КИБЕРБЕЗОПАСНОСТЬ / CYBERSECURITY

DOI: https://doi.org/10.60797/COMP.2024.3.1

ИННОВАЦИОННЫЕ ПОДХОДЫ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ СРЕДСТВ БЕЗОПАСНОСТИ ПРОТИВ КИБЕРУГРОЗ

Научная статья

Лисица Н.В.[1, *]
[1] ORCID : 0009-0005-6814-4697;
[1] Университет ИТМО, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (super-nikita-lisi[at]yandex.ru)

Аннотация

В данной статье рассматриваются новаторские подходы к оценке эффективности средств безопасности в условиях современных киберугроз. Традиционные методы оценки часто не справляются из-за их неспособности адаптироваться к новым угрозам. В статье обсуждаются ограничения традиционных методов и представляются инновационные подходы, использующие искусственный интеллект, машинное обучение и квантовые технологии для улучшения предсказательных возможностей и надежности безопасности. С помощью реальных примеров демонстрируется эффективность этих методов, а также предлагаются рекомендации по интеграции этих нововведений в существующие системы. Статья нацелена на предоставление всестороннего обзора современных инноваций в оценке кибербезопасности и взгляд в будущее этой критически важной области.

Ключевые слова: кибербезопасность, искусственный интеллект в безопасности, квантовая криптография, машинное обучение, оценка эффективности безопасности, киберугрозы, автоматизация безопасности, предсказательные меры безопасности, инновации в кибербезопасности, стратегии киберзащиты.

INNOVATIVE APPROACHES TO EVALUATING THE EFFECTIVENESS OF SECURITY TOOLS AGAINST CYBER THREATS

Research article

Lisitsa N.V.[1, *]
[1] ORCID : 0009-0005-6814-4697;
[1] Saint Petersburg State University Of Information Technologies, Mechanics And Optics, Saint-Petersburg, Russian Federation

* Corresponding author (super-nikita-lisi[at]yandex.ru)

Abstract

This article examines innovative approaches to assessing the effectiveness of security tools in the face of today's cyber threats. Traditional evaluation methods often fail due to their inability to adapt to new threats. The work discusses the limitations of traditional methods and presents innovative approaches that utilize artificial intelligence, machine learning and quantum technologies to improve predictive capabilities and security robustness. Using real-world examples, the effectiveness of these techniques is demonstrated and recommendations are offered for integrating these innovations into existing systems. The paper aims to provide a comprehensive overview of current innovations in cybersecurity assessment and a glimpse into the future of this critical field.

Keywords: cybersecurity, artificial intelligence in security, quantum cryptography, machine learning, security performance evaluation, cyber threats, security automation, predictive security measures, cybersecurity innovation, cyber defence strategies.

Введение

В современном мире, где зависимость от цифровых технологий неуклонно растет, актуальность и важность кибербезопасности продолжают усиливаться [1]. Каждый день организации всех масштабов сталкиваются с разнообразными киберугрозами, которые могут подорвать не только финансовую стабильность, но и репутацию. В этом контексте крайне важно не только использовать средства защиты, но и регулярно оценивать их эффективность. Традиционные методы оценки, однако, зачастую не справляются с задачей адекватного реагирования на новые и адаптирующиеся угрозы [2]. Это порождает необходимость в поиске и внедрении инновационных подходов, которые могли бы обеспечить более высокий уровень защиты. Инновационные подходы, о которых пойдет речь в данной статье, включают использование искусственного интеллекта и машинного обучения для анализа и предсказания угроз, развитие квантовой криптографии для защиты данных, а также применение автоматизированных инструментов для проведения стресс-тестов систем безопасности [1]. Эти методы предлагают обновленный взгляд на проблемы кибербезопасности и открывают новые горизонты для защиты информационных активов в эпоху цифровизации.

Проблемы существующих методов оценки

Одной из ключевых проблем в сфере кибербезопасности является несоответствие традиционных методов оценки современным требованиям и условиям. Основные ограничения этих подходов заключаются в следующем:

– Неучет новых видов угроз.

Современный цифровой мир характеризуется постоянным появлением новых типов киберугроз, которые быстро эволюционируют. Традиционные методы оценки, как правило, базируются на исторических данных и известных сценариях атак, что снижает их эффективность в условиях новых и адаптирующихся угроз. Многие из этих методов не

могут предсказывать или распознавать угрозы до момента их активации, что оставляет системы без защиты перед лицом новых и неизвестных атак [3].

– Примеры неэффективности традиционных методов.

Примером неэффективности традиционных методов может служить использование антивирусного программного обеспечения, которое опирается на сигнатуры известных вирусов для их обнаружения. Этот метод оказывается бессильным перед zero-day атаками, которые используют ранее неизвестные уязвимости. Еще одним примером является фокус на периметральную защиту, которая уязвима в случае атак с использованием украденных учетных данных, поскольку после проникновения, атакующего внутрь системы этот тип защиты становится практически бесполезным [3] Традиционные методы оценки кибербезопасности требуют пересмотра и адаптации к текущему динамично меняющемуся цифровому ландшафту, чтобы адекватно отвечать на современные угрозы и защищать информационные системы от вредоносных атак.

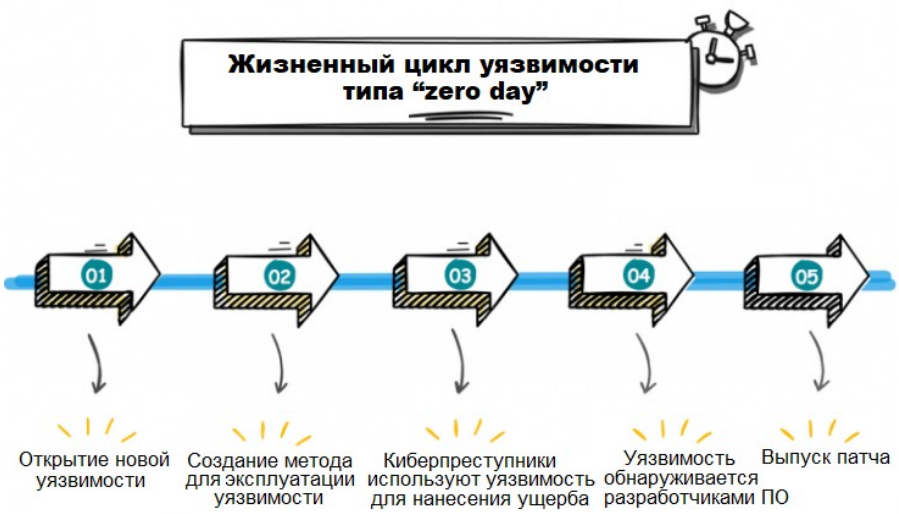

Рисунок 1 - Жизненный цикл уязвимости типа "zero day"
DOI: https://doi.org/10.60797/COMP.2024.3.1.1

На картинке представлен жизненный цикл уязвимости типа "zero day". Жизненный цикл состоит из пяти этапов:

1. Открытие новой уязвимости. На данном этапе обнаруживается новая уязвимость, о которой до этого не было известно.

2. Создание метода для эксплуатации уязвимости. Здесь разрабатывается способ, с помощью которого возможно использовать найденную уязвимость для атаки.

3. Киберпреступники используют уязвимость для нанесения ущерба. На этом этапе злоумышленники начинают активно использовать уязвимость, чтобы причинить вред.

4. Уязвимость обнаруживается разработчиками ПО. Разработчики программного обеспечения замечают уязвимость.

5. Выпуск патча (исправления) разработчиками ПО. Наконец, разработчики выпускают обновление, которое устраняет уязвимость.

– Инновационные подходы к оценке.

С учетом ограничений традиционных подходов к оценке эффективности средств кибербезопасности, на передний план выходят инновационные методы. Они позволяют не только реагировать на существующие угрозы, но и прогнозировать новые, а также повышать уровень защищенности систем. Ниже рассмотрены ключевые инновационные подходы.

– Использование искусственного интеллекта и машинного обучения для предсказания угроз.

Искусственный интеллект (ИИ) и машинное обучение (МО) открывают новые возможности для анализа и обработки больших объемов данных, что позволяет выявлять закономерности и предсказывать потенциальные атаки до их осуществления. ИИ может анализировать трафик в режиме реального времени, выявляя аномалии, которые могут свидетельствовать о подготовке кибератак. Модели МО могут обучаться на данных о прошлых инцидентах и на их основе прогнозировать будущие угрозы, позволяя предпринимать проактивные шаги по укреплению безопасности.

– Применение квантовых технологий для усиления криптографических методов.

Квантовые технологии вносят революцию в область криптографии. Они обещают значительное увеличение скорости вычислений и уровня безопасности благодаря разработке новых типов криптографических алгоритмов, устойчивых к квантовому дешифрованию. Это включает в себя разработку квантово-устойчивых алгоритмов шифрования, которые не могут быть взломаны даже с помощью квантового компьютера [3].

– Автоматизация тестирования безопасности с помощью программного обеспечения для имитации атак.

Автоматизированные инструменты тестирования безопасности, такие как фреймворки для проведения имитационных атак, позволяют на регулярной основе проводить комплексные проверки системы на предмет

уязвимостей [2]. Это включает в себя использование программного обеспечения для автоматизированного тестирования проникновения, которое имитирует атаки злоумышленников для выявления и устранения слабых мест в защите. Эти подходы отражают тенденцию к усилению предсказательных способностей в кибербезопасности и к сокращению времени реакции на угрозы, что делает процесс оценки более динамичным и адаптируемым к меняющейся киберобстановке.

Рисунок 2 - Квантовая криптография
DOI: https://doi.org/10.60797/COMP.2024.3.1.2

На изображении представлена схема объяснения квантовой криптографии. Мы видим двух участников, которые хотят безопасно обменяться ключом с помощью квантовой криптографии. Источник фотонов генерирует фотоны, которые затем проходят через поляризаторы, выбираемые одним участником (диагональные и горизонтальные-вертикальные). Эти поляризованные фотоны передаются другому. У него есть фотонные детекторы и два типа поляризационных преобразователей (диагональные и горизонтальные-вертикальные), которые используются для определения состояния поляризации фотонов, посланных Алисой. После прохождения через эти устройства, Боб измеряет фотоны, получая биты информации. Внизу изображения показана последовательность битов и результаты измерений. После процесса отбора, в ходе которого исключаются биты, где поляризация была выбрана несоответствующим образом, получается «просеянный ключ» (sifted key), который совпадает у них. Этот ключ затем может быть использован для безопасного шифрования сообщений. Этот процесс является частью протокола квантового распределения ключей, который считается крайне безопасным, потому что любая попытка перехватить ключ изменит состояние фотонов и будет обнаружена как нарушение [3].

Примеры применения ИИ и МО в кибербезопасности

Искусственный интеллект (ИИ) и машинное обучение (МО) активно внедряются в сферу кибербезопасности, предлагая новые возможности для улучшения защиты информационных систем. Эти технологии помогают не только в обнаружении и предотвращении угроз, но и в адаптации защитных мер к постоянно меняющемуся ландшафту киберугроз.

3.1. Конкретные примеры использования ИИ и МО

1. Прогнозирование кибератак.

Системы, основанные на ИИ, анализируют огромные объемы данных о сетевом трафике, чтобы выявлять необычные или подозрительные паттерны, указывающие на возможные атаки. Например, ИИ-алгоритмы могут предсказывать атаки типа «отказ в обслуживании» (DDoS), анализируя аномалии в запросах к серверам.

2. Автоматическое обнаружение вредоносного ПО

Модели МО обучаются на характеристиках уже известных вирусов и вредоносных программ, что позволяет им эффективно распознавать новые варианты вредоносного ПО до того, как они нанесут ущерб. Эти системы способны обновлять свои базы данных в реальном времени, предоставляя защиту от самых свежих угроз.

3. Адаптивная сетевая безопасность.

ИИ-системы адаптируют настройки сетевой безопасности в реальном времени, реагируя на текущую ситуацию в сети. Например, они могут автоматически изменять правила брандмауэра в зависимости от уровня угрозы или поведения пользователей.

3.2. Анализ случаев из практики

1. Кейс с финансовой организацией.

Одна из крупнейших банковских систем внедрила ИИ для анализа поведения своих клиентов и обнаружения подозрительных транзакций, что значительно уменьшило количество успешных мошенничеств. ИИ помог идентифицировать нестандартные трансферты средств, которые были бы пропущены традиционными методами.

2. Кейс с крупным ритейлером.

Ритейлер использовал систему на основе МО для мониторинга своих внутренних сетей на предмет нарушений безопасности, что позволило своевременно обнаружить и предотвратить утечку данных.

3.3. Этические и правовые вопросы

1. Автоматизация и ответственность.

Один из ключевых вопросов заключается в том, кто несет ответственность за действия и решения, принятые автоматизированными системами. Важно определить, какие меры ответственности должны применяться к производителям и пользователям ИИ-систем.

2. Приватность данных.

Использование ИИ в кибербезопасности требует обработки больших объемов личных и конфиденциальных данных. Необходимо строго соблюдать нормы защиты данных и учитывать потенциальные риски для конфиденциальности.

3. Надежность и непредвиденные последствия.

Важно рассмотреть вопросы надежности ИИ-систем и возможность непредвиденных действий, особенно в критических приложениях, где ошибки могут привести к серьезным последствиям.

3.4. Промежуточные выводы

Использование ИИ и МО в кибербезопасности открывает новые возможности для защиты информационных систем. Однако это также требует тщательного рассмотрения этических и правовых аспектов, а также разработки надежных и ответственных подходов к внедрению этих технологий.

Будущее кибербезопасности — технологические прогнозы:

В мире, где киберугрозы становятся всё более сложными и изощренными, технологии в области кибербезопасности постоянно развиваются, чтобы предоставлять эффективные средства защиты. Особое внимание в этом процессе уделяется искусственному интеллекту и квантовым технологиям, которые обещают могут значительно изменить стратегии киберзащиты.

3.5. Развитие искусственного интеллекта и квантовых технологий

В области кибербезопасности искусственный интеллект с каждым годом становится всё более продвинутым, предлагая более мощные инструменты для анализа и реагирования на угрозы в реальном времени. Ожидается, что ИИ сможет не только обнаруживать известные типы атак, но и прогнозировать возможные направления атак, анализируя текущие тенденции и поведение в сети.

Квантовые вычисления обещают революционизировать криптографию, предлагая квантово-устойчивое шифрование, которое не может быть взломано с помощью традиционных или даже квантовых компьютеров. Это направление будет особенно важно для защиты данных на государственном уровне и в критически важных инфраструктурах.

3.6. Воздействие новых технологий на стратегии киберзащиты

1. Проактивная защита.

С развитием ИИ системы безопасности становятся способными не только реагировать на угрозы, но и активно предотвращать их, анализируя потенциальные риски и автоматически адаптируя защитные механизмы.

2. Адаптивные сетевые защиты.

Квантовые технологии и ИИ могут содействовать созданию сетей, которые самостоятельно адаптируются к меняющимся условиям безопасности, автоматически настраивая уровни доступа и защиты данных в зависимости от обнаруженных угроз.

3.7. Прогнозы относительно новых угроз и методов их нейтрализации

1. Квантовый взлом.

Появление квантовых компьютеров представляет собой потенциальную угрозу для традиционных методов шифрования. Развитие квантово-устойчивых криптографических технологий будет ключевым для нейтрализации этой угрозы.

2. Угрозы, связанные с ИИ.

С развитием ИИ появляются новые типы кибератак, такие как использование ИИ для создания и распространения сложных фишинговых атак или автоматизированного создания вредоносного ПО. Разработка контрмер, основанных на ИИ, будет важным шагом в борьбе с этими угрозами.

Будущее кибербезопасности обещает быть увлекательным, поскольку технологии, основанные на искусственном интеллекте и квантовых вычислениях, предлагают новые возможности для защиты в мире, где угрозы становятся всё более сложными. Это требует не только технологических инноваций, но и стратегического планирования на международном уровне для обеспечения глобальной кибербезопасности.

Технологии блокчейн и биометрия представляют собой два важных направления в современной кибербезопасности, каждое из которых предлагает уникальные методы для усиления защиты данных и систем. Вот более подробный обзор последних разработок в этих областях:

3.8. Блокчейн-технологии

1. Распределенная защита данных: блокчейн предоставляет распределенную и децентрализованную сеть, где данные хранятся в зашифрованной форме на множестве узлов, что делает их устойчивыми к традиционным атакам, направленным на централизованные базы данных.

2. Улучшение управления доступом: с использованием смарт-контрактов, которые автоматически выполняются при выполнении заданных условий, можно регулировать доступ к данным более надежным и прозрачным способом.

3. Аутентификация и аудит: блокчейн позволяет проводить аудит процессов без возможности их подделки или изменения, что критически важно для соблюдения нормативных и юридических требований.

4. Инновации в квантово-устойчивом шифровании: развитие квантовых вычислений ставит под угрозу традиционные методы шифрования, но блокчейн-технологии активно исследуют использование квантово-устойчивых алгоритмов для обеспечения долгосрочной защиты данных.

3.9. Биометрическая аутентификация

1. Многофакторная аутентификация: сочетание биометрических данных (отпечатки пальцев, распознавание лица, сканирование сетчатки) с другими методами аутентификации значительно усиливает безопасность, снижая риск несанкционированного доступа.

2. Адаптивная биометрия: разработки в области искусственного интеллекта позволяют биометрическим системам адаптироваться к изменениям во внешности или биометрических данных пользователя, тем самым поддерживая высокий уровень защиты даже при долгосрочном использовании.

3. Биометрические данные как ключи шифрования: использование уникальных биометрических данных для генерации ключей шифрования обеспечивает то, что только конкретный пользователь может расшифровать или получить доступ к своим данным.

4. Устойчивость к спуфингу: разработка новых технологий, способных распознавать попытки подделки биометрических данных (например, использование масок или фальсифицированных отпечатков пальцев), увеличивает надежность биометрических систем.

3.10. Совместное применение блокчейн и биометрии

Интеграция блокчейн и биометрии может привести к созданию новых систем идентификации и аутентификации, где биометрические данные хранятся в блокчейне, обеспечивая высокий уровень безопасности и приватности. Такие системы могут найти применение в голосовании, электронной коммерции, управлении доступом в критически важные инфраструктуры и многих других областях.

Эти разработки значительно расширяют возможности защиты от киберугроз, предоставляя дополнительные уровни безопасности и надежности, которые крайне важны в современном мире угроз и постоянно развивающихся технологиях.

Облачная безопасность стоит в авангарде кибербезопасности, поскольку всё больше компаний и организаций переходят к использованию облачных технологий для хранения данных и размещения приложений. Распределённые и мультиоблачные среды представляют собой особенно сложные системы, где данные и приложения размещены в нескольких облачных сервисах, что требует новых подходов к защите данных.

3.11. Основные вызовы облачной безопасности

– Управление доступом: в мультиоблачных средах управление идентификацией и доступом становится более сложным, так как необходимо обеспечить согласованность политик безопасности между разными облачными платформами.

– Сегментация данных: эффективная сегментация данных критически важна для предотвращения несанкционированного доступа и минимизации ущерба в случае успешной кибератаки.

– Шифрование: непрерывное шифрование данных в покое и в движении необходимо для защиты конфиденциальной информации, особенно когда данные перемещаются между разными облачными сервисами.

– Наблюдение и мониторинг: продвинутые инструменты мониторинга и управления событиями безопасности (SIEM) жизненно важны для обнаружения и реагирования на угрозы в реальном времени.

– Соблюдение нормативных требований: компании должны соответствовать многочисленным стандартам и законодательным требованиям, таким как GDPR, HIPAA и другим, что становится сложнее в мультиоблачных средах.

3.12. Современные подходы и технологии

Zero Trust модель: модель «Нулевого доверия» подразумевает, что никакому устройству или пользователю не доверяется по умолчанию, даже если они уже находятся в сети. Этот подход требует строгой проверки всех запросов на доступ к ресурсам, независимо от их источника.

CASB (Cloud Access Security Broker): брокеры безопасности доступа к облачным сервисам предоставляют централизованное управление безопасностью и политиками для мультиоблачных сред, что позволяет компаниям видеть и контролировать свои данные независимо от того, где они находятся.

Интеграция ИИ и машинного обучения: использование искусственного интеллекта для автоматического обнаружения аномалий и потенциальных угроз в облачных средах, что позволяет оперативно реагировать на инциденты безопасности.

Расширенное шифрование: разработка новых методов криптографической защиты, включая управляемое шифрование ключей и гомоморфное шифрование, которое позволяет работать с зашифрованными данными без необходимости их дешифровки.

Автоматизация управления безопасностью: автоматизированные решения для управления безопасностью и соблюдения требований помогают уменьшить человеческий фактор и обеспечить соблюдение политик безопасности на всех уровнях.

Облачные технологии продолжают развиваться, и с этим развитием появляются новые вызовы и возможности в области кибербезопасности. Интеграция продвинутых технологий и стратегий, таких как Zero Trust, CASB, расширенное шифрование, и автоматизация, является ключевым элементом для защиты данных в мультиоблачных и распределенных средах, обеспечивая компаниям необходимую гибкость и безопасность для эффективного ведения бизнеса в современном цифровом мире.

3.13. Научные идеи и предложения для усиления облачной безопасности

– Разработка новой модели управления идентификацией в мультиоблачных средах:

Идея: создание унифицированной и адаптивной системы идентификации, которая может динамически менять уровни доступа на основе анализа контекста пользователя и текущих угроз в реальном времени.

Обоснование: в средах, где ресурсы распределены между несколькими облачными платформами, стандартные подходы к IAM (Identity and Access Management) могут быть неэффективны. Адаптивная система идентификации позволит более гибко реагировать на изменения в среде безопасности и обеспечить более строгий контроль доступа.

– Разработка кросс-платформенного протокола шифрования для облачных сервисов:

Идея: создание стандартизированного, открытого протокола шифрования, который обеспечивает безопасную передачу данных между различными облачными платформами и приложениями.

Обоснование: на данный момент каждый облачный провайдер использует свой собственный механизм шифрования, что может приводить к проблемам совместимости и уязвимостям при передаче данных между системами. Единый протокол упростит интеграцию и повысит общий уровень безопасности.

– Использование распределенного реестра для аудита и мониторинга в мультиоблачных средах:

Идея: применение технологии блокчейн для создания непрерывного и неизменяемого реестра всех операций с данными в облачной среде.

Обоснование: такой подход обеспечит прозрачность и возможность верификации всех операций с данными, что критически важно для отслеживания и предотвращения несанкционированного доступа и утечек данных.

– Модель предсказательной безопасности на основе машинного обучения:

Идея: разработка алгоритмов машинного обучения, которые способны анализировать поведение системы и пользователей для предсказания и предотвращения потенциальных атак до их реализации.

Обоснование: большинство существующих систем безопасности реагирует на угрозы постфактум. Модель, способная предсказывать атаки на основе анализа аномального поведения, позволит перейти от реактивных к проактивным методам защиты.

– Гибридные модели безопасности для интеграции облачных и локальных ресурсов:

Идея: создание модели безопасности, которая эффективно интегрирует облачные и локальные ресурсы, обеспечивая единый уровень защиты данных и приложений независимо от их расположения.

Обоснование: с многообразием облачных и локальных ресурсов организации нуждаются в гибкой и масштабируемой модели безопасности, которая могла бы обеспечивать непрерывную защиту в изменяющемся ИТ-ландшафте.

Заключение

В заключении данной статьи подводим итоги о неоценимом вкладе инноваций в область оценки эффективности кибербезопасности. Инновационные подходы, такие как применение искусственного интеллекта и машинного обучения для предсказания угроз, использование квантовой криптографии и автоматизация тестирования безопасности, уже сегодня заметно изменяют ландшафт кибербезопасности. Они не только повышают эффективность защиты информационных систем, но и способствуют опережающему обнаружению и предотвращению угроз. Взгляд в будущее кибербезопасности обещает быть увлекательным. Ожидается, что инновации будут продолжать развиваться, включая появление еще более продвинутых алгоритмов искусственного интеллекта, расширение возможностей квантовых вычислений и криптографии, а также усиление интеграции автоматизированных систем защиты в повседневную практику кибербезопасности. Вероятно, мы увидим новые решения для защиты от угроз, основанные на блокчейне, развитие биометрических систем аутентификации и появление адаптивных сетевых защит, способных самостоятельно масштабироваться и реагировать на угрозы в реальном времени. Вместе с технологическим прогрессом растет и необходимость в развитии международного сотрудничества и стандартов в области кибербезопасности. Это потребует совместных усилий правительств, частного сектора и научного сообщества для создания устойчивых и безопасных киберпространств, способных противостоять будущим угрозам. В конечном итоге инновации в оценке кибербезопасности будут играть ключевую роль в обеспечении надежной защиты в эпоху глобальной цифровизации.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Cem Dilmegani. Quantum Cryptography / Cem Dilmegani // Encryption in 2024: In-Depth Guide. — URL: https://research.aimultiple.com/quantum-cryptography/ (accessed: 01.04.2024)

2. Zero day exploit definition. — URL: https://www.balbix.com/insights/what-is-a-zero-day-exploit/ (accessed: 01.04.2024)

3. Mary Pratt. What is zero trust? A model for more effective security / Mary Pratt. — URL: https://www.csoonline.com/article/564201/what-is-zero-trust-a-model-for-more-effective-security.html (accessed: 01.04.2024)

4. Yuchong Li. A comprehensive review study of cyber-attacks and cyber security. Emerging trends and recent developments / Yuchong Li, Qinghui Liu // Energy Reports. — 2021. — Volume 7. — P. 8176-8186. — DOI: 10.1016/j.egyr.2021.08.126

5. Prümmer J. A systematic review of current cybersecurity training methods / Julia Prümmer, Tommy van Steen, Bibi van den Berg // Computers & Security. — 2024. — Volume 136. — 103585. — DOI: 10.1016/j.cose.2023.103585.

6. The Future of Cybersecurity: Tools and Strategies. — URL: https://www.gartner.com/peer-community/oneminuteinsights/future-cybersecurity-tools-strategies-jgj (accessed: 01.04.2024)

7. Лебедь С.В. Инновационные технологии в сфере кибербезопасности / С.В. Лебедь // Современные информационные технологии и ИТ-образование. — 2022. — №2. — URL: https://cyberleninka.ru/article/n/innovatsionnye-tehnologii-v-sfere-kiberbezopasnosti (дата обращения: 12.04.2024).

8. Орлов Г.А. Применение Big Data при анализе больших данных в компьютерных сетях Земли / Г.А. Орлов, А.В. Красов, А.М. Гельфанд // Наукоемкие технологии в космических исследованиях. — 2020. — Т. 12. — № 4. — С. 76-84.

9. Косов Н.А. Способы защиты от инсайдерских атак / Н.А. Косов, Н.А. Голубов // 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.

10. Гельфанд А.М. Оценка рисков и угроз безопасности в среде “Умный дом” / А.М. Гельфанд, А.А. Казанцев, А.В. Красов [и др.] // 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.

11. Штеренберг С.И. Анализ безопасности доменных систем / С.И. Штеренберг, Г.С. Бударный, И.В. Чумаков // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. — Санкт-Петербург, 2022. — С. 587-588.

12. Алехин Р.В. Облачные сервисы. принцип работы, классификация и модели обслуживания / Р.В. Алехин, А.В. Красов, А.Д. Макарова и др. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИ-НО 2022). XI Международная научно-техническая и научно-методическая конференция. — Санкт-Петербург, 2022. — С. 70-74.

13. Агаев Р.Ш. Безопасность информационного сопровождения в системе экономической безопасности / Р.Ш. Агаев, А.А. Графов [и др.] // Национальная безопасность и стратегическое планирование. — 2022. — № 2 (38). — С. 98–104. — URL: https://futurepubl.ru/ru/storage/viewWindow/97159 (дата обращения: 01.04.2024). — DOI: 10.37468/2307-1400-2022-2-98-104.

14. Лапыгин Д.Ю. Обеспечение экономической безопасности инструментами информационных технологий / Д.Ю. Лапыгин, К.С. Караман // Экономическая безопасность. — 2023. — Т. 6. — № 1. — С. 429–442. — URL: https://1economic.ru/lib/117577 (дата обращения: 01.04.2024). — DOI: 10.18334/ecsec.6.1.117577.

15. Дубень А.К. Теоретико-методологические основы информационной безопасности / А.К. Дубень // Национальная безопасность. — 2023. — № 2 (47). — С. 48–54. — URL: https://nbpublish.com/library_read_ arti-cle.php?id=40068 (дата обращения: 01.04.2024)

16. Ладжуз М. Кибербезопасность как фактор конкурентоспособности / М. Ладжуз // Kazan Digital Week: сб. матлов Междунар. форума (г. Казань, 21–22 сентября 2022 г.). — Казань: Научный центр безопасности жизнедеятельности, 2022. — С. 299–303. — URL: https://elibrary.ru/item.asp?id=50028850 (дата обращения: 01.04.2024).

17. Tunggal A. What is Cybersecurity Risk? A Thorough Definition / A. Tunggal // UpGuard: Cybersecurity. — 2023. — URL: https://www.upguard.com/blog/cybersecurity-risk (accessed: 01.04.2024).

18. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия / Г.В. Семеко // Социальные новации и социальные науки. — 2020. — №1 (1). — URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-finansovom-sektore-kiberprestupnost-i-strategiya-protivodeystviya (дата обращения: 22.04.2024).

Список литературы на английском языке / References in English

1. Cem Dilmegani. Quantum Cryptography / Cem Dilmegani // Encryption in 2024: In-Depth Guide. — URL: https://research.aimultiple.com/quantum-cryptography/ (accessed: 01.04.2024)

2. Zero day exploit definition. — URL: https://www.balbix.com/insights/what-is-a-zero-day-exploit/ (accessed: 01.04.2024)

3. Mary Pratt. What is zero trust? A model for more effective security / Mary Pratt. — URL: https://www.csoonline.com/article/564201/what-is-zero-trust-a-model-for-more-effective-security.html (accessed: 01.04.2024)

4. Yuchong Li. A comprehensive review study of cyber-attacks and cyber security. Emerging trends and recent developments / Yuchong Li, Qinghui Liu // Energy Reports. — 2021. — Volume 7. — P. 8176-8186. — DOI: 10.1016/j.egyr.2021.08.126

5. Prümmer J. A systematic review of current cybersecurity training methods / Julia Prümmer, Tommy van Steen, Bibi van den Berg // Computers & Security. — 2024. — Volume 136. — 103585. — DOI: 10.1016/j.cose.2023.103585.

6. The Future of Cybersecurity: Tools and Strategies. — URL: https://www.gartner.com/peer-community/oneminuteinsights/future-cybersecurity-tools-strategies-jgj (accessed: 01.04.2024)

7. Lebed' S.V. Innovacionnye tekhnologii v sfere kiberbezopasnosti [Innovative technologies in the field of cybersecurity] / S.V. Lebed' // Sovremennye informa-cionnye tekhnologii i IT-obrazovanie [Modern information technologies and OT-education]. — 2022. — №2. — URL: https://cyberleninka.ru/article/n/innovatsionnye-tehnologii-v-sfere-kiberbezopasnosti (accessed: 12.04.2024) [in Russian].

8. Orlov G.A. Primenenie Big Data pri analize bol'shih dannyh v komp'yuternyh setyah Zemli [The use of Big Data in the analysis of big data in computer networks of the Earth] / G.A. Orlov, A.V. Krasov, A.M. Gel'fand // Naukoemkie tekhnologii v kosmicheskih issledovaniyah [High-tech technologies in space research]. — 2020. — V. 12. — № 4. — P. 76-84 [in Russian].

9. Kosov N.A. Sposoby zashchity ot insajderskih atak [Ways to protect against insider attacks] / N.A. Kosov, N.A. Golubov // Innovacionnye resheniya so-cial'nyh, ekonomicheskih i tekhnologicheskih problem sovremennogo obshchestva. Sbornik nauchnyh statej po itogam kruglogo stola so vserossijskim i mezhdunarodnym uchastiem [Innovative solutions to social, economic and technological problems of modern society. Collection of scientific articles based on the results of the round table with national and international participation]. — Moskva, 2021. — P. 149-151 [in Russian].

10. Gel'fand A.M. Ocenka riskov i ugroz bezopasnosti v srede “Umnyj dom” [Risk assessment and security threat in the Smart Home environment] / A.M. Gel'fand, A.A. Kazancev, A.V. Krasov [et al.] // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2020). IX Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya : sbornik nauchnyh statej [Actual problems of infotelecommunications in science and education (APINA 2020). IX International Scientific-technical and scientific-methodical Conference: collection of scientific articles]. —St.Petersburg, 2020. — P. 316-321 [in Russian].

11. SHterenberg S.I. Analiz bezopasnosti domennyh system [Security analysis of internal systems] / S.I. SHterenberg, G.S. Budarnyj, I.V. CHumakov // Regional'naya informatika (RI-2022). YUbilejnaya XVIII Sankt-Peterburgskaya mezhdunarodnaya konferenciya. Materialy konferencii [Regional Informatics (RI-2022). Anniversary of the St. Petersburg International Conference. Conference materials]. — St.Petersburg, 2022. — P. 587-588 [in Russian].

12. Alekhin R.V. Oblachnye servisy. princip raboty, klassifikaciya i modeli obsluzhivaniya [Cloud services. the principle of operation, classification and service models] / R.V. Alekhin, A.V. Krasov, A.D. Makarova et al. // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (API-NO 2022). XI Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya [Actual problems of infotelecommunications in science and education (API 2022). XI International Scientific-Technical and Scientific-Methodical Conference]. — Sankt-Peterburg, 2022. — P. 70-74 [in Russian].

13. Agaev R.SH. Bezopasnost' informacionnogo soprovozhdeniya v sisteme ekonomicheskoj bezopasnosti [Security of information support in the economic security system] / R.SH. Agaev, A.A. Grafov [et al.] // Nacional'naya bezopasnost' i strategicheskoe planirovanie [National security' and strategic planning]. — 2022. — № 2 (38). — P. 98–104. — URL: https://futurepubl.ru/ru/storage/viewWindow/97159 (accessed: 01.04.2024). — DOI: 10.37468/2307-1400-2022-2-98-104 [in Russian].

14. Lapygin D.YU. Obespechenie ekonomicheskoj bezopasnosti instrumentami informacionnyh tekhnologij [Ensuring economic security with information technology tools] / D.YU. Lapygin, K.S. Karaman // Ekonomicheskaya bezopasnost' [Economic security]. — 2023. — V. 6. — № 1. — P. 429–442. — URL: https://1economic.ru/lib/117577 (accessed: 01.04.2024). — DOI: 10.18334/ecsec.6.1.117577 [in Russian].

15. Duben' A.K. Teoretiko-metodologicheskie osnovy informacionnoj bezopasnosti [Theoretical and methodological foundations of information security] / A.K. Duben' // Nacio-nal'naya bezopasnost' [National security]. — 2023. — № 2 (47). — P. 48–54. — URL: https://nbpublish.com/library_read_ arti-cle.php?id=40068 (accessed: 01.04.2024) [in Russian]

16. Ladzhuz M. Kiberbezopasnost' kak faktor konkurentosposobnosti [Cybersecurity' as a factor of competitiveness] / M. Ladzhuz // Kazan Digital Week: sb. mat-lov Mezhdunar. foruma (g. Kazan', 21–22 sentyabrya 2022 g.) [Kazan Digital Week: Proceedings of the International Forum (Kazan, 21-22 September 2022).]. — Kazan: Nauchnyj centr bezopasnosti zhiznedeyatel'nosti [Scientific Center for Life Safety], 2022. — P. 299–303. — URL: https://elibrary.ru/item.asp?id=50028850 (accessed: 01.04.2024) [in Russian].

17. Tunggal A. What is Cybersecurity Risk? A Thorough Definition / A. Tunggal // UpGuard: Cybersecurity. — 2023. — URL: https://www.upguard.com/blog/cybersecurity-risk (accessed: 01.04.2024).

18. Semeko G.V. Informacionnaya bezopasnost' v finansovom sektore: kiberprestupnost' i strategiya protivo-dejstviya [Information security'in the financial sector: Cybercrime' and counteraction strategy] / G.V. Semeko // Social'nye novacii i social'nye nauki [Social innovation and social sciences]. — 2020. — №1 (1). — URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-finansovom-sektore-kiberprestupnost-i-strategiya-protivodeystviya (accessed: 22.04.2024) [in Russian].