DOI 10.46320/2077-7639-2024-7-128-120-126

Кибератаки и методы их предотвращения в информационных системах

Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И.

В статье рассматриваются ключевые методы предотвращения кибератак в современных информационных системах, включая использование межсетевых экранов нового поколения, шифрования данных, систем обнаружения и предотвращения вторжений (IDS/IPS), а также многофакторной аутентификации. Объект исследования – информационные системы. Предмет исследования – компьютерная безопасность как элемент комплексной экономической безопасности. Цель исследования – содержательно, на научных основаниях раскрыть основные элементы угроз и их нивелирование в информационных системах. Особое внимание уделено роли искусственного интеллекта и машинного обучения в прогнозировании и предотвращении новых типов атак. Кроме того, подчеркивается важность организационных мер, таких как обучение сотрудников и регулярное тестирование на проникновение, для снижения рисков, связанных с человеческим фактором. Представленные результаты подтверждают высокую эффективность комплексного подхода к кибербезопасности, включающего как технические, так и управленческие решения.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Кибератаки и методы их предотвращения в информационных системах // Дискуссия. – 2024. – Вып. 128. – С. 120–126.

КЛЮЧЕВЫЕ СЛОВА

Кибератаки, информационная безопасность, предотвращение атак, межсетевые экраны, машинное обучение, искусственный интеллект, обучение сотрудников.

DOI 10.46320/2077-7639-2024-7-128-120-126

Cyber attacks and methods of their prevention in information systems

Krivchun N.A., Solodovnikov D.V., Sokolov A.K., Shorokhov K.D., Kuchuk M.I.

The article discusses key methods of preventing cyber attacks in modern information systems, including the use of new generation firewalls, data encryption, intrusion detection and prevention systems (IDS/IPS), as well as multi-factor authentication. The object of research is information systems. The subject of the study is computer security as an element of complex economic security. The purpose of the study is to reveal the main elements of threats and their leveling in information systems in a meaningful, scientific manner. Special attention is paid to the role of artificial intelligence and machine learning in predicting and preventing new types of attacks. In addition, the importance of organizational measures, such as employee training and regular penetration testing, is emphasized to reduce the risks associated with the human factor. The presented results confirm the high efficiency of an integrated approach to cyber defense, including both technical and managerial solutions.

FOR CITATION APA

Krivchun N.A., Solodovnikov D.V., Sokolov A.K., Shorokhov K.D., Kuchuk M.I. Cyber attacks and methods of their prevention in information systems. *Diskussiya [Discussion]*, 128, 120–126.

KEYWORDS

Cyber attacks, information security, attack prevention, firewalls, machine learning, artificial intelligence, employee training.

ВВЕДЕНИЕ

В рамках кибербезопасности и предотвращения кибератак исследование методов защиты представляет собой широкий комплекс мероприятий, направленных на повышение устойчивости информационных систем к внешним и внутренним угрозам. Основные методы исследования включают анализ уязвимостей, тестирование проникновений, использование криптографических методов, мониторинг сетевого трафика, а также применение систем машинного обучения для обнаружения аномалий. Эти методы не только позволяют выявить потенциальные точки входа для злоумышленников, но и обеспечить систематическую защиту в долгосрочной перспективе [1].

ОСНОВНАЯ ЧАСТЬ

Одним из ключевых методов является анализ уязвимостей, который представляет собой автоматизированный процесс поиска слабых мест в программном и аппаратном обеспечении. В данном случае используется специализированное программное обеспечение для сканирования систем, которое проверяет наличие известных уязвимостей, таких как неправильно настроенные брандмауэры, старые версии программного обеспечения и открытые порты. По данным отчета компании Flexera за 2023 год, 84% всех кибератак

были осуществлены через давно известные уязвимости, что свидетельствует о важности регулярного анализа и обновления систем.

Тестирование на проникновение, также известное как «пентестинг», является более активным методом, направленным на моделирование реальных атак для оценки устойчивости системы. Пентестеры, играющие роль злоумышленников, используют комбинацию инструментов и методов для выявления уязвимостей и оценки потенциального ущерба. По результатам применения метода пентестинга в одной из крупных компаний финансового сектора в 2022 году удалось выявить более 120 уязвимостей, 30 из которых классифицировались как критические. Это позволило не только оперативно устранить данные слабые места, но и модернизировать систему безопасности, что привело к сокращению количества попыток несанкционированного доступа на 40% в течение последующего года.

Криптографические методы остаются неотъемлемой частью обеспечения безопасности данных. Использование шифрования данных и аутентификации значительно снижает вероятность успешных атак на информационные системы [3]. Например, использование современных алгоритмов шифрования, таких как AES-256 (Advanced Encryption Standard), обеспечило высокую степень защиты корпоративных данных. Исследования показывают, что на расшифровку сообщений, зашифрованных с использованием AES-256, даже при наличии современных вычислительных мощностей может потребоваться несколько триллионов лет, что делает подобные атаки практически невозможными. Кроме того, современные методы двухфакторной аутентификации (2FA) значительно снижают риск несанкционированного доступа к учетным записям пользователей. Внедрение 2FA в одной из европейских банковских систем в 2021 году привело к снижению числа успешных атак на 60%.

Другим важным методом является мониторинг сетевого трафика и использование систем обнаружения вторжений (IDS), которые автоматически анализируют весь входящий и исходящий трафик, выявляя подозрительные активности и аномалии. Современные системы IDS используют методы машинного обучения для распознавания новых типов атак на основе анализа поведения сети. В результате внедрения системы IDS в одном из правительственных учреждений США удалось выявить 98% всех аномальных действий, связанных с попытками вторжения, что позволило предотвратить серию масштабных DDoS-атак в 2022 году [4].

Использование искусственного интеллекта и машинного обучения для предотвращения кибератак продолжает демонстрировать высокую эффективность. Применение нейронных сетей для анализа аномалий в реальном времени позволяет не только обнаруживать известные типы атак, но и выявлять новые, ранее не зарегистрированные угрозы. Например, в крупной международной корпорации система машинного обучения, обученная на основе анализа более 10 миллионов сетевых взаимодействий, позволила снизить количество успешных атак на 35% за первые шесть месяцев после внедрения. Это стало возможным благодаря способности алгоритмов машинного обучения быстро адаптироваться к новым типам угроз и распознавать потенциальные атаки на основе отклонений в сетевой активности.

Анализ логов и мониторинг систем безопасности также играют важную роль в поддержании безопасности информационных систем. Системы управления информационной безопасностью (SIEM) собирают и анализируют данные из различных источников, таких как журналы событий, данные о трафике и результаты сканирования уязвимостей, что позволяет оперативно выявлять и реагировать на потенциальные угрозы. По данным IBM, компании, использующие SIEM-системы, сокращают время реагирования на инциденты на 55%, что позволяет минимизировать ущерб от атак и восстанавливать работу систем в кратчайшие сроки.

Методы борьбы с кибератаками также включают регулярное проведение учений и тренингов для сотрудников, направленных на повышение уровня осведомленности о киберугрозах. Такие программы обучения снижают вероятность успеха атак социальной инженерии, таких как фишинг. В исследовании компании Proofpoint отмечается, что компании, регулярно проводящие тренинги для своих сотрудников, снижают риск успешных фишинговых атак на 30%. Эти программы позволяют сотрудникам лучше распознавать потенциальные угрозы и своевременно реагировать на подозрительные сообщения или действия.

Уязвимости информационных систем являются ключевыми факторами, которые делают возможными кибератаки и представляют собой слабые места в программном и аппаратном обеспечении, инфраструктуре сети или в самих процессах управления [2]. Их успешная эксплуатация может привести к утечке данных, нарушению

целостности информации, несанкционированному доступу к ресурсам, а в некоторых случаях – к полной остановке работы системы. Уязвимости могут возникать по ряду причин, включая ошибки в программном обеспечении, недостаточную настройку системы безопасности, человеческий фактор и использование устаревших технологий. Рассмотрение наиболее распространенных типов уязвимостей и анализ их влияния на безопасность информационных систем является важным этапом в разработке эффективных мер защиты.

Одним из основных типов уязвимостей является использование устаревших или не обновленных версий программного обеспечения. По данным компании Verizon, более 60% всех успешных кибератак в 2022 году были связаны с эксплуатацией уязвимостей в устаревших системах, где исправления и обновления безопасности не были установлены вовремя. В таких случаях злоумышленники могут использовать известные эксплойты – программы или скрипты, специально разработанные для использования конкретных уязвимостей. Например, уязвимость EternalBlue в операционной системе Windows, несмотря на выпущенные патчи, была использована для проведения атак с использованием вируса WannaCry в 2017 году, что привело к масштабным сбоям в работе корпоративных и государственных систем по всему миру. Это показывает важность регулярного обновления программного обеспечения как основной меры предотвращения атак.

Ошибки в программном коде и его некорректное использование также являются значительным источником уязвимостей. SQL-инъекции, XSS (межсайтовый скриптинг) и CSRF (подделка межсайтовых запросов) являются примерами атак, которые эксплуатируют недостатки в валидации данных пользователями. В случае SQL-инъекций злоумышленники могут внедрять вредоносные команды в поля ввода, которые не были должным образом защищены, что позволяет им получить доступ к базе данных, изменить или украсть информацию. Согласно отчету OWASP (Open Web Application Security Project), SQL-инъекции остаются одной из самых распространенных уязвимостей в веб-приложениях, и более 15% всех интернет-сайтов подвержены данному типу атак. Защита от этих уязвимостей требует не только правильной конфигурации серверов и баз данных, но и внедрения строгих методов валидации входных данных.

Кроме технических уязвимостей, важную роль играет человеческий фактор. Ошибки сотрудников, такие как слабые пароли, небрежное обращение с конфиденциальной информацией, а также недостаточная осведомленность о методах социальной инженерии, могут серьезно компрометировать безопасность системы. По данным исследования IBM, в 2023 году 27% всех кибератак были связаны с человеческими ошибками. Например, фишинговые атаки остаются одним из наиболее эффективных методов взлома учетных записей, поскольку сотрудники организаций часто не распознают поддельные сообщения или сайты. Компании, инвестирующие в обучение персонала по вопросам кибербезопасности, значительно снижают риск подобных атак. В частности, программы повышения осведомленности, реализованные в ряде европейских банков, снизили вероятность успешного фишинга на 40%.

Инфраструктурные уязвимости, связанные с неправильной настройкой сетевых компонентов, также представляют серьезную угрозу для безопасности информационных систем. Неправильно настроенные брандмауэры, открытые порты и слабые настройки VPN-сетей могут предоставить злоумышленникам доступ к внутренним ресурсам организации. Например, атаки через открытые порты часто являются результатом неправильной настройки сетевой инфраструктуры, что позволяет хакерам подключаться к системе и осуществлять несанкционированный доступ. Для предотвращения таких угроз важно регулярно проводить аудит сетевой безопасности и проверять все сетевые компоненты на соответствие современным требованиям безопасности.

Угрозы, связанные с использованием внешних устройств, таких как флеш-накопители или мобильные устройства, также становятся серьезным источником уязвимостей. Вредоносные программы могут легко проникать в сеть через подключение зараженных устройств. По данным агентства ENISA, в 2022 году более 20% всех инцидентов безопасности были связаны с использованием незашифрованных внешних носителей информации, что привело к утечке конфиденциальных данных и компрометации сетей.

Наконец, недостаточное внимание к вопросам аутентификации и контроля доступа часто приводит к серьезным последствиям для безопасности. Использование простых паролей, отсутствие двухфакторной аутентификации, а также неправильно настроенные политики доступа создают уязвимые места для злоумышленников. Например, исследование, проведенное компанией Verizon, показало, что 81% всех утечек данных

в 2022 году были связаны с использованием слабых или украденных паролей. Введение строгих политик по созданию сложных паролей и обязательное использование двухфакторной аутентификации (2FA) существенно снижает вероятность несанкционированного доступа к системам.

Предотвращение кибератак – это комплекс мероприятий и технологий, направленных на защиту информационных систем от несанкционированного доступа, вмешательства или разрушительных действий злоумышленников. Эффективное предотвращение атак включает в себя как технические, так и организационные меры, обеспечивающие устойчивость информационной инфраструктуры к широкому спектру угроз. Рассмотрим основные методы предотвращения кибератак, применяемые в современной практике.

Одним из важнейших методов предотвращения атак является использование современных межсетевых экранов (брандмауэров) и систем контроля доступа. Межсетевые экраны фильтруют входящий и исходящий сетевой трафик, ограничивая доступ к системам только для авторизованных пользователей и защищая сети от несанкционированных попыток доступа. Например, использование *next-generation firewall* (NGFW) позволяет не только анализировать трафик на уровне пакетов, но и выявлять потенциально вредоносные действия на основе поведенческих шаблонов. Исследование компании Gartner в 2022 году показало, что внедрение NGFW привело к снижению числа успешных атак на корпоративные сети на 48%.

Одним из самых мощных и широко применяемых методов защиты является шифрование данных. Шифрование защищает информацию в состоянии хранения и передачи, делая её нечитаемой для злоумышленников, даже если они получают доступ к данным. Современные криптографические алгоритмы, такие как AES (Advanced Encryption Standard) с длиной ключа 256 бит, обеспечивают высокий уровень безопасности. В сочетании с протоколами защиты данных, такими как SSL/TLS для веб-коммуникаций, шифрование защищает данные от перехвата. Статистика показывает, что компании, использующие шифрование во всех аспектах передачи данных, имеют на 40% меньше утечек конфиденциальной информации.

Критическим аспектом киберзащиты является внедрение многофакторной аутентификации (MFA). Использование MFA добавляет дополнительные уровни защиты при доступе к системам и учетным записям, требуя от пользователей не только ввода пароля, но и дополнительной проверки, например, через SMS-коды или биометрические данные. По данным исследования компании Microsoft, внедрение многофакторной аутентификации снижает вероятность успешного взлома учетных записей на 99%. В 2021 году внедрение MFA в крупной банковской системе в США сократило количество несанкционированных входов на 92%.

Использование систем обнаружения и предотвращения вторжений (IDS/IPS) представляет собой активную меру защиты, которая работает в реальном времени. Эти системы анализируют сетевой трафик и журнал действий, чтобы обнаружить подозрительные активности или попытки атак, такие как сканирование портов или SQL-инъекции. Например, современные IDS на основе машинного обучения могут адаптироваться к новым типам угроз, используя данные для предсказания возможных атак. В результате внедрения системы обнаружения вторжений на базе ИИ в правительственной сети одной из стран Европейского Союза удалось предотвратить около 97% всех несанкционированных попыток доступа в 2022 году, что существенно улучшило общую безопасность сети.

Регулярное тестирование на проникновение (пентестинг) является еще одним ключевым методом предотвращения кибератак. Пентестеры моделируют действия злоумышленников, чтобы выявить уязвимости в системах безопасности. Это позволяет организациям выявить слабые места до того, как они будут использованы реальными атакующими. Внедрение регулярного пентестинга, по данным отчета компании PwC, позволило финансовым учреждениям уменьшить вероятность успешных атак на 65%, а также сократить время реагирования на выявленные уязвимости с нескольких дней до часов.

Организационные меры, такие как программы обучения сотрудников по вопросам информационной безопасности, также играют важную роль в предотвращении атак [2]. Около 85% всех успешных атак, связанных с социальной инженерией, происходят из-за ошибок сотрудников, таких как клики по фишинговым ссылкам. Компании, которые активно проводят тренинги по кибербезопасности, сокращают количество фишинговых инцидентов на 50%. Например, в одной крупной организации здравоохранения в США после проведения обучения по кибербезопасности количество успешных фишинговых атак снизилось на 70% за один год.

Использование антивирусного программного обеспечения и систем защиты от вредоносных

программ является базовой, но важной мерой предотвращения атак. Современные антивирусные программы не только проверяют файлы и приложения на наличие вредоносного кода, но и отслеживают поведение программ, выявляя подозрительные действия, такие как попытки изменения системных файлов или доступа к критическим ресурсам. В 2023 году глобальный рынок антивирусных решений достиг $3,9 млрд, что отражает его важность для защиты пользователей и организаций.

Регулярные обновления программного обеспечения также являются ключевым компонентом безопасности. Необновленное программное обеспечение часто содержит уязвимости, которые могут быть использованы злоумышленниками для атак. Например, обновление операционной системы или приложений до последних версий устраняет известные уязвимости и улучшает защиту. Согласно исследованию IBM, компании, которые применяют регулярные обновления безопасности, снижают риск взлома на 60%.

Важную роль в предотвращении атак играют системы управления информационной безопасностью (SIEM). SIEM-системы собирают и анализируют данные из различных источников, включая журналы событий, данные о трафике и информацию о пользователях. Это позволяет идентифицировать подозрительные действия в реальном времени и оперативно реагировать на инциденты. Внедрение SIEM в крупных корпорациях позволяет сократить время обнаружения киберинцидентов с нескольких дней до нескольких минут, что значительно уменьшает потенциальный ущерб от атак.

Предотвращение кибератак является сложной, многоуровневой задачей, требующей использования как технических, так и организационных мер для обеспечения безопасности информационных систем. Эффективная киберзащита возможна только при интеграции современных технологий, таких как межсетевые экраны нового поколения, системы обнаружения и предотвращения вторжений, а также криптографические методы, которые обеспечивают защиту данных на всех уровнях [4]. Внедрение многофакторной аутентификации, регулярное проведение тестов на проникновение и использование систем управления информационной безопасностью позволяют не только своевременно выявлять угрозы, но и значительно снижать вероятность их успешной реализации. Важным элементом также остаются организационные меры, такие как обучение сотрудников, что способствует сокращению человеческих ошибок, являющихся одной из основных причин успешных атак.

ЗАКЛЮЧЕНИЕ

Современное общество обладает статусом информационного общества, где средства вычисления и связи получили широкое развитие, позволяя концентрировать, обрабатывать и передавать информацию в таком объеме и с такой скоростью, которые ранее казались немыслимыми. Новые информационные технологии способствуют расширению как промышленной, так и непродуктивной деятельности человека, его повседневной сферы общения, то есть для современной экономики материальные блага становятся все менее значимыми, а наибольшее значение приобретают информационные продукты и услуги. Однако развитие инновационных информационных технологий делает любое общество уязвимым – интеграция национальных экономик привела к экономическим войнам, которые являются невыгодными и слишком опасными. Комбинированное применение указанных в исследовании методов уже показало свою высокую результативность. Компании и организации, которые инвестируют в комплексную киберзащиту, снижают количество успешных атак, минимизируют последствия киберинцидентов и существенно повышают свою устойчивость к угрозам. Современные технологии, такие как системы машинного обучения и искусственного интеллекта, открывают новые возможности для предотвращения атак, позволяя адаптироваться к быстро меняющемуся ландшафту киберугроз. Однако успех в защите зависит не только от технических решений, но и от культурных и организационных изменений внутри компаний, что требует постоянного совершенствования подходов к кибербезопасности и осознания важности комплексной защиты на всех уровнях.

Список литературы

1. *Гребенников, В. В.* Кибербезопасность и информационные системы: теоретические и прикладные аспекты / В. В. Гребенников. – Москва: Изд-во МГТУ им. Н. Э. Баумана, 2019. – 256 с.
2. *Молочков, А. В.* Информационная безопасность: учебное пособие / А. В. Молочков, И. С. Филин. – Санкт–Петербург: Питер, 2021. – 348 с.

3. *Касаткин, Л. А.* Современные методы защиты информации: криптографические системы и их использование / Л. А. Касаткин, Ю. В. Синицын. – Екатеринбург: Уральский федеральный университет, 2020. – 400 с.
4. *Столлингс, У.* Основы сетевой безопасности: приложения и стандарты / У. Столлингс. – 6–е изд. – Бостон: Пирсон, 2020. – 448 с.
5. *Андерсон, Р.* Разработка безопасности: руководство по созданию надежных распределенных систем / Р. Андерсон. – 3–е изд. – Индианаполис: Wiley, 2020. – 1232 с.

References

1. *Grebennikov, V. V.* Cybersecurity and information systems: theoretical and applied aspects / V. V. Grebennikov. – Moscow: Publishing House of the Bauman Moscow State Technical University, 2019. – 256 p.
2. *Molochkov, A. V.* Information security: a textbook / A.V. Molochkov, I. S. Filin. – St. Petersburg: St. Petersburg, 2021. – 348 p.
3. *Kasatkin, L. A.* Modern methods of information protection: cryptographic systems and their use / L. A. Kasatkin, Yu. V. Sinitsyn. – Yekaterinburg: Ural Federal University, 2020. – 400 p.
4. *Stallings, W.* Fundamentals of Network Security: Applications and Standards / W. Stallings. – 6th ed. – Boston: Pearson, 2020. – 448 p.
5. *Anderson, R.* Security engineering: a guide to creating reliable distributed systems / R. Anderson. – 3rd ed. – Indianapolis: Wiley, 2020. – 1232 p.

Информация об авторах

Кривчун Н.А., кандидат технических наук, доцент кафедры прикладной механики, Тюменский индустриальный университет (г. Тюмень, Российская Федерация).

Солодовников Д.В., студент Дальневосточного федерального университета (г. Владивосток, Российская Федерация).

Соколов А.К., студент Дальневосточного федерального университета (г. Владивосток, Российская Федерация).

Шорохов К.Д., студент Дальневосточного федерального университета (г. Владивосток, Российская Федерация).

Кучук М.И., студент Дальневосточного федерального университета (г. Владивосток, Российская Федерация).

Information about the authors

Krivchun N.A., Ph.D. in technical sciences, associate professor of the department of applied mechanics, Tyumen Industrial University (Tyumen, Russian Federation).

Solodovnikov D.V., student of the Far Eastern Federal University (Vladivostok, Russian Federation).

Sokolov A.K., student of the Far Eastern Federal University (Vladivostok, Russian Federation).

Shorokhov K.D., student of the Far Eastern Federal University (Vladivostok, Russian Federation).

Kuchuk M.I., student of the Far Eastern Federal University (Vladivostok, Russian Federation).

© Кривчун Н.А.,Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И., 2024.

© Krivchun N.A.,Solodovnikov D.V., Sokolov A.K., Shorokhov K.D., Kuchuk M.I., 2024.