNs and proxy servers.*

A comprehensive approach with secure protocols, software updates, monitoring and user training is important. This will help minimize risk and ensure that data is securely protected.

***Ключевые слова**: IP-адрес, безопасность, защита, информация, данные, угрозы, DDoS-атака, атака, спуфинг, аутентификация, шифрование, утечка, конфиденциальность, VPN, прокси-серверы, протоколы, обновление ПО, мониторинг, обучение пользователей, риски, надежность.*

***Keywords**: IP address, security, protection, information, data, threats, DDoS attack, attack, spoofing, authentication, encryption, leak, privacy, VPN, proxy servers, protocols, software update, monitoring, user training, risks, reliability.*

В современном цифровом мире безопасность IP-адресов является одним из ключевых аспектов обеспечения защиты информации и данных. IP-адрес — это уникальный идентификатор устройства в сети, который может стать объектом различных угроз и атак со стороны злоумышленников. Рассмотрим основные угрозы безопасности IP и способы их предотвращения.

DDoS-атака (атака распределенного отказа в обслуживании) является одним из наиболее распространенных и опасных видов кибератак, которые могут быть направлены на IP-адреса. Подобные атаки могут привести к серьезным последствиям, таким как перерывы в работе сети, потеря данных, снижение производительности и даже финансовые потери. Злоумышленники, организующие DDoS-атаку, используют ботнеты (сети зараженных компьютеров) для генерации огромного объема трафика и направляют его на целевой IP-адрес, перегружая его и вызывая отказ в обслуживании для легитимных пользователей. Это может быть особенно разрушительно для онлайн-сервисов, интернет-магазинов, банков и других организаций, зависящих от непрерывной доступности своих ресурсов. Для защиты от DDoS-атак необходимо применять специализированные решения, такие как программные и аппаратные устройства для фильтрации трафика. Эти решения могут анализировать входящий сетевой трафик, выявлять потенциально вредоносные пакеты данных и блокировать их до достижения целевого IP-адреса. Также используются технологии облачной безопасности, распределенные системы мониторинга и другие методы для обеспечения непрерывной работы сети даже в усло-

виях активной DDoS-атаки. Важно иметь план действий и готовность к реагированию на подобные угрозы, чтобы минимизировать их воздействие на бизнес-процессы и обеспечить безопасность данных и сервисов. Еще одной угрозой является IP-спуфинг (или IP-подделка) представляет собой метод, при котором злоумышленники изменяют или фальсифицируют исходный IP-адрес отправителя пакетов данных с целью скрыть свою истинную личность и маскировать свою активность в сети. Это может быть использовано для обмана систем безопасности, обхода фильтров и блокировок, а также для проведения кибератак на различные цели. Для борьбы с IP-спуфингом необходимо применять механизмы аутентификации и шифрования данных, чтобы обеспечить подлинность и целостность передаваемой информации. Например, применение протоколов шифрования данных, таких как SSL/TLS, помогает защитить передаваемые данные от подмены и подделки. Также рекомендуется использовать механизмы аутентификации, такие как двухфакторная аутентификация, для проверки легитимности отправителя данных.

Для предотвращения подделки IP-адресов также можно использовать технологии аутентификации на уровне сети, например, применять фильтрацию пакетов на уровне маршрутизаторов и брандмауэров сети. Такие механизмы могут помочь выявить и блокировать поддельные пакеты данных, поступающие из несанкционированных источников.гда злоумышленники фальсифицируют IP-адреса с целью маскировки своей активности и обмана систем безопасности. Для борьбы с IP-спуфингом рекомендуется использовать механизмы аутентификации и шифрования данных, чтобы предотвратить подделку IP-адресов.

Кроме того, утечка IP-адресов также является серьезной угрозой для безопасности. При публичной передаче данных или использовании незащищенных соединений IP-адрес может быть доступен злоумышленникам, что создает риск для конфиденциальности информации. Для предотвращения утечки IP-адресов рекомендуется использовать виртуальные частные сети (VPN) или прокси-серверы для шифрования и защиты передаваемых данных.

В целом, для обеспечения безопасности IP-адресов необходимо применять комплексный подход, включающий в себя использование защи-

щенных сетевых протоколов, регулярное обновление программного обеспечения, мониторинг сетевой активности и обучение пользователей по вопросам кибербезопасности.

Соблюдая эти рекомендации, организации и частные пользователи смогут минимизировать риски угроз безопасности IP-адресов и обеспечить надежную защиту своих данных и информации в сети. Внимание к безопасности IP-адресов — это залог сохранения конфиденциальности и целостности информации в цифровой эпохе.

Список литературы

1. Абрамова Е.А., Красов А.В., Поляничева А. В. Тенденции развития и безопасность IP-телефонии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т. Санкт-Петербург, 2023. С. 23–28.
2. Штеренберг С.И., Москальчук А.И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47–58.
3. Волкогонов В.Н., Казанцев А.А., Катасонов А.И., Орлов Г. А. Анализ безопасности wi-fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 270–275.
4. Казанцев А. А. Криптография и криптоанализ // Школьная секция: информационные технологии. Материалы 57-й Международной научной студенческой конференции. 2019. С. 18.
5. Ермолаев М.И., Ушаков И. А. Анализ производительности реализации алгоритмов шифрования в сетях LTE // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С. В. Бачевского. 2018. С. 255–358.

УДК 004

Как защититься от стеганографических атак и обнаружить скрытую информацию

Микков Александр Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Стеганография — угроза безопасности данных. Рекомендации по защите: использование специализированных программ, внимательность при обмене файлами, регулярные проверки безопасности и обучение сотрудников. Соблюдение этих мер поможет предотвратить угрозы и обнаружить скрытую информацию.*

***Abstract**: Steganography is a threat to data security. Usage of specialized software, careful file sharing, regular security checks and employee training are protection recommendations. Following these measures will help prevent threats and detect hidden information.*

***Ключевые слова**: скрытая информация, стеганография, безопасность данных, защита от атак, специализированные программы, обмен файлами, проверки безопасности, обучение сотрудников, угрозы безопасности, конфиденциальность, анализ файлов, скрытые сообщения, риски стеганографических атак.*

***Keywords**: Hidden information, steganography, data security, protection against attacks, specialized programs, file sharing, security checks, employee training, security threats, confidentiality, file analysis, hidden messages, risks of steganographic attacks.*

Современные технологии делают возможным скрытие информации внутри других данных, что создает угрозу для безопасности и конфиденциальности. Стеганография — это методология, которая позволяет встраивать секретные сообщения в невинные файлы, такие как изображения, видео или звуковые файлы, без вызывания подозрений.

Чтобы защитить себя от стеганографических атак и обнаружить скрытую информацию, следует принимать ряд мер предосторожности. Вот несколько советов:

1. Используйте специализированные программы для обнаружения стеганографии. Существует несколько специализированных программ, которые могут помочь в обнаружении стеганографии в файлах. Эти

инструменты обычно работают путем анализа структуры и содержимого файлов на наличие скрытой информации. Они могут обнаруживать подозрительные паттерны, изменения в битовой последовательности или другие признаки, указывающие на использование стеганографии. Некоторые из таких программ могут автоматически сканировать файлы и предупреждать пользователя о возможном наличии скрытой информации. Другие инструменты могут предоставлять дополнительные функции для анализа и декодирования скрытых сообщений. Использование специализированных программ для обнаружения стеганографии может быть полезным в случаях, когда необходимо проверить файлы на наличие скрытых данных, например, при расследовании инцидентов безопасности или при проверке цифровых доказательств.

2. Будьте внимательны при обмене файлами. При обмене файлами из ненадежных источников необходимо проявлять особую осторожность, так как такие файлы могут содержать скрытые сообщения или информацию, которая может быть вредной для вас или вашей системы. Вот несколько рекомендаций, которые помогут вам быть более внимательными при обмене файлами:
   - Проверяйте источник: Перед тем как открыть или загрузить файл из ненадежного источника, убедитесь, что источник действительно доверенный. Проверьте адрес отправителя, ссылку или источник файла на предмет подозрительных признаков.
   - Используйте антивирусное ПО: Убедитесь, что ваш антивирусный программный продукт обновлен и работает корректно. Перед открытием файла проведите сканирование на наличие вредоносных программ или скрытых сообщений.
   - Будьте осторожны с файлами неизвестного формата: Файлы с необычными расширениями или форматами могут содержать скрытые данные. Будьте бдительны при открытии таких файлов и убедитесь, что они безопасны.
   - Избегайте сомнительных ссылок и вложений: Если вы получили файл или ссылку от незнакомого отправителя или через ненадежный канал связи, будьте предельно осторожны. Не открывайте подозрительные вложения или ссылки без предварительной проверки.

- Обращайте внимание на объем и тип данных: Если размер файла значительно превышает ожидаемый для данного типа данных или содержит неожиданные элементы (например, текст, который не соответствует заявленному содержанию), это может быть признаком скрытой информации.

3. Проведение регулярных проверок безопасности является важным шагом для обеспечения защиты вашей информации и устройств от потенциальных угроз. Вот несколько подробностей о том, почему это так важно и как это можно сделать:
   - Обнаружение вредоносного ПО: Регулярные сканирования помогут выявить наличие вредоносного программного обеспечения (вирусов, троянов, шпионского ПО и т. д.), которое может быть скрыто на вашем устройстве или в файлах. Это позволит вам своевременно принять меры по удалению угроз и защите от дальнейших атак.
   - Проверка целостности данных: При проведении проверок безопасности также можно обнаружить изменения в файлах или структуре устройства, которые могут быть признаком несанкционированного доступа или воздействия. Это поможет вам быстро реагировать на подобные инциденты и предотвращать утечку конфиденциальной информации.
   - Обновление антивирусного ПО и баз данных: Регулярные проверки позволяют обновлять ваше антивирусное программное обеспечение и базы данных, что обеспечивает более эффективную защиту от новых видов угроз и вирусов.
   - Повышение осведомленности о безопасности: Проведение регулярных проверок безопасности также способствует повышению вашего осведомленности о возможных угрозах и методах защиты. Это поможет вам принимать более обоснованные решения по обеспечению безопасности вашей информации и устройств.
4. Обучение сотрудников по вопросам кибербезопасности играет ключевую роль в обеспечении защиты информации и устройств организации от различных угроз, включая стеганографические атаки. Вот подробнее, почему это важно и какие меры предосторожности могут быть приняты:

- Осознание рисков стеганографических атак: Стеганография — это метод скрытой передачи информации, когда данные встраиваются в другие файлы или носители, чтобы они казались обычными. Сотрудники, обученные в области кибербезопасности, смогут осознавать потенциальные угрозы стеганографии и быть более бдительными при обращении с файлами и сообщениями.
- Распознавание признаков стеганографических атак: Обучение позволит сотрудникам распознавать признаки стеганографической активности, такие как необычные изменения в размере файлов, странные символы или шум при передаче данных. Это поможет им быстро реагировать на подобные ситуации и предотвращать утечку конфиденциальной информации.
- Принятие соответствующих мер предосторожности: Обученные сотрудники смогут применять соответствующие меры предосторожности для защиты информации от стеганографических атак. Это может включать в себя использование надежных шифрованных каналов связи, проверку подлинности файлов и сообщений, а также регулярное обновление программного обеспечения для предотвращения уязвимостей.
- Создание культуры безопасности: Обучение персонала по вопросам кибербезопасности способствует формированию культуры безопасности в организации, где каждый сотрудник понимает свою роль в защите информации и действует соответственно. Это поможет уменьшить риск утечки данных или компрометации системы из-за стеганографических угроз.

Соблюдая эти рекомендации, вы сможете укрепить свою защиту от стеганографических атак и обнаружить скрытую информацию до того, как она нанесет ущерб вашей безопасности и конфиденциальности.

Список литературы

1. Синельщиков В.С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петер-

бургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2021. С. 653–657.
2. Косов Н.А., Гельфанд А.М., Лаптев А. А. Анализ темных данных для обеспечения устойчивости информационных систем от нарушения конфиденциальности или несанкционированных действий // Colloquium-Journal. 2019. № 13–2 (37). С. 100–103.
3. Красов А. В. Метод обнаружения сетевой стеганографии на основе машинного обучения // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 3. С. 100–108.
4. Красов А. В. Методы выявления сетевой стеганографии // Методы и технические средства обеспечения безопасности информации. 2023. № 32. С. 52–54.
5. Коржик В.И., Красов А. В. Цифровая стеганография // Учебник. Москва, 2023.

УДК 004.056

Техники встраивания информации в медиа-файлы: преимущества и недостатки

Микков Александр Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч- Бруевича

***Аннотация**: В цифровом мире можно скрыто встраивать данные в медиа-файлы для передачи информации, защиты авторских прав и креативных целей. Однако это может привести к потере качества, обнаружению данных и ограничениям формата файлов. При использовании таких техник важно учитывать цели, особенности контента и соблюдать законодательство и этические нормы.*

***Abstract**: It is possible to implicitly embed data in media files for information transfer, copyright protection and creative purposes in the digital world. However, this can lead to loss of quality, data discovery, and file format limitations. When using such techniques, it is important to consider the purpose, content characteristics and comply with legislation and ethical standards.*

Ключевые слова: *Цифровой мир, медиа-файлы, встраивание информации, скрытая передача данных, защита авторских прав, креативные возможности, потеря качества, обнаружение данных, ограничения формата, стеганография, метаданные, цифровая подпись, сжатие данных, уязвимость.*

Keywords: *Digital world, media files, information embedding, hidden data transfer, copyright protection, creative possibilities, loss of quality, data detection, format limitations, steganography, metadata, digital signature, data compression, vulnerability.*

Современный цифровой мир предоставляет широкий спектр возможностей для работы с медиа-файлами, включая техники встраивания информации в них. Данный процесс позволяет скрыто внедрять данные в аудио-, видео- или изображения, открывая перед пользователями новые перспективы в креативной сфере и обеспечивая возможности для скрытой передачи информации. Давай подробнее рассмотрим основные преимущества и недостатки техник встраивания информации в медиа-файлы

Преимущества:

1. Конфиденциальность: стеганография обеспечивает скрытность передаваемой информации, так как данные могут быть встроены в медиа-файлы без вызывания подозрений у посторонних лиц. Это позволяет обеспечить конфиденциальность обмена информацией.
2. Защита от обнаружения: в отличие от криптографии, где сам факт шифрования может привлечь внимание к сообщению, стеганография позволяет скрыть сам факт наличия скрытой информации. Это делает ее более эффективной в случаях, когда необходимо избежать обнаружения.
3. Расширение возможностей: использование стеганографии позволяет расширить функциональность медиа-файлов, добавляя к ним дополнительные данные или контент. Например, можно внедрить в аудиофайл текстовое сообщение или в видеофайл скрыть изображение.
4. Устойчивость к атакам: при правильном использовании стеганографические методы могут быть устойчивы к различным атакам, таким как перехват и анализ трафика. Это делает их полезными для передачи конфиденциальной информации в условиях повышенной безопасности.
5. Креативные возможности: стеганография может быть использована для создания интересных и оригинальных проектов в области искусства

и дизайна. Внедрение скрытых сообщений или изображений может придать медиа-файлам дополнительную глубину и интерес для зрителя.

Использование стеганографии представляет собой мощный инструмент для защиты конфиденциальной информации. Она позволяет расширить функциональность медиа-файлов и создать уникальные проекты. Например, скрыть сообщение в изображении или аудиофайле, что может быть полезно в различных областях, включая информационную безопасность, цифровую форензику и креативное искусство.

Однако, при использовании стеганографии следует учитывать потенциальные риски и ограничения, связанные с возможностью неправомерного использования этой техники. Например, некоторые могут использовать стеганографию для скрытой передачи вредоносных данных или для обхода механизмов контроля информационной безопасности.

Поэтому важно использовать стеганографию ответственно и осознанно, соблюдая законы и этические принципы. Также необходимо применять другие технические и организационные меры для обеспечения всесторонней защиты информации.

Недостатки:

1. Потеря качества: Встраивание данных в медиа-файлы может привести к потере качества исходного контента. Это особенно заметно в случае сжатых форматов, где добавление дополнительной информации может повлиять на видео- или аудио-качество.
2. Обнаружение: Некоторые методы стеганографии могут быть обнаружены при анализе медиа-файлов специальными программами или алгоритмами. Это может привести к раскрытию скрытой информации и нарушению конфиденциальности.
3. Ограниченность вместимости: Емкость медиа-файлов ограничена, что может стать проблемой при попытке встроить большой объем данных. Это может привести к необходимости выбора между объемом скрываемой информации и сохранением качества файла.
4. Сложность извлечения: Извлечение скрытой информации из медиа-файла может быть сложным процессом, особенно если используются сложные методы стеганографии. Это может затруднить доступ к важным данным в случае необходимости.

5. Уязвимость к атакам: Некоторые методы стеганографии могут быть уязвимы к различным видам атак, таким как атаки на ключи шифрования или на методы встраивания данных. Это может угрожать безопасности скрытой информации.
6. Этические соображения: Использование стеганографии для скрытой передачи информации может вызвать этические вопросы, особенно если такие методы применяются без согласия всех заинтересованных сторон.

Таким образом, техники встраивания информации в медиа-файлы имеют как свои преимущества (Конфиденциальность, Защита от обнаружения, Расширение возможностей, Устойчивость к атакам, Креативные возможности), так и недостатки(Потеря качества, Обнаружение, Ограниченность вместимости, Сложность извлечения, Уязвимость к атакам, Этические соображения). При использовании данного подхода необходимо учитывать цели и задачи, а также выбирать подходящие методы с учетом особенностей контента и формата файлов. Важно также помнить о необходимости соблюдения законодательства и этических норм при работе с информацией, встраиваемой в медиа-файлы.

Список литературы

1. Красов А. В. Метод обнаружения сетевой стеганографии на основе машинного обучения // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 3. С. 100–108.
2. Ушаков И.А., Салита А.С., Пешков А. И. Программа для выявления сетевой стеганографии в пакетах протокола IPV4 // Свидетельство о регистрации программы для ЭВМ RU 2023663702, 27.06.2023. Заявка № 2023662483 от 14.06.2023.
3. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д. В. Построение доверенной вычислительной среды, Санкт-Петербург, 2019.
4. Василишин Н.С., Ушаков И.А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших

данных для обнаружения компьютерных атак // Аллея науки. 2018. Т. 3. № 6 (22). С. 1012–1021.
5. Салита А.С., Красов А. В. Создание стеганографического канала при помощи полей // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 36–40.

УДК 004.56

Технологии и стандарты для обеспечения безопасности в беспроводных сетях: обзор и сравнительный анализ

Микков Александр Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Беспроводные сети широко используются в нашей повседневной жизни, но они подвержены угрозам безопасности. Для защиты информации в таких сетях применяются различные технологии, такие как WPA/WPA2, WEP, WPA3, VPN и брандмауэры. Выбор метода зависит от потребностей и уровня защиты. Обновление программного обеспечения и следование новым уязвимостям играют ключевую роль в обеспечении безопасности беспроводных сетей.*

***Abstract**: Wireless networks are widely used in daily life, but they are prone to security threats. Various technologies such as WPA/WPA2, WEP, WPA3, VPNs and firewalls are used to protect information on such networks. The choice of method depends on the needs and level of protection. Updating software and keeping up with new vulnerabilities play a key role in securing wireless networks.*

***Ключевые слова**: беспроводные сети, безопасность, WPA/WPA2, WEP, WPA3, VPN, брандмауэры, угрозы, защита данных, шифрование, аутентификация, уязвимости, обновление ПО, защита от атак, сравнительный анализ, потребности, надежность, технологии.*

***Keywords**: wireless networks, security, WPA/WPA2, WEP, WPA3, VPN, firewalls, threats, data protection, encryption, authentication, vulnerabilities, software updates, attack protection, comparative analysis, needs, reliability, technologies.*

В современном мире беспроводные сети играют ключевую роль в повседневной жизни, обеспечивая связь без проводов и ускоряя обмен информацией. Однако, с появлением новых технологий, безопасность беспроводных сетей становится все более уязвимой. Различные методы и стандарты применяются для защиты данных в таких сетях. Рассмотрим основные подходы к обеспечению безопасности в беспроводных сетях путем проведения обзора и сравнительного анализа.

Один из самых распространенных методов обеспечения безопасности в беспроводных сетях — протокол WPA/WPA2 (Wi-Fi Protected Access). Он обеспечивает защиту доступа к сети через шифрование данных и аутентификацию пользователей, что делает его неотъемлемой составляющей современных технологий.

Существует множество способов, которыми злоумышленники могут использовать уязвимости в стандарте WPA/WPA2. Например, атака по словарю (WPA/WPA2 dictionary attack) предполагает использование обширного словаря паролей для взлома защищенной сети. Для этого требуются специализированные программы и мощные компьютерные ресурсы. Еще один метод — атака на PIN-код (WPS PIN brute-force attack) и захват рукопожатия (WPA/WPA2 handshake capture attack) — может быть успешным при определенных условиях.

Предложение нового стандарта безопасности для беспроводных сетей — WPA3 — оказалось эффективным средством защиты информации. Усовершенствованные методы шифрования и аутентификации делают его превосходным по сравнению с предыдущими стандартами, такими как WPA/WPA2. Одной из ключевых особенностей WPA3 является использование более надежного алгоритма шифрования, что делает его устойчивым к различным видам атак. Кроме того, в рамках протокола WPA3 предусмотрена защита от попыток взлома паролей, что делает процесс взлома беспроводной сети более сложным для злоумышленников. В отличие от устаревшего протокола WEP, который имеет недостатки и не рекомендуется для использования в современных беспроводных сетях, новый стандарт безопасности Wi-Fi, WPA3, представляет собой более современный и надежный вариант защиты информации.

Для обеспечения безопасности беспроводных сетей используются различные средства, такие как брандмауэры и VPN. Сетевые атаки, такие как атаки типа Man-in-the-Middle, могут быть предотвращены благодаря использованию новых методов аутентификации, например Simultaneous Authentication of Equals (SAE), которые предлагаются протоколом WPA3. VPN — это инновационная технология, которая обеспечивает шифрование данных в туннеле для безопасной передачи через публичные сети, включая интернет. Эти меры повышают общую надежность беспроводной связи и обеспечивают безопасное установление связи между устройствами и точками доступа к сети.

Безопасность в беспроводных сетях обеспечивается защитными барьерами, известными как брандмауэры. Они эффективно фильтруют и контролируют поток данных, обеспечивая защиту от внешних угроз. Эти барьеры могут быть настроены на различные уровни безопасности, чтобы соответствовать потребностям среды. Ограничивая доступ к ресурсам и обнаруживая попытки несанкционированного доступа, брандмауэры играют ключевую роль в предотвращении атак и нарушений безопасности сети.

В беспроводных сетях, виртуальные частные сети (VPN) представляют собой сильный инструмент безопасности. Они создают шифрованный туннель для передачи информации между устройствами через общедоступные сети, что повышает защиту данных. VPN обеспечивают конфиденциальность и целостность информации, защищая ее от несанкционированного доступа. Кроме того, они скрывают IP-адреса пользователей, обеспечивая анонимность и снижая риски отслеживания злоумышленниками их действий в сети.

Для обеспечения надежной защиты беспроводных сетей необходимо учитывать различные технологии и стандарты, способные повысить безопасность сетей. Проведение анализа уровня защиты, требуемого для конкретной сети, является ключевым моментом при выборе подходящего метода защиты. Учитывая особенности данных, объем передаваемой информации, структуру сети и потенциальные угрозы, необходимо подбирать наилучшие технологии и меры для соответствия потребностям бизнеса или организации, обеспечивая эффективную защиту информации и предотвращая возможные атаки.

Обеспечение безопасности беспроводных сетей требует не только регулярного обновления программного обеспечения на всех устройствах в сети, включая компьютеры, мобильные устройства, маршрутизаторы и точки доступа, но и правильного выбора технологий и стандартов. Только актуальные методы защиты смогут эффективно сдерживать постоянно изменяющиеся угрозы и риски. Установка обновлений играет ключевую роль в этом процессе, поскольку они содержат исправления для новых уязвимостей и улучшения безопасности, что существенно снижает вероятность успешных кибератак.

Список литературы

1. Подшибякин А.С., Ушаков И.А., Шинкаренко А. Ф. Результаты анализа функционирования механизмов защиты в беспроводных сетях передачи данных // Труды Военно-космической академии имени А.Ф.Можайского. 2021. № 678. С. 163–174.
2. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д. В. Построение доверенной вычислительной среды. Санкт-Петербург, 2019.
3. Красов А.В., Штеренберг С.И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей. Электросвязь. 2019. № 11. С. 39–47.
4. Цветков А.Ю., Эллауи Ю. Б. Поиск уязвимостей в программном обеспечении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2021. С. 684–688.
5. Волкогонов В.Н., Преображенский А.И., Ушаков И. А. Уязвимости программно-определяемых сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 279–284.

УДК 004.056

Этические аспекты эксплуатации уязвимостей в программном обеспечении

Микков Александр Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч- Бруевича

***Аннотация**: Статья обсуждает этические аспекты эксплуатации уязвимостей в программном обеспечении, включая мотивации злоумышленников, последствия использования уязвимостей и понятие «белого хакера». Подчеркивается важность этичного поведения для обеспечения безопасности в цифровом пространстве.*

***Abstract**: This article discusses the ethical aspects of exploiting vulnerabilities in software, including the motivations of attackers, the consequences of exploiting vulnerabilities, and the 'white hacker' concept. The importance of ethical behavior for maintaining security in the digital space is emphasized.*

***Ключевые слова**: цифровые технологии, безопасность программного обеспечения, уязвимости, злоумышленники, этика, конфиденциальность данных, кибератаки, этичный хакер, белый хакер, ответственное поведение, информационная безопасность.*

***Keywords**: digital technologies, software security, vulnerabilities, intruders, ethics, data privacy, cyber attacks, ethical hacker, white hacker, responsible behavior, information security.*

В современном мире, где цифровые технологии проникают во все сферы нашей жизни, вопрос безопасности программного обеспечения становится все более актуальным. Однако, вместе с постоянным развитием защитных механизмов, появляются и те, кто стремится использовать уязвимости в программном обеспечении для своих целей. В данной статье мы рассмотрим этические аспекты эксплуатации уязвимостей в программном обеспечении.

Злоумышленники, ищущие и использующие уязвимости в программном обеспечении, могут иметь различные мотивации, которые определяют их действия и цели. Одним из наиболее распространенных мотивов является финансовая выгода. Киберпреступники могут использовать уязвимости для кражи личных данных, финансовых средств, шантажа или других мошеннических действий с целью получения прибыли. Например,

атаки на банковские системы или онлайн-магазины могут быть направлены на похищение денежных средств или конфиденциальной информации о клиентах.

Помимо финансовой мотивации, злоумышленники могут быть мотивированы политическими или идеологическими убеждениями. Нападения на государственные учреждения, политически значимые организации или компании с целью нанесения ущерба или выражения своих взглядов могут быть осуществлены с использованием уязвимостей в программном обеспечении. Такие атаки могут иметь широкий спектр последствий, включая нарушение работы систем, утечку конфиденциальной информации и даже повреждение репутации.

Независимо от мотивации злоумышленников, эксплуатация уязвимостей в программном обеспечении представляет серьезную угрозу как для отдельных пользователей, так и для организаций в целом. Потенциальные последствия могут включать в себя потерю данных, финансовые потери, нарушение работы бизнес-процессов, утечку конфиденциальной информации, а также повреждение репутации и доверия клиентов. Поэтому важно принимать все необходимые меры для защиты от уязвимостей и обеспечения безопасности программного обеспечения и сетей.

С точки зрения этики, использование уязвимостей в программном обеспечении является недопустимым и неэтичным действием по нескольким причинам. Во-первых, эксплуатация уязвимостей приводит к нарушению конфиденциальности данных. Когда злоумышленники получают доступ к системе или сети через уязвимость, они могут получить доступ к чувствительной информации, такой как личные данные пользователей, финансовые сведения, медицинская информация и другие конфиденциальные сведения. Это может привести к серьезным последствиям для пользователей, включая кражу личной информации, финансовые потери и даже идентификационный краже.

Во-вторых, использование уязвимостей может привести к вымогательству и шантажу. Злоумышленники могут использовать уязвимости для блокировки доступа к данным или системам и требовать выкуп за их восстановление. Это форма кибервымогательства, которая может причинить серьезный ущерб как для отдельных пользователей, так и для организаций.

Эксплуатация уязвимостей может послужить отправной точкой для масштабных кибератак, способных нанести серьезный ущерб как материальный (в виде финансовых потерь или повреждения ресурсов), так и моральный (воздействие на доверие и безопасность общества).

Нападения на критическую инфраструктуру, государственные учреждения и крупные компании могут иметь катастрофические последствия для экономики, безопасности и общества в целом. Такие атаки могут привести к простоям в работе важных систем, слежке за гражданами, утечке конфиденциальных данных или даже потенциальным чрезвычайным ситуациям.

Эксплуатация уязвимостей в программном обеспечении поднимает ряд важных этических вопросов, которые необходимо учитывать при обсуждении данной проблемы. В первую очередь, это связано с моральным аспектом использования уязвимостей для незаконных целей, таких как кража данных, нарушение конфиденциальности или нанесение ущерба другим пользователям. Это может привести к серьезным последствиям как для отдельных лиц, так и для общества в целом.

Важно помнить, что действия в цифровом пространстве имеют реальные последствия, и каждый пользователь программного обеспечения должен стремиться к ответственному поведению. Это означает не только избегать злоупотребления уязвимостями, но и активно участвовать в обеспечении безопасности и защиты информации. Пользователи программного обеспечения должны следить за обновлениями и патчами, устанавливать антивирусное программное обеспечение, использовать надежные пароли и другие меры безопасности.

Только при соблюдении этических принципов и ответственного поведения можно обеспечить безопасность и защиту информации для всех пользователей программного обеспечения. Сознательное отношение к цифровой безопасности поможет предотвратить возможные угрозы и сохранить конфиденциальность данных.

Список литературы

1. Волкогонов В.Н., Преображенский А.И., Ушаков И. А. Уязвимости программно-определяемых сетей // Актуальные проблемы инфотеле-

коммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 279–284.
2. Шемякин С.Н., Гельфанд А.М., Орлов Г. А. Критическая информационная инфраструктура // Наука и инновации — современные концепции. Сборник научных статей по итогам работы Международного научного форума. Отв. ред. Хисматуллин.Д.Р. 2020. С. 114–118.
3. Кравцова В.А., Ушаков И. А. Обнаружение аномалий сетевого трафика с использованием больших данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 697–701.
4. Синельщиков В.С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2021. С. 653–657.
5. Косов Н.А., Гельфанд А.М., Лаптев А. А. Анализ темных данных для обеспечения устойчивости информационных систем от нарушения конфиденциальности или несанкционированных действий // Colloquium-Journal. 2019. № 13–2 (37). С. 100–103.

УДК 004

Мобильные технологии: возможности и вызовы

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Настоящая научная статья исследует разнообразные аспекты мобильных технологий, рассматривая их возможности и вызовы в современном информационном обществе. Обсуждается эволюция мобильных устройств и их влияние на различные сферы жизни, начиная от коммуникаций и заканчивая бизнесом и здравоохранением.*

В работе также анализируются технологические инновации, такие как расширенная реальность (AR), искусственный интеллект (AI) и интернет вещей (IoT), и их роль в формировании будущего мобильных технологий. В контексте возможностей обсуждаются новые перспективы в развитии приложений и сервисов для мобильных устройств. В то же время статья выделяет вызовы, связанные с безопасностью данных, конфиденциальностью, а также вопросы этического и социального характера, которые возникают в связи с широким распространением мобильных технологий. В целом, данная статья представляет собой обзор современного состояния и перспектив развития мобильных технологий, а также вызовов, которые стоят перед исследователями, разработчиками и обществом в целом.

***Abstract**: This research paper explores various aspects of mobile technology, examining its opportunities and challenges in today's information society. It discusses the evolution of mobile devices and their impact on various spheres of life, ranging from communications to business and healthcare. The paper also analyzes technological innovations such as Augmented Reality (AR), Artificial Intelligence (AI) and the Internet of Things (IoT) and their role in shaping the future of mobile technology. In the context of opportunities, new perspectives in the development of applications and services for mobile devices are discussed. At the same time, the article highlights challenges related to data security, privacy, and ethical and social issues that arise from the widespread adoption of mobile technologies. Overall, this article provides an overview of the current state of the art and prospects of mobile technologies, as well as the challenges that researchers, developers, and society at large face.*

***Ключевые слова**: мобильные технологии, мобильные приложения, безопасность данных, конфиденциальность, образование, мобильный интерфейс, инновации.*

***Keywords**: mobile technology, mobile applications, data security, privacy, education, mobile interface, innovation.*

1. Введение

В современном мире мобильные технологии играют ключевую роль в повседневной жизни миллионов людей по всему миру. С развитием информационных технологий и появлением все более инновационных мобильных устройств, этот сегмент технологического прогресса стал незаменимым инструментом для коммуникации, работы, развлечений и образования. Одной из важнейших характеристик мобильных технологий является их доступность. Смартфоны и планшеты стали не просто средством связи, но и мощными персональными компьютерами, которые все-

гда под рукой. Благодаря этому, люди могут оставаться в курсе событий, общаться с друзьями и коллегами, а также выполнять различные задачи, даже находясь в движении. Одним из ключевых достижений в области мобильных технологий является развитие приложений. Мобильные приложения предоставляют пользователю огромное количество возможностей: от просмотра новостей и видеороликов до онлайн-покупок и управления финансами. Кроме того, разработчики активно внедряют новые технологии, такие как искусственный интеллект и расширенная реальность, что дополняет функциональность мобильных устройств и делает их еще более универсальными. Однако, помимо бесспорных преимуществ, мобильные технологии также сталкиваются с рядом вызовов. Безопасность данных и приватность пользователей становятся все более актуальными вопросами, в связи с ростом киберугроз и угрозами утечки персональной информации. Кроме того, технологическая зависимость и неравенство в доступе к мобильным устройствам вызывают определенные социальные и этические вопросы.

2. Мобильные технологии: возможности

Повышение доступности: Мобильные технологии обеспечивают людей возможность быть подключенными к информации и услугам в любое время и в любом месте.

Расширенные возможности коммуникации: С помощью мобильных устройств люди могут обмениваться сообщениями, звонить, видеочатить, даже если находятся на больших расстояниях друг от друга.

Повышение эффективности работы: Мобильные приложения позволяют выполнять широкий спектр задач, начиная от управления делами до редактирования документов, даже без доступа к стационарному компьютеру.

Инновационные технологии: Мобильные устройства становятся платформой для внедрения новых технологий, таких как расширенная реальность (AR), искусственный интеллект (AI), и интернет вещей (IoT), открывая новые возможности для развития бизнеса и улучшения пользовательского опыта.

3. Мобильные технологии: вызовы

Безопасность данных: Угрозы кибербезопасности, такие как вирусы, хакерские атаки и утечки данных, представляют серьезный вызов для мобильных технологий, требуя постоянного совершенствования мер безопасности.

Приватность и конфиденциальность: Сбор и использование персональной информации пользователей становятся объектом озабоченности, и эффективное управление приватностью и конфиденциальностью является важным аспектом развития мобильных технологий.

Технологическая зависимость: Использование мобильных устройств во всех аспектах жизни может привести к зависимости и негативным последствиям для здоровья и социальных взаимодействий.

4. Заключение

В будущем мобильные технологии будут продолжать играть ключевую роль в трансформации общества и бизнеса. С развитием интернета вещей и расширенной реальности, мобильные устройства станут еще более умными и функциональными, что откроет новые перспективы для инноваций и развития. Однако, важно помнить о необходимости соблюдения принципов безопасности и уважения к приватности пользователей, чтобы обеспечить устойчивое и справедливое развитие мобильных технологий в будущем.

Список литературы

1. Орлов Г.А., Красов А.В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 4. С. 76–84.»
2. Косов Н.А., Голубов Н. А. Способы защиты от инсайдерских атак // Инновационные решения социальных, экономических и технологических проблем современного общества. Сборник научных статей по итогам круглого стола со всероссийским и международным участием. Москва, 2021. С. 149–151.

3. Гельфанд А.М., Казанцев А.А., Красов А.В., Орлов Г. А. Оценка рисков и угроз безопасности в среде “Умный дом” // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 316–321.
4. Штеренберг С.И., Бударный Г.С., Чумаков И. В. Анализ безопасности доменных систем // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 587–588.
5. Алехин Р.В., Красов А.В., Макарова А.Д., Орлов Г. А. Облачные сервисы. Принцип работы, классификация и модели обслуживания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 70–74.

УДК 004

Облачные вычисления: эффективность, гибкость, надежность

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья представляет собой исследование современных тенденций и перспектив развития облачных вычислений. Облачные вычисления представляют собой инновационную парадигму организации информационных технологий, позволяющую пользователям получать доступ к вычислительным ресурсам и сервисам через интернет по требованию. В статье анализируются ключевые аспекты облачных вычислений, включая их эффективность, гибкость и надежность. Обсуждаются методы оптимизации использования облачных ресурсов, такие как динамическое масштабирование и автоматизация управления ресурсами. Также статья рассматривает вызовы, связанные с обеспечением безопасности данных, конфиденциальности и управлением рисками в контексте облачных вычислений. В заключение, предлагаются практические рекомендации для эффективного использования облачных вычислений*

с целью достижения бизнес-целей и обеспечения устойчивого развития информационных технологий.

***Abstract**: This article is a study of the current trends and prospects of cloud computing. Cloud computing is an innovative paradigm of information technology organization that allows users to access computing resources and services via the Internet on demand. The paper analyzes the key aspects of cloud computing including its efficiency, flexibility, and reliability. Methods for optimizing cloud resource utilization such as dynamic scaling and resource management automation are discussed. The paper also addresses challenges related to data security, privacy, and risk management in the context of cloud computing. Finally, practical recommendations are offered for the effective utilization of cloud computing to achieve business goals and sustainable information technology development.*

***Ключевые слова**: информационные технологии, вычислительные ресурсы, безопасность данных, конфиденциальность, цифровая трансформация, оптимизация, ИТ-инфраструктура.*

***Keywords**: information technology, computing resources, data security, privacy, digital transformation, optimisation, IT infrastructure.*

1. Введение

Облачные вычисления представляют собой модель предоставления различных услуг через Интернет. Эти услуги включают хранение данных, серверы, базы данных, сети и программное обеспечение. Вместо того чтобы хранить файлы на локальном жестком диске или хранить данные в локальном центре обработки данных, облачные вычисления позволяют пользователю доступ к данным и программам через Интернет с любого устройства.

2. Основные характеристики облачных вычислений

Самообслуживание на запрос: Пользователи могут самостоятельно настраивать и получать доступ к ресурсам облачных вычислений, обычно через Интернет, используя веб-интерфейс.

Широкий доступ к сети: Услуги доступны через сеть и доступны через стандартные механизмы, которые обеспечивают использование почти любым устройством (например, мобильными телефонами, планшетами, ноутбуками).

Пул ресурсов: Ресурсы облачных вычислений объединены для обслуживания множества пользователей с использованием мульти-арендной модели, с различными физическими и виртуальными ресурсами, динамически присваиваемыми и перераспределяемыми в соответствии с потребностями пользователей.

Быстрая эластичность: Ресурсы могут быть быстро предоставлены и масштабированы, часто автоматически, чтобы соответствовать спросу — к примеру, расширять или сокращать мощности сервера в реальном времени.

Измеряемый сервис: Системы облачных вычислений автоматически контролируют и оптимизируют ресурсы использования, предоставляя прозрачность как для поставщика облачных услуг, так и для потребителя.

3. Эффективность

Одним из главных преимуществ облачных вычислений является их эффективность в использовании ресурсов. Пользователи могут масштабировать вычислительные мощности в зависимости от текущей нагрузки, что позволяет сократить издержки на оборудование и поддержку. Также облачные провайдеры обычно предоставляют услуги платежей за использование, что означает, что пользователи платят только за те ресурсы, которые они фактически используют, что делает экономические затраты более прозрачными и предсказуемыми.

4. Гибкость

Облачные вычисления также обладают высокой степенью гибкости. Пользователи могут легко настраивать и изменять свои вычислительные ресурсы в соответствии с требованиями и изменяющимися потребностями бизнеса. Это позволяет организациям быстро реагировать на изменяющиеся рыночные условия, запускать новые проекты и масштабировать бизнес при необходимости без необходимости в длительном времени и дополнительных затратах на обновление оборудования.

5. Надежность

Одним из важнейших аспектов облачных вычислений является их надежность. Облачные провайдеры обычно обеспечивают высокую доступность и резервное копирование данных, что гарантирует, что пользователи могут получать доступ к своим данным и приложениям в любое время, даже в случае сбоев оборудования или других проблем. Кроме того, облачные провайдеры часто предлагают гибкие опции резервирования данных и вычислительных ресурсов, что обеспечивает защиту от потери данных и обеспечивает бесперебойную работу бизнеса.

6. Заключение

В заключение, облачные вычисления представляют собой мощный и гибкий инструмент, который преобразует способы ведения бизнеса, разработки и развертывания программного обеспечения, а также хранения и обработки данных. Эффективность облачных сервисов проявляется в их способности предоставлять масштабируемые ресурсы по требованию, что позволяет компаниям оптимизировать свои операционные расходы и избегать излишних капиталовложений. Гибкость облачных решений вносит значительный вклад в ускорение разработки и инноваций, поскольку разработчики получают возможность экспериментировать и развертывать новые приложения с небывалой скоростью.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.

3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004

Автоматизация и роботизация: как они изменят рабочие места

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В современном мире автоматизация и роботизация становятся ключевыми тенденциями в развитии промышленности и бизнеса, оказывая глубокое влияние на рынок труда и характер выполняемой работы. Статья исследует, как эти технологии трансформируют рабочие места, анализируя текущие тенденции и прогнозируя будущие изменения. Рассматриваются положительные и отрицательные аспекты автоматизации, включая повышение производительности, создание новых видов профессий и потенциальную угрозу для традиционных рабочих мест. В статье поднимаются важные вопросы адаптации рабочей силы к новым условиям, необходимости переобучения и обновления навыков сотрудников. Также обсуждаются стратегии компаний и государственных организаций по минимизации негативного воздействия технологических изменений на занятость, в том числе через разработку социальных программ и систем поддержки работников.*

***Abstract**: In today's world, automation and robotization are becoming key trends in industrial and business development, with a profound impact on the labor market and the nature of work performed. This article explores how these technologies are transforming the workplace*

by analyzing current trends and predicting future changes. The positive and negative aspects of automation are examined, including increased productivity, the creation of new types of occupations, and the potential threat to traditional jobs. The article raises important issues of workforce adaptation to the new environment and the need for retraining and updating employee skills. Strategies of companies and government organizations to minimize the negative impact of technological change on employment, including through the development of social programs and employee support systems, are also discussed

***Ключевые слова**: автоматизация, роботизация, искусственный интеллект, инновационные технологии, устойчивое развитие, экономическая адаптация, технологические инновации.*

***Keywords**: automation, robotisation, artificial intelligence, innovative technologies, sustainable development, economic adaptation, technological innovation.*

1. Введение

В эпоху беспрецедентных технологических прорывов автоматизация и роботизация выступают как два важнейших драйвера изменений в рабочем мире. Они уже начали радикально преобразовывать промышленные процессы, услуги и даже творческие профессии, затрагивая каждую отрасль и сектор экономики. Эти изменения обещают повысить эффективность, уменьшить количество ошибок, вызванных человеческим фактором, и открыть новые возможности для инноваций и развития. Однако вместе с обещаниями приходят и вызовы: риск потери рабочих мест, необходимость в адаптации рабочей силы и переосмысление самой сущности труда. Введение в мир автоматизации и роботизации неизбежно, и наше общество стоит на пороге значительных изменений. Понимание того, как мы можем навигировать через эти изменения, сохраняя при этом устойчивый экономический рост и социальное благополучие, является ключевым для всех участников рабочего процесса — от руководителей и политиков до каждого работника.

Автоматизация и роботизация являются двумя из наиболее значительных технологических тенденций современности, которые оказывают глубокое влияние на рабочие места во всех отраслях. Эти изменения приводят к переосмыслению традиционных подходов к труду, профессиям и управлению бизнесом. Рассмотрим ключевые аспекты этого процесса и как он может изменить будущее работы.

2. Повышение эффективности и производительности

Автоматизация позволяет компаниям выполнять рутинные, повторяющиеся задачи быстрее и эффективнее, сокращая время на выполнение работы и минимизируя вероятность ошибок. Роботизация привносит в процесс физическую автоматизацию, позволяя машинам выполнять тяжелую или опасную работу, что раньше требовало человеческого вмешательства. Это не только повышает безопасность на производстве, но и открывает новые возможности для работников заниматься более креативными и стратегическими задачами.

3. Трансформация рабочих мест

Многие профессии и рабочие места, как известно, исчезнут или претерпят серьезные изменения в результате автоматизации и роботизации. Однако в то же время создаются новые рабочие места, требующие новых навыков, включая управление автоматизированными системами, разработку и обслуживание робототехнического оборудования. Это подчеркивает важность переобучения и обновления навыков для сотрудников.

4. Новые навыки и роли

Сдвиг в сторону автоматизации и роботизации требует от работников развития новых навыков, таких как аналитика данных, программирование, кибербезопасность и управление технологическими процессами. Кроме того, умение работать совместно с автоматизированными системами и роботами становится все более важным. Это влечет за собой необходимость в новых подходах к образованию и профессиональной подготовке.

5. Социальные и экономические вопросы

Автоматизация и роботизация также поднимают важные социальные и экономические вопросы, такие как увеличение неравенства, изменение структуры занятости и потребность в социальной защите для тех, кто по-

терял работу из-за технологических изменений. Решение этих вопросов требует активного участия всех заинтересованных сторон, включая правительства, предприятия и образовательные учреждения.

6. Заключение

Автоматизация и роботизация представляют собой мощные силы, способные трансформировать рабочие места и экономику в целом. Хотя они несут определенные вызовы, также существуют значительные возможности для создания более производительных, безопасных и интересных рабочих мест. Ключ к успеху в этом новом ландшафте — адаптация и обучение, позволяющие работникам и компаниям максимально использовать преимущества, предоставляемые технологиями.

Список литературы

1. Пестов И. Е. Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик. диссертация на соискание ученой степени кандидата технических наук / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2022.
2. Пестов И.Е., Фёдоров П.О., Кошелева С.А., Алёхин Р. В. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // I-methods. 2022. Т. 14. № 1.
3. Пестов И.Е., Шинкарева П.С., Кошелева С.А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.
4. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д. В. Построение доверенной вычислительной среды // Санкт-Петербург, 2019.

5. Пестов И.Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества. Сборник научных статей по итогам круглого стола со всероссийским и международным участием. Москва, 2021. С. 113–115.

УДК 004

Финтех революция: как технологии меняют финансовый мир

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье рассматривается воздействие финансовых технологий (финтех) на современную финансовую индустрию, подчеркивая, как инновации вносят коренные изменения в традиционные финансовые услуги и практики. Исследуя широкий спектр технологий, включая блокчейн, искусственный интеллект, мобильные платежи и облачные вычисления, авторы демонстрируют, как эти инструменты способствуют созданию более инклюзивных, доступных и эффективных финансовых систем. Статья освещает ключевые тенденции финтех-революции, такие как децентрализация финансовых услуг, персонализация предложений для потребителей и усиление акцента на кибербезопасности и защите данных. Особое внимание уделяется влиянию этих изменений на потребителей, финансовые учреждения и регуляторные органы, а также рассматриваются возможные вызовы и риски, связанные с быстрым развитием финтех-сектора.*

***Abstract**: This article examines the impact of financial technology (fintech) on today's financial industry, highlighting how innovation is bringing fundamental changes to traditional financial services and practices. Exploring a wide range of technologies, including blockchain, artificial intelligence, mobile payments, and cloud computing, the authors demonstrate how these tools are contributing to more inclusive, accessible, and efficient financial systems. The article highlights key trends in the fintech revolution, such as the decentralization of financial services, personalization of offerings for consumers, and increased emphasis on cybersecurity and data protection. The impact of these changes on consumers, financial institutions and regulators is emphasized, and the potential challenges and risks associated with the rapid evolution of the fintech sector are discussed*

***Ключевые слова**: финтех, блокчейн, искусственный интеллект, облачные вычисления, финансовые инновации, цифровая трансформация, кибербезопасность, регулирование финтех, экосистемы финтех.*

***Keywords**: fintech, blockchain, artificial intelligence, cloud computing, financial innovation, digital transformation, cybersecurity, fintech regulation, fintech ecosystems.*

1. Введение

В последние десятилетия мир стал свидетелем бурного развития финансовых технологий, которые коренным образом трансформировали традиционную финансовую индустрию. Этот процесс, широко известный как «финтех революция», ознаменовал собой эру инноваций, привнося в финансовый мир новые технологии, такие как блокчейн, искусственный интеллект, мобильные платежи и облачные вычисления. Эти технологии не только предоставили потребителям более быстрые, удобные и доступные способы доступа к финансовым услугам, но и вызвали значительные изменения в операционных моделях, стратегиях и бизнес-процессах традиционных финансовых институтов.

Финтех-революция — это процесс глубоких изменений в финансовой индустрии, вызванный внедрением новых технологий. Эти инновации не только улучшают существующие финансовые услуги, но и создают совершенно новые продукты и бизнес-модели, делая финансовые операции более доступными, эффективными и безопасными. Рассмотрим ключевые аспекты финтех-революции и то, как она меняет финансовый мир.

2. Блокчейн и криптовалюты

Одним из самых заметных проявлений финтех-революции является развитие блокчейна и криптовалют, таких как Биткойн и Эфириум. Блокчейн обеспечивает высокий уровень безопасности и прозрачности транзакций, что нашло применение не только в криптовалютах, но и в смарт-контрактах, цифровых идентификаторах и даже в голосовании онлайн.

3. Мобильные платежи и деньги

Финтех упрощает повседневные финансовые операции через мобильные платежные системы и приложения. Это позволяет пользователям совершать покупки, переводить деньги и управлять своими финансами прямо со своего смартфона, часто без необходимости посещения банковского отделения.

4. Искусственный интеллект и машинное обучение

AI и машинное обучение революционизируют финансовый сектор, предоставляя инструменты для анализа больших объемов данных, автоматизации решений по кредитам, персонализации финансовых услуг и борьбы с мошенничеством. Эти технологии способствуют более глубокому пониманию потребностей клиентов и предложению им наиболее подходящих продуктов.

5. Платформы краудфандинга и P2P кредитования

Финтех демократизировал доступ к финансированию через платформы краудфандинга и P2P (peer-to-peer) кредитования. Теперь малые предприятия и стартапы могут привлекать средства напрямую от инвесторов, минуя традиционные банковские и инвестиционные институты.

6. Регуляторные технологии (RegTech)

Внедрение финтех-инноваций также требует нового подхода к регулированию. RegTech использует технологии для упрощения и улучшения процессов регуляторного соответствия, снижая риски и издержки для финансовых учреждений.

7. Влияние на традиционные банки

Традиционные банки и финансовые учреждения под давлением финтех-конкурентов активно интегрируют новые технологии в свою деятель-

ность, чтобы не уступать в конкурентной борьбе. Это включает партнерства с финтех-стартапами, создание инновационных лабораторий и запуск собственных технологических решений.

8. Заключение

Финтех-революция представляет собой одно из самых значимых и динамичных направлений в современной экономике, кардинально меняющее ландшафт финансовой индустрии. Принимая во внимание анализированные тенденции и инновации, можно уверенно заявить, что финансовые технологии не только уже оказали огромное влияние на методы предоставления финансовых услуг и их доступность, но и продолжат трансформировать финансовый мир в будущем. Благодаря блокчейну, искусственному интеллекту, мобильным платежам, облачным вычислениям и другим инновациям, финтех улучшает доступность, скорость и безопасность финансовых операций, открывая новые возможности для потребителей и предприятий по всему миру. При этом финтех-революция несет не только возможности, но и вызовы, включая вопросы регулирования, кибербезопасности и защиты данных.

Список литературы

1. Пестов И. Е. Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик. диссертация на соискание ученой степени кандидата технических наук / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2022
2. Пестов И.Е., Фёдоров П.О., Кошелева С.А., Алёхин Р. В. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // I-methods. 2022. Т. 14. № 1.

3. Пестов И.Е., Шинкарева П.С., Кошелева С.А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.
4. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.
5. Пестов И.Е., Сахаров Д.В., Сергеева И.Ю., Чернобородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С. В. Бачевского. 2017. С. 525–527.

УДК 004

Управление данными в эпоху GDPR: лучшие практики для защиты личной информации

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья представляет собой комплексное исследование ключевых требований GDPR, в том числе механизмов соблюдения приватности данных, обязательств организаций перед субъектами данных и стратегий минимизации рисков, связанных с обработкой личной информации. Делается акцент на необходимости интеграции принципов защиты данных на всех уровнях организационной структуры и во всех фазах жизненного цикла данных. Проанализированы методологии оценки воздействия на защиту данных (DPIA), внедрение мер защиты данных по умолчанию и с момента проектирования систем, а также стратегии обучения и повышения осведомленности персонала в области защиты данных. Рассмотрены лучшие практики и рекомендации для управления данными в соответствии с GDPR, включая разработку и реализацию внутренних политик и процедур, которые обеспечивают не только юридическую, но и техническую защиту личных данных. Особое внимание уделено аспектам обес-*

печения прозрачности в обработке данных, гарантирования прав субъектов данных и укрепления доверия клиентов.

***Abstract**: The article is a comprehensive study of key GDPR requirements, including data privacy compliance mechanisms, organizations' obligations to data subjects, and strategies to minimize risks associated with the processing of personal information. Emphasis is placed on the need to integrate data protection principles at all levels of organizational structure and in all phases of the data lifecycle. Data Protection Impact Assessment (DPIA) methodologies, implementation of data protection measures by default and from the design of systems, and data protection training and awareness strategies for staff are analyzed. Best practices and recommendations for data management under GDPR are reviewed, including the development and implementation of internal policies and procedures that ensure not only legal but also technical protection of personal data. Special attention is paid to aspects of ensuring transparency in data processing, guaranteeing the rights of data subjects, and building customer trust.*

***Ключевые слова**: GDPR, управление данными, конфиденциальность данных, безопасность данных, обработка личных данных, принципы защиты данных, нарушения данных, меры по обеспечению безопасности данных.*

***Keywords**: GDPR, data governance, data privacy, data security, personal data processing, data protection principles, data breaches, data security measures.*

1. Введение

В мае 2018 года вступил в силу Общий регламент по защите данных (GDPR), значительно изменивший ландшафт управления и защиты личной информации в Европейском Союзе и за его пределами. Этот регламент не только установил новые стандарты для обработки данных, но и предоставил пользователям больше контроля над своей личной информацией, повысив требования к транспарентности и безопасности для организаций, обрабатывающих данные. В эпоху цифровизации и всевозрастающего объема данных, управление информацией становится ключевым элементом для достижения соответствия нормам GDPR и защиты прав конечных пользователей.

Управление данными в эпоху GDPR (Общего регламента по защите данных Европейского Союза) стало ключевым вызовом и приоритетом для организаций по всему миру. GDPR, введенный в мае 2018 года, направлен на укрепление и унификацию защиты данных для всех лиц в Европейском

Союзе, а также на регулирование экспорта личных данных за пределы ЕС. Этот регламент внес значительные изменения в подходы к управлению личной информацией, повысив требования к прозрачности, безопасности и ответственности организаций при обработке данных.

2. Лучшие практики управления данными в эпоху GDPR

1. Прозрачность и согласие

GDPR требует от организаций получения ясного, осознанного согласия от пользователей на обработку их личных данных. Прозрачность в информировании субъектов данных о том, какие данные собираются, с какой целью и как долго они будут храниться, является фундаментальным требованием.

2. Оценка воздействия на защиту данных (DPIA)

DPIA помогает идентифицировать и минимизировать риски для личной информации при новых проектах или системах. Это ключевой инструмент для соблюдения принципа «защиты данных на стадии проектирования».

3. Назначение ответственного за защиту данных (DPO)

Для организаций, осуществляющих обработку данных в больших масштабах, GDPR требует назначения DPO, который будет контролировать соответствие процессов обработки данных требованиям регламента.

4. Минимизация данных и управление доступом

Сохранение только тех данных, которые необходимы для конкретных законных целей, и предоставление доступа к данным только авторизованным лицам.

5. Безопасность данных

Внедрение адекватных технических и организационных мер для защиты данных от несанкционированного доступа, потери или разрушения. Это включает шифрование, регулярные аудиты безопасности и обучение сотрудников.

6. Уведомление о нарушениях

GDPR требует от организаций уведомлять надзорные органы о любых нарушениях безопасности данных в течение 72 часов после их обнаруже-

ния, а также информировать субъектов данных, если нарушение представляет высокий риск для их прав и свобод.

7. Права субъектов данных

Укрепление прав индивидов, включая право на доступ к своим данным, право на исправление, удаление («право быть забытым») и ограничение обработки, а также право на перенос данных.

Эффективное управление данными в эпоху GDPR не только обеспечивает соответствие регулятивным требованиям, но и способствует построению доверительных отношений с клиентами, повышая тем самым репутацию и конкурентоспособность организации. Организации, принимающие эти лучшие практики, лучше подготовлены к защите личной информации в динамично меняющемся цифровом мире.

3. Заключение

В заключение, управление данными в эпоху GDPR является не только вызовом, но и возможностью для организаций повысить свои стандарты в области защиты данных. Принятие лучших практик и стратегий управления данными не только обеспечивает соответствие регулятивным требованиям, но и способствует развитию более прозрачного, надежного и клиентоориентированного бизнеса. В эпоху цифровизации и все более строгих требований к конфиденциальности данных, эффективное управление данными становится критически важным компонентом успеха любой организации.

Список литературы

1. Рыжков А.А., Цветков А. Ю. Разработка программного комплекса по аудиту устройств в сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 779–782.
2. Таргонская А.И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы

инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 734–739.
3. Красов А.В., Левин М.В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. Т. 1. С. 141–146.
4. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.
5. Билятдинов К.З., Красов А.В., Меняйло В.В., Пешков А.И., Карпов А. Н. Теория информационных процессов и систем. — Санкт-Петербург, 2019.

УДК 004

Анализ эффективности алгоритмов машинного обучения в обнаружении кибератак

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В современном мире, где объемы цифровых данных растут с каждым днем, а методы кибератак становятся всё более изощренными, вопрос обеспечения кибербезопасности приобретает критическое значение. Эффективное обнаружение и нейтрализация угроз в реальном времени являются ключевыми задачами для защиты информационных систем. В данной статье проводится глубокий анализ эффективности алгоритмов машинного обучения в задачах обнаружения кибератак, выделяя их способность адаптироваться к новым и развивающимся угрозам без необходимости предварительного определения их признаков.Статья также рассматривает вызовы и ограничения, с которыми сталкиваются специалисты по кибербезопасности при интеграции машинного обучения в существующие системы защиты, включая необ-*

ходимость в больших объемах обучающих данных, проблемы с фальсификацией атак и вопросы приватности.

***Abstract**: In today's world, where the volume of digital data is growing every day and cyberattack methods are becoming more and more sophisticated, the issue of cybersecurity becomes critical. Effective real-time detection and neutralization of threats are the key tasks for protecting information systems. This paper provides an in-depth analysis of the effectiveness of machine learning algorithms in the task of detecting cyberattacks, highlighting their ability to adapt to new and evolving threats without the need to first identify their attributes. The paper also examines the challenges and limitations cybersecurity professionals face when integrating machine learning into existing defense systems, including the need for large amounts of training data, problems with attack falsification, and privacy issues.*

***Ключевые слова**: машинное обучение, кибератаки, кибербезопасность, нейронные сети, анализ данных, противодействие угрозам, автоматизация обнаружения, приватность данных, оптимизация алгоритмов.*

***Keywords**: machine learning, cyberattacks, cybersecurity, neural networks, data analysis, countering threats, detection automation, data privacy, algorithm optimisation.*

1. Введение

В эпоху цифровизации, когда информационные технологии проникают во все сферы жизни общества, вопросы кибербезопасности становятся всё более актуальными и важными. С ростом количества и сложности кибератак, традиционные методы их обнаружения и предотвращения оказываются неэффективными перед лицом постоянно меняющихся и адаптирующихся угроз. В этом контексте машинное обучение выступает как перспективное направление в усилении обороноспособности информационных систем, предлагая инновационные подходы к обнаружению и анализу кибератак. Анализ эффективности алгоритмов машинного обучения в обнаружении кибератак фокусируется на изучении и оценке различных методов машинного обучения, применяемых для идентификации и предотвращения киберугроз. В современном мире, где технологии развиваются с невероятной скоростью, кибератаки становятся всё более сложными и изощренными, что требует от систем кибербезопасности способности к быстрому обучению и адаптации.

Анализ эффективности алгоритмов машинного обучения в обнаружении кибератак охватывает несколько ключевых аспектов, каждый из кото-

рых играет важную роль в оценке способности этих технологий укреплять кибербезопасность. Вот подробнее о каждом из этих аспектов:

2. Методы машинного обучения

Нейронные сети: имитируют человеческий мозг и способны обнаруживать сложные шаблоны в данных. Особенно эффективны в обнаружении новых и неизвестных типов атак, благодаря глубокому обучению.

Алгоритмы обучения с подкреплением: учатся на основе награды за правильные действия, что позволяет им адаптироваться к изменяющимся угрозам и оптимизировать стратегии обнаружения атак.

Деревья решений: предоставляют ясную и логическую структуру для классификации и принятия решений, полезны для обнаружения атак на основе известных признаков и правил.

3. Эффективность и точность

Оценивается способность алгоритма точно идентифицировать кибератаки, минимизируя количество ложных срабатываний (ложноположительных результатов) и пропущенных угроз (ложноотрицательных результатов).

Включает в себя скорость обработки данных и способность алгоритма работать в реальном времени для своевременного обнаружения и реагирования на угрозы.

4. Проблемы и вызовы

Данные для обучения: Доступ к качественным и репрезентативным данным для обучения моделей остается одним из главных вызовов, поскольку это напрямую влияет на эффективность алгоритмов.

Приватность и безопасность: Обеспечение безопасности и защиты данных, используемых для обучения и тестирования моделей, особенно с учетом нормативных и юридических ограничений, таких как GDPR.

Адаптация к новым угрозам: Быстрая адаптация алгоритмов к постоянно меняющимся и развивающимся киберугрозам без постоянного ручного вмешательства.

5. Кейсы из практики

Приведение реальных примеров успешного применения алгоритмов машинного обучения в системах кибербезопасности, демонстрирующих их способность обнаруживать разнообразные типы атак, включая фишинг, вредоносное ПО и атаки на отказ в обслуживании (DDoS).

Анализ эффективности алгоритмов машинного обучения в обнаружении кибератак показывает значительный потенциал этих технологий для укрепления кибербезопасности. Однако для достижения максимальной эффективности необходимо преодолеть ряд проблем, включая обеспечение достаточного количества качественных обучающих данных, защиту приватности и безопасность данных, а также разработку адаптивных моделей, способных справляться с новыми и меняющимися угрозами

6. Заключение

В заключении можно отметить, что исследования в этой области могут способствовать дальнейшему развитию и оптимизации алгоритмов машинного обучения, улучшению их адаптивности и точности, что сделает их еще более эффективными в борьбе с киберугрозами. Развитие этих технологий открывает новые горизонты в обеспечении кибербезопасности, делая наш цифровой мир более защищенным.

Список литературы

1. Волкогонов В.Н., Гапоненко В.А., Катасонов А. И. Сравнительный анализ программных систем хранения данных специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 294–298.

2. Катасонов А.И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 563–568.
3. Гельфанд А. М. Программный комплекс по оценке защищенности узлов сети объектов критической информационной инфраструктуры // Свидетельство о регистрации программы для ЭВМ RU 2022684460, 14.12.2022. Заявка № 2022684050 от 07.12.2022.
4. Красов А.В., Гельфанд А.М., Фадеев И.И., Казанцев А. А. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры // Свидетельство о регистрации программы для ЭВМ RU 2020617705, 10.07.2020. Заявка № 2020616731 от 29.06.2020.
5. Гельфанд А.М., Казанцев А.А., Красов А.В., Орлов Г. А. Оценка рисков и угроз безопасности в среде «Умный дом» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 316–321.

УДК 004.738.5

Развитие веб-технологий: от статических страниц к динамическим веб-приложениям

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье исследуется эволюция веб-технологий с начала их существования до настоящего времени. Авторы анализируют переход от простых статических страниц, содержащих только HTML, к сложным динамическим веб-приложениям, использующим широкий спектр технологий, включая CSS, JavaScript, AJAX и различные серверные языки. Особое внимание уделяется ключевым моментам в истории веб-разработки, таким как появление фреймворков, введение концепций отзывчивого дизайна и появление одностраничных приложений (SPA). Анализируются тех-*

нические, социальные и экономические факторы, которые способствовали развитию веб-технологий. Рассматриваются текущие тенденции и предсказываются будущие направления развития, включая влияние искусственного интеллекта, машинного обучения и блокчейн технологий на веб-разработку.

***Abstract**: This paper explores the evolution of Web technologies from their inception to the present. The authors analyze the transition from simple static pages containing only HTML to complex dynamic web applications using a wide range of technologies including CSS, JavaScript, AJAX, and various server-side languages. Special attention is given to key moments in the history of web development, such as the emergence of frameworks, the introduction of responsive design concepts, and the advent of single page applications (SPAs). Technical, social, and economic factors that have contributed to the development of web technologies are analyzed. Current trends are examined and future directions predicted, including the impact of artificial intelligence, machine learning, and blockchain technologies on web development.*

***Ключевые слова**: веб-технологии, статические страницы, динамические веб-приложения, HTML, CSS, JavaScript, AJAX, фреймворки веб-разработки, машинное обучение, блокчейн технологии.*

***Keywords**: web technologies, static pages, dynamic web applications, HTML, CSS, JavaScript, AJAX, web development frameworks, machine learning, blockchain technologies.*

1. Введение

В последние десятилетия интернет претерпел значительные изменения, превратившись из набора простых, статических страниц в сложную экосистему динамических веб-приложений и сервисов. Это развитие веб-технологий отражает не только технический прогресс, но и изменение потребностей и ожиданий пользователей, а также эволюцию глобальной цифровой экономики. В начале своего пути, веб был местом, где доминировали статические HTML-страницы, предоставляющие ограниченный пользовательский опыт и минимальную интерактивность. С течением времени, появление и развитие таких технологий, как каскадные таблицы стилей (CSS), JavaScript и различных серверных языков программирования, кардинально изменило ландшафт веб-разработки.

Современные веб-технологии позволяют создавать сложные, высокоинтерактивные веб-приложения, которые предлагают пользовательский опыт, сопоставимый с традиционными настольными приложениями. От простых

блогов и веб-страниц до сложных корпоративных порталов и социальных сетей — веб-технологии теперь способны поддерживать широкий спектр функционала и предоставлять услуги миллиардам пользователей по всему миру.

2. Статические страницы

Изначально веб-сайты состояли из статических страниц, созданных с помощью HTML. Эти страницы были просты в создании и обслуживании, но ограничены в функциональности. Они не могли предоставлять пользователю интерактивный опыт или динамически менять содержимое в зависимости от пользовательских данных или поведения.

3. Появление CSS и JavaScript

Со временем в разработку стали внедряться CSS и JavaScript, что позволило улучшить внешний вид страниц и добавить элементы интерактивности, соответственно. CSS предоставил разработчикам возможность отделять дизайн от содержания, делая веб-страницы более гибкими и легкими для стилизации. JavaScript же позволил создавать более сложные пользовательские взаимодействия и динамически изменять содержимое страниц без необходимости их перезагрузки.

4. Динамические веб-приложения и серверные языки

Следующим большим шагом в развитии стали динамические веб-приложения, которые использовали серверные языки программирования, такие как PHP, Ruby, Python или Java, для создания страниц, динамически меняющихся в зависимости от пользовательских запросов или данных. Это позволило веб-сайтам предлагать более персонализированный и интерактивный опыт.

5. Одностраничные приложения и фреймворки

Более недавние технологические инновации привели к развитию одностраничных приложений (SPA), где большая часть содержимого загружа-

ется один раз, а затем динамически обновляется на стороне клиента. Это было достигнуто благодаря фреймворкам и библиотекам JavaScript, таким как Angular, React и Vue.js, которые обеспечивают более быструю и плавную пользовательскую навигацию.

6. Влияние новых технологий

В статье также обсуждаются последние технологические тренды, такие как искусственный интеллект, машинное обучение и блокчейн, которые начинают интегрироваться в веб-разработку, предоставляя новые возможности для создания инновационных веб-сервисов.

7. Заключение

В заключение, эволюция веб-технологий от простых статических страниц до сложных динамических веб-приложений является свидетельством неуклонного прогресса в области цифровых технологий. Мы стали свидетелями трансформации интернета из ограниченного ресурса в неисчерпаемую экосистему, способную удовлетворять разнообразные потребности и предпочтения пользователей. Такой прогресс не только расширил возможности веб-разработчиков и дизайнеров, но и радикально изменил способы взаимодействия людей с информацией, друг с другом и с цифровыми сервисами.

Современные динамические веб-приложения предоставляют глубоко персонализированный и интерактивный пользовательский опыт, благодаря интеграции передовых технологий, таких как искусственный интеллект, машинное обучение и реактивное программирование. Эти технологии не только улучшают удобство и функциональность веб-сайтов, но и открывают новые горизонты для инноваций в различных отраслях.

Однако, несмотря на значительные достижения, развитие веб-технологий не останавливается. Постоянно появляются новые вызовы и возможности, требующие от веб-разработчиков и дизайнеров не только адаптации к текущим трендам, но и предвидения будущих изменений. Важно подчеркнуть, что успех в сфере веб-разработки в значительной степени зависит от готовности к постоянному обучению, экспериментам и сотрудничеству.

Список литературы

1. Орлов Г.А., Красов А.В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 4. С. 76–84.»
2. Косов Н.А., Голубов Н. А. Способы защиты от инсайдерских атак // Инновационные решения социальных, экономических и технологических проблем современного общества. Сборник научных статей по итогам круглого стола со всероссийским и международным участием. Москва, 2021. С. 149–151.
3. Гельфанд А.М., Казанцев А.А., Красов А.В., Орлов Г. А. Оценка рисков и угроз безопасности в среде «Умный дом // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 316–321.
4. Штеренберг С.И., Бударный Г.С., Чумаков И. В. Анализ безопасности доменных систем // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 587–588.
5. Алехин Р.В., Красов А.В., Макарова А.Д., Орлов Г. А. Облачные сервисы. принцип работы, классификация и модели обслуживания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 70–74.

УДК 004.738.5

Методы и инструменты для улучшения доступности веб-сайтов

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная научная статья посвящена анализу методов и инструментов, способствующих улучшению доступности веб-сайтов для людей с различными ограничениями. В условиях глобализации цифрового пространства вопрос доступности веб-ресурсов становится особенно актуален, обеспечивая равные возможности доступа к информации и услугам для всех пользователей, включая лиц с ограниченными возможностями здоровья. В статье представлен обзор существующих подходов к созданию доступных веб-сайтов, включая применение стандартов Всемирной организации по стандартизации веб-контента (W3C) и инициативы по обеспечению веб-доступности (WCAG). Рассматриваются различные аспекты доступности, такие как визуальная, аудиальная, моторная и когнитивная, и предлагают конкретные рекомендации по их улучшению на веб-сайтах.*

***Abstract**: This research paper analyzes methods and tools that help improve the accessibility of websites for people with various disabilities. In the context of globalization of the digital space, the issue of accessibility of web resources becomes especially relevant, providing equal opportunities to access information and services for all users, including people with disabilities. The paper presents an overview of existing approaches to creating accessible websites, including the application of World Wide Web Content Standardization Organization (W3C) and Web Content Accessibility Guidelines (WCAG) standards. Different aspects of accessibility, such as visual, auditory, motor, and cognitive, are examined and specific recommendations for improving them in websites are offered.*

***Ключевые слова**: веб-доступность, доступность интерфейса, визуальная доступность, аудиальная доступность, моторная доступность, когнитивная доступность, адаптивный дизайн, тестирование доступности, принципы универсального дизайна, разработка веб-сайтов.*

***Keywords**: web accessibility, interface accessibility, visual accessibility, auditory accessibility, motor accessibility, cognitive accessibility, adaptive design, accessibility testing, universal design principles, website development.*

1. Введение

В современном мире интернет стал неотъемлемой частью повседневной жизни миллиардов людей по всему миру, предоставляя неограниченный доступ к информации, образованию, услугам и социальному взаимодействию. Однако, несмотря на его всеобщность, существует значительный разрыв в доступности веб-сайтов для людей с различными ограничениями. Проблема доступности веб-ресурсов стоит на порядке дня как с этической, так и с юридической точки зрения, требуя от разработчиков и владельцев веб-сайтов активных действий для обеспечения равного доступа к цифровому контенту для всех пользователей.

2. Улучшение доступности веб-сайтов

Улучшение доступности веб-сайтов — это комплексная задача, требующая внимательного подхода к дизайну, разработке и тестированию. Процесс включает в себя адаптацию веб-контента и интерфейса таким образом, чтобы они были доступны для пользователей с различными ограничениями, включая зрительные, слуховые, моторные и когнитивные.

На пути к доступности веб-сайтов ключевым аспектом является понимание того, что веб-доступность не касается только некоторой группы пользователей. На самом деле, улучшения, направленные на увеличение доступности, часто делают сайт более удобным и понятным для всех. Это достигается за счет использования ясного и логического структурирования контента, обеспечения достаточного контраста цветов, предоставления альтернативных текстов для изображений и видео, а также улучшения навигации и интерактивных элементов.

Применение стандартов доступности, таких как WCAG (Web Content Accessibility Guidelines), помогает разработчикам следовать проверенным рекомендациям и лучшим практикам. Эти руководства предоставляют конкретные указания по созданию более доступного контента, например, как делать видео и аудио контент доступным для слабослышащих или как обеспечить возможность навигации по сайту с помощью клавиатуры для пользователей, которые не могут использовать мышь.

Тестирование играет жизненно важную роль в процессе улучшения доступности. Оно может проводиться как с помощью специализированных инструментов, так и реальными пользователями. Автоматизированные инструменты могут быстро выявить многие проблемы доступности, но ручное тестирование с участием пользователей с различными ограничениями помогает понять реальные проблемы в интерфейсе, которые могут быть неочевидны при автоматической проверке.

Улучшение доступности — это непрерывный процесс. Технологии, стандарты и потребности пользователей постоянно развиваются. Веб-разработчики и дизайнеры должны стремиться к постоянному обучению и адаптации своих веб-сайтов к новым требованиям и технологиям. Это не только улучшает доступность и удобство веб-сайта, но и способствует созданию более инклюзивного и доступного цифрового пространства для всех пользователей.

3. Заключение

В заключении, улучшение доступности веб-сайтов является важным шагом в создании инклюзивного и равноправного цифрового пространства. Внедрение методов и инструментов для повышения доступности не только помогает удовлетворить потребности широкого круга пользователей с различными ограничениями, но и улучшает общее качество веб-ресурсов, делая их более понятными, удобными и функциональными для всех.

Процесс повышения доступности веб-сайтов требует осмысленного подхода, который начинается с понимания разнообразия пользовательских потребностей и принципов универсального дизайна. Следование международным стандартам, таким как WCAG, регулярное тестирование и вовлечение пользователей с различными ограничениями в этот процесс позволяют создавать более доступные и инклюзивные веб-ресурсы.

Необходимо подчеркнуть, что улучшение доступности — это не разовая задача, а непрерывный процесс обучения, тестирования и адаптации к изменяющимся технологиям и потребностям пользователей. Разработчики, дизайнеры и владельцы веб-сайтов должны стремиться к созданию

доступного цифрового контента, осознавая, что каждое улучшение делает интернет более открытым и доступным для всех.

В конечном счете, повышение доступности веб-сайтов способствует созданию более справедливого и инклюзивного общества, где каждый человек имеет равный доступ к информации, образованию и коммуникации. Поэтому важно, чтобы разработчики и дизайнеры продолжали искать новые методы и инструменты для улучшения доступности, стремясь к созданию более удобного и включающего всех интернет-пространства.

Список литературы

1. Катасонов А.И., Цветков А.Ю., Андрианов В. И. Cisco TrustSec // Информационные технологии и телекоммуникации. 2017. Т. 5. № 4. С. 85–95.
2. Катасонова Г. Р. Основные тренды образовательной цифровой экосистемы // Конструктивные педагогические заметки. 2024. № 12–1 (21). С. 13–19.
3. Абрамова Е.А., Красов А.В., Поляничева А. В. Тенденции развития и безопасность IP-телефонии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 23–28.
4. Богомаз М.Э., Михайлова Л.А., Поляничева А. В. Инструменты обеспечения безопасности IP-телефонии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 170–172.
5. Ковцур М.М., Поляничева А. В. Исследование механизма авторизации пользователей для доступа к IP-TB сервисам с применением Radius-сервера // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С. В. Бачевского. 2018. С. 466–471.

УДК 004.056

Безопасность программного обеспечения: современные вызовы и стратегии защиты

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В эпоху цифровизации обеспечение безопасности программного обеспечения является ключевым аспектом для защиты данных и поддержания доверия пользователей. Статья делает акцент на современных вызовах в области безопасности программного обеспечения, таких как усиление угроз кибербезопасности, развитие сложных вирусов и техник хакерских атак. Исследуются различные угрозы, с которыми сталкиваются организации и индивидуальные пользователи, включая вредоносное ПО, атаки "через день ноль", фишинг и другие методы киберпреступности. В статье представлены современные методы и стратегии защиты программного обеспечения, начиная с традиционных антивирусных решений и заканчивая передовыми технологиями кибербезопасности, такими как искусственный интеллект и машинное обучение. Авторы обсуждают важность комплексного подхода к безопасности, который включает в себя проектирование безопасности на этапе разработки, регулярное обновление и патчинг систем, а также обучение и повышение осведомленности пользователей.*

***Abstract**: In the era of digitalization, software security is a key aspect to protect data and maintain user trust. The paper emphasizes on current challenges in software security such as increasing cybersecurity threats, development of sophisticated viruses and hacker attack techniques. Various threats faced by organizations and individual users are explored, including malware, day zero attacks, phishing and other cybercrime techniques. The article presents current software defense techniques and strategies, ranging from traditional antivirus solutions to advanced cybersecurity technologies such as artificial intelligence and machine learning. The authors discuss the importance of a comprehensive approach to security that includes security design during the development phase, regular updating and patching of systems, and user training and awareness.*

***Ключевые слова**: кибербезопасность, угрозы кибербезопасности, методы защиты программного обеспечения, антивирусные технологии, управление уязвимостями, фишинг и вредоносное ПО, проектирование безопасности, обновление и патчинг систем, защита данных.*

***Keywords**: cybersecurity, cybersecurity threats, software protection methods, anti-virus technologies, vulnerability management, phishing and malware, security engineering, system updating and patching, data protection.*

1. Введение

В наше время, когда цифровизация глубоко проникла во все аспекты нашей жизни, вопросы безопасности программного обеспечения приобретают особую актуальность и важность. С ростом зависимости общества от информационных технологий увеличивается и количество угроз, нацеленных на эксплуатацию уязвимостей в программном обеспечении. Вредоносные атаки, утечки данных, фишинг, вирусы и другие киберугрозы постоянно эволюционируют, становясь всё более изощрёнными и труднообнаружимыми.

Защита программного обеспечения становится не просто задачей отдельных IT-специалистов, но и приоритетом для всей организации. Современные вызовы в области кибербезопасности требуют комплексного подхода, который включает в себя как технические решения, так и стратегии управления, образовательные программы и политики безопасности.

2. Безопасность программного обеспечения

Безопасность программного обеспечения — это обширная область, касающаяся защиты программ и систем от вредоносных атак, нарушений конфиденциальности, потери данных и других форм киберугроз. В современном мире, где технологии проникают в каждый аспект нашей жизни, вопросы безопасности становятся особенно актуальными. Хакеры и злоумышленники неустанно ищут новые способы атаки, а это значит, что методы защиты должны развиваться соответствующим образом.

В контексте программного обеспечения безопасность начинается на этапе дизайна и продолжается на протяжении всего жизненного цикла продукта. Это включает в себя не только внедрение технических мер, например шифрование и использование антивирусного ПО, но и организационные меры, такие как политики безопасности и обучение персонала.

Одной из главных задач является обеспечение того, чтобы уязвимости были идентифицированы и устранены до того, как злоумышленники смогут их эксплуатировать. Это требует регулярного тестирования, аудитов безопасности и обновления программного обеспечения. Кроме того, важно постоянно отслеживать и анализировать сетевой трафик и системные журналы на предмет признаков неавторизованной активности.

С учетом постоянного развития технологий и угроз, безопасность программного обеспечения требует подхода, основанного на постоянном обучении и адаптации. Это не только технологическая, но и организационная задача, требующая вовлеченности всех уровней организации.

Безопасность программного обеспечения в современном мире представляет собой комплексную и многоуровневую дисциплину, направленную на защиту программ и систем от вредоносных атак и других угроз кибербезопасности. Это включает в себя защиту от вирусов, шпионского ПО, троянских программ, а также защиту от атак, направленных на нарушение работы программ и кражу или повреждение данных.

3. Современные вызовы

Развитие угроз: Киберугрозы становятся всё более сложными и изощренными. Хакеры постоянно разрабатывают новые способы атак и методы обхода существующих мер безопасности.

Распространение облачных технологий: Хотя облачные сервисы предлагают множество преимуществ, они также вносят дополнительные риски и вызовы для безопасности, требуя новых подходов к защите данных и инфраструктуры.

Интернет вещей (IoT): Увеличение числа подключенных устройств расширяет потенциальные точки входа для злоумышленников и увеличивает сложность сетей.

Мобильность и удалённая работа: Рост мобильных устройств и удаленной работы увеличивает сложность управления безопасностью за пределами традиционных корпоративных сетей.

4. Стратегии защиты

Проектирование с учетом безопасности: Включение практик безопасности на всех этапах разработки программного обеспечения помогает предотвратить уязвимости с самого начала.

Обновления и патчи: Регулярное обновление программного обеспечения и операционных систем помогает защититься от известных угроз и уязвимостей.

Шифрование: Использование сильного шифрования для защиты данных в покое и во время передачи помогает предотвратить их утечку или кражу.

Обнаружение и реагирование на инциденты: Системы обнаружения и реагирования на инциденты позволяют быстро идентифицировать и устранять угрозы, ограничивая возможный ущерб.

Обучение и осведомленность пользователей: Повышение осведомленности среди пользователей о рисках и лучших практиках безопасности снижает вероятность успешных фишинговых атак и других видов социальной инженерии.

Многоуровневая защита: Применение подхода «защиты в глубину», сочетающего несколько уровней безопасности, помогает создать более надежную систему защиты.

5. Заключение

В заключение, можно подчеркнуть, что в условиях непрерывно эволюционирующего цифрового мира, защита программного обеспечения остается одним из самых важных аспектов поддержания целостности и конфиденциальности данных, а также обеспечения непрерывности бизнес-процессов. Современные киберугрозы становятся всё более изощренными, что требует от организаций постоянного внимания к вопросам безопасности и готовности адаптироваться к новым вызовам.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных

системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004.7

Эволюция протоколов маршрутизации в беспроводных сенсорных сетях

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье проводится всесторонний анализ развития механизмов маршрутизации, применяемых в сфере беспроводных сенсорных сетей (БСС). Исследование начинается с обзора основных концепций и архитектурных решений, заложенных в основу современных сенсорных сетей, подчеркивая их значимость для различных приложений, от мониторинга окружающей среды до систем умного дома и здравоохранения. Рассматривается историческое развитие протоколов маршрутизации, начиная с простых алгоритмов, базирующихся на фиксированных маршрутах, до более сложных адаптивных и иерархических систем, разработанных для повышения эффективности и устойчивости сети в условиях ограниченной энергии, вычислительных ресурсов и динамичных изменений в топологии сети.*

***Abstract**: This paper provides a comprehensive analysis of the development of routing mechanisms used in the field of wireless sensor networks (WSNs). The study begins with an overview of the basic concepts and architectures underlying modern sensor networks, emphasizing their relevance for applications ranging from environmental monitoring to smart home and healthcare systems. The historical evolution of routing protocols is reviewed, from simple fixed-route-based algorithms to more complex adaptive and hierarchical systems designed to improve network efficiency and resilience in the face of limited energy, computational resources, and dynamic changes in network topology.*

***Ключевые слова**: беспроводные сенсорные сети, протоколы маршрутизации, адаптивная маршрутизация, топология сети, устойчивость сети, динамические сетевые условия, оптимизация ресурсов, инновации в маршрутизации, сетевая безопасность.*

***Keywords**: wireless sensor networks, routing protocols, adaptive routing, network topology, network stability, dynamic network conditions, resource optimisation, routing innovations, network security.*

1. Введение

В последние годы беспроводные сенсорные сети (БСС) нашли широкое применение в различных областях, включая экологический мониторинг, здравоохранение, военные приложения и умные города. Эти сети состоят из большого числа распределенных датчиков, собирающих и передающих данные к центральным узлам обработки. Одним из ключевых аспектов, определяющих эффективность и надежность БСС, является маршрутизация, то есть процесс определения и управления путями передачи данных от источника к получателю.

Протоколы маршрутизации в беспроводных сенсорных сетях испытывают уникальные вызовы, обусловленные ограниченными ресурсами устройств, такими как память, вычислительная мощность и, что наиболее критично, энергия. Кроме того, динамичная природа среды, в которой оперируют сенсорные сети, требует от протоколов маршрутизации высокой степени адаптивности и устойчивости к изменениям.

С учетом этих вызовов, исследователи и инженеры в течение последних десятилетий активно разрабатывали и совершенствовали различные подходы к маршрутизации в БСС. Целью данной статьи является предоставление обзора эволюции протоколов маршрутизации, от простых ран-

них моделей до современных сложных систем, включая те, что используют принципы искусственного интеллекта и машинного обучения.

2. Эволюция протоколов маршрутизации

Эволюция протоколов маршрутизации в беспроводных сенсорных сетях (БСС) отражает развитие технологий и потребностей в различных областях применения. Процесс этот можно условно разделить на несколько этапов, от ранних экспериментов до современных адаптивных и интеллектуальных систем.

3. Ранние стадии: статическая маршрутизация

В начале развития БСС протоколы маршрутизации были довольно примитивными и основывались на статической маршрутизации. Данные передавались через фиксированные маршруты без учета изменений в сетевых условиях. Такой подход был довольно эффективен в стабильных и предсказуемых средах, но не обеспечивал должной гибкости и масштабируемости.

4. Развитие динамической маршрутизации

С ростом сложности сетей и задач появилась необходимость в более гибких решениях. Это привело к разработке динамических протоколов маршрутизации, способных адаптироваться к изменениям в топологии сети и условиях передачи данных. Протоколы, такие как LEACH (Low Energy Adaptive Clustering Hierarchy), предложили иерархическую организацию сети и динамическое формирование кластеров для более эффективного управления энергоресурсами.

5. Энергосберегающие протоколы

Энергопотребление является критическим параметром для БСС, так как большинство сенсорных устройств работают от батарей. Разработка

протоколов, направленных на минимизацию энергопотребления, стала приоритетной задачей. В результате появились такие протоколы, как SPIN (Sensor Protocols for Information via Negotiation), которые оптимизировали энергопотребление за счет выборочной передачи данных.

6. Использование машинного обучения

Последние исследования в области маршрутизации БСС сосредоточены на применении методов машинного обучения и искусственного интеллекта для улучшения эффективности и надежности сетевых операций. Использование алгоритмов предсказательного анализа и адаптивного обучения позволяет системам самостоятельно оптимизировать маршруты передачи данных, учитывая текущее состояние сети и предполагаемые изменения.

7. Направления будущих исследований

В будущем ожидается дальнейшее развитие интеллектуальных протоколов маршрутизации, интеграция с технологиями Интернета вещей (IoT) и киберфизическими системами. Особое внимание будет уделено обеспечению безопасности данных, управлению сетевыми ресурсами и разработке устойчивых к ошибкам систем.

8. Заключение

В заключение следует подчеркнуть, что развитие протоколов маршрутизации в беспроводных сенсорных сетях продолжится и в будущем. Исследователям предстоит решить множество задач, связанных с безопасностью данных, управлением ресурсами и интеграцией с другими технологиями, такими как Интернет вещей и киберфизические системы. Прогресс в этой области будет способствовать развитию не только самих сенсорных сетей, но и множества связанных с ними приложений, от умных городов до промышленного интернета вещей.

Список литературы

1. Пестов И. Е. Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик: диссертация на соискание ученой степени кандидата технических наук / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2022
2. Пестов И.Е., Фёдоров П.О., Кошелева С.А., Алёхин Р. В. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // I-methods. 2022. Т. 14. № 1.
3. Пестов И.Е., Шинкарева П.С., Кошелева С.А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.
4. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.
5. Пестов И.Е., Сахаров Д.В., Сергеева И.Ю., Чернобородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С. В. Бачевского. 2017. С. 525–527.

УДК 004.056

Безопасность сетевых систем: проблемы, решения и будущее

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья детально рассматривает существующие решения и стратегии защиты сетевых систем, включая шифрование, аутентификацию, сетевые брандмауэры и системы обнаружения и предотвращения вторжений. Авторы обсуждают преимущества и недостатки каждого подхода, а также предлагают рекомендации по созданию комплексной сетевой безопасности, учитывая различные архитектурные и операционные аспекты. Особый акцент делается на будущих тенденциях и инновациях в области безопасности сетевых систем. Рассматриваются перспективные технологии, такие как искусственный интеллект и машинное обучение в контексте кибербезопасности, блокчейн-технологии для усиления прозрачности и надежности сетевых транзакций, а также развитие квантового шифрования как средства защиты от новых видов кибератак. Статья заканчивается обсуждением важности сотрудничества между организациями и государственными структурами в борьбе с киберпреступностью и развитием стандартов кибербезопасности.*

***Abstract**: This article takes a detailed look at existing solutions and strategies for securing networked systems, including encryption, authentication, network firewalls, and intrusion detection and prevention systems. The authors discuss the advantages and disadvantages of each approach and offer recommendations for creating comprehensive network security, taking various architectural and operational aspects into account. Special emphasis is placed on future trends and innovations in network system security. Promising technologies such as artificial intelligence and machine learning in the context of cybersecurity, blockchain technologies to enhance the transparency and reliability of network transactions, and the development of quantum encryption as a means of defense against new types of cyberattacks are discussed. The article concludes with a discussion of the importance of cooperation between organizations and government agencies in combating cybercrime and developing cybersecurity standards.*

***Ключевые слова**: кибербезопасность, сетевые атаки, методы защиты, криптография, аутентификация, брандмауэры, управление уязвимостями, стандарты кибербезопасности.*

***Keywords**: cybersecurity, network attacks, defence methods, cryptography, authentication, firewalls, vulnerability management, cybersecurity standards.*

1. Введение

В эпоху глобальной цифровизации и всепроникающей интернетизации, безопасность сетевых систем выходит на первый план как один из ключевых аспектов сохранения данных, конфиденциальности и целостности информационных процессов. С каждым днем в мире происходит всё больше кибератак различного масштаба, начиная от индивидуального фишинга и заканчивая организованными атаками на государственные и корпоративные системы. В этом контексте разработка и внедрение эффективных средств и методов защиты сетевых систем становится не просто актуальной задачей, но и неотложной необходимостью.

2. Безопасность сетевых систем

Безопасность сетевых систем — это комплексная дисциплина, целью которой является защита данных и ресурсов, доступных в сети, от несанкционированного доступа, использования, раскрытия, нарушения доступности, изменения или уничтожения. Эта область охватывает различные аспекты, включая физическую безопасность оборудования, безопасность передаваемых данных и программное обеспечение для обеспечения безопасности.

Основная задача безопасности сетевых систем заключается в обеспечении конфиденциальности, целостности и доступности данных. Конфиденциальность означает, что информация доступна только тем, кто имеет на это право. Целостность обеспечивает, что данные не были изменены несанкционированно, в то время как доступность гарантирует, что данные и ресурсы доступны легитимным пользователям, когда они в этом нуждаются.

В рамках безопасности сетевых систем используются различные технологии и методы. Шифрование играет ключевую роль в защите данных во время их передачи по сети или при хранении. Аутентификация и авторизация помогают убедиться, что доступ к данным и ресурсам имеют только те пользователи, которые обладают соответствующими правами. Сетевые брандмауэры и системы обнаружения и предотвращения вторжений (IDS/

IPS) используются для мониторинга и контроля входящего и исходящего сетевого трафика с целью обнаружения и предотвращения подозрительной активности.

3. Проблемы

Среди ключевых проблем в области безопасности сетевых систем выделяются новые и эволюционирующие формы киберугроз, такие как вредоносное программное обеспечение, фишинг, спам, DDoS-атаки и атаки «человек посередине». Сложность и разнообразие этих атак требуют от специалистов по безопасности постоянной бдительности и адаптации. Дополнительные проблемы включают управление большими объемами данных, обеспечение конфиденциальности и интеграции новых технологических решений в существующие сетевые структуры.

4. Решения

В ответ на эти вызовы разработаны различные решения, направленные на укрепление сетевой безопасности. К ним относятся фаерволы, системы обнаружения и предотвращения вторжений, политики безопасности, регулярные аудиты и проверки на уязвимости, а также обучение пользователей. Прогресс в области криптографии и аутентификации также значительно улучшил способность сетевых систем защищаться от несанкционированного доступа и других видов киберугроз.

5. Будущее

Будущее безопасности сетевых систем видится в интеграции передовых технологий, таких как искусственный интеллект и машинное обучение, для более эффективного обнаружения и реагирования на угрозы в реальном времени. Разработки в области квантовых вычислений и блокчейн-технологий обещают новые подходы к защите данных и транзакций. Кроме того, ожидается, что улучшение международного сотрудничества и разработка глобальных стандартов и политик в области кибербезопас-

ности сыграют ключевую роль в обеспечении защиты сетевых систем на международном уровне.

6. Заключение

В заключение статьи о безопасности сетевых систем, можно отметить, что эта область представляет собой динамично развивающуюся и чрезвычайно важную часть современных информационных технологий. С учетом непрерывного роста объемов генерируемых данных и их значимости для функционирования как бизнес-структур, так и государственных организаций, вопросы обеспечения безопасности этих данных становятся всё более актуальными. Сохранение конфиденциальности, целостности и доступности информации в условиях постоянно меняющегося ландшафта угроз требует от специалистов по безопасности не только глубоких технических знаний, но и способности адаптироваться к новым вызовам. Решения, применяемые сегодня для защиты сетевых систем, должны сочетать в себе как проверенные временем технологии, так и новейшие разработки в области кибербезопасности.

Список литературы

1. Золотова Д.С., Катасонов А. И. Сравнительный анализ средств по ограничению запускаемых пользователями приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 541–546.
2. Штеренберг С.И., Бударный Г.С., Чумаков И. В. Методика обеспечения безопасности доменных систем доверенной зоны // Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. Санкт-Петербург, 2022. С. 621–625.
3. Красов А.В., Цветков А. Ю. Разработка системы контроля текущей успеваемости студентов вуза // Актуальные проблемы инфотелеком-

муникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция. 2013. С. 844–847.
4. Кузнецов Д.Д., Цветков А. Ю. Использование систем принудительного контроля доступа для обеспечения безопасности контейнеризации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 723–727.
5. Захарова Т.Е., Цветков А. Ю. Анализ существующих нормативных документов для формирования политики безопасности в системе электронного документооборота вуза // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С. В. Бачевского. 2017. С. 337–343.

УДК 004.7

Анализ пропускной способности в современных беспроводных сетях

Васенин Руслан Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье осуществляется всесторонний анализ текущего состояния и проблематики пропускной способности в беспроводных сетевых технологиях, включая Wi-Fi, 4G, 5G, и технологии Интернета вещей (IoT). Исследование начинается с обзора основных факторов, влияющих на пропускную способность беспроводных сетей, таких как радиочастотные помехи, протоколы передачи данных, стандарты модуляции и использование спектра. В рамках анализа рассматриваются текущие проблемы и ограничения существующих беспроводных сетей, включая вопросы интерференции, ограничения пропускной способности в условиях высокой плотности подключений и проблемы безопасности.*

***Abstract**: This article provides a comprehensive analysis of the status and bandwidth challenges in wireless networking technologies, including Wi-Fi, 4G, 5G, and Internet of Things (IoT)*

technologies. The study begins with an overview of the major factors affecting wireless network throughput, such as RF interference, transmission protocols, modulation standards, and spectrum utilization. The analysis addresses the current challenges and limitations of existing wireless networks, including interference issues, capacity limitations in high density connectivity environments, and security concerns.

***Ключевые слова**: беспроводные сети, пропускная способность, протоколы передачи данных, стандарты модуляции, MIMO (Multiple Input Multiple Output), управление спектром, интерференция, безопасность сетей, оптимизация сетевой пропускной способности, технологии беспроводной связи.*

***Keywords**: wireless networks, throughput, data transmission protocols, modulation standards, MIMO (Multiple Input Multiple Output), spectrum management, interference, network security, network throughput optimisation, wireless communication technologies.*

1. Введение

В современном мире беспроводные сети стали неотъемлемой частью повседневной жизни, поддерживая широкий спектр приложений, от личного общения до критически важных промышленных систем. С увеличением количества устройств, подключаемых к Интернету вещей (IoT), а также постоянным ростом потребностей в передаче данных высокой скорости, вопросы, связанные с пропускной способностью беспроводных сетей, приобретают все большее значение. Эффективное использование спектра и оптимизация пропускной способности становятся ключевыми задачами для обеспечения надежности и производительности сетевых соединений.

2. Анализ пропускной способности

Анализ пропускной способности в современных беспроводных сетях — это критически важная задача, которая лежит в основе разработки и оптимизации сетевых технологий. В условиях постоянно растущего спроса на передачу данных и расширения функционала Интернета вещей (IoT), пропускная способность беспроводных сетей становится ключевым фактором, определяющим их эффективность и надежность. Данная тема включает в себя исследование и анализ широкого спектра аспектов, начи-

ная от физических ограничений и заканчивая программно-определенными методами управления сетью.

Пропускная способность сети определяет максимальный объем данных, который может быть передан через сеть за определенный промежуток времени. В контексте беспроводных сетей, пропускная способность зависит от множества факторов, включая радиочастотные условия, используемые технологии модуляции и кодирования, а также архитектуру и конфигурацию сети. Кроме того, на пропускную способность оказывают влияние и внешние помехи, включая интерференцию от других беспроводных устройств и физические препятствия.

В последние годы значительное внимание уделяется разработке и внедрению новых технологий, таких как 4G, 5G и даже перспективы 6G, которые обещают значительно увеличить пропускную способность и уменьшить задержки в беспроводных сетях. Технологии, такие как MIMO и технологии управления спектром, играют важную роль в увеличении эффективности использования доступного радиочастотного спектра и, как следствие, в повышении пропускной способности сетей.

Однако увеличение пропускной способности беспроводных сетей сопряжено с рядом вызовов. В частности, нужно учитывать баланс между повышением пропускной способности и обеспечением безопасности передаваемых данных. Кроме того, важно обеспечить справедливое распределение ресурсов сети между пользователями, особенно в условиях высокой плотности подключений.

Исследования в области анализа пропускной способности беспроводных сетей продолжают расширять понимание этих и многих других вопросов, предлагая новые методы и решения для оптимизации сетевых ресурсов. Эти работы имеют важное значение для развития сетевых технологий, позволяя удовлетворить растущие потребности пользователей в высокоскоростном доступе к данным.

3. Заключение

В заключение исследования на тему «Анализ пропускной способности в современных беспроводных сетях» можно подчеркнуть, что эффектив-

ность и производительность беспроводных сетей являются ключевыми факторами в обеспечении надежной и быстрой передачи данных в современном мире. Развитие технологий 4G, 5G и перспективы внедрения 6G открывают новые возможности для увеличения пропускной способности и снижения задержек, что, в свою очередь, способствует развитию таких направлений, как Интернет вещей, автономные транспортные средства и дистанционное обучение.

Анализ показал, что преодоление проблем, связанных с радиочастотными помехами, управлением спектром и оптимизацией алгоритмов маршрутизации, требует комплексного подхода, включающего как аппаратные, так и программные решения. Важную роль играют инновации в области технологий модуляции, использование принципов MIMO и разработка эффективных механизмов управления сетевым трафиком. Таким образом, исследование пропускной способности современных беспроводных сетей не только выявляет текущие тенденции и вызовы, но и намечает пути развития для обеспечения удовлетворения будущих потребностей пользователей в высокоскоростном и надежном доступе к информационным ресурсам. Продолжение научных разработок в этой области будет способствовать развитию всех аспектов цифровой экономики, делая технологии более доступными, надежными и безопасными для конечных пользователей.

Список литературы

1. Катасонов А.И., Цветков А. Ю. Разработка метода аппаратного обнаружения руткита в ОС Linux // Безопасность в профессиональной деятельности. сборник научных статей. Санкт-Петербург, 2021. С. 132–147. Темная тема / [Электронный ресурс] // Apple: [сайт]. — URL: https://developer.apple.com/design/human-interface-guidelines/dark-mode#dark-mode-colors (дата обращения: 22.12.2023).
2. OpenType / [Электронный ресурс] // Wikipedia: [сайт]. — URL: https://ru.wikipedia.org/wiki/OpenType (дата обращения: 22.12.2023).
3. Горбань С.А., Красов А.В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux // Актуальные про-

блемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 345–348.
4. Цветков А. Ю. Анализ существующих механизмов защиты и атак в операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 927–931.
5. Темченко В.И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 740–745.

УДК 004

Блокчейн в образовании: сертификаты, степени и управление знаниями

Голубятников Артем Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье исследуется потенциал технологии блокчейн в образовательной сфере с акцентом на три ключевые области: выдачу сертификатов, признание степеней и управление знаниями. Блокчейн, технология распределенного реестра, известная своей прозрачностью, неизменяемостью и децентрализацией, предлагает новые возможности для повышения эффективности, надежности и безопасности в учебных и административных процессах. Статья начинается с обзора основ блокчейн технологии и ее текущего применения в различных секторах, затем переходит к анализу ее роли в образовании. Особое внимание уделяется применению блокчейна для улучшения систем выдачи сертификатов и степеней, обеспечивая их подлинность, проверяемость и доступность. Также рассматриваются перспективы использования блокчейна для управления знаниями, включая создание надежных баз данных образовательных ресурсов и учебных достижений. Статья стремится выявить потенциаль-*

ные преимущества и вызовы внедрения блокчейн технологий в образовательной среде и предлагает рекомендации для дальнейших исследований и разработки.

***Abstract**: This paper explores the potential of blockchain technology in the educational field, focusing on three key areas: certificate issuance, degree recognition, and knowledge management. Blockchain, a distributed ledger technology known for its transparency, immutability, and decentralization, offers new opportunities to improve efficiency, reliability, and security in educational and administrative processes. The article begins with an overview of the basics of blockchain technology and its current applications in various sectors, before moving on to analyze its role in education. Particular attention is paid to the application of blockchain to improve certificate and degree systems, ensuring their authenticity, verifiability, and accessibility. The prospects for using blockchain for knowledge management, including the creation of robust databases of educational resources and learning achievements, are also discussed. The article seeks to identify the potential benefits and challenges of implementing blockchain technologies in educational environments and offers recommendations for further research and development.*

***Ключевые слова**: блокчейн, образование, сертификаты, степени, кибербезопасность в образовании, цифровые удостоверения личности, технологии распределенного реестра.*

***Keywords**: blockchain, education, certificates, degrees, cybersecurity in education, digital ID cards, distributed ledger technologies.*

Введение

Блокчейн в образовании — это инновационное применение технологии распределённого реестра, которая изначально стала известна благодаря криптовалютам, таким как Bitcoin. Но за пределами финансового сектора, блокчейн начинает играть важную роль в образовании, предлагая новые подходы к сертификации, управлению степенями и знаниями. Вот основные аспекты использования блокчейна в образовательной сфере:

Цифровая сертификация и верификация

Одним из ключевых применений блокчейна в образовании является создание цифровых сертификатов для студентов. Эти сертификаты могут включать дипломы, транскрипты и другие академические квалификации. Благодаря технологии блокчейна, каждый цифровой документ становится неизменяемым и верифицируемым, что делает подделку практически не-

возможной. Это позволяет работодателям и учебным заведениям быстро и безопасно проверять академические данные без необходимости обращаться напрямую в учебное заведение.

Управление академическими записями

Блокчейн может использоваться для создания надежной и легкодоступной системы управления академическими записями. В такой системе данные о студентах и их учебных достижениях хранятся в зашифрованном виде и могут быть доступны в любой момент. Это упрощает административные процедуры и обеспечивает студентам легкий доступ к своим записям.

Улучшение доступа к образовательным ресурсам

С помощью блокчейна можно создать децентрализованные платформы для обмена учебными материалами и курсами. Это позволяет учебным заведениям, преподавателям и студентам обмениваться информацией и ресурсами в безопасной и надежной среде. Кроме того, такие платформы могут использоваться для распространения онлайн-курсов, чему способствует технология смарт-контрактов блокчейна, автоматизируя процессы регистрации и оплаты.

Поддержка пожизненного обучения

Блокчейн может играть значительную роль в поддержке пожизненного обучения, позволяя индивидуам накапливать и систематизировать свои образовательные достижения в цифровом формате на протяжении всей жизни. Это может включать формальное образование, профессиональное обучение, онлайн-курсы и другие виды обучения.

Вызовы и перспективы

Несмотря на потенциальные преимущества, внедрение блокчейна в образовании сталкивается с рядом вызовов. Они включают в себя необ-

ходимость стандартизации данных, вопросы конфиденциальности и безопасности, а также необходимость в обучении и подготовке преподавателей и административного персонала к использованию новых технологий.

Тем не менее, блокчейн продолжает привлекать внимание как инновационное решение для образовательной сферы. По мере того, как технология развивается и совершенствуется, можно ожидать увеличения количества пилотных проектов и инициатив, направленных на исследование и внедрение блокчейна в различных аспектах образования.

Заключение

В заключение, блокчейн предлагает революционные подходы к образованию, обещая трансформацию традиционных методов выдачи сертификатов, управления степенями и обмена знаниями. Эта технология не только упрощает верификацию академических достижений и повышает их надежность, но и обеспечивает улучшенную безопасность, прозрачность и доступность образовательных ресурсов. Цифровые сертификаты и степени на основе блокчейна могут сыграть ключевую роль в создании более инклюзивного и глобального образовательного пространства.

Тем не менее, успех внедрения блокчейна в образовательные системы во многом будет зависеть от преодоления технических, юридических и культурных препятствий. Важно будет сосредоточить усилия на разработке стандартов, обеспечении совместимости систем и повышении осведомленности и компетентности всех заинтересованных сторон. Кроме того, необходимо будет уделять особое внимание защите конфиденциальности и обеспечению безопасности данных.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.

2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004

Гибридные облачные архитектуры: оптимизация производительности и безопасности в мультиоблачных средах

Голубятников Артем Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В современном мире информационных технологий, гибридные облачные архитектуры становятся все более востребованными из-за их способности объединять локальные и облачные вычислительные ресурсы, обеспечивая высокую производительность, масштабируемость и гибкость. Эта статья рассматривает стратегии оптимизации производительности и безопасности для гибридных и мультиоблачных сред, обсуждая ключевые вызовы и предлагая эффективные решения. Анализируются различные аспекты гибридных облачных архитектур, включая интеграцию, управление данными, сетевые настройки и соответствие нормативным требованиям. Статья также рассматривает последние тенденции и инновации в области гибридных облачных технологий, включая искусственный интеллект и машинное обучение для анализа данных и управления безопасностью.*

***Abstract**: In today's world of information technology, hybrid cloud architectures are becoming increasingly sought after because of their ability to combine on-premises and cloud computing resources, providing high performance, scalability, and flexibility. This paper examines strategies for optimizing performance and security for hybrid and multi-cloud environments, discussing key challenges, and proposing effective solutions. Various aspects of hybrid cloud architectures are analyzed, including integration, data management, network settings, and compliance. The paper also reviews the latest trends and innovations in hybrid cloud technologies, including artificial intelligence and machine learning for data analysis and security management.*

***Ключевые слова**: гибридные облачные архитектуры, мультиоблачные среды, оптимизация производительности, облачная безопасность, интеграция облачных сервисов, управление данными в облаке, кибербезопасность, искусственный интеллект в облачных вычислениях, машинное обучение для безопасности данных, автоматизация облачных процессов.*

***Keywords**: hybrid cloud architectures, multi-cloud environments, performance optimization, cloud security, cloud service integration, cloud data management, cybersecurity, artificial intelligence in cloud computing, machine learning for data security, cloud process automation.*

Введение

Гибридные облачные архитектуры сочетают в себе локальные (on-premises), частные и публичные облачные ресурсы, предоставляя организациям гибкость, масштабируемость и оптимизированные затраты. Эти архитектуры позволяют компаниям персонализировать свои ИТ-решения в соответствии с конкретными бизнес-потребностями, обеспечивая при этом эффективное управление данными и приложениями.

Оптимизация производительности

Оптимизация производительности в гибридных облачных архитектурах требует интеграции различных вычислительных ресурсов для обеспечения высокой скорости обработки данных и минимизации задержек. Это включает в себя автоматизацию масштабирования ресурсов, балансировку нагрузки между облаками и оптимизацию сетевых подключений. Также важным аспектом является использование передовых технологий, таких

как контейнеризация и микросервисная архитектура, которые обеспечивают гибкость и легкость в управлении приложениями.

Безопасность в мультиоблачных средах

Безопасность в мультиоблачных средах — это сложная область, которая требует комплексного подхода из-за уникальных вызовов, связанных с использованием нескольких облачных сервисов и платформ. При работе с мультиоблачной средой, организации сталкиваются с необходимостью защиты данных и приложений, распределенных между различными облачными поставщиками. Вот некоторые ключевые аспекты, которые следует учитывать:

Шифрование данных: важно использовать шифрование данных во время их передачи (in-transit) и хранения (at-rest) для защиты от несанкционированного доступа. Это означает, что данные должны быть зашифрованы как при их передаче между облачными сервисами и пользователями, так и когда они хранятся в облаке.

Управление идентификацией и доступом: управление доступом к ресурсам и услугам в мультиоблачной среде должно быть строго контролируемым. Для этого применяются методы многофакторной аутентификации, минимальных привилегий и регулярного пересмотра прав доступа.

Сегментация сети и защита периметра: сегментация сети помогает изолировать ресурсы и данные, уменьшая риск распространения атак внутри сети. Важно также обеспечить защиту периметра сети с помощью межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS) и других средств кибербезопасности.

Регулярное тестирование безопасности: регулярное проведение тестов на проникновение и оценки уязвимостей необходимо для выявления и устранения потенциальных слабых мест в системе безопасности мультиоблачной среды.

Вызовы и решения

Гибридные облачные архитектуры сталкиваются с рядом вызовов, включая сложность управления мультиоблачными ресурсами, интегра-

цию разнородных систем и сохранение высокого уровня безопасности. Для решения этих проблем применяются различные методы, такие как использование унифицированных платформ управления облаком, автоматизация IT-процессов и внедрение централизованных систем мониторинга и управления безопасностью.

Будущее гибридных облачных архитектур

Гибридные облачные архитектуры продолжают развиваться, предлагая новые возможности для бизнеса благодаря инновациям в области искусственного интеллекта, машинного обучения и автоматизации данных. Ожидается, что в будущем гибридные облака станут еще более интегрированными, умными и безопасными, предоставляя компаниям еще большую гибкость и контроль над их ИТ-инфраструктурой.

Заключение

В заключении, подчеркивается важность адаптации к гибридным и мультиоблачным архитектурам для удовлетворения современных бизнес-требований. Основное внимание уделено стратегиям, обеспечивающим высокую производительность и безопасность данных в сложных облачных средах. В конечном счете, гибридные облачные архитектуры предлагают значительные преимущества, включая гибкость, масштабируемость и оптимизацию затрат, но при этом требуют тщательной реализации и управления для минимизации потенциальных рисков и обеспечения надежной работы систем.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.

2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004

Стратегии и вызовы современной информационной безопасности в эпоху цифровой трансформации

Голубятников Артем Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В статье рассматриваются ключевые стратегии и вызовы в области информационной безопасности, с которыми сталкиваются организации в условиях бурно развивающихся цифровых технологий. Основное внимание уделяется анализу новых угроз безопасности, возникающих в результате цифровой трансформации, а также изучению современных методов и технологий защиты информации. Авторы подробно рассматривают такие темы, как кибератаки нового поколения, проблемы обеспечения конфиденциальности и целостности данных, а также стратегии защиты критически важной инфраструктуры и личной информации пользователей. В работе освещаются передовые практики и решения в области информационной безопасности, включая использование искусственного интеллекта и машинного обучения для обнару-*

жения и предотвращения угроз, развитие криптографических технологий и применение систем управления идентификацией и доступом. Особое внимание уделено анализу правовых и нормативных аспектов информационной безопасности, а также вопросам управления рисками и соответствия стандартам.

***Abstract**: The article examines the key information security strategies and challenges organizations face in a rapidly evolving digital environment. The focus is on analyzing new security threats resulting from digital transformation, as well as studying modern information security methods and technologies. The authors delve into topics such as next-generation cyberattacks, data confidentiality and integrity issues, and strategies for protecting critical infrastructure and users' personal information. The work highlights best practices and solutions in information security, including the use of artificial intelligence and machine learning to detect and prevent threats, the development of cryptographic technologies, and the application of identity and access management systems. Special attention is given to analyzing the legal and regulatory aspects of information security, as well as risk management and compliance issues.*

***Ключевые слова**: информационная безопасность, кибератаки, защита данных, криптография, конфиденциальность данных, безопасность критически важной инфраструктуры, проактивная защита, мониторинг и обнаружение угроз.*

***Keywords**: information security, cyber attacks, data protection, cryptography, data confidentiality, critical infrastructure security, proactive protection, threat monitoring and detection.*

Введение

В настоящее время мир переживает эпоху цифровой трансформации, которая затрагивает все аспекты человеческой деятельности, от бизнеса и образования до здравоохранения и правительственного управления. Эта трансформация приводит к глубоким изменениям в способах обработки, хранения и передачи информации, а также в интеракциях между людьми и технологиями. В то время как цифровизация открывает перед человечеством новые возможности для роста и инноваций, она также порождает сложные вызовы в области информационной безопасности.

С ростом количества подключенных устройств, расширением сетевых инфраструктур и увеличением объемов цифровых данных организации всех размеров сталкиваются с постоянно меняющимся ландшафтом угроз, которые могут подвергать риску их операции, данные и репутацию. В этом контексте информационная безопасность превращается не просто в тех-

ническую задачу, но в ключевой элемент стратегического планирования и управления.

Современная информационная безопасность в эпоху цифровой трансформации охватывает ряд ключевых аспектов и вызовов, поскольку организации и индивидуумы внедряют новые технологии и цифровые платформы. Эта трансформация влечет за собой не только новые возможности для роста и инноваций, но и новые риски и угрозы безопасности. Вот несколько основных элементов современной информационной безопасности в этом контексте:

Стратегии информационной безопасности

Проактивный подход: Одна из ключевых стратегий заключается в переходе от реактивного к проактивному подходу в области безопасности, что включает предварительное обнаружение угроз и их нейтрализацию до того, как они нанесут ущерб.

Использование искусственного интеллекта и машинного обучения: Эти технологии позволяют анализировать большие объемы данных о безопасности для выявления потенциальных угроз и необычных паттернов поведения, что значительно ускоряет обнаружение и реагирование на инциденты.

Криптографические технологии: Шифрование данных продолжает оставаться одной из самых надежных методик защиты информации, особенно в условиях роста числа кибератак и утечек данных.

Образование и тренинги: Обучение сотрудников является критически важным элементом стратегии информационной безопасности, поскольку многие атаки происходят из-за человеческого фактора.

Вызовы информационной безопасности

Рост кибератак: С увеличением числа подключенных устройств и сложности информационных систем увеличивается и количество потенциальных уязвимостей, что приводит к росту числа кибератак различного типа.

Соблюдение нормативных требований: Законодательные требования к защите данных постоянно меняются и становятся более строгими, что требует от организаций постоянного мониторинга и обновления их политик и процедур безопасности.

Интеграция безопасности в цифровую трансформацию: Безопасность должна учитываться на всех этапах проектов цифровой трансформации, начиная с дизайна систем и заканчивая их эксплуатацией.

Управление идентификацией и доступом: По мере роста числа пользователей и сервисов управление идентификационными данными и доступами становится все более сложной задачей.

Обеспечение приватности данных: Защита личных данных и обеспечение их конфиденциальности остается одним из главных вызовов, особенно с учетом глобализации и распределенности информационных систем.

Заключение

В заключении, статья подчеркивает, что в условиях стремительной цифровизации современные организации сталкиваются с постоянно эволюционирующими угрозами информационной безопасности. Это требует от них не только разработки и реализации комплексных стратегий безопасности, но и непрерывной адаптации к новым вызовам. Цифровая трансформация представляет собой как возможности, так и вызовы для информационной безопасности. Однако, при правильном подходе и применении соответствующих стратегий, можно не только снизить потенциальные риски, но и усилить доверие и безопасность в цифровом пространстве. В конечном счете, укрепление информационной безопасности является совместной задачей, требующей участия всех заинтересованных сторон.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.

2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004

Автоматизация DevOps: улучшение производительности и безопасности в процессах непрерывной интеграции и доставки

Голубятников Артем Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье рассматривается влияние автоматизации DevOps на производительность и безопасность в рамках процессов непрерывной интеграции (CI) и непрерывной доставки (CD). Подробно анализируются, как интеграция автоматизированных инструментов и практик в жизненный цикл разработки программного обеспечения может способствовать ускорению выпуска продуктов, повышению их качества и обеспечению более высокого уровня безопасности. Особое внимание уделяется тому, как автоматизация DevOps способствует улучшению сотрудничества между разработчиками, тестировщиками и операционными командами, что ведет к более эффективному устранению ошибок, оптимизации рабочих процессов и минимизации человеческих ошибок. Статья также охватывает ключевые аспекты безопасности, связанные с автоматизацией DevOps, включая управление доступом, шифрование, мониторинг и автоматическое обнаружение угроз.*

***Abstract**: This research paper examines the impact of DevOps automation on performance and security within Continuous Integration (CI) and Continuous Delivery (CD) processes. It analyzes in detail how integrating automated tools and practices into the software development lifecycle can help accelerate product release, improve product quality, and ensure higher levels of security. Particular attention is paid to how DevOps automation fosters better collaboration between developers, testers, and operations teams, leading to better bug fixing, streamlined workflows, and minimized human error. The article also covers key security aspects associated with DevOps automation, including access control, encryption, monitoring, and automatic threat detection.*

***Ключевые слова**: DevOps, автоматизация, непрерывная интеграция (CI), непрерывная доставка (CD), безопасность программного обеспечения, мониторинг и логирование, шифрование, оптимизация рабочих процессов, кибербезопасность, автоматическое тестирование.*

***Keywords**: DevOps, automation, continuous integration (CI), continuous delivery (CD), software security, monitoring and logging, encryption, workflow optimization, cybersecurity, automated testing.*

Введение

В современной динамичной среде разработки программного обеспечения требования к скорости доставки продуктов и их качеству непрерывно возрастают. Эти вызовы привели к появлению и распространению практик DevOps, которые направлены на ускорение и оптимизацию процессов разработки, тестирования и внедрения программных решений. В основе DevOps лежит идея непрерывного цикла обратной связи между разработчиками и операционными командами, что обеспечивается через практики непрерывной интеграции (CI) и непрерывной доставки (CD). Однако для достижения высокой эффективности и обеспечения безопасности в этих процессах требуется автоматизация. Автоматизация DevOps становится ключевым элементом в достижении этих целей, позволяя сократить время разработки, уменьшить количество ошибок и улучшить безопасность продуктов. Она включает в себя автоматическое управление инфраструктурой, автоматизацию тестирования, автоматическое развертывание и мониторинг. Такой подход позволяет командам быстрее реагировать на изменения, повышать качество продукции и уменьшать время на рутинные процессы**,** сосредотачиваясь на инновациях и улучшении продукта.

Улучшение производительности

Автоматизация в контексте DevOps направлена на сокращение времени разработки и доставки программного обеспечения за счет устранения ручных и повторяющихся задач. Это достигается через внедрение инструментов и практик, которые позволяют автоматически собирать, тестировать и развертывать код в продакшн среду. Процессы непрерывной интеграции позволяют разработчикам часто и регулярно объединять изменения кода в основную ветку разработки, тем самым минимизируя конфликты между версиями и ускоряя циклы разработки.

Обеспечение безопасности

В контексте DevOps безопасность не отделяется от процесса разработки и внедряется на всех этапах жизненного цикла ПО. Автоматизация помогает внедрять безопасность на ранних этапах (подход «Security as Code»), обеспечивая автоматическое сканирование кода на наличие уязвимостей, проверку зависимостей и выполнение автоматизированных тестов на безопасность. Это позволяет идентифицировать и устранять угрозы безопасности до того, как продукт будет развернут.

Непрерывная интеграция и доставка

CI/CD являются центральными компонентами автоматизации DevOps. Непрерывная интеграция подразумевает автоматическое слияние всех изменений кода от разработчиков в единую ветку, проведение тестов и создание сборок. Непрерывная доставка расширяет этот процесс, автоматизируя развертывание приложений в тестовые и предпродакшн среды, что позволяет командам быстрее выпускать новые функции и исправления.

Преимущества и вызовы

Автоматизация DevOps приводит к увеличению скорости, стабильности и надежности процессов разработки и доставки программного обес-

печения, повышая при этом общую безопасность продуктов. Однако она также представляет определенные вызовы, включая необходимость культурных изменений в организации, обучение персонала новым инструментам и методологиям, а также интеграцию и поддержку многочисленных инструментов и платформ.

Заключение

Подводя итог, можно сказать, что успешная автоматизация DevOps требует культурных изменений внутри организации, включая поддержку от руководства, готовность команд к изменениям и постоянное обучение. При правильном подходе и использовании подходящих инструментов автоматизация DevOps обеспечивает значительные преимущества для организаций любого размера, включая повышение производительности, улучшение качества продуктов и укрепление безопасности. В завершение, автоматизация DevOps представляет собой ключевую стратегию для достижения высокой скорости, эффективности и безопасности в разработке и доставке программного обеспечения. Как показывает практика, компании, внедряющие автоматизированные DevOps-процессы, могут не только значительно сократить время вывода продукта на рынок, но и обеспечить более высокий уровень удовлетворенности клиентов и повысить общую безопасность своих IT-систем.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.

4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004

Программное обеспечение будущего: тенденции и перспективы развития

Голубятников Артем Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В статье проводится анализ современных тенденций в области разработки программного обеспечения и их влияния на будущие направления развития. Особое внимание уделяется новым подходам к разработке, таким как DevOps, микросервисная архитектура, контейнеризация и использование облачных технологий. Статья также рассматривает перспективы развития и новые возможности, которые предоставляют современные технологии, такие как искусственный интеллект, машинное обучение, квантовые вычисления и блокчейн. Проанализированы потенциальные преимущества и вызовы, связанные с внедрением этих технологий в сферу разработки программного обеспечения.*

***Abstract**: The article analyzes current trends in software development and their impact on future development directions. Special attention is paid to new development approaches such as DevOps, microservice architecture, containerization, and the use of cloud technologies. The article also examines the development prospects and new opportunities offered by modern technologies such as artificial intelligence, machine learning, quantum computing and blockchain. The potential benefits and challenges associated with the introduction of these technologies into the field of software development are analyzed.*

***Ключевые слова**: программное обеспечение, перспективы развития, разработка ПО, технологии, инновации, DevOps, микросервисная архитектура, облачные технологии, искусственный интеллект, машинное обучение, квантовые вычисления, блокчейн.*

***Keywords**: software, development prospects, software development, technology, innovation, DevOps, microservice architecture, cloud technologies, artificial intelligence, machine learning, quantum computing, blockchain.*

Введение

Современный мир переживает быстрый технологический прогресс, который влияет на все сферы жизни, включая разработку программного обеспечения. В наше время программное обеспечение играет ключевую роль во многих аспектах нашей повседневной жизни, от мобильных приложений до критически важных систем для бизнеса и государственных учреждений. Однако, как вся технология, программное обеспечение также находится в процессе непрерывного изменения и развития. Цель данной научной статьи состоит в том, чтобы проанализировать современные тенденции в области разработки программного обеспечения и выявить перспективы его будущего развития. В контексте быстро меняющейся технологической среды и постоянно растущих потребностей пользователей, важно понимать, какие новые технологии и подходы могут повлиять на будущее программного обеспечения.

Концепция программного обеспечения будущего

Одной из ключевых особенностей программного обеспечения будущего является его гибкость и адаптивность. Программные продукты должны быть способными быстро реагировать на изменяющиеся потребности пользователей и технологические тренды, что требует разработки модульных, масштабируемых и легко модифицируемых решений. Еще одной важной составляющей программного обеспечения будущего является его интеграция с новыми технологиями, такими как искусственный интеллект, машинное обучение, интернет вещей, блокчейн и квантовые вычисления. Эти технологии предоставляют новые возможности для со-

здания более интеллектуальных, эффективных и безопасных программных решений. Важным аспектом программного обеспечения будущего является также его экологическая устойчивость и энергоэффективность. С развитием облачных вычислений и распределенных систем становится все важнее учитывать потребление ресурсов и влияние программного обеспечения на окружающую среду.

В данном контексте следует рассмотреть несколько ключевых тенденций и перспектив, определяющих будущее программного обеспечения:

Искусственный интеллект и машинное обучение: Продвижение искусственного интеллекта и машинного обучения открывает новые горизонты для программного обеспечения. Эти технологии позволяют создавать более интеллектуальные и адаптивные системы, способные анализировать данные, принимать решения и обучаться на основе опыта.

DevOps и непрерывная поставка: Методологии DevOps и непрерывной поставки (CI/CD) становятся стандартом в современной разработке программного обеспечения. Они способствуют ускорению процесса разработки, автоматизации тестирования и доставки программного обеспечения в продакшн, что улучшает его качество и реакцию на изменения.

Микросервисная архитектура и контейнеризация: Микросервисная архитектура и контейнеризация позволяют создавать более гибкие, масштабируемые и надежные приложения. Они разбивают приложение на небольшие независимые компоненты, которые могут развиваться, масштабироваться и обновляться независимо друг от друга.

Блокчейн: Технология блокчейн представляет собой новый подход к обработке и хранению данных, который обеспечивает прозрачность, надежность и безопасность. Она может быть применена в различных областях, включая финансы, здравоохранение, логистику и управление поставками.

Эти тенденции и перспективы являются лишь некоторыми из множества факторов, которые будут влиять на развитие программного обеспечения в будущем. Понимание этих факторов поможет разработчикам и предпринимателям адаптироваться к изменяющейся среде и создавать инновационные решения, отвечающие требованиям рынка.

Заключение

В заключение, рассмотренная в научной статье «Программное обеспечение будущего: тенденции и перспективы развития» тема является крайне актуальной и значимой в контексте быстрого технологического развития и постоянно меняющихся потребностей пользователей. Однако, помимо новых возможностей, программное обеспечение будущего также сталкивается с вызовами, такими как обеспечение безопасности и защиты данных, экологическая устойчивость и управление ресурсами. Решение этих проблем потребует совместных усилий со стороны разработчиков, предпринимателей, государства и общества в целом.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

УДК 004

Смарт технологии: путь к цифровому будущему

Голубятников Артем Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной статье исследуется влияние смарт технологий на цифровое будущее. Рассматриваются различные аспекты смарт технологий, их применение в различных сферах жизни и бизнеса, а также их влияние на общество в целом. Основной акцент делается на том, как смарт технологии изменяют нашу жизнь, работу, коммуникации и взаимодействие с окружающей средой. Рассматриваются новейшие разработки в области смарт устройств, сетей, городов и домов, а также анализируются перспективы развития этого направления в будущем. В итоге статья приходит к выводу о том, что смарт технологии играют ключевую роль в формировании цифрового будущего и представляют собой важный инструмент для достижения устойчивого и инновационного развития общества.*

***Abstract**: This paper explores the impact of smart technologies on the digital future. Different aspects of smart technologies, their application in different spheres of life and business, and their impact on society as a whole are examined. The focus is on how smart technologies are changing the way people live, work, communicate and interact with their environment. The latest developments in the field of smart devices, networks, cities, and homes are considered, and the prospects for the development of this area in the future are analyzed. In the end, the article concludes that smart technologies play a key role in shaping the digital future and represent an important tool for achieving sustainable and innovative development of society.*

***Ключевые слова**: смарт технологии, цифровое будущее, инновации, технологический прогресс, смарт устройства, автоматизация, умные системы, цифровая трансформация, устойчивое развитие, коммуникации, безопасность данных, интеграция.*

***Keywords**: smart technologies, digital future, innovation, technological progress, smart devices, automation, smart systems, digital transformation, sustainable development, communications, data security, integration.*

Введение

Современный мир переживает быстрый технологический прогресс, который перепрофилирует нашу повседневную жизнь и приводит к по-

явлению новых возможностей и вызовов. Одним из наиболее значимых направлений этого прогресса являются смарт технологии, которые играют ключевую роль в формировании цифрового будущего. Научная статья «Смарт Технологии: Путь к Цифровому Будущему» предназначена для исследования и анализа влияния смарт технологий на различные сферы жизни, бизнеса и общества в целом. В настоящее время смарт технологии проникают в различные аспекты нашей жизни, начиная от умных устройств в доме и заканчивая смарт городами и мобильными приложениями.

Концепт смарт технологий

«Смарт Технологии: Путь к Цифровому Будущему» — это концепция, включающая в себя широкий спектр инновационных технологий, направленных на повышение уровня комфорта, эффективности и безопасности в различных сферах жизни. Смарт технологии представляют собой комплексное сочетание аппаратных и программных решений, которые используются для сбора, обработки и анализа данных с целью управления различными аспектами нашей повседневной жизни.

Роль смарт технологий в формировании цифрового будущего невозможно переоценить. Они играют ключевую роль в создании интеллектуальных и умных систем, которые изменяют наш образ жизни, работу, образование, здравоохранение и городскую инфраструктуру. Вот несколько аспектов, которые демонстрируют их значимость:

Улучшение комфорта и качества жизни: Смарт технологии позволяют нам контролировать и автоматизировать различные аспекты нашей жизни, начиная от умного дома с автоматическим регулированием температуры и освещения до умных городов с интеллектуальными системами управления транспортом и общественной безопасностью.

Эффективность и продуктивность: В бизнесе смарт технологии помогают оптимизировать процессы производства, логистики, маркетинга и управления ресурсами, что приводит к повышению эффективности и конкурентоспособности предприятий.

Инновации в здравоохранении: Смарт медицинские устройства и системы позволяют мониторить здоровье пациентов в реальном времени, пред-

упреждать о возможных проблемах и обеспечивать своевременное медицинское вмешательство.

Создание экологически устойчивых решений: Смарт технологии способствуют улучшению управления энергопотреблением, снижению выбросов и эффективному использованию ресурсов, что важно для достижения устойчивого развития.

Улучшение образования: В образовательной сфере смарт технологии предоставляют новые возможности для персонализации обучения, доступа к знаниям и сотрудничества, что способствует повышению уровня образования и развитию навыков будущего.

Развитие городской инфраструктуры: Смарт технологии помогают городам стать более умными, эффективными и устойчивыми, предоставляя новые возможности для управления транспортом, энергоснабжением, водоснабжением и общественными услугами.

Таким образом, смарт технологии играют критическую роль в формировании цифрового будущего, создавая инновационные решения, которые способствуют улучшению качества жизни, повышению эффективности и устойчивости общества, а также созданию новых возможностей для развития.

Заключение

В заключение, смарт технологии представляют собой мощный инструмент, который способен изменить наш мир к лучшему. Они не только повышают уровень комфорта и эффективности, но и помогают нам решать сложные проблемы, такие как изменение климата, устойчивое развитие и социальная справедливость. Однако, несмотря на все преимущества, смарт технологии также сталкиваются с рядом вызовов, включая проблемы приватности данных, кибербезопасности, и социального неравенства. Поэтому важно продолжать исследования и разработки в этой области с целью создания более безопасных, устойчивых и инклюзивных технологий. Надежда на цифровое будущее, опирающееся на смарт технологии, заключается в их способности преобразовывать наш мир к лучшему, обеспечивая умные, эффективные и устойчивые решения для разнообразных вызовов, с которыми мы сталкиваемся.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.
3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

ДЛЯ ЗАМЕТОК

Журнал «Научный аспект №3 2024»
Эл. почта редакции: public@na-journal.ru
Подробнее на сайте: https://na-journal.ru