НАУЧНЫЙ АСПЕКТ

na-journal.ru

2024

№3

ТОМ 26

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 . – Т26 . – 132 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 7,92 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

УДК 004.056

Внедрение защищенных систем связи на предприятиях: требования, процессы и практики

Пронин Александр Дмитриевич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная статья рассматривает актуальную проблему внедрения защищенных систем связи на предприятиях с учетом современных киберугроз. В тексте обсуждаются основные требования к таким системам, включая шифрование данных, аутентификацию, управление доступом и защиту от вредоносного программного обеспечения. Подробно описываются процессы внедрения, начиная от аудита безопасности и разработки политики до обучения сотрудников и интеграции новых технологий. В статье также выделяются вызовы и перспективы в области кибербезопасности, такие как соблюдение регуляторных требований и человеческий фактор. Заключение подчеркивает важность постоянного обновления и мониторинга систем для обеспечения эффективной защиты предприятия от современных кибер-угроз.*

***Abstract**: This article examines the current problem of implementing secure communication systems in enterprises with respect to modern cyber threats. The text discusses the basic requirements for such systems, including data encryption, authentication, access control, and malware protection. Implementation processes ranging from security audits and policy development to employee training and integration of new technologies, are described in detail. The article also highlights cybersecurity challenges and perspectives such as regulatory compliance and human factors. The conclusion emphasizes the importance of continually updating and monitoring systems to ensure that the enterprise is effectively protected from today's cyber threats.*

***Ключевые слова**: защищенные системы связи, информационная безопасность, кибербезопасность, шифрование данных, аутентификация.*

***Keywords**: secure communication systems, information security, cybersecurity, data encryption, authentication.*

Современные предприятия сталкиваются с растущей угрозой кибератак и нарушений безопасности данных. В условиях постоянного развития технологий и увеличения объемов информации защита корпоративной связи становится ключевым аспектом в обеспечении бизнес-стабильности и сохранности конфиденциальной информации. Внедрение защищенных систем связи становится неотъемлемой частью стратегии информационной безопасности предприятий.

Требования к защищенным системам связи:

1. Шифрование данных:

Защита информации начинается с ее шифрования. Защищенные системы связи должны обеспечивать эффективное и современное шифрование данных на всех этапах передачи — от отправителя к получателю.

2. Аутентификация:

Предотвращение несанкционированного доступа требует надежной системы аутентификации. Использование многофакторной аутентификации, биометрии и других современных методов становится необходимостью.

3. Управление доступом:

Защищенные системы связи должны обеспечивать гибкое управление правами доступа, предоставляя сотрудникам доступ только к необходимой информации в соответствии с их ролями и обязанностями.

4. Защита от вредоносного программного обеспечения:

Эффективная защита от вредоносных программ требует внедрения антивирусных и антифишинговых решений, а также постоянного мониторинга и обновления систем.

5. Системы мониторинга и обнаружения инцидентов:

Быстрое обнаружение и реагирование на инциденты — ключевой момент в обеспечении безопасности. Внедрение систем мониторинга и обнаружения аномалий позволяет своевременно выявлять потенциальные угрозы.

Процессы внедрения защищенных систем связи:

1. Аудит безопасности:

Начинать следует с проведения аудита текущих систем связи и выявления потенциальных уязвимостей. Это поможет разработать индивидуальную стратегию защиты.

2. Разработка политики безопасности:

Определение правил и стандартов безопасности, которые будут регулировать использование корпоративной связи. Это включает в себя правила паролей, уровни доступа и политику обновлений.

3. Обучение сотрудников:

Обучение персонала основам информационной безопасности является неотъемлемой частью внедрения защищенных систем связи. Информированные сотрудники способствуют общей безопасности предприятия.

4. Интеграция новых технологий:

Выбор и внедрение современных технологий, соответствующих потребностям предприятия. Это включает в себя обновление аппаратного и программного обеспечения, а также внедрение новых методов шифрования и защиты.

Практики внедрения защищенных систем связи:

1. Регулярное обновление систем:

Системы связи и безопасности должны регулярно обновляться для обеспечения защиты от новых угроз и уязвимостей.

2. Системы резервного копирования:

Регулярное создание резервных копий данных обеспечивает быстрое восстановление после инцидентов безопасности или сбоев в работе систем.

3. Постоянный мониторинг безопасности:

Внедрение систем постоянного мониторинга позволяет быстро реагировать на аномалии и угрозы, минимизируя риск утечки данных.

Вызовы и перспективы внедрения защищенных систем связи:

1. Соблюдение регуляторных требований:

С ужесточением законодательства в области информационной безопасности, предприятиям необходимо не только внедрять защищенные системы связи, но и активно следить за изменениями в законодательстве и обеспечивать соблюдение требований.

2. Совершенствование технологий:

Технологии в области кибербезопасности постоянно совершенствуются. Предприятия должны быть готовы к инновациям и активному внедрению передовых технологий для обеспечения максимальной защиты.

3. Человеческий фактор:

Социальная инженерия и ошибки персонала остаются одними из основных угроз для безопасности. Эффективные программы обучения и создание культуры безопасности на рабочем месте являются критическими компонентами.

4. Управление угрозами в реальном времени:

Системы связи должны быть способными обнаруживать и реагировать на угрозы в реальном времени. Это требует автоматизированных систем, способных анализировать потоки данных и выявлять аномалии.

Заключение

Внедрение защищенных систем связи на предприятиях — это непрерывный процесс, требующий не только технических решений, но и культурных изменений в организации. Безопасность связи становится неотъемлемой частью успешного бизнеса, и предприятия, осознавая риски, должны инвестировать в современные технологии и обучение персонала.

С учетом постоянно меняющейся угрозовой среды, предприятия должны принимать проактивные меры, обеспечивая надежную защиту от кибератак и утечек конфиденциальной информации. В конечном итоге, внедрение защищенных систем связи становится важным стратегическим элементом, обеспечивающим стойкость предприятия в условиях современного цифрового мира.

Список литературы

1. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании.— 2015. — С. 193–197.
2. 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.

3. 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.
4. Штеренберг С. И. Методика применения в адаптивной системе локальных вычислительных сетей стего-вложения в исполнимые файлы на основе самомодифицирующегося кода //Системы управления и информационные технологии.— 2016.— № . 1. — С. 51–54.
5. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности //Известия высших учебных заведений. Технология легкой промышленности.— 2017. — Т. 37.— № . 3. — С. 5–9.

УДК 004.056

Защита данных от программ-вымогателей

Пронин Александр Дмитриевич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная статья рассматривает важность паролей в обеспечении безопасности данных в цифровой среде. Она подчеркивает роль паролей как первоначального барьера для защиты информации и предотвращения несанкционированного доступа. Статья обсуждает важность использования надежных и уникальных паролей, их периодическую смену, а также сочетание с другими методами аутентификации. Автор подчеркивает, что правильное создание и управление паролями способствует обеспечению безопасности данных и снижению риска несанкционированного доступа.*

***Abstract**: This paper examines the importance of passwords in securing data in a digital environment. It highlights the role of passwords as the initial barrier to protect information and prevent unauthorized access. The article discusses the importance of using strong and unique passwords, changing them periodically, and combining them with other authentication meth-*

ods. The author emphasizes that proper password creation and management contributes to data security and reduces the risk of unauthorized access

***Ключевые слова**: пароли, безопасность данных, аутентификация, управление паролями, сложность паролей, уникальность паролей, периодическая смена паролей, двухфакторная аутентификация, многофакторная аутентификация.*

***Keywords**: passwords, data security, authentication, password management, password complexity, password uniqueness, periodic password change, two-factor authentication, multi-factor authentication.*

Введение

Программы-вымогатели стали крупным бизнесом, и каждая организация является потенциальной мишенью. По данным представленным за 2024 год, видно что в этом году глобальные потери от программ-вымогателей превысят 20 миллиардов долларов.

Существует множество инструментов, затрудняющих проникновение программ-вымогателей, но самая большая уязвимость в любом центре обработки данных — это та, которую невозможно исправить: человеческая природа. Основным вектором атаки программ-вымогателей является социальная инженерия, которая использует человеческую природу для внедрения вредоносного кода в целевую сеть. Обучение сотрудников может снизить риск, но не устранить его.

Защита наилучшим образом

Программа-вымогатель работает путем шифрования данных. Таким образом, защита файлов от программ-вымогателей означает сделать их недоступными для программ-вымогателей или, если они доступны, обеспечить их неизменяемость. Отключить все ваше хранилище и запереть его в сейфе явно непрактично, поэтому на самом деле это означает, что копия данных становится недоступной или неизменяемой. В случае атаки программы-вымогателя эта копия используется для восстановления. Частота, с которой создаются копии, а также место и способ их хранения, имеет важное значение и будет обсуждаться позже. Полезно проверить свои предположения

как о потенциальных злоумышленниках, так и о вашей стратегии защиты. Эти нападения не совершаются человеком в черной толстовке с капюшоном. Они являются объектом внимания чрезвычайно сложных и хорошо финансируемых преступных организаций. Они могут потратить месяцы на перехват нажатий клавиш и пароли администратора, прежде чем начать атаку. Они обладают навыками компрометации ваших резервных копий и получения root-доступа к узлам вашей объектной системы хранения. Даже ваши облачные учетные записи не в безопасности. К сожалению, единственное, на что вы можете резонно рассчитывать, — это то, что у злоумышленников не будет физического доступа к вашему хранилищу данных. Программы-вымогатели и киберпреступления в целом почти всегда совершаются удаленно.

Офлайн-данные — безопасные данные Консервативный подход заключается в предположении, что все, что каким-либо образом подключено к сети, потенциально может быть взломано. Даже системы, предназначенные для неизменяемого хранения данных, могут оказаться уязвимыми, если базовая операционная система будет скомпрометирована. Единственный способ полностью защитить копию данных от программ-вымогателей — создать физический барьер для доступа к ним, который удаленный злоумышленник не сможет преодолеть. Классический физический барьер часто называют «воздушным зазором». Первоначально этот термин использовался в отношении сетевой безопасности, где изолированная система — это система, не подключенная к каким-либо внешним сетям. Его также можно применить к хранилищу данных, где оно относится к хранилищу, не подключенному к сети или сетевой системе. Другими словами, оффлайн. Ключ к автономной копии заключается в том, что к ней нельзя получить доступ без того, чтобы человек сначала сделал что-то, чтобы разместить ее в Интернете. Классическими примерами являются кассеты или другие съемные носители, лежащие на полке.

Роль программной блокировки

Доступен ряд технологий, которые обещают сделать данные, находящиеся на жестком или твердотельном диске, неизменяемыми, обычно путем установки программных временных «блокировок» на хранимые фай-

лы или объекты. Это работает, если все попытки доступа осуществляются через ожидаемые каналы, но если система хранения или сама программа блокировки взломана или использована, все ставки отменяются. Несмотря на то, что технология блокировки файлов и объектов по времени не идеальна, она полезна для снижения шансов на успех атаки, но этого недостаточно. Автономная копия по-прежнему требуется.

А как насчет аппаратных червей?

Аппаратные технологии Write-Once, Read Multiple (WORM) делают невозможным стирание или перезапись однажды записанных данных. Это обеспечивает дополнительный уровень защиты, который может быть полезен. Аппаратная технология WORM доступна как на оптических носителях, так и на ленточных носителях, причем оба используют специальные носители. Оптический WORM основан на физических изменениях, которые происходят с носителем на момент написания и не могут быть отменены. При использовании ленты LTO WORM физический ленточный носитель в картридже идентичен носителю в картриджах без WORM, но различия в записанных на заводе серводорожках и памяти картриджа работают с микропрограммой стримера для обеспечения соблюдения WORM. Теоретически возможно обойти все встроенные средства защиты и стереть или перезаписать картридж LTO WORM, но для этого потребуются глубокие знания системы и, как минимум, умение писать собственный микрокод стримера. Кибер преступники никогда не станут тратить на это время, поскольку всегда доступны более мягкие цели. LTO WORM чрезвычайно безопасен.

Почему лента?

Поскольку магнитная лента существует уже так долго, возникает соблазн отказаться от магнитной ленты как от устаревшей. Но лента сегодняшнего дня настолько же отличается от ленты 1951 года как Тесла от Студебеккера. Есть и другие варианты со своими плюсами и минусами, но лента обладает лучшим сочетанием характеристик для автономного хранения данных. Давайте рассмотрим варианты:

Портативный жесткий диск/твердотельный накопитель

С точки зрения «простого» автономного хранения трудно превзойти жесткий диск USB, по крайней мере, на концептуальном уровне. Скопируйте на него свои данные, отключите его от сети, положите на полку и спите спокойно. Ваши данные защищены от программ вымогателей. Это правда, это отличное и простое решение, если вы обычный человек. Но это дорогое решение с точки зрения соотношения долларов за ТБ, и оно не масштабируется. У твердотельных накопителей те же проблемы, но они стоят еще дороже. Для всех организаций, кроме самых маленьких, необходимы другие варианты.

Оптическое хранилище

Записываемые DVD-диски и диски Blu-Ray — еще один вариант, который на первый взгляд кажется привлекательным и, как и портативные жесткие диски, представляет собой довольно знакомый форм-фактор. Оптические носители могут обеспечить гораздо более высокую стабильность. С течением времени по сравнению с хранилищем на жестком диске, в зависимости от состава носителя. Плотность может быть разумной: емкость до 128 ГБ для Blu-Ray, а носители меньшей емкости доступны по цене. Носитель WORM доступен для создания неизменяемых копий. Но оптическая запись очень медленная и не менее дорогая, чем портативный жесткий диск. Носители высокой плотности обычно рассчитаны только на скорость 4x или 17 МБ/с. Если вам нужно записать много ТБ или требуется быстрое извлечение, низкая скорость является препятствием. В лучшем случае он может подойти для создания архивной копии не изменяющихся данных, которые необходимо хранить в течение многих десятилетий.

Заключение

Кибер преступные атаки становятся все более изощренными и частыми. Человеческая природа используется для совершения атак, что делает невозможным надежное предотвращение. Программы-вымогатели обыч-

но используются для вымогательства атакованных организаций, поэтому крайне важно поддерживать автономную копию данных, которую невозможно скомпрометировать. Лента LTO — лучшая универсальная технология для хранения автономных копий, которая еще безопаснее при использовании сверх защищённых ленточных библиотеках Quantum Scalar

Список литературы

1. Смирнов А. «Защита информации от несанкционированного доступа». Санкт-Петербург: БХВ-Петербург, 2017.
2. Соколов И. «Сетевая безопасность: архитектура и программирование». Москва: ДМК Пресс, 2018.
3. Шнайдер В. «Безопасность Linux. Руководство администратора». Санкт-Петербург: Питер, 2016.
4. Гибсон Д. «Хакеры: герои и злодеи». Москва: Эксмо, 2019.
5. Мартин Э. «Криптография и безопасность сетей: принципы и практика». Москва: Вильямс, 2014.
6. Росс А. «Безопасность в сетях TCP/IP». Москва: ДМК Пресс, 2017.
7. Столл К. «Хакеры и хранилище тайн». Москва: АСТ, 2018.
8. Гарвин П., Кинг Д., Стрикленд Ш. «Сетевая безопасность: анализ угроз и моделирование». Санкт-Петербург: Питер, 2015.
9. Шнайдер В., Карек Д. «Практика хакинга и безопасности в сетях». Москва: Вильямс, 2019.
10. Нечаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом //СПб.: СПбГУТ.— 2014. — Т. 176.
11. Березина Е. О., Цветкова Л. А., Вахрамеева К. А. Классификация угроз информационной безопасности в сетях IT //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 2. — С. 11–18.
12. Виррих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 111–114.
13. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфо-

телекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 107–110.

УДК 004.056

Нарушения безопасности удаленной работы

Пронин Александр Дмитриевич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Научный руководитель **Гельфанд Артем Максимович**

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная статья рассматривает актуальную проблему безопасности, связанную с распространением удалённой работы. В условиях быстро меняющейся рабочей среды, вызванной пандемией COVID-19, автор анализирует риски и вызовы, которые возникают при работе на удалённых платформах. Статья фокусируется на основных аспектах уязвимостей, таких как безопасность конечных точек, сетевая безопасность, атаки методом социальной инженерии и утечки данных.*

***Abstract**: This paper addresses a current security issue related to the proliferation of remote work. In a rapidly changing work environment caused by the COVID-19 pandemic, the author analyzes the risks and challenges that arise when working on remote platforms. The paper focuses on the main aspects of vulnerabilities such as endpoint security, network security, social engineering attacks and data breaches.*

***Ключевые слова**: удалённая работа, безопасность, кибербезопасность, уязвимости, конечные точки.*

***Keywords**: remote work, security, cybersecurity, vulnerabilities, endpoints.*

В последние годы сфера занятости претерпела значительные изменения в связи с широким внедрением удаленной работы. Возможность работать из любого места обеспечила сотрудникам новообретенную гибкость

и удобство, но это также подвергло организации целому ряду нарушений безопасности и проблем. Поскольку предприятия продолжают использовать удаленную работу, становится необходимым решить эти проблемы безопасности, чтобы обеспечить защиту конфиденциальных данных и поддерживать операционную целостность.

1. Распространение удаленной работы и ее последствия для безопасности

Пандемия COVID-19 ускорила переход к удаленной работе, вынудив организации быстро адаптироваться к распределенной рабочей силе. Хотя удаленная работа дает множество преимуществ, таких как снижение накладных расходов и повышение удовлетворенности сотрудников, она также создает множество уязвимостей в системе безопасности.

1. Безопасность конечных точек: самое слабое звено

Одной из основных проблем безопасности, связанных с удаленной работой, является безопасность конечных точек. Сотрудники часто используют персональные устройства для доступа к ресурсам компании, что затрудняет организациям поддержание контроля над этими конечными точками. Незащищенные устройства могут стать шлюзами для проникновения киберпреступников в сеть организации, что потенциально может привести к утечке данных, заражению вредоносными программами и несанкционированному доступу.

2. Недостаточная безопасность сети

Удаленные работники часто полагаются на домашние сети, в которых могут отсутствовать надежные меры безопасности, применяемые в офисных средах. Слабые пароли Wi-Fi, устаревшие маршрутизаторы и отсутствие защиты брандмауэром могут сделать эти сети уязвимыми для атак. Киберпреступники могут использовать эти уязвимости для перехвата конфиденциальных данных, передаваемых между удаленными сотрудниками и серверами компании.

3. Фишинговые атаки и атаки социальной инженерии

Фишинговые атаки и атаки социальной инженерии стали более изощренными, нацеливаясь на удаленных работников с помощью вводящих

в заблуждение электронных писем, поддельных веб-сайтов и вредоносных вложений. Отсутствие личного общения в удаленных настройках затрудняет сотрудникам проверку подлинности запросов, увеличивая вероятность стать жертвой такой тактики.

4. Утечка данных и несанкционированный доступ

Децентрализованный характер удаленной работы может затруднить мониторинг и контроль за перемещением конфиденциальных данных. Без надлежащих мер предосторожности сотрудники могут непреднамеренно передавать конфиденциальную информацию по незащищенным каналам, облачным хранилищам или личным учетным записям электронной почты. Кроме того, средства удаленного доступа и слабые методы аутентификации могут предоставить неавторизованным лицам доступ к критически важным системам.

2. Снижение рисков безопасности удаленной работы

Несмотря на проблемы безопасности, связанные с удаленной работой, существует несколько стратегий, которые организации могут реализовать для повышения своей кибербезопасности:

1. Надежная защита конечных точек:

Обеспечьте использование устройств, предоставляемых компанией, или примените строгие меры безопасности на личных устройствах, получающих доступ к ресурсам компании.

Разверните программное обеспечение для защиты конечных точек, включающее антивирус, защиту от вредоносных программ и шифрование устройств.

2. Защищенная сетевая инфраструктура:

Предоставьте рекомендации по защите домашних сетей, включая надежные пароли Wi-Fi, регулярные обновления маршрутизатора и включение защиты брандмауэром.

Поощряйте использование виртуальных частных сетей (VPN) для шифрования данных, передаваемых по сетям общего пользования.

3. Обучение и информированность сотрудников:

Информируйте удаленных работников о новейших методах фишинга и социальной инженерии, подчеркивая важность проверки запросов перед передачей конфиденциальной информации.

Проводите регулярные тренинги по кибербезопасности, чтобы информировать сотрудников о возникающих угрозах.

4. Многофакторная аутентификация (MFA):

Внедрите MFA для удаленного доступа к системам и ресурсам компании, чтобы добавить дополнительный уровень защиты от несанкционированного доступа.

5. Защита данных и шифрование:

Применяйте политики защиты данных, которые определяют, как следует обрабатывать, хранить и передавать конфиденциальную информацию.

Используйте шифрование для сохраняемых и передаваемых данных, чтобы предотвратить несанкционированный доступ.

3. Вывод

Удаленная работа никуда не денется, и ее преимущества неоспоримы. Однако организации должны активно устранять нарушения безопасности и связанные с ними проблемы. Применяя комплексный подход, включающий надежную защиту конечных точек, сетевые средства защиты, обучение сотрудников, многофакторную аутентификацию и меры по защите данных, предприятия могут гарантировать, что удаленная работа остается продуктивным и безопасным способом ведения операций в эпоху цифровых технологий.

Список литературы

1. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании.— 2021. — С. 409–414.
2. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи.— 2021.— № . 1 (19). — С. 57–67.
3. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные пробле-

мы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 563–568.
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. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017).— 2017. — С. 343–348.

УДК 004.056

Что нужно знать о SSL-сертификатах для веб-сайтов

Пронин Александр Дмитриевич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья рассматривает ключевые аспекты функционирования SSL-сертификатов в контексте шифрования данных и обеспечения доверия в онлайн-среде. Статья выделяет две основные функции SSL-сертификатов: шифрование текстовой информации для защиты от несанкционированного доступа и установление доверия, предоставляемое символом блокировки SSL в браузере. Статья также обсуждает правила и положения, установленные Форумом центров сертификации и браузеров (CA/Browser), который объединяет глобальные и региональные центры сертификации, поставщиков программного обеспечения и других приложений.*

***Abstract**: The article examines key aspects of SSL certificates in the context of data encryption and trust in the online environment. The article highlights the two main functions of SSL certificates: encrypting textual information to protect against unauthorized access and establishing the trust provided by the SSL lock symbol in the browser. The article also discusses the rules and regulations established by the CA/Browser Forum, which brings global and regional certificate authorities, software vendors, and other application providers together.*

***Ключевые слова**: SSL, шифрование данных, доверие в онлайн-среде, SSL-сертификаты, блокировка SSL в браузере, форум центров сертификации и браузеров, максимальный срок действия сертификата, типы шифрования SSL, доверительное рукопожатие.*

***Keywords**: SSL, data encryption, trust in online environment, SSL certificates, SSL blocking in browser, certificate authority and browser forum, maximum certificate validity, SSL encryption types, trust handshake.*

Роль ИТ-специалистов в использовании SSL

Организации различаются по тому, кто покупает и управляет сертификатами SSL для веб-сайтов, и эти различия могут привести к путанице и ошибкам. ИТ-отдел часто запрашивает сертификаты SSL, но лицо, заказывающее SSL, может быть сотрудником отдела закупок, маркетинга/бренд-менеджмента, юриста или ИТ-специалиста. В идеале SSL-сертификаты управляются одной централизованной группой внутри организации, а не различными ИТ-специалистами, заказывающими специальные сертификаты, что может привести к угрозам безопасности. Использование системы продажи билетов или документированного внутреннего процесса может гарантировать, что сертификаты SSL запрашиваются и приобретаются организованным образом.

ИТ-специалисты часто участвуют в отслеживании уведомлений об истечении срока действия SSL, чтобы предотвратить сбои в покрытии сертификата. Организациям следует создать центральный адрес электронной почты для распространения, на который будут отправляться все уведомления об истечении срока действия, и этот адрес электронной почты должен постоянно отслеживаться, даже когда отдельные члены команды уходят в отпуск, получают повышение или покидают компанию.

Как SSL шифрует данные и укрепляет доверие

Сертификаты SSL реализуют два механизма. Во-первых, они шифруют любой набираемый текст, чтобы третьи лица не могли получить доступ

к содержимому в текстовом формате после его отправки. Во-вторых, SSL обеспечивают доверие. Наличие значка блокировки SSL в браузере показывает, что на веб-сайте предусмотрено шифрование. Пока есть значок замка, сайт считается безопасным. Без SSL и значка блокировки на веб-сайте пользователи отправляют свой необработанный текст в эфир, чтобы его мог кто-нибудь перехватить.

ИТ-специалистам, отвечающим за безопасность любого веб-сайта, ориентированного на потребителя, следует рассмотреть возможность наличия сертификата SSL, даже если пользователям негде вводить контент. Даже если шифрование не требуется, компания захочет выглядеть более профессионально и показать потребителям, что ей можно доверять.

Правила и положения для SSL

Форум центров сертификации и браузеров (CA/Browser или CAB) определяет правила для SSL. Форум CAB, организованный в 2005 году, не является государственным учреждением. Вместо этого это добровольная группа глобальных и региональных центров сертификации (CA), поставщиков программного обеспечения для интернет-браузеров и поставщиков других приложений, которые используют цифровые сертификаты X.509 v.3 для SSL, Transport Layer Security (TLS), подписи кода. и безопасные/многофункциональные расширения почты Интернета (S/MIME).

Многие правила и требования CAB Forum исходят от Google и его браузера Chrome, которые доминируют в мире браузеров и имеют огромное влияние. Google продвигает инновации и хочет внедрить дополнительные меры безопасности, такие как сертификаты SSL, действительные в течение все более короткого периода времени. Таким образом, если хакеры попытаются взломать шифрование сертификата, у них будет меньше времени на это. В настоящее время максимальный срок действия сертификата составляет 396 дней, но Google хочет сократить его до меньшего количества дней, чтобы предотвратить злоумышленников.

SSL-шифрование и проверка

SSL имеют несколько типов шифрования. Три различных типа проверки сертификатов включают в себя:

- Domain Vetted (DV) — шифрование базового уровня, подходящее для защиты внутренних коммуникаций через интрасеть/портал и VPN.
- Организация проверена (OV) — шифрование среднего уровня, подходящее для сайтов электронной коммерции.
- Расширенная проверка (EV) — шифрование самого высокого уровня, подходящее для банков или финансовых компаний. Центры сертификации придерживаются высоких стандартов CAB Forum и могут потерять свои сертификаты, если они нарушают правила или не соответствуют минимальным требованиям.

Поддерживая «рукопожатие доверия»

«Доверительное рукопожатие» относится к аутентификации, которую отвечающему серверу назначил владелец сертификата. Это рукопожатие начинается с корневого сервера, который подключается к форуму CAB, а затем доходит до сервера организации, на котором размещен веб-сайт. Рукопожатие доверия работает следующим образом:

1. Браузер или сервер пытается подключиться к веб-серверу веб-сайта, защищенному сертификатом SSL.
2. Затем браузер/сервер запрашивает веб-сервер идентифицировать себя.
3. Веб-сервер идентифицирует себя, отправляя браузеру/серверу свой SSL-сертификат.
4. Наконец, браузер/сервер проверяет, доверяет ли он сертификату SSL.

Для этого соединения «рукопожатие доверия» существует закрытый ключ, который хранится на сервере компании. Этот закрытый ключ никогда не следует передавать по электронной почте; он должен храниться только на сервере, обслуживающем сайт. Именно так потребитель узнает, что веб-сайт безопасен, поскольку все необходимые части подключаются друг к другу и существуют промежуточные сертификаты, которые подключаются к корневому серверу. На ИТ-отдел может быть возложена

ответственность за сертификаты, что может включать заказ, установку, управление промежуточными сертификатами, подключающими сайт к «доверительному подтверждению», а также управление сроком действия и заменой каждого сертификата.

В эту динамичную эпоху сертификаты SSL часто меняются, и соединения могут быть разорваны. Центры сертификации находятся посередине, и путь ведет к форуму CAB, где эти корневые серверы соединяются с браузерами. Убедитесь, что сертификат SSL подключается в нужных точках, чтобы обеспечить безопасность работы пользователя.

Заручиться помощью регистраторов

Регистраторы могут предоставить инструменты и ресурсы, которые помогут корпоративным ИТ-отделам и другим отделам с предложениями SSL и регистрацией доменов. Например, назначенный компанией менеджер по работе с клиентами в регистраторе может помочь проверить SSL, а также отслеживать и решать связанные с этим проблемы. ИТ-специалисты, начинающие работать в сфере доменов/SSL, могут воспользоваться ресурсами регистратора для запроса, заказа и управления SSL.

Программные продукты, предоставляемые регистраторами или независимыми поставщиками технологий, также могут помочь организациям эффективно приобретать, отслеживать и управлять сертификатами SSL. Чрезвычайно полезно просматривать все данные о портфеле доменов в одном центральном интерфейсе и гарантировать, что сроки не будут сорваны, а сайты не останутся незащищенными из-за истечения срока действия или проблем с безопасностью.

Заключение

Многие организации уже требуют от своих ИТ-специалистов хорошо разбираться в SSL для веб-сайтов, а другие готовы последовать этому примеру. Понимание сертификатов SSL является критически важной частью управления безопасностью и снижения рисков, а также имеет значение для юридических, маркетинговых и брендинговых вопросов. Поскольку

на карту поставлено так много, следует рассмотреть возможность интеграции сертификатов SSL в пресловутую рулевую рубку ИТ.

Список литературы

1. Смирнов А. «Защита информации от несанкционированного доступа». Санкт-Петербург: БХВ-Петербург, 2017.
2. Соколов И. «Сетевая безопасность: архитектура и программирование». Москва: ДМК Пресс, 2018.
3. Шнайдер В. «Безопасность Linux. Руководство администратора». Санкт-Петербург: Питер, 2016.
4. Гибсон Д. «Хакеры: герои и злодеи». Москва: Эксмо, 2019.
5. Мартин Э. «Криптография и безопасность сетей: принципы и практика». Москва: Вильямс, 2014.
6. Росс А. «Безопасность в сетях TCP/IP». Москва: ДМК Пресс, 2017.
7. Столл К. «Хакеры и хранилище тайн». Москва: АСТ, 2018.
8. Гарвин П., Кинг Д., Стрикленд Ш. «Сетевая безопасность: анализ угроз и моделирование». Санкт-Петербург: Питер, 2015.
9. Шнайдер В., Карек Д. «Практика хакинга и безопасности в сетях». Москва: Вильямс, 2019.
10. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
11. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции» Национальная безопасность России: актуальные аспекты» ГНИИ» Нацразвитие». Июль 2018.— 2018. — С. 31–35.
12. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных / Региональная информатика и информационная безопасность.— 2020. — С. 260–262.
13. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 270–275.

14. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 406–411.

УДК 004.056

Информационная безопасность в условиях атак с использованием социальной инженерии

Нечипуровский Дмитрий Игоревич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Научный руководитель **Гельфанд Артем Максимович**

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Атаки с использованием социальной инженерии стали обычным явлением на предприятиях на протяжении многих лет. Несмотря на то, что все более строгие меры безопасности разрабатываются, продвигаются и внедряются, количество нарушений безопасности продолжает расти. Это может быть связано с тем, что киберпреступники часто нацеливаются на слабую и простую точку доступа — пользователя. Ни одна проблема безопасности не может возникнуть, если нет слабости, которой могут воспользоваться киберпреступники. Нарушения безопасности наносят значительный ущерб организациям в различных отраслях из-за снижения доверия клиентов. В данной статье рассматриваются понятие социальной инженерии, какие существуют виды атак и какие рекомендации лучше предпринять для предотвращения атак с использованием социальной инженерии.*

***Abstract**: Social engineering attacks have become commonplace in enterprises over the years. Although increasingly stringent security measures are being developed, promoted and implemented, security breaches continue to increase. This can be attributed to the fact that cybercriminals often target a weak and simple access point — the user. No security problem can occur unless there is a weakness that cybercriminals can exploit. Security breaches cause sig-*

nificant damage to organizations in various industries due to decreased customer trust. This paper discusses the concept of social engineering, what types of attacks exist and what are the best recommendations to prevent social engineering attacks.

***Ключевые слова**: социальная инженерия, виды социальной инженерии, черты атак социальной инженерии, фишинговые атаки.*

***Keywords**: social engineering, types of social engineering, features of social engineering attacks, phishing attacks.*

Социальная инженерия уже некоторое время большой угрозой безопасности. Она обсуждается специалистами по информационной безопасности. Но не все в полной мере понимают возможную угрозу, которую она представляет, и насколько опасной может быть. Типы информации, которую ищут преступники, могут различаться, но, когда целью становятся отдельные лица, преступники обычно пытаются обманом заставить вас передать им ваши пароли банковские данные, или получить доступ к вашему компьютеру для тайной установки вредоносного ПО, которое предоставит им доступ к вашим паролям и банковской информации, а также даст им контроль над вашим компьютером.

При атаке с использованием социальной инженерии злоумышленник использует человеческое взаимодействие (социальные навыки) для получения или компрометации информации об организации или ее компьютерных системах. Злоумышленник может казаться непритязательным и респектабельным, возможно, выдавая себя за нового сотрудника, ремонтника или исследователя и даже предлагая учетные данные для подтверждения своей личности. Однако, задавая вопросы, он или она может собрать достаточно информации, чтобы проникнуть в сеть организации. Если злоумышленник не может собрать достаточно информации из одного источника, он или она может связаться с другим источником в той же организации и полагаться на информацию из первого источника, чтобы повысить свой авторитет.

Преступники используют тактику социальной инженерии, потому что обычно легче воспользоваться вашей естественной склонностью к доверию, чем находить способы взлома вашего программного обеспечения.

Например, гораздо проще обмануть кого-либо, заставив сообщить вам свой пароль, чем пытаться взломать его пароль (если только пароль действительно слабый).

Для хакеров социальная инженерия, вероятно, является самым простым и эффективным способом взлома протоколов безопасности. Развитие интернета дало людям очень мощные возможности, поскольку устройства соединяются между собой, не обращая внимания на расстояния. Это дало людям прогресс в общении и взаимодействии, однако создало лазейки, которые могут привести к нарушению личной информации и конфиденциальности.

Атаки социальной инженерии остаются специализированным видом кибератак, которые в значительной степени зависят от взаимодействия людей и часто включают психологические манипуляции, которые заставляют людей совершать ошибки в системе безопасности или передавать конфиденциальную информацию. Несмотря на широкое использование, термин «атаки социальной инженерии» во многих отношениях описывает очень узкие черты.

Вот некоторые ключевые черты атак социальной инженерии:

- Социальные инженеры используют в своих интересах слабые стороны людей, такие черты характера, как страх, любопытство или даже жадность, чтобы играть со своей добычей. Используют также доверие и готовность быть полезными.
- Социальным инженерам потребуется время, чтобы многократно исследовать свои цели, чтобы сделать атаки лично привлекательными и их было труднее обнаружить или избежать.
- Социальные инженеры часто могут пытаться создать ощущение срочности, чтобы подтолкнуть свои цели к быстрым, но обреченным на неудачу действиям. Лучше всего этого можно достичь, представив ситуацию как надвигающийся кризис, требующий быстрых действий.
- Использование знакомых каналов коммуникации. В большинстве случаев социальные инженеры часто могут охотиться на своих жертв, используя знакомые каналы коммуникации, например, через почту, телефонные звонки или даже социальные сети. Это дает им шанс и пространство для того, чтобы быть каким-то образом предсказуемыми, и, таким образом, их атака менее подозрительна и вполне правдоподобна.

- Они запрашивают личную конфиденциальную информацию, такую как пароли, номера кредитных карт или номера социального страхования. Это возможно, выдавая себя за источники, которые активно взаимодействуют с пользователем, такие как банки или правительства.

Существуют различные типы социальной инженерии:

Фишинг — это наиболее распространенный тип социальной инженерии. Злоумышленники могут создать поддельный веб-сайт или портал поддержки известной компании и отправить ссылку на него адресатам по электронной почте или в социальных сетях. Человек, который не знает о реальном злоумышленнике, в конечном итоге может раскрыть свою личную информацию и даже данные своей кредитной карты.

Чтобы избежать фишинговых писем, следует использовать фильтры нежелательной почты в своих учетных записях электронной почты. В настоящее время большинство почтовых провайдеров делают это по умолчанию. Также лучше не открывать электронные письма, которые приходят из ненадежных источников.

Вишинг — это метод социальной инженерии, при котором злоумышленники могут быть где угодно в Интернете, но часто предпочитают использовать старомодный способ — телефонные звонки. Они могут имитировать систему интерактивного голосового ответа компании и привязать ее к бесплатному номеру. Затем они обманом заставляют людей звонить по этому номеру и вводить свои данные.

Претекстинг — это тип атаки, при котором злоумышленник пытается убедить жертву раскрыть конфи денциальную информацию или отправить ему деньги, придумывая убедительную историю. Злоумышленник обычно выдает себя за друга, члена семьи, коллегу или начальника, поэтому жертва более склонна предоставить ему конфиденциальную информацию. Такие атаки могут происходить посредством телефонных звонков, текстовых сообщений, электронных писем или личных встреч.

Черви — это еще один тип атаки, при котором киберпреступник пытается привлечь внимание пользователя к ссылке или зараженному файлу, а затем заставить пользователя нажать на него. Примеры таких атак включают:

Червь LoveLetter, который в 2000 году перегрузил почтовые серверы многих компаний. Жертвы получали электронное письмо, в котором им

предлагалось открыть прикрепленное любовное письмо. Открыв прикрепленный файл, червь скопировал себя во все контакты в адресной книге жертвы. Этот червь до сих пор считается одним из самых разрушительх с точки зрения финансового ущерба, который он нанес.

Почтовый червь Mydoom, появившийся в Интернете в январе 2004 года, использовал тексты, имитирующие технические сообщения, выдаваемые почтовым сервером. Червь Swen выдавал себя за сообщение, отправленное отMicrosoft. В нем утверждалось, что вложение является патчем, который устранит уязвимости Windows. Неудивительно, что многие люди восприняли это заявление всерьез и попытались установить фальшивый патч безопасности, хотя на самом деле это был червь.

Фарминг. При этом типе онлайн-мошенничества киберпреступник устанавливает на компьютер или сервер вредоносный код, который автоматически направляет пользователя на поддельный веб-сайт, где пользователь может быть обманут, чтобы предоставить личную информацию.

Есть следующие рекомендации, которые могут помочь повысить вашу бдительность в отношении взломов социальной инженерией:

- Не открывать электронные письма и вложения из подозрительных источников. Если вы не знаете отправителя, о котором идет речь, вам не нужно отвечать на электронное письмо. Даже если вы их знаете и у вас возникли подозрения по поводу их сообщений, перепроверьте и подтвердите новости из других источников, например, по телефону или непосредственно с сайта поставщика услуг. Помните, что адреса электронной почты постоянно подделываются; даже электронное письмо, предположительно пришедшее из надежного источника, на самом деле может быть инициировано злоумышленником.
- Использовать многофакторную аутентификацию. Одной из наиболее ценных частей информации, которую ищут злоумышленники, являются учетные данные пользователя. Использование многофакторной аутентификации помогает обеспечить защиту вашей учетной записи в случае взлома системы.
- Быть осторожными с заманчивыми предложениями. Если предложение звучит слишком заманчиво, стоит быть бдительными, прежде чем принимать его как факт.

- Обновлять свое антивирусное программное обеспечение. Необходимо убедиться, что включены автоматические обновления. Периодически проверять, были ли применены обновления, сканировать свою систему на предмет возможных заражений.

Киберпреступники постоянно ищут новые методы обмана пользователей, стремясь украсть их средства и конфиденциальную информацию, поэтому очень важно просвещать себя и окружающих. Интернет предоставляет убежище для этих видов мошенничества. Стоит быть осторожными и бдительными, чтобы не попасться в ловушки социальной инженерии.

Список литературы

1. Митник К. и Саймон В. Л. (2002). «Искусство обмана: контроль над человеческим элементом безопасности». Уайли.
2. Хаднаги С. (2010). «Социальная инженерия: искусство взлома человеком». Уайли.
3. Вакка, Дж. Р. (2012). «Руководство по компьютерной и информационной безопасности». Морган Кауфманн.
4. Финкл Дж. и Вильянуэва М. (2015). «Социальная инженерия: наука о взломе человека». Джон Уайли и сыновья.
5. Босворт С. и Кабаи М. Э. (2002). «Руководство по компьютерной безопасности». Уайли.
6. Стиннон Р. (2008). «Кибервойна будет: как переход к сетецентрической войне проложил путь к кибервойне». IT-Harvest Press.
7. Каппелли, Д. М., Мур, А. П., Тржециак, Р. Ф. и Шимолл, Т. Дж. (2012). «Руководство по инсайдерской угрозе CERT: как предотвращать, обнаруживать преступления в области информационных технологий (кражи, саботаж, мошенничество) и реагировать на них». Эддисон — профессионал Wesley.
8. Коул Э., Круз Р. Л. и Конли Дж. (2015). «Социальная инженерия в ИТ-безопасности: инструменты, тактика и методы». Специалист McGraw Hill.
9. Шнайер, Б. (2000). «Секреты и ложь: цифровая безопасность в сетевом мире». Уайли.

10. Хаднаги, К., & Финчер, М. (2011). «Разоблачение социального инженера: фактор безопасности человека». Уайли.
11. Шемякин С. Н. и др. Теоретическая оценка использования математических методов прогнозирования загрузки виртуальной инфраструктуры //Наукоемкие технологии в космических исследованиях Земли.— 2021. — Т. 13.— № . 4. — С. 66–75.
12. 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.
13. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 4. — С. 72–76.
14. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 570–573.
15. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядрав системах специального назначения //I-methods.— 2020. — Т. 12.— № . 3. — С. 2.

УДК 004.056

Киберугрозы в искусственном интеллекте

Нечипуровский Дмитрий Игоревич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Научный руководитель **Гельфанд Артем Максимович**

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В статье рассматриваются возможные кибер-угрозы в системе искусственного интеллекта. С ростом кибер-угроз и угроз безопасности в цифровой среде важность роли искусственного интеллекта в кибербезопасности становится все более очевидной. Эффективное использование алгоритмов машинного обучения, автоматизация обнаружения и реагирования на кибератаки, решение этических вопросов, связанных с использованием искусственного интеллекта в этой сфере, являются ключевыми аспектами современной кибербезопасности. В данной статье рассматриваются кибербезопасность, определяются преимущества и угрозы в искусственном интеллекте, а также обсуждаются этические аспекты этого вопроса.*

***Abstract**: This article discusses the possible cyber threats in artificial intelligence system. With the rise of cyber threats and security threats in the digital environment, the importance of the role of artificial intelligence in cybersecurity is becoming more and more evident. Effective use of machine learning algorithms, automation of detection and response to cyberattacks, and addressing ethical issues related to the use of artificial intelligence in this field are key aspects of modern cybersecurity. This paper examines cybersecurity, identifies the benefits and threats in artificial intelligence, and discusses the ethical aspects of this issue.*

***Ключевые слова**: искусственный интеллект, кибер-угрозы в искусственном интеллекте, кибератаки, алгоритмы на основе искусственного интеллекта.*

***Keywords**: artificial intelligence, cyber threats in artificial intelligence, cyber attacks, algorithms based on artificial intelligence.*

Искусственный интеллект позволяет машинам учиться на опыте, приспосабливаться к новым входным данным и выполнять задачи, подоб-

ные человеческим. Большинство примеров искусственного интеллекта, о которых мы слышим сегодня — от компьютеров для игры в шахматы до самоуправляемых автомобилей — в значительной степени зависят от глубокого обучения и обработки естественного языка.

Поскольку технология искусственного интеллекта продолжает развиваться, вполне вероятно, что в будущем возможны более изощренные и сложные кибератаки с использованием искусственного интеллекта. Например, генеративно-состязательная сеть (GAN), класс платформ ML, может использоваться для создания «глубоких подделок» путем замены или манипулирования лицами или голосами на изображении или видео. Алгоритмы на основе искусственного интеллекта также могут подготавливать убедительные фишинговые электронные письма. Искусственный интеллект также можно использовать для повышения эффективности вредоносных программ. Вредоносное ПО, управляемое искусственным интеллектом, может использовать методы обучения с подкреплением, чтобы совершенствоваться и проводить еще более успешные атаки. Злоумышленники могут использовать обучающие данные для создания «черного хода» в алгоритме искусственного интеллекта. Злоумышленники также могут использовать искусственный интеллект, чтобы решить, какую уязвимость, скорее всего, стоит использовать. Это всего лишь несколько примеров кибератак с использованием искусственного интеллекта, которые уже вызывают серьезную озабоченность.

Атака искусственного интеллекта (атака ИИ) — это целенаправленное манипулирование системой искусственного интеллекта с конечной целью вызвать ее сбои. В отличие от традиционных кибератак, которые вызваны «ошибками» или человеческими ошибками в коде, атаки искусственного интеллекта возможны из-за ограничений, присущих базовым алгоритмам искусственного интеллекта, которые в настоящее время не могут быть исправлены. Кроме того, атаки ИИ фундаментально расширяют набор сущностей, которые могут быть использованы для выполнения кибератак. Впервые физические объекты могут быть использованы для кибератак (например, атака ИИ может превратить знак «Стоп» в зеленый свет в глазах беспилотного автомобиля, просто поместив несколько кусков ленты на сам знак «Стоп»). Данные также могут быть использованы в качестве

оружия новыми способами с помощью этих атак, что потребует изменений в способах сбора, хранения и использования данных.

Эти атаки могут принимать различные формы, которые наносят удар по различным слабым местам в базовых алгоритмах:

1. Атаки на ввод: манипулирование тем, что вводится в систему искусственного интеллекта, с целью изменения выходных данных системы для достижения цели злоумышленника. Поскольку по своей сути каждая система искусственного интеллекта является простой машиной — она принимает входные данные, выполняет некоторые вычисления и возвращает выходные данные, — манипулирование входными данными позволяет злоумышленникам влиять на выходные данные системы.
2. Отравление атак: повреждение процесса, в ходе которого создается система искусственного интеллекта, таким образом, что результирующая система работает со сбоями так, как хочет злоумышленник. Одним из прямых способов выполнить атаку отравления является повреждение данных, используемых во время этого процесса. Это связано с тем, что современные методы машинного обучения, лежащие в основе искусственного интеллекта, работают, «обучаясь» тому, как выполнять задачу, но они «учатся» из одного источника и только из одного источника: данных. Данные — это вода, пища, воздух и настоящая любовь. Отравить данные, отравить систему искусственного интеллекта. Отравление также может поставить под угрозу сам процесс обучения.

Поскольку системы искусственного интеллекта интегрируются в критически важные коммерческие и военные приложения, эти атаки могут иметь серьезные последствия, вплоть до жизни и смерти. Атаки искусственного интеллекта могут использоваться несколькими способами для достижения вредоносной конечной цели:

1. Нанести ущерб: злоумышленник хочет нанести ущерб, вызвав сбой в работе системы искусственного интеллекта. В качестве примера можно привести атаку, направленную на то, чтобы заставить автономное транспортное средство игнорировать знаки остановки. Атакуя систему искусственного интеллекта таким образом, что она неправильно распознает знак «Стоп» как другой знак или символ. Злоумышленник может заста-

вить автономное транспортное средство проигнорировать знак «Стоп» и врезаться в другие транспортные средства и пешеходов.

2. Что-нибудь скрыть: злоумышленник хочет избежать обнаружения системой искусственного интеллекта. В качестве примера можно привести атаку, направленную на то, чтобы вызвать сбои в работе контент-фильтра, которому поручено блокировать размещение террористической пропаганды в социальной сети, что позволяет материалу беспрепятственно распространяться.
3. Снижение веры в систему: злоумышленник хочет, чтобы оператор потерял веру в систему искусственного интеллекта, что в итоге приведет к отключению системы. В качестве примера можно привести атаку, в результате которой автоматическая сигнализация системы безопасности ошибочно классифицировала обычные события как угрозы безопасности, вызывая шквал ложных срабатываний, которые могут привести к отключению системы. Например, атака на систему видеонаблюдения с целью классифицировать проходящую мимо бездомную кошку или упавшее дерево как угрозу безопасности может привести к отключению системы безопасности, что позволит реальной угрозе избежать обнаружения.

Атаки на ввод приводят к сбоям в работе системы искусственного интеллекта, изменяя входные данные, подаваемые в систему. Это делается путем добавления «шаблона атаки» к входным данным, например, внесения небольших изменений в цифровую фотографию, загружаемую в социальную сеть.

В заключение стоит отметить, что атаки ввода не требуют, чтобы злоумышленник повредил систему искусственного интеллекта и атаковал ее. Полностью современные системы искусственного интеллекта, которые отличаются высокой точностью и никогда не подвергались компрометации целостности, наборов данных или алгоритмов, по-прежнему уязвимы для атак ввода. И в отличие от других кибератак, сама атака не всегда использует компьютер. Эти атаки особенно опасны, потому что паттерны атак не обязательно должны быть заметными и даже могут быть совершенно незаметными. Злоумышленники могут изменять лишь небольшой аспект входных данных таким образом, чтобы разрушить шаблоны, ранее изученные моделью. Для атак на физические объекты, которые должны быть зафик-

сированы датчиком или камерой перед передачей в систему искусственного интеллекта, злоумышленники могут создавать небольшие изменения, которые достаточно велики, чтобы их можно было зафиксировать датчиком. Для атак на цифровые объекты, которые подаются непосредственно в систему искусственного интеллекта, такие как изображение, загруженное в социальную сеть, паттерны атак могут быть незаметны для человеческого глаза. Это связано с тем, что в этой полностью цифровой среде изменения могут происходить на уровне отдельных пикселей, создавая изменения, которые настолько малы, что буквально невидимы для человеческого глаза.

Список литературы

1. Гудфеллоу, И., Бенгио, Ю., и Курвиль, А. (2016). Глубокое обучение. Издательство Массачусетского технологического института.
2. Рассел, С. Дж., и Норвиг, П. (2020). Искусственный интеллект: современный подход. Пирсон.
3. Шалев-Шварц С. И Бен-Дэвид С. (2014). Понимание машинного обучения: от теории к алгоритмам. Издательство Кембриджского университета.
4. Брандейдж, М., Авин, С., Кларк, Дж., Таннер, Х., Экерсли, П., Гарфанкел, Б., ... & Цейтцофф, Т. (2018). Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий. препринт архива arXiv: 1802.07228.
5. Амодей В., Олах С., Стейнхардт О., Кристиано Р., Шульман О. и Ман В. (2016). Конкретные проблемы безопасности ИИ. архивный препринт arXiv: 1606.06565.
6. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 262–266.
7. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки.— 2018.— № . 8. — С. 91–97.

8. 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.
9. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
10. 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.

УДК 004.056

Основные угрозы и вызовы, с которыми сталкиваются предприятия в цифровой экономике

Нечипуровский Дмитрий Игоревич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Научный руководитель **Гельфанд Артем Максимович**

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В статье рассматриваются основные угрозы и вызовы, с которыми сталкиваются предприятия в условиях цифровой экономики. Обсуждаются такие ключевые аспекты, как кибербезопасность, технологические инновации, регулирование и соответствие, защита данных и приватность, цифровое неравенство и угрозы для инфраструктуры. Анализируются факторы, влияющие на конкурентоспособность предприятий и необходимость их адаптации к быстро меняющимся условиям цифро-*

вой среды. Полученные выводы могут служить основой для разработки стратегий управления рисками и обеспечения устойчивого развития в цифровом мире.

***Abstract**: This article examines the main threats and challenges that businesses face in the digital economy. Such key aspects as cybersecurity, technological innovation, regulation and compliance, data protection and privacy, digital inequality and threats to infrastructure are discussed. Factors affecting the competitiveness of enterprises and the need for them to adapt to the rapidly changing conditions of the digital environment are analyzed. The findings can serve as a basis for developing strategies for risk management and sustainable development in the digital world.*

***Ключевые слова**: цифровая экономика, угрозы, вызовы, предприятия, кибербезопасность, технологические инновации, регулирование, соответствие, данные, приватность, цифровое неравенство, инфраструктура, конфиденциальность, кибератаки.*

***Keywords**: digital economy, threats, challenges, enterprises, cybersecurity, technological innovation, regulation, compliance, data, privacy, digital inequality, infrastructure, privacy, cyber-attacks.*

В эпоху цифровой революции предприятия сталкиваются с непрерывно возрастающими угрозами и вызовами, которые проникают в каждый аспект их деятельности. Риск кибератак значительно возрос в результате стремительной оцифровки корпораций и правительств, что требует внимания лидеров и политиков по всему миру. Кибер угрозы — это широкая категория незаконных действий, предпринимаемых людьми, организациями или даже национальными государствами с целью компрометации компьютерных систем, сетей и данных. Эти опасности могут принимать самые разные формы, такие как отключение критически важной инфраструктуры, кража интеллектуальной собственности, утечка данных и атаки программ-вымогателей. Такие атаки могут осуществляться по целому ряду причин, включая денежную выгоду, геополитические цели или даже акты активности. Воздействие кибер угроз на экономику носит широкомасштабный и значительный характер. Прежде всего, кибератаки на организации приводят к огромному финансовому ущербу. Особенно для малых и средних предприятий (МСП), которым может не хватать потенциала для быстрого восстановления, затраты, связанные с утечками данных, операциями по исправлению и репутационным ущербом, могут быть

огромными. Согласно исследованию Института Понемон, средняя стоимость утечки данных в 2020 году, как ожидалось, составило 3,86 миллиона долларов, что подчеркивает значительные финансовые последствия, которые кибератаки могут оказать на предприятия.

Цифровая экономика, хотя и предлагает несметные возможности для роста и инноваций, также приносит со собой новые уязвимости и риски, требующие постоянного внимания и адаптации.

1. Кибербезопасность

Одним из основных вызовов для предприятий в цифровой экономике является обеспечение кибербезопасности. Взломы, кибератаки и кражи данных становятся все более распространенными, угрожая конфиденциальности, целостности и доступности информации. Предприятия должны постоянно улучшать свои меры безопасности, чтобы защитить себя от потенциальных угроз, таких как вредоносные программы, фишинговые атаки и DDoS-атаки.

Поскольку социальная инженерия, такая как фишинг, является основным способом получения киберпреступниками учетных данных для доступа, игнорирование человеческого фактора при разработке системы кибербезопасности является фатальным.

Организации, особенно те, которые являются частью критически важной инфраструктуры, должны повышать осведомленность о проблемах кибербезопасности и важности информационной безопасности. Крайне важно, чтобы у каждого предприятия были задокументированные политики информационной безопасности и чтобы сотрудники знали, кому сообщать о проблемах кибербезопасности при их возникновении.

Лучшие практики кибербезопасности, которые каждый сотрудник бизнеса должен знать и внедрять, включают:

- Политика организации в отношении социальной инженерии
- Процедуры защиты данных для защиты данных кредитной карты и предотвращения кражи личных данных
- Соблюдение правил безопасности паролей
- Многофакторная аутентификация

- Распознавание фишинговых атак
- Обновление систем и программного обеспечения
- Внедрение базовой сетевой безопасности

Образовательные и просветительские кампании также могут способствовать формированию культуры кибербезопасности, предоставляя людям возможность вести себя более безопасно в Интернете. Продвижение культуры кибер грамотности, в которой люди осознают опасности и принимают соответствующие меры безопасности, может значительно минимизировать уязвимость и повысить экономическую безопасность.

2. Цифровые трансформации и технологические инновации

Быстрый темп развития технологий в цифровой экономике представляет собой как возможность, так и вызов для предприятий. С одной стороны, цифровые трансформации и инновации могут повысить эффективность и конкурентоспособность предприятий. С другой стороны, неспособность адаптироваться к новым технологиям или использовать их эффективно может оставить предприятия на заднем плане. Ускорение проектов цифровой трансформации усилило угрозы и вызовы, с которыми сталкиваются компании. Сложность навигации и разрозненный менталитет по-прежнему возглавляют список проблем для большинства организаций. Применение управления изменениями с учетом сложностей внедрения также остается в центре внимания. Все это связано с созданием культуры непрерывного обучения. Повышение квалификации или переподготовка персонала важно для непрерывного процесса успешной трансформации бизнеса с меньшим количеством сбоев на этом пути.

Как и в предыдущие годы, многие компании снижают операционную неэффективность, обращаясь к устаревшим ИТ-системам. Они также стремятся преобразовать бизнес-процессы и расширить цифровые инновации. Это отражает настоятельную необходимость повышения гибкости и отказоустойчивости с помощью стратегий цифровой трансформации.

Быстрое развитие технологий, бизнес-моделей и способов работы кардинально влияет на ее сотрудников. Трансформация приносит новые технологии, но без должного таланта для продвижения инициативы слабые

стороны становятся совершенно очевидными. Создание новых процессов работы и сотрудничества друг с другом и внешними партнерами стало важным шагом в дополнение к поиску новых кадровых резервов.

Ключевым моментом является выявление, количественная оценка и предложение программ обучения и развития, ориентированных на сотрудников. При поиске новых специалистов для выполнения критически важных ИТ-ролей, таких как инженеры-программисты, разработчики и архитекторы, 40% организаций говорят, что на заполнение этих должностей уходит шесть месяцев или больше. Это может привести к замедлению процессов трансформации. Интеграция искусственного интеллекта, автоматизации и инструментов совместной работы может устранить некоторые пробелы в навыках, но для преодоления этих проблем потребуются креативные, целостные стратегии привлечения талантов, чтобы компании могли приобретать и развивать навыки, необходимые им для формирования рабочей силы, готовой к будущему.

3. Регулирование и соответствие

В условиях быстрого технологического развития и расширения цифровой экономики регуляторы всегда пытаются приспособиться к новым вызовам. Предприятия должны соответствовать различным правилам, нормативам и стандартам, что может представлять значительные затраты и сложности. Невыполнение требований регуляторов может привести к санкциям, штрафам и утрате репутации.

4. Ответственность за данные и приватность

С увеличением объема собираемых и обрабатываемых данных предприятиям приходится сталкиваться с растущими требованиями в области защиты личной информации и соблюдения приватности пользователей. Нарушение конфиденциальности данных может привести к серьезным юридическим последствиям и утрате доверия со стороны клиентов.

Кибер риски также могут снизить доверие клиентов к онлайн-транзакциям, что замедлит экономику. В связи с ростом онлайн-сервисов и элек-

тронной коммерции люди должны чувствовать себя в безопасности при совершении покупок и раскрытии конфиденциальной информации. Доверие потребителей часто снижается в результате громких утечек данных и кибератак, что снижает онлайн-активность и может стоить компаниям денег. Инвестиции в обеспечение кибербезопасности и навыки эффективного реагирования на инциденты должны быть значительными, чтобы восстановить доверие и свести к минимуму эти экономические последствия.

5. Цифровое неравенство и угрозы для инфраструктуры

Цифровая экономика неодинаково влияет на различные отрасли и регионы, что может привести к усилению цифрового неравенства. Неоднородность социально-экономического пространства и неравномерность процесса распространения ИКТ породили проблему цифрового неравенства, или цифрового разрыва (от англ. digital divide). Под ними понимаются различия в доступе к инфраструктуре ИКТ, навыках и целях использования цифровых технологий. Выделяются три основных уровня:

1. доступ в Интернет: наличие физической инфраструктуры и доступность с точки зрения стоимости подключения и абонентской платы;
2. умение жителей пользоваться цифровыми технологиями: цифровая грамотность, компетенции, умение заказывать товары, услуги и т.д.;
3. умение жителей и предпринимателей применять Интернет для коммерческих целей: размещение онлайн-заказов, интернет-банкинг, электронная коммерция (e-commerce) и т.д. Предприятия также подвергаются угрозам в виде кибератак на критическую инфраструктуру, такую как энергетические сети или транспортные системы, что может иметь серьезные экономические и социальные последствия.

Развитие цифровых технологий становится ключевым фактором достижения целей устойчивого развития для каждой страны, сектора и региона, в том числе и для современной России.

Россия заметно улучшила свои позиции в некоторых международных цифровых рейтингах, продвигаясь по пути развития цифровой экономики и общества. Одно из последних исследований Школы Флетчера при Университете Тафтса в партнерстве с компанией Mastercard разделило страны

мира на несколько групп, поместив Россию в группу «прорывных» стран, для которых характерен и потенциал цифрового роста, и заметные темпы цифровизации. Несмотря на высокий импульс цифрового развития и значительный потенциал для роста цифровой экономик.

В заключение следует отметить, что рост кибер рисков породил совершенно новый набор проблем для экономической безопасности. Цифровая экономика находится в значительной опасности из-за финансовых потерь, потери доверия и нарушения работы важнейшей инфраструктуры, вызванных кибератаками. Для преодоления этих препятствий необходимы активные действия, командная работа и инвестиции в возможности кибербезопасности. Необходимо укреплять цифровую инфраструктуру и гарантировать более безопасное и устойчивое экономическое будущее, реализуя комплексную стратегию, охватывающую кампании и отдельных лиц. Цифровая экономика предлагает предприятиям огромные возможности для роста и развития, однако сопряжена с множеством угроз и вызовов. Предприятия должны быть готовы к постоянной адаптации и инвестированию в кибербезопасность, инновации и соответствие, чтобы успешно функционировать в этом быстро меняющемся цифровом мире.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика» РИ-2018».— 2018. — С. 149–149.
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. 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.

4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика» РИ-2018».— 2018. — С. 149–149.
5. 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.

УДК 004.056

Уязвимости безопасности блокчейна: потенциальные слабые места в технологии блокчейн и способы их устранения

Нечипуровский Дмитрий Игоревич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Научный руководитель **Гельфанд Артем Максимович**

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная статья исследует уязвимости безопасности в технологии блокчейн и предлагает способы их устранения. Рассматриваются основные слабые места, такие как 51%-ые атаки, уязвимости смарт-контрактов и атаки на приватность, и предлагаются соответствующие превентивные меры. Автор подчеркивает важность постоянного развития методов защиты и обеспечения децентрализации сети, а также необходимость тщательного тестирования и аудита смарт-контрактов. Заключение подчеркивает важность сотрудничества и постоянного обучения для обеспечения более безопасной и устойчивой среды в области блокчейн-технологий.*

***Abstract**: This paper investigates security vulnerabilities in blockchain technology and suggests ways to address them. Major weaknesses such as 51% attacks, smart contract vulnerabilities*

and privacy attacks are discussed and appropriate preventive measures are proposed. The author emphasizes the importance of continuous development of security techniques and network decentralization, as well as the need for thorough testing and auditing of smart contracts. The conclusion emphasizes the importance of collaboration and continuous learning to ensure a more secure and sustainable blockchain technology environment.

***Ключевые слова**: блокчейн, безопасность, уязвимости, 51%-ые атаки, смарт-контракты, приватность*

***Keywords**: blockchain, security, vulnerabilities, 51% attacks, smart contracts, privacy*

Уязвимости безопасности блокчейна: исследование и превентивные меры

Блокчейн, технология, лежащая в основе криптовалют и множества других инновационных решений, стала предметом широкого интереса как среди технологических энтузиастов, так и среди специалистов по информационной безопасности. Несмотря на свою стойкость к манипуляциям и отсутствие централизованного контроля, блокчейн не лишен недостатков. Уязвимости безопасности, хоть и редко, но все же возникают, и понимание этих уязвимостей становится все более важным в контексте широкого принятия технологии блокчейн. Давайте рассмотрим несколько потенциальных слабых мест в блокчейне и способы их устранения.

1. 51%-ая атака

Одной из угроз для блокчейна является атака на его консенсусный механизм. В случае с блокчейнами, работающими на принципе Proof of Work (PoW), такая атака может быть реализована в форме 51%-ой атаки, когда злоумышленник получает контроль над более чем половиной вычислительной мощности сети. Что позволяет ему создавать фальшивые транзакции и проводить двойные расходы.

Для предотвращения таких атак важно продолжать развивать методы защиты и обеспечения децентрализации сети. Это может включать в себя улучшение алгоритмов консенсуса, использование дополнительных мер безопасности, таких как проверка меритократии и создание дополнительных слоев защиты.

2. Уязвимости смарт-контрактов

Смарт-контракты, представляющие собой программные коды, которые выполняются на блокчейне при выполнении определенных условий, могут быть еще одной потенциальной точкой уязвимости. Ошибки в коде смарт-контрактов могут привести к непредвиденным последствиям, таким как утечка средств или даже взлом контракта.

Для борьбы с этой уязвимостью необходимо проводить тщательное тестирование и аудит смарт-контрактов перед их развертыванием на блокчейне. Также важно обновлять и улучшать стандарты разработки смарт-контрактов, внедрять механизмы обнаружения и автоматического исправления ошибок.

3. Атаки на приватность

Несмотря на свою прозрачность, блокчейн также сталкивается с вызовом обеспечения конфиденциальности пользователей. Информация о транзакциях, хранящаяся в блокчейне, доступна для всех участников сети, что может быть проблемой для пользователей, желающих сохранить свою анонимность.

Для решения этой проблемы могут быть применены различные методы шифрования и анонимизации, такие как смешивание транзакций или использование смарт-контрактов с нулевым разглашением данных. Например, конфиденциальные транзакции повышают конфиденциальность без ущерба для безопасности. Однако необходимо учитывать баланс между прозрачностью и конфиденциальностью, чтобы не угрожать безопасности сети.

4. Управление ключами

Слабое управление ключами может привести к несанкционированному доступу или потере средств. Лучшие практики:

- Аппаратные кошельки: Хранят приватные ключи в автономном режиме.
- Кошельки с несколькими подписями: Для транзакций требуется несколько подписей.

5. Риски, связанные с алгоритмом консенсуса

Различные алгоритмы консенсуса (например, Proof of Work, Proof of Stake) имеют разные риски. Разбирайтесь в компромиссах и делайте мудрый выбор.

6. Уязвимости цепочки поставок

Блокчейн используется для отслеживания цепочки поставок. Обеспечение целостности данных путем проверки входных данных и защиты точек доступа.

7. Оракулы и каналы передачи данных

Оракулы предоставляют внешние данные для смарт-контрактов. Убедитесь, что оракулы безопасны и заслуживают доверия, чтобы предотвратить дезинформацию.

8. Атаки на разделение сети

Если блокчейн-сеть распадается на несколько ответвлений, злоумышленники могут воспользоваться этим. Внедрите механизмы «правило самой длинной цепочки» и «контрольные точки».

9. Социальная инженерия

Существенным риском остается человеческая ошибка. Информируйте пользователей о фишинговых атаках, соблюдении правил использования паролей и методах обеспечения безопасности.

10. Неизменяемые ошибки

Неизменяемость блокчейна означает, что ошибки являются постоянными. Перед внедрением смарт-контрактов тщательно протестируйте их.

В заключение, хотя технология блокчейн обладает огромным потенциалом, понимание ее уязвимостей и внедрение надежных мер безопасности имеет решающее значение. Устраняя эти недостатки, мы можем создать более устойчивую и заслуживающую доверия экосистему блокчейна.

Список литературы

1. Шемякин С. Н. и др. Теоретическая оценка использования математических методов прогнозирования загрузки виртуальной инфраструктуры //Наукоемкие технологии в космических исследованиях Земли.— 2021. — Т. 13.— № . 4. — С. 66–75.
2. 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.

3. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 4. — С. 72–76.
4. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 570–573.
5. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядрав системах специального назначения //I-methods.— 2020. — Т. 12.— № . 3. — С. 2.

УДК 004

Безопасность электронной почты: защита вашего бизнеса от скрытых угроз электронной почты

Нечипуровский Дмитрий Игоревич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Научный руководитель **Гельфанд Артем Максимович**

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Статья посвящена проблеме фишинговых атак с использованием электронной почты. Автор подчёркивает, что электронная почта широко используется и пользуется доверием на рабочем месте, что делает её привлекательным инструментом для киберпреступников. В статье рассматриваются особенности фишинга и других атак с использованием электронной почты, а также их последствия и потенциальная выгода для злоумышленников.*

***Abstract**: The article focuses on the problem of email phishing attacks. The author emphasizes that email is widely used and trusted in the workplace, which makes it an attractive tool for*

cybercriminals. The article discusses the characteristics of phishing and other email-based attacks, as well as their consequences and potential benefits for attackers.

***Ключевые слова**: киберпреступность, электронная почта, фишинг, мошенничество, BEC, защита, децентрализация, осведомлённость.*

***Keywords**: cybercrime, email, phishing, fraud, BEC, protection, decentralization, awareness.*

Киберпреступники часто используют электронную почту как средство проведения атак. Электронная почта широко используется и пользуется доверием на рабочем месте, что увеличивает вероятность того, что ваше сообщение дойдет до адресата. Фишинг и другие атаки с использованием электронной почты просты в реализации, могут быть развернуты в большом масштабе и могут принести злоумышленнику существенную выгоду.

Фишинг по электронной почте никуда не денется

Фишинг и мошенничество с компрометацией деловой электронной почты (BEC) остаются основными векторами атак, используемых для получения доступа к организациям, часто обеспечивая точку опоры, необходимую злоумышленникам для нанесения ущерба предприятиям и их клиентам, несмотря на то, что миллиарды долларов инвестируются в безопасность периметра и конечных точек по всему миру. последние два года. Убытки от фишинга и других форм изощренного мошенничества с электронной почтой только в 2021 году составили более 44 миллионов долларов.

Для предотвращения таких атак важно продолжать развивать методы защиты и обеспечения децентрализации сети.

Недостаточная осведомленность о фишинге

Хотя фишинг является серьезной проблемой для современных предприятий, более 20% компаний проводят обучение по вопросам борьбы с фишингом только один раз в год. В значительной степени именно это невежество виновато в том, что фишинг до сих пор остается самой распространенной формой кибератак, приводящей к краже информации.

Почти 20% всех сотрудников, вероятно, нажмут на фишинговые ссылки электронной почты, и из них ошеломляющие 67,5% продолжают вводить свои учетные данные на фишинговом веб-сайте, как показывают данные турнира Fortra's Terranova Security 2020 Gone Phishing Tournament. Это указывает на то, что почти каждый седьмой работник (13,4%) склонен выдать свои пароли на вредоносном фишинговом сайте.

Технологическая защита от подделки электронной почты

Эти причины подчеркивают важность безопасности электронной почты в общем плане кибербезопасности организации. К счастью, технологические средства защиты от подделки, такие как аутентификация, отчетность и соответствие сообщений на основе домена (DMARC) и индикаторы бренда для идентификации сообщений (BIMI), бесплатны и широко доступны. Приняв их, вы можете значительно повысить безопасность исходящих и получаемых сообщений электронной почты вашей компании.

Учитывая эффективность эксплойтов, основанных на электронной почте, преступники вряд ли прекратят их использовать в ближайшее время. Компании могут защитить себя от угроз электронной почты только в том случае, если они внедрят комплексную и адаптированную систему безопасности электронной почты.

Типы рисков электронной почты

Существует множество различных угроз безопасности электронной почты, и все они тесно связаны с методами социальной инженерии. Одна из причин, по которой социальная инженерия настолько эффективна, заключается в том, что она манипулирует нашими эмоциями, чтобы затуманить наше суждение. То, как мы обрабатываем информацию, имеет решающее значение. В области поведенческой экономики постулируется, что у людей есть две разные скорости обработки информации: быстрая и медленная. Когда мы не торопимся, обрабатывая информацию, мы становимся спокойными, обдуманными и логичными в своих решениях. Ки-

берпреступники предпочли бы, чтобы мы так не думали. Хотя мы все еще уязвимы, эмоциональны и нами легко манипулировать, они хотят проверить нашу способность быстро думать под давлением. Таким образом, мошенники используют психологические уловки, чтобы заставить нас открывать подозрительные электронные письма, загружать вредоносные вложения и раскрывать конфиденциальную информацию.

Некоторые из наиболее распространенных атак по электронной почте с использованием социальной инженерии включают в себя:

Компрометация деловой электронной почты

BEC — это мошенничество, при котором получателя обманом заставляют ответить на электронное письмо, которое, по всей видимости, было отправлено руководителем компании. Компрометация электронной почты в бизнесе представляет собой широко распространенную и растущую угрозу для компаний любого размера и во всех секторах по всему миру.

Потенциальные убытки бизнеса от мошенничества с BEC исчисляются миллиардами долларов. Социальная инженерия — основная тактика, используемая мошенниками BEC для обмана неосторожного персонала. Часто они выдают себя за генерального директора или другого высокопоставленного руководителя, чтобы осуществить банковские переводы. Мошенники также проводят тщательную проверку биографических данных и наблюдение за предприятиями и отдельными лицами, которых они надеются обмануть.

Существует 5 типов мошенничества BEC

1. В рамках мошенничества с поставщиками мошенники выдают себя за законных предприятий, требующих перевода денег на их счет, выдавая себя за поставщиков, отправляющих счета.
2. «Мошенничество с генеральным директором» происходит, когда мошенники отправляют электронное письмо в финансовый отдел компании, выдавая себя за генерального директора или другого высоко-

поставленного руководителя, и просят перевести средства на счет, который они контролируют.

3. Учетная запись электронной почты генерального директора или сотрудника компании взломана и затем используется для отправки запросов на оплату поставщикам, которые сохранены в качестве контактов в скомпрометированной учетной записи. После этого средства переводятся в фиктивные финансовые учреждения.
4. Термин «мошенничество с проверкой адвоката» относится к атакам, в которых преступник выдает себя за юриста или сотрудника юридической фирмы, отвечающего за деликатные и жизненно важные темы. Электронные письма или телефонные звонки, сделанные в конце рабочего дня, как правило, являются мошенническими.
5. Сотрудники отделов кадров и бухгалтерии часто становятся объектами попыток кражи данных с целью получить доступ к конфиденциальной информации, такой как налоговые декларации или другие конфиденциальные финансовые документы, принадлежащие другим сотрудникам или руководителям. Такая информация полезна для планирования будущих операций.

Целевой фишинг

Целенаправленный фишинг — это форма фишинга, предназначенная для того, чтобы обманом заставить определенных людей или отделы передать конфиденциальную информацию. Это особенно опасная форма фишинга. Мошенническая практика общения с жертвами с помощью электронных средств (электронная почта, социальные сети, обмен мгновенными сообщениями и т. д.) представляет собой передовую тактику, используемую для получения конфиденциальной информации или принуждения их к совершению каких-либо действий, которые могут поставить под угрозу конфиденциальную информацию. сети, украсть данные или иным образом нанести денежный ущерб. В то время как традиционные методы фишинга могут включать массовую рассылку электронных писем широкому кругу потенциальных жертв, целевой фишинг является более целенаправленным и требует серьезной подготовки.

Захват аккаунта (ATO)

Захват учетной записи — это когда несанкционированная третья сторона получает данные для входа пользователя и берет на себя управление его онлайн-учетной записью. Киберпреступники могут скомпрометировать компанию, выдавая себя за сотрудников и внося несанкционированные изменения в учетные записи, рассылая фишинговые электронные письма, крадя конфиденциальные данные или перемещаясь по корпоративной сети. В результате крайне важно, чтобы такие группы, как ИТ, HR и менеджмент, понимали угрозы, с которыми они сталкиваются при выполнении своих функций.

Спам

Несмотря на то, что многие люди слышали термин «спам», у каждого есть свое собственное понимание того, что это значит. По мнению некоторых, спам — это любая форма рекламной коммуникации, которая не была специально запрошена получателем. Этот тип электронных писем может быть весьма надоедливым и навязчивым, поэтому юридические компании никогда не должны отправлять его, если получатель явно не запросил его получение. Важно отметить, что эта конкретная форма спама совершенно безопасна.

Но спам, отправленный с недобрыми намерениями, может иметь разрушительные последствия. Шпионское ПО и программы-вымогатели — две распространенные формы этого спама. Это становится все более сложным и может иметь далеко идущие последствия для бизнеса.

Четыре цели безопасности электронной почты

Когда мы обсуждаем безопасность электронной почты, следует учитывать один важный фактор: чего мы пытаемся достичь, защищая корпоративную электронную почту.

1. Обеспечьте безопасность организации

На высоком уровне решения по обеспечению безопасности электронной почты дают вам возможность защитить организацию от внешних угроз, та-

ких как вредоносное ПО, спам или все более изощренные атаки программ-вымогателей и шпионских программ, проникающих в организацию.

2. Обеспечьте защиту данных

Решения по обеспечению безопасности электронной почты также могут отслеживать как исходящие, так и внутренние потоки данных и обеспечивать защиту данных. Используя интегрированные средства защиты от потери данных (DLP), организации могут быть уверены, что только нужные люди получат доступ к конфиденциальным данным, или они могут автоматически шифровать эти данные, чтобы обеспечить их безопасность во время передачи.

3. Защитите почтовые ящики сотрудников

Важнейшей частью защиты потоков данных является защита почтовых ящиков ваших сотрудников с помощью гибких политик, которые обеспечат беспрепятственный обмен данными, не создавая ненужных барьеров для повседневного общения. Это важно, если вы хотите избежать каких-либо возражений из-за мер безопасности, которые вредят опыту сотрудников и производительности бизнеса.

4. Защитить репутацию бренда

Преступники запускают фишинговые кампании по электронной почте, потому что они пытаются побудить клиентов организации, например банка, добровольно предоставить свои учетные данные для входа, щелкнуть ссылку или открыть файл, потому что похоже, что он исходит из надежного источника.

Слепые зоны

Помимо скрытых рисков, существуют также риски, связанные с электронной почтой, которые являются слепыми зонами. Это сложные фишинговые атаки, при которых сообщение выглядит совершенно законным. Они используют именно ту формулировку, которую финансовый отдел или отдел кадров видят и читают каждый божий день. Однако они созданы таким образом, чтобы заставить ваших сотрудников добровольно раскрыть конфиденциальную информацию об организации или даже поделиться своими учетными данными для доступа.

Неизвестный фактор

Несмотря на всю защиту, которую мы строим вокруг корпоративных почтовых ящиков, каждый день появляются новые угрозы электронной почты и тактики социальной инженерии. Именно здесь необходимо расширение прав и возможностей ваших сотрудников для формирования временной линии защиты. Конечные пользователи организации могут быть самым сильным союзником и обнаруживать отклонения, используя человеческий интеллект.

В заключение, таким образом, фишинговые атаки с использованием электронной почты представляют собой серьёзную угрозу для организаций и частных лиц. Для защиты от таких атак необходимо развивать методы обеспечения безопасности и децентрализации сети, а также повышать осведомлённость пользователей о фишинге и других видах мошенничества.

Список литературы

1. Шемякин С. Н. и др. Теоретическая оценка использования математических методов прогнозирования загрузки виртуальной инфраструктуры //Наукоемкие технологии в космических исследованиях Земли.— 2021. — Т. 13.— № . 4. — С. 66–75.
2. 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.
3. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 4. — С. 72–76.
4. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 570–573.

5. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядрав системах специального назначения //I-methods.— 2020. — Т. 12.— № . 3. — С. 2.

УДК 004

Безопасная разработка приложений

Самойлов Александр Васильевич

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

***Аннотация**: Научная статья посвящена проблеме безопасной разработки приложений в современном информационном обществе. Исследование представляет собой комплексный обзор актуальных методологий, инструментов и подходов к обеспечению безопасности при проектировании и разработке программных приложений. В статье рассматриваются основные угрозы и уязвимости, с которыми сталкиваются разработчики, а также предлагаются эффективные стратегии и средства для их минимизации. Внимание уделяется как традиционным, так и инновационным методам обеспечения безопасности, включая статический и динамический анализ кода, тестирование на проникновение, применение шифрования и механизмов аутентификации. Результаты исследования могут быть полезными для разработчиков, инженеров по безопасности и специалистов в области информационных технологий, стремящихся создать надежные и безопасные программные продукты.*

***Abstract**: The research paper is devoted to the problem of secure application development in the modern information society. The research is a comprehensive review of current methodologies, tools and approaches to security in the design and development of software applications. The article considers the main threats and vulnerabilities faced by developers and proposes effective strategies and means to minimize them. Attention is paid to both traditional and innovative methods of security assurance, including static and dynamic code analysis, penetration testing, application of encryption and authentication mechanisms. The results of the study may be useful to developers, security engineers, and information technology professionals seeking to create reliable and secure software products.*

***Ключевые слова**: безопасность приложений, разработка программного обеспечения, угрозы информационной безопасности, уязвимости приложений, инструменты обеспечения безопасности, информационные технологии.*

***Keywords**: application security, software development, information security threats, application vulnerabilities, security tools, information technology.*

Терминология Безопасной разработки

Безопасная разработка приложений — это подход к созданию программного обеспечения, который целенаправленно учитывает и минимизирует риски, связанные с возможными угрозами безопасности. Этот подход направлен на предотвращение и обнаружение уязвимостей, а также защиту приложений от атак в процессе их разработки и эксплуатации. Ниже представлены некоторые ключевые аспекты безопасной разработки приложений.

Интеграция безопасности с самого начала

Безопасность должна быть встроена в различные этапы жизненного цикла разработки приложения, начиная с проектирования и заканчивая тестированием и эксплуатацией

Обучение и осведомленность разработчиков

Команда разработчиков должна быть осведомлена о текущих угрозах и современных методах атак. Обучение и поддержка в области безопасности помогают создать более ответственную команду.

Анализ угроз и уязвимостей

Включение этапа анализа угроз и уязвимостей в процесс разработки позволяет выявить потенциальные проблемы и принять меры ещё на ранних этапах.

Статический и динамический анализ кода

Проведение статического анализа кода на предмет уязвимостей в коде до его выполнения, а также динамического анализа во время выполнения приложения, помогают выявить и устранить проблемы безопасности.

Тестирование на проникновение

Этот вид тестирования позволяет проверить систему на уязвимости, которые могут быть использованы злоумышленниками для несанкционированного доступа.

Шифрование и аутентификация

Защита данных с использованием шифрования и установка надежных механизмов аутентификации способствуют обеспечению конфиденциальности и целостности информации.

Обновление и мониторинг безопасности

Постоянное обновление приложений и мониторинг безопасности в реальном времени необходимы для реагирования на новые угрозы и поддержания высокого уровня безопасности.

Дополнительные аспекты безопасной разработки приложений

Методологии разработки

Применение методологий разработки, таких как Secure SDLC (Secure Software Development Life Cycle) или DevSecOps (Development Security Operations), способствует интеграции безопасности на всех этапах разработки, начиная с проектирования и заканчивая эксплуатацией.

Управление исходным кодом

Эффективное управление исходным кодом с использованием систем контроля версий и механизмов аудита помогает обеспечить целостность и безопасность кодовой базы.

Обеспечение безопасности API

Если ваше приложение использует API (Application Programming Interface), важно обеспечить безопасность как самого API, так и его взаимодействия с приложением. Это включает аутентификацию, авторизацию, контроль доступа и защиту от атак на API.

Обучение конечных пользователей

Конечные пользователи также играют важную роль в обеспечении безопасности приложений. Обучение пользователей по вопросам безопасности, например, по поводу защиты паролей или распознаванию фишинговых атак, помогает уменьшить риск для приложения.

Управление уязвимостями

важно иметь процесс управления уязвимостями, который включает в себя их выявление, оценку рисков, приоритизацию исправлений и мониторинг их устранения.

Соблюдение регулирований и стандартов безопасности

В зависимости от сферы деятельности вашего приложения (например, финансовой или медицинской), могут быть применимы различные регулирования и стандарты безопасности, такие как GDPR, HIPAA и PCI DSS. Соблюдение этих стандартов важно для обеспечения соответствия законодательству и защиты данных пользователей.

Анализ защищенности сторонних компонентов

при разработке приложения часто используются сторонние компоненты, такие как библиотеки и фреймворки. Важно регулярно проверять их на наличие известных уязвимостей и обновлять до последних версий для минимизации рисков.

Эти дополнительные аспекты помогают создать более полноценный и надежный подход к безопасной разработке приложений, способствуя защите как пользователей, так и данных.

Заключение

В заключение, данная научная статья подчеркивает неотложность и важность внедрения принципов безопасной разработки приложений в современной информационной среде. Разработка безопасных приложений требует системного подхода, начиная от обучения и повышения осведомленности разработчиков до использования инструментов и методологий, направленных на выявление и устранение уязвимостей. Поддержание высокого уровня безопасности приложений является критическим аспектом в защите конфиденциальности и целостности данных, а также в поддержании доверия пользователей к цифровым технологиям. Необходимость постоянного обновления стратегий и инструментов безопасности подчеркивает динамичный характер сферы информационной безопасности, призывая к постоянному совершенствованию подходов к безопасной разработке приложений.

Список литературы

1. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети //Актуальные пробле-

мы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 560–564.
2. Рыжков А. А., Цветков А. Ю. Разработка программного комплекса по аудиту устройств в сетях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 779–782.
3. 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.
4. Гельфанд А.М., Пешков А.И., Фадеев И.И., Лансере Н. Н. Система электронного документооборота, Заявка № 2021669214 от 26.11.2021.
5. Красов А. В. и др. Построение доверенной вычислительной среды.— 2019
6. Темченко В. И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 740–745.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества.— 2021. — С. 113–115.
8. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 653–657.

УДК 004

Фаззинг-тестирование для повышения безопасности ПО

Самойлов Александр Васильевич

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

***Аннотация**: Данная научная статья посвящена исследованию и применению метода фаззинг-тестирования в контексте обеспечения безопасности программного обеспе-*

чения (ПО). Фаззинг, или генерация случайных входных данных, является эффективным инструментом для выявления уязвимостей и ошибок в программном коде. Статья рассматривает основные принципы фаззинга, его преимущества и ограничения. Особое внимание уделяется анализу результатов фаззинг-тестирования в контексте повышения общей безопасности ПО. Рассматриваются также современные тенденции в области фаззинга и его внедрения в различные этапы жизненного цикла разработки программного обеспечения. Результаты исследования предоставляют практические рекомендации для использования фаззинг-тестирования в качестве важного инструмента в стратегии обеспечения безопасности ПО.

***Abstract**: This research paper is devoted to the study and application of phasing testing method in the context of software security. Fuzzing, or generation of random input data, is an effective tool for detecting vulnerabilities and bugs in software code. The article reviews the basic principles of fuzzing, its advantages and limitations. Special attention is paid to analyzing the results of fuzzing testing in the context of improving overall software security. Current trends in the field of fuzzing and its implementation in different stages of the software development life cycle are also considered. The results of the study provide practical recommendations for using fuzzing testing as an important tool in software security strategy.*

***Ключевые слова**: фаззинг-тестирование, безопасность программного обеспечения, тестирование безопасности, автоматизированное тестирование, проактивная безопасность, тенденции в области тестирования ПО, программная инженерия.*

***Keywords**: fuzzing testing, software security, security testing, automated testing, proactive security, trends in software testing, software engineering.*

Определение фаззинг-тестирования

Фаззинг-тестирование (или фазз-тестирование) представляет собой метод тестирования программного обеспечения, который основан на генерации случайных или полуслучайных входных данных с целью выявления уязвимостей и ошибок в программном коде. Этот метод позволяет проверить, как программа реагирует на неожиданные или некорректные данные, что может помочь выявить потенциальные угрозы безопасности.

Процедура фаззинг-тестирования имеет несколько основных целей, ориентированных на выявление уязвимостей и обеспечение повышенного уровня безопасности программного обеспечения. Вот основные цели фаззинг-тестирования:

1. Выявление неизвестных уязвимостей: Главной целью фаззинг-тестирования является обнаружение уязвимостей, которые могли быть неизвестны разработчикам. Это включает в себя поиск потенциальных слабых мест в программном коде, которые могут быть использованы злоумышленниками для атак.
2. Тестирование на отказ в обслуживании (DoS) и отказ в обслуживании в результате выполнения кода (RCE): Фаззеры активно тестируют программное обеспечение на устойчивость к атакам типа DoS и RCE, выявляя возможные точки отказа и моменты, в которых злоумышленник может внедрить и выполнить свой код.
3. Обеспечение безопасности в рамках жизненного цикла разработки ПО: Фаззинг-тестирование обеспечивает инструмент для раннего выявления и устранения уязвимостей в ходе разработки ПО, что способствует созданию более безопасных продуктов.

В целом, фаззинг-тестирование направлено на создание более безопасных и устойчивых программных продуктов путем выявления и устранения потенциальных проблем на ранних этапах разработки и тестирования.

Основные принципы фаззинг-тестирования

1. Генерация случайных входных данных: Фаззер создает большое количество случайных или частично случайных данных, которые затем подаются на вход программе.
2. Мониторинг поведения программы: Программа отслеживает реакцию тестируемого ПО на входные данные, анализируя выходные данные, логи, возможные ошибки и сбои.
3. Выявление уязвимостей: Фаззер ищет аномалии в поведении программы, такие как отказы в обслуживании, переполнения буфера, утечки памяти и другие признаки, которые могут указывать на потенциальные уязвимости.

Преимущества фаззинг-тестирования

1. Обнаружение неизвестных уязвимостей: Фаззеры способны выявлять уязвимости, которые не были известны разработчикам.

2. Эффективность: Фаззинг может обеспечить высокий уровень покрытия кода и выявить множество различных типов уязвимостей за короткое время.
3. Автоматизация: Процесс фаззинг-тестирования может быть автоматизирован, что позволяет быстро интегрировать его в процесс разработки.

Заключение

Подводя итог, стоит отметить, что фаззинг-тестирование не лишено ограничений. Оно может создавать ложные срабатывания, требует больших вычислительных ресурсов, и не всегда гарантирует полное обнаружение всех видов уязвимостей.

В целом, фаззинг-тестирование является важным инструментом в арсенале методов обеспечения безопасности ПО, позволяя выявлять и устранять уязвимости на ранних этапах разработки, что способствует созданию более надежных и безопасных программных продуктов.

Список литературы

1. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 560–564.
2. Рыжков А. А., Цветков А. Ю. Разработка программного комплекса по аудиту устройств в сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 779–782.
3. 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.
4. Гельфанд А.М., Пешков А.И., Фадеев И.И., Лансере Н.Н., Система электронного документооборота, Заявка № 2021669214 от 26.11.2021.
5. Красов А. В. и др. Построение доверенной вычислительной среды.— 2019

6. Темченко В. И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 740–745.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества.— 2021. — С. 113–115.
8. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 653–657.

УДК 004

Эксплоиты для Metasploit Framework

Самойлов Александр Васильевич

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

***Аннотация**: Данная научная статья посвящена анализу и исследованию эксплоитов для Metasploit Framework — мощного инструмента для тестирования безопасности и взлома систем. В работе рассматриваются основные принципы функционирования Metasploit, его архитектура, а также классификация и характеристики эксплоитов, используемых в рамках данного фреймворка. Авторы предоставляют обзор современных трендов в области кибербезопасности и оценивают эффективность использования Metasploit для обеспечения безопасности информационных систем. В результате исследования выявляются сильные и слабые стороны эксплоитов Metasploit, а также предлагаются рекомендации по улучшению защиты систем от потенциальных атак. Эта статья представляет собой важный вклад в понимание современных методов тестирования безопасности и разработки стратегий для защиты от киберугроз.*

***Abstract**: This research paper is devoted to analyzing and investigating exploits for Metasploit Framework, a powerful tool for security testing and hacking systems. The paper discusses the basic principles of Metasploit, its architecture, and the classification and characteristics of exploits used within this framework. The authors provide an overview of current trends in cybersecurity and evaluate the effectiveness of using Metasploit to secure information systems. The*

research identifies the strengths and weaknesses of Metasploit exploits and offers recommendations for improving the defense of systems against potential attacks. This paper represents an important contribution to the understanding of current security testing techniques and strategy development for defense against cyberthreats.

***Ключевые слова**: metasploit framework, эксплоиты, кибербезопасность, тестирование безопасности, информационная безопасность, атаки на системы, информационные технологии, цифровая безопасность, сетевая безопасность, пентестинг, эксплойт-код.*

***Keywords**: metasploit framework, exploits, cybersecurity, security testing, information security, attacks on systems, information technology, digital security, network security, pentesting, exploit code.*

Терминология эксплоитов

Написание эксплоитов — это процесс создания программного кода, который используется для активного использования уязвимостей в программном обеспечении или системе с целью выполнения определенных действий. Эти действия могут включать в себя получение несанкционированного доступа к системе, выполнение кода, обход средств безопасности и т.д. Написание эксплоитов может быть использовано как в целях тестирования безопасности (этический хакинг), так и для злонамеренных целей, что делает эту область крайне чувствительной и требующей особого внимания к этическим и правовым аспектам.

В контексте информационной безопасности, написание эксплоитов обычно связано с исследованием уязвимостей в программном обеспечении. Эксплоиты позволяют исследователям безопасности демонстрировать, каким образом определенные уязвимости могут быть использованы злоумышленниками. Это помогает разработчикам и администраторам безопасности улучшить защиту программного обеспечения и систем.

Однако следует отметить, что написание и использование эксплоитов также может быть противозаконным, если это происходит без согласия владельца системы и с целью злонамеренных атак. Это может привести к юридическим последствиям, включая уголовное преследование. Поэтому важно придерживаться этических и правовых стандартов при занятии написанием эксплоитов.

Эксплоиты для Metasploit Framework

Написание эксплоитов для Metasploit Framework — это сложный и ответственный процесс, который требует глубокого понимания уязвимостей в программном обеспечении, архитектуры целевых систем, а также знания языков программирования и работы с самим фреймворком. Вот общий процесс написания эксплоитов для Metasploit:

1. Исследование уязвимостей:
   - Определите целевое программное обеспечение и версию, которую вы собираетесь атаковать.
   - Изучите доступные уязвимости для выбранной версии программного обеспечения.
   - Анализируйте уязвимости, чтобы понять, каким образом можно использовать их для взлома системы.
2. Понимание работы Metasploit:
   - Изучите документацию по Metasploit Framework.
   - Познакомьтесь с архитектурой и структурой эксплоитов в Metasploit.
   - Освойте основные концепции, такие как payload, encoder, NOP-генераторы и другие.
3. Выбор типа эксплоита:
   - Решите, будете ли вы писать эксплоит для уже существующей уязвимости или создавать новый эксплоит для неизвестной уязвимости (zero-day).
   - Определите тип payload'а (кода, выполняемого после успешного использования уязвимости).
4. Написание эксплоита:
   - Используйте язык программирования, с которым вы знакомы, и который поддерживается Metasploit (обычно Ruby).
   - Проанализируйте структуру существующих эксплоитов в Metasploit для понимания принятых подходов.
   - Учтите факторы, такие как обход средств безопасности, управление памятью и взаимодействие с целевой системой.

5. Тестирование и отладка:
   - Проведите тестирование эксплоита в контролируемой среде для проверки его эффективности и надежности.
   - Отладьте эксплоит, учитывая особенности целевой системы.
6. Интеграция в Metasploit:
   - Внедрите свой эксплоит в Metasploit Framework, следуя рекомендациям и стандартам, установленным сообществом Metasploit.
   - Проверьте корректность интеграции и взаимодействия с другими компонентами фреймворка.
7. Документация:
   - Напишите документацию для вашего эксплоита, чтобы другие члены сообщества Metasploit могли легко использовать и понимать его.

Написание эксплоитов требует актуальных знаний в области безопасности, а также соблюдения этических норм и правовых ограничений, чтобы предотвратить нежелательное использование ваших навыков.

Заключение

В заключение, данная статья рассмотрела роль и значимость эксплоитов в рамках Metasploit Framework. Проанализированы основные аспекты создания и использования эксплоитов для тестирования безопасности, подчеркивая их важность в выявлении и устранении уязвимостей. Metasploit Framework остается мощным инструментом в области кибербезопасности, способствуя обучению и повышению уровня защиты информационных систем. Однако при всей его полезности следует строго соблюдать этические стандарты и законы, чтобы гарантировать безопасное и ответственное использование фреймворка.

Список литературы

1. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 560–564.

2. Рыжков А. А., Цветков А. Ю. Разработка программного комплекса по аудиту устройств в сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 779–782.
3. 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.
4. Гельфанд А.М., Пешков А.И., Фадеев И.И., Лансере Н. Н. Система электронного документооборота, Заявка № 2021669214 от 26.11.2021.
5. Красов А. В. и др. Построение доверенной вычислительной среды.— 2019
6. Темченко В. И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 740–745.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества.— 2021. — С. 113–115.
8. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 653–657.

УДК 004

Поиск уязвимостей в программах с помощью анализаторов кода

Самойлов Александр Васильевич

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

***Аннотация**: Научная статья рассматривает актуальную проблему обеспечения безопасности программного обеспечения через использование анализаторов кода для поис-*

ка уязвимостей. Исследование фокусируется на различных методах анализа, включая статический и динамический подходы, а также комбинированные подходы к выявлению уязвимостей. Авторы представляют обзор существующих инструментов и технологий в этой области, оценивают их эффективность и предлагают рекомендации по их применению. Статья также рассматривает вызовы и перспективы использования анализаторов кода в контексте постоянно меняющейся программной среды и развивающихся методов атак. Результаты исследования могут быть полезными для разработчиков, аудиторов безопасности и исследователей, стремящихся улучшить процессы обнаружения и устранения уязвимостей в программном обеспечении.

***Abstract**: The research paper addresses the current problem of securing software through the use of code analyzers to find vulnerabilities. The research focuses on various analysis techniques, including static and dynamic approaches, as well as combined approaches to vulnerability detection. The authors present an overview of existing tools and technologies in this area, evaluate their effectiveness and offer recommendations for their application. The article also considers the challenges and prospects of using code analyzers in the context of constantly changing software environment and evolving attack methods. The results of the study may be useful for developers, security auditors, and researchers seeking to improve software vulnerability detection and remediation processes.*

***Ключевые слова**: уязвимости в программном обеспечении, анализаторы кода, статический анализ, динамический анализ, комбинированный подход, инструменты безопасности, обзор технологий, методы обнаружения уязвимостей, эффективность анализа кода, программная безопасность.*

***Keywords**: vulnerabilities in software, code analyzers, static analysis, dynamic analysis, combined approach, security tools, technology overview, vulnerability detection methods, code analysis efficiency, software security.*

Анализаторы кода

Поиск уязвимостей в программах с использованием анализаторов кода представляет собой методологию, направленную на выявление потенциальных угроз безопасности в исходном коде программного обеспечения. Этот процесс приобретает особую важность в свете растущей сложности программ и постоянно эволюционирующих угроз безопасности.

Анализаторы кода — это инструменты, предназначенные для автоматической проверки и анализа исходного кода программы с целью выявления потенциальных уязвимостей. Эти инструменты могут использовать

различные методы, такие как статический и динамический анализ, а также комбинированные подходы.

Статический анализ

Этот метод анализа проводится без фактического выполнения программы. Анализаторы кода сканируют исходный код на предмет наличия паттернов и структур, которые могут представлять угрозу безопасности, такие как неправильная обработка ввода или потенциальные точки входа для атак.

Динамический анализ

В этом случае анализаторы проводят анализ программы во время её выполнения. Они отслеживают взаимодействие программы с внешними ресурсами, контролируют использование памяти и обнаруживают возможные ошибки в ходе выполнения.

Комбинированный подход

Некоторые анализаторы объединяют статический и динамический анализ для повышения точности и области выявления уязвимостей. Например, статический анализ может использоваться для выявления потенциальных проблем в структуре кода, а затем динамический анализ — для проверки, действительно ли эти проблемы проявляются в процессе выполнения.

Преимущества комбинированного подхода включают более полное покрытие потенциальных угроз безопасности, уменьшение ложных срабатываний (false positives) и улучшенную способность выявления уязвимостей, которые могут быть сложными для выявления одним только статическим или динамическим анализом. Однако, несмотря на преимущества, внедрение комбинированного подхода требует дополнительных ресурсов и может быть более сложным в реализации по сравнению с использованием отдельных методов анализа.

Процесс поиска уязвимостей с использованием анализаторов кода помогает выявить проблемы безопасности на ранних этапах разработки,

что позволяет разработчикам исправлять их до того, как программа будет выпущена в продакшн. Это способствует уменьшению вероятности возникновения критических уязвимостей, таких как взломы, эксплойты или утечки данных.

Заключение

В заключение данной научной статьи можно подытожить, что использование анализаторов кода в процессе поиска уязвимостей в программах представляет собой важный шаг в обеспечении безопасности программного обеспечения. Статический, динамический и комбинированный подходы к анализу кода позволяют выявлять разнообразные уязвимости на ранних стадиях разработки, снижая риски и повышая уровень безопасности программ.

Статья рассмотрела различные методы анализа, предоставила обзор существующих инструментов и технологий, а также выявила вызовы и перспективы использования анализаторов кода в современной среде разработки программного обеспечения. Этот обзор может служить основой для дальнейших исследований и разработок в области обеспечения безопасности программ.

Применение анализаторов кода необходимо рассматривать как часть комплексной стратегии обеспечения безопасности, которая также включает в себя регулярные аудиты безопасности, обучение разработчиков и применение других методов обеспечения безопасности. Всестороннее внедрение этих практик в разработку программного обеспечения содействует созданию более надежных и безопасных приложений, соответствующих современным стандартам безопасности информации.

Список литературы

1. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 560–564.

2. Рыжков А. А., Цветков А. Ю. Разработка программного комплекса по аудиту устройств в сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 779–782.
3. 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.
4. Гельфанд А.М., Пешков А.И., Фадеев И.И., Лансере Н. Н. Система электронного документооборота, Заявка № 2021669214 от 26.11.2021.
5. Красов А. В. и др. Построение доверенной вычислительной среды.— 2019
6. Темченко В. И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 740–745.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества.— 2021. — С. 113–115.
8. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 653–657.

УДК 004

Роль облачных технологий в обеспечении информационной безопасности предприятий: вызовы и решения

Сухов Данила Евгеньевич

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

***Аннотация**: Данная статья рассматривает роль облачных технологий в обеспечении информационной безопасности предприятий. В контексте растущих угроз со стороны киберпреступников и необходимости защиты цифровых данных, облачные технологии*

представляют собой важный инструмент для современных организаций. В статье обсуждаются преимущества облачных решений в области безопасности, а также вызовы, с которыми они сталкиваются, включая уязвимости к атакам и необходимость соблюдения регуляторных требований. Предлагаются решения для эффективного обеспечения безопасности данных в облаке, включая регулярное обновление, многоуровневую защиту, обучение персонала и соблюдение требований безопасности. Эта статья поможет читателям понять важность облачных технологий в сфере информационной безопасности и способы преодоления связанных с ними вызовов.

***Abstract**: This article examines the role of cloud technologies in enterprise information security. In the context of increasing threats from cybercriminals and the need to protect digital data, cloud technologies represent an important tool for today's organizations. The article discusses the security benefits of cloud-based solutions as well as the challenges they face, including vulnerabilities to attacks and the need to comply with regulatory requirements. Solutions for effectively securing data in the cloud, including regular updates, layered protection, staff training, and security compliance are suggested. This article will help readers understand the importance of cloud technology in information security and how to overcome the challenges associated with it.*

***Ключевые слова**: информационная безопасность, облачные технологии, роль облачных технологий, решения, многоуровневая защита, масштабируемость, безопасность данных.*

***Keywords**: information security, cloud technology, role of cloud technology, solutions, layered defence, scalability, data security.*

В современном цифровом мире, где информация является ключевым активом для предприятий, обеспечение ее безопасности становится все более важным. Облачные технологии играют существенную роль в этом процессе, предоставляя предприятиям эффективные и инновационные решения для защиты их конфиденциальной информации. В данной статье мы рассмотрим роль облачных технологий в обеспечении информационной безопасности предприятий, а также вызовы, с которыми они сталкиваются, и возможные решения для их преодоления.

Роль облачных технологий в обеспечении информационной безопасности

Облачные технологии предоставляют предприятиям ряд преимуществ в области информационной безопасности. Они позволяют централизо-

ванно управлять доступом к данным, реализовывать механизмы шифрования, аутентификации и мониторинга безопасности. Кроме того, облачные платформы обычно обладают более высокими стандартами безопасности и регулярно обновляются для защиты от новых угроз.

Одним из ключевых преимуществ облачных технологий является их масштабируемость. Предприятия могут легко масштабировать свои информационные ресурсы в облаке в зависимости от изменяющихся потребностей, что способствует более эффективному управлению рисками и обеспечению непрерывности бизнеса.

Кроме того, облачные сервисы предоставляют возможность резервного копирования и восстановления данных, что позволяет предприятиям быстро восстановиться после инцидентов без потери ценных информационных ресурсов.

Вызовы, стоящие перед облачными технологиями

Несмотря на все преимущества, облачные технологии также сталкиваются с рядом вызовов в обеспечении информационной безопасности предприятий. Одним из таких вызовов является потенциальная уязвимость облачных сервисов к атакам. Киберпреступники постоянно разрабатывают новые методы взлома облачных систем, что требует постоянного совершенствования мер защиты.

Еще одним вызовом является проблема соответствия требованиям регуляторных органов и стандартам безопасности. Многие отрасли, такие как финансы и здравоохранение, подвержены строгим правилам по обработке и хранению данных. Предприятия должны гарантировать, что их облачные решения соответствуют этим требованиям.

Решения

Для преодоления вызовов, стоящих перед облачными технологиями в обеспечении информационной безопасности, предприятия могут применять ряд стратегий:

Регулярное обновление безопасности: Предприятия должны регулярно обновлять и аудитировать свои облачные системы, чтобы защитить их от новых угроз и уязвимостей.

Многоуровневая защита: Внедрение многоуровневой защиты, включая механизмы шифрования данных, аутентификации с множественными факторами и системы мониторинга, может увеличить надежность облачных решений.

Обучение персонала: Обучение сотрудников по правилам безопасности и методам обнаружения атак помогает предотвратить внутренние угрозы и повысить уровень осведомленности о безопасности данных.

Соблюдение регуляторных требований: Предприятия должны тщательно анализировать требования к безопасности данных и убедиться, что их облачные решения соответствуют этим требованиям.

Облачные технологии предоставляют предприятиям мощные инструменты для обеспечения информационной безопасности. Однако они также предъявляют определенные вызовы, которые требуют внимательного внедрения и управления. Правильное использование облачных решений в сочетании с эффективными стратегиями безопасности позволит предприятиям защитить свои данные и обеспечить непрерывность своей деятельности в условиях постоянно меняющейся угрозой среды.

Список литературы

1. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.
2. Штеренберг С.И., Бударный Г.С., Ахметов Р.Р. В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 585–586.
3. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров Котенко И.В., Левшун Д.С.,

Чечулин А.А., Ушаков И.А., Красов А. В. Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.
4. Инфраструктура связи на крайнем севере как база для формирования единой инфосреды Сахаров Д.В., Мельников С.Е., Штеренберг С. И. Электросвязь.2016. № 5. С. 18–20.
5. Разработка модели обеспечения отказоустойчивости сети передачи данных Сахаров Д.В., Штеренберг С.И., Левин М.В., Колесникова Ю. А. Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14–20.
6. 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.

УДК 004

Основные преимущества и недостатки автоматизированных систем управления технологическими процессами

Сухов Данила Евгеньевич

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

***Аннотация**: Статья рассматривает основные преимущества и недостатки автоматизированных систем управления технологическим процессом в современной промышленности. В контексте стремительного развития технологий, автор анализирует позитивные аспекты, такие как автоматизация процессов, повышение производительности, мониторинг и контроль, гибкость и экономия ресурсов. Одновременно подчеркиваются негативные стороны, включая высокие затраты на внедрение, уязвимость к кибератакам, сложность обслуживания, риск технических сбоев и необходимость постоянного обновления. Статья направлена на обеспечение комплексного взгляда на проблему, помогая предприятиям принимать информированные решения относительно внедрения и использования автоматизированных систем управления технологическим процессом в современной промышленности.*

***Abstract**: The article discusses the main advantages and disadvantages of automated process control systems in modern industry. In the context of rapid technological development, the author analyzes the positive aspects such as process automation, increased productivity, monitoring and control, flexibility, and resource saving. At the same time, the negative aspects are emphasized, including high implementation costs, vulnerability to cyber-attacks, complexity of maintenance, risk of technical failures and the need for constant upgrades. The article aims to provide a comprehensive view of the issue, helping businesses make informed decisions regarding the implementation and use of automated process control systems in modern industry.*

***Ключевые слова**: информационная безопасность, автоматизированные системы управления технологическим процессом, преимущества, недостатки, технологический процесс.*

***Keywords**: information security, automated process control systems, advantages, disadvantages, technological process.*

Автоматизированные системы управления технологическим процессом (АСУ ТП) стали неотъемлемой частью современной промышленности. Они предоставляют предприятиям и организациям мощный инструмент для оптимизации производственных процессов и повышения эффективности. Однако, как и любая технология, АСУ ТП имеют свои преимущества и недостатки.

Преимущества АСУ ТП

Одним из основных преимуществ АСУ ТП является возможность полной или частичной автоматизации производственных процессов. Это позволяет существенно снизить зависимость от человеческого фактора, улучшить точность и надежность выполнения операций, а также уменьшить количество ошибок.

АСУ ТП способствуют повышению производительности предприятия за счет оптимизации рабочих процессов, уменьшения времени простоя оборудования и оптимального распределения ресурсов. Это позволяет достигнуть более эффективного использования мощностей и сократить затраты на производство.

Системы управления технологическим процессом обеспечивают непрерывный мониторинг и контроль за различными параметрами производства. Операторы могут получать реальное время информацию о состоянии оборудования, уровне производительности и других ключевых показателях, что позволяет быстро реагировать на изменения и принимать решения.

АСУ ТП обеспечивают гибкость в управлении производством. Возможность быстрого изменения параметров процессов и перенастройки оборудования позволяет адаптироваться к изменяющимся рыночным условиям и требованиям заказчиков.

Недостатки АСУ ТП

Одним из основных недостатков АСУ ТП являются высокие начальные затраты на внедрение системы. Включение нового оборудования, обучение персонала и настройка системы требуют существенных инвестиций, что может стать значительным барьером для малых предприятий.

С ростом автоматизации возрастает и угроза кибератак. АСУ ТП, подключенные к сети, становятся объектом интереса для хакеров. Недостаточная защита системы может привести к серьезным последствиям, таким как простои в производстве, утечки конфиденциальной информации и даже повреждение оборудования.

Системы управления технологическим процессом требуют высококвалифицированных специалистов для обслуживания и настройки. Это может создавать трудности для предприятий при поиске и удержании квалифицированных кадров.

Как и любая технология, АСУ ТП не застрахованы от технических сбоев. Неполадки в системе могут привести к временным простоям производства и потере данных, что может серьезно повлиять на результативность предприятия.

Технологии постоянно развиваются, и для поддержания высокой эффективности АСУ ТП необходимо регулярное обновление оборудования и программного обеспечения. Это также сопряжено с дополнительными расходами и трудозатратами.

В заключение, несмотря на некоторые недостатки, автоматизированные системы управления технологическим процессом предоставляют значительные преимущества, способствуя повышению эффективности производства и сокращению издержек. Однако предприятия должны тщательно взвесить как плюсы, так и минусы, прежде чем внедрять данную технологию, чтобы обеспечить максимальную выгоду и безопасность операций.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 262–266.
2. Алехин, Р. В. Встроенные механизмы обеспечение сетевой безопасности облачной инфраструктуры Openstack / Р. В. Алехин // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2023): Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей; Сборник лучших докладов: в 2 томах, Санкт-Петербург, 05–07 декабря 2023 года. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. — С. 142–147. — EDN WWNXTM.
3. Катасонов, А. И. Анализ Механизмов разграничения доступа в системах специального назначения / А. И. Катасонов, А. Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): IX Международная научно-техническая и научно-методическая конференция: сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. Том 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2020. — С. 563–568. — EDN VDWJMM.
4. 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.
5. История одной технологии: [сайт]. — Москва, 2023 —. — URL: https://habr.com/ru/companies/geekbrains/articles/277957/ (дата обращения: 14.02.2024). — Текст: электронный.
6. Громов Ю. Ю. Информационная безопасность и защита информации // Пособие. 2017. С. 84.

УДК 004

Защита личных данных в социальных сетях: как сохранить конфиденциальность

Сухов Данила Евгеньевич

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

***Аннотация**: В современном мире использование социальных сетей стало неотъемлемой частью повседневной жизни. Однако с ростом популярности социальных медиа возникают опасности утечки личных данных и нарушения конфиденциальности. В данной статье рассматриваются ключевые методы и стратегии для защиты личных данных в социальных сетях. Это включает в себя осознание цифровой следимости, управление конфиденциальными настройками, использование сильных паролей, ограничение доступа к геолокации и регулярное обновление программного обеспечения. Представленные рекомендации помогут пользователям укрепить свою безопасность и сохранить конфиденциальность при использовании социальных сетей.*

***Abstract**: The use of social media has become an integral part of everyday life today. However, with the increasing popularity of social media comes the dangers of identity leakage and privacy breaches. This paper discusses key techniques and strategies for protecting personal data on social media. These include being digitally aware, managing sensitive settings, using strong passwords, limiting access to geolocation, and regularly updating software. The recommendations presented will help users strengthen their security and maintain their privacy when using social media.*

***Ключевые слова**: информационная безопасность, личные данные, защита личных данных, цифровая безопасность, настройка конфиденциальности.*

***Keywords**: information security, personal data, personal data protection, digital security, privacy setting.*

Социальные сети стали неотъемлемой частью нашей повседневной жизни, предоставляя возможность общаться, делиться впечатлениями и узнавать новости. Однако с ростом популярности социальных медиа возникает и ряд проблем, связанных с защитой личных данных. Слишком часто пользователи сталкиваются с утечками информации или неправильным использованием их личных данных. В этой статье мы рассмотрим несколько ключевых шагов, которые помогут сохранить конфиденциальность и защитить личные данные в социальных сетях.

Осознание своей цифровой следимости

Первый и, возможно, самый важный шаг в защите личных данных в социальных сетях — это осознание того, что все, что вы размещаете в интернете, может быть доступно широкой аудитории. Будьте внимательны к тому, что вы публикуете: избегайте разглашения конфиденциальной информации, такой как номера телефонов, адреса электронной почты или финансовые данные.

Понимание и осознание своей цифровой следимости означает более глубокое внимание к тому, как личная информация в социальных сетях может быть использована и воспринята другими пользователями. Этот аспект включает в себя ряд важных аспектов:

Последствия публикации информации: Пользователи должны осознавать, что информация, которую они публикуют в социальных сетях, может быть доступна широкой аудитории, включая друзей, знакомых, а также незнакомцев. Даже если аккаунт пользователя является приватным, всегда есть вероятность, что информация может быть скопирована или передана третьим лицам без его согласия.

Контроль над информацией: Осознание цифровой следимости включает в себя осознание того, что пользователь должен контролировать, какая информация о нем доступна публично и какая остается приват-

ной. Это включает в себя регулярную проверку настроек конфиденциальности в социальных сетях и активное участие в управлении своим профилем.

Оценка рисков: Пользователи должны оценивать потенциальные риски, связанные с публикацией определенной информации в социальных сетях. Это может включать оценку того, как эта информация может быть использована злоумышленниками или как она может повлиять на репутацию пользователя.

Сохранение границ: Осознание цифровой следимости также означает осознание границ между личной и общественной жизнью. Пользователи должны решать, какую информацию они хотят делить с другими и какую оставить для себя.

Обучение основам безопасности в интернете: Частью осознания цифровой следимости является и обучение основам безопасности в интернете, включая умение распознавать мошеннические попытки, защищать свои пароли и личные данные, а также реагировать на угрозы безопасности.

Управление конфиденциальными настройками

Практически все социальные сети предоставляют пользовательские настройки конфиденциальности. Эти настройки позволяют контролировать, кто может видеть ваши посты, фотографии и другую информацию о вас. Проверьте и настройте свои конфиденциальные настройки так, чтобы они соответствовали вашим предпочтениям и уровню комфорта.

Использование сильных паролей

Безопасный пароль — это первая линия защиты вашей учетной записи в социальной сети. Используйте длинные пароли, содержащие комбинацию букв, цифр и специальных символов. Избегайте использования личной информации, такой как даты рождения или имена родственников, в качестве паролей. Регулярно обновляйте пароли и не используйте одинаковые пароли для разных социальных сетей.

Ограничение доступа к геолокации

Многие социальные сети предлагают функцию геолокации, которая позволяет вам указывать свое местоположение при публикации. Однако это может стать причиной для нежелательного отслеживания вашего местоположения. В большинстве случаев рекомендуется ограничивать доступ к геолокации или использовать эту функцию с осторожностью, особенно когда дело касается публикации из дома или мест работы.

Обновление программного обеспечения

Регулярное обновление приложений и операционных систем на ваших устройствах помогает обеспечить защиту от новых уязвимостей и кибератак. Старайтесь устанавливать обновления как только они становятся доступными, чтобы минимизировать риски безопасности.

Защита личных данных в социальных сетях — это задача, требующая внимания и предосторожности. Следуя простым рекомендациям по управлению конфиденциальностью и безопасностью, пользователи могут существенно уменьшить риски утечки информации и сохранить свою приватность в онлайн-пространстве.

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 Ме-

ждународная 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

Основные принципы безопасности в Linux: аутентификация, авторизация и аудит

Сухов Данила Евгеньевич

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

***Аннотация**: Статья «Основные принципы безопасности в Linux: аутентификация, авторизация и аудит» представляет собой обзор основных механизмов обеспечения безопасности в операционной системе Linux. Описывая принципы аутентификации, авторизации и аудита, статья объясняет их роль в обеспечении безопасности информационных систем. Авторизация рассматривается в контексте управления доступом пользователей к ресурсам системы, включая файлы, каталоги и привилегии выполнения команд. Обсуждаются различные механизмы управления доступом в Linux, такие как права доступа к файлам и каталогам, ACL, механизмы sudo и управление группами. Аннотация призвана заинтересовать читателей и подготовить их к погружению в более подробное изучение безопасности в среде Linux.*

***Abstract**: The "Linux Security Fundamentals: Authentication, Authorization, and Auditing" article provides an overview of the basic security mechanisms in the Linux operating system. Describing the principles of authentication, authorization, and auditing, the article explains their role in securing information systems. Authorization is discussed in the context of managing user access to system resources, including files, directories, and command execution privileges.*

Various access control mechanisms in Linux such as file and directory permissions, ACLs, sudo mechanisms, and group management are discussed. The abstract is intended to interest readers and prepare them to dive into a more detailed study of security in the Linux environment.

***Ключевые слова**: информационная безопасность, Linux, основные принципы безопасности, аутентификация, авторизация.*

***Keywords**: information security, Linux, basic security principles, authentication, authorisation.*

В мире информационной безопасности операционная система Linux часто воспринимается как стандарт золотого стандарта. Однако, чтобы действительно обеспечить безопасность в Linux-среде, необходимо понимать и применять основные принципы безопасности, включая аутентификацию, авторизацию и аудит.

Аутентификация: подтверждение личности

Аутентификация — это процесс подтверждения личности пользователя или системы. В Linux это может включать в себя использование паролей, SSH-ключей, биометрических данных и других методов идентификации. Пароли являются наиболее распространенным методом аутентификации в Linux. Хотя использование сложных и уникальных паролей является важным, также важно использовать механизмы двухфакторной аутентификации (2FA), такие как одноразовые пароли или биометрические данные, для дополнительного уровня безопасности.

SSH-ключи представляют собой альтернативный метод аутентификации, который предлагает более высокий уровень безопасности, чем пароли. Они особенно полезны для удаленного доступа к серверам Linux. При правильной настройке и использовании, SSH-ключи могут значительно снизить риск атак на систему.

Авторизация: управление доступом

После успешной аутентификации пользователя необходимо авторизовать для выполнения определенных действий или доступа к определен-

ным ресурсам. В Linux это достигается путем использования механизмов контроля доступа, таких как права доступа к файлам и каталогам (через механизмы POSIX или ACL), а также механизмы sudo (superuser do), который позволяет ограничить привилегии пользователей для выполнения определенных команд с привилегиями администратора.

Авторизация в Linux относится к процессу управления доступом пользователей к ресурсам системы, таким как файлы, каталоги, устройства и привилегии выполнения команд. Важно понимать, что успешная аутентификация пользователя (подтверждение его личности) еще не означает, что этот пользователь имеет доступ ко всем ресурсам и функциям системы. Авторизация определяет, какие действия может совершать пользователь после того, как его личность была подтверждена.

Правильная настройка прав доступа к файлам и каталогам является критически важной частью обеспечения безопасности в Linux. Неправильные настройки могут привести к утечке конфиденциальной информации или возможности злоумышленникам получить несанкционированный доступ к системе.

Эффективное управление доступом в Linux требует от администраторов систем понимания потребностей и ролей пользователей, а также соответствующей настройки прав доступа и привилегий. Правильная конфигурация уровня доступа минимизирует риск компрометации системы и обеспечивает соблюдение принципов безопасности информации. Регулярное аудитирование прав доступа и мониторинг активности пользователей также важны для обнаружения и предотвращения потенциальных угроз безопасности.

Аудит: отслеживание событий

Аудит — это процесс отслеживания и регистрации событий, происходящих в системе. В Linux это включает в себя регистрацию входов пользователя, изменений прав доступа, запуска привилегированных команд и других важных событий. Системы аудита, такие как Auditd, предоставляют механизмы для записи таких событий в журналы, что позволяет администраторам анализировать их в случае необходимости для обнаружения потенциальных угроз безопасности или инцидентов.

В заключение, основные принципы безопасности в Linux — это ключевые аспекты обеспечения безопасности информационных систем. Правильное применение аутентификации, авторизации и аудита помогает минимизировать риски безопасности и обеспечить защиту системы от широкого спектра угроз. Регулярное обновление и мониторинг этих механизмов также важно для поддержания высокого уровня безопасности в Linux-среде.

Список литературы

1. Разновидности нарушений безопасности и типовые атаки на операционную систему / Г. С. Бударный, А. А. Казанцев, А. В. Красов, А. В. Поляничева // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): Сборник научных статей XI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 15–16 февраля 2022 года / Под редакцией А. В. Шестакова, сост. В. С. Елагин, Е. А. Аникевич. Том 4. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. — С. 406–411. — EDN LSTCSC.
2. 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, 26–28 октября 2022 года. — Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. — С. 587–588. — EDN EGVVFU.
3. Методы обеспечения безопасности Astra Linux special Edition / П. С. Зылева, И. Е. Пестов, И. С. Тремель, У. С. Юрова // 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, 28 февраля — 01 2023 года. Том 1. — Санкт-Петербург: Санкт-Петер-

бургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. — С. 553–558. — EDN UMLNSB
4. Цветков, А. Ю. Исследование существующих механизмов защиты операционных систем семейства linux / А. Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля — 01 2018 года / Под редакцией С. В. Бачевского. Том 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. — С. 657–662. — EDN XSUGRV.
5. Горбань, С. А. Оценка эффективности механизмов контроля правами доступа в ос Linux / С. А. Горбань, А. В. Красов, А. Ю. Цветков // 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, 28 февраля — 01 2023 года. Том 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. — С. 345–348. — EDN CIKVBB.

УДК 004.7

Обзор возможностей интеграции Интернета Вещей и облачных вычислений

Заозерский Александр Александрович

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

***Аннотация**: В статье рассматриваются вопросы обеспечения интеграции Интернета Вещей (Internet of Things, IoT) и технологии облачных вычислений. Устройства в Интернете Вещей генерируют большой объём данных, известных как Большие Данные (Big Data). Для решения проблем хранения таких данных была введена концепция облачных вычислений, но данные в Интернете подвержены риску, а сложные алгоритмы шифрования не подходят для IoT-устройств. Главная цель данного исследования —*

обзор методов шифрования в Интернете Вещей и в облачных вычислениях и рассмотрение проблем интеграции двух концепций.

***Abstract**: This paper discusses ways to ensure the integration of Internet of Things (IoT) and cloud computing technology. Devices in the Internet of Things generate a large amount of data known as Big Data. The concept of cloud computing has been introduced to solve the problems of storing such data, but data on the Internet is at risk and complex encryption algorithms are not suitable for IoT devices. The main objective of this research is to review encryption techniques in Internet of Things and cloud computing and to address the challenges of integrating the two concepts.*

***Ключевые слова**: Интернет Вещей, облачные вычисления, Big Data, криптография.*

***Keywords**: Internet of Things, cloud computing, Big Data, cryptography.*

Введение

Интернет Вещей — это технология, объединяющая миллиарды устройств и обеспечивающая производство Больших Данных. С каждым днем количество типов данных увеличивается. Вещами в данном контексте могут быть любые устройства: телефоны, камеры, датчики, транспортные средства и т.д. Суть Интернета Вещей заключается в сборе, обмене и обработке данных без значительного вмешательства человека. Эта технология преобразует нашу жизнь, делая ее более умной: от умных домов до здоровья и городов. Умные вещи имеют ограниченные ресурсы, такие как батарея и оперативная память. Они требуют уникального протокола (Internet Protocol (IP)) для подключения к Интернету. Технология IoT основана на физических объектах, которые используют датчики для сбора и обмена данными через Интернет. Устройства в Интернете Вещей генерируют различные типы данных, которые можно разделить на три типа: мультиструктурные, структурные и неструктурные. Управление огромным объемом данных, генерируемых устройствами, является сложной задачей.

Одной из основных проблем является обеспечение конфиденциальности и безопасности данных в среде Интернета вещей, где множество приложений и устройств подвержены риску. Возможные риски включают потерю конфиденциальной информации или ее модификацию. Алгоритмы шифрования, хоть и являются более сложными, потребляют

больше энергии устройств. Следовательно, важно разработать эффективный механизм защиты IoT-устройств от злоумышленников и мощный алгоритм шифрования, который бы потреблял меньше вычислительных ресурсов.

В настоящее время связь между устройствами IoT становится все более удобной благодаря развитию технологий, таких как RFID (Radio Frequency Identification), мобильная связь, облачные вычисления и WSN (Wireless Sensor Networks). Различные датчики встроены в объекты и устройства, подключенные к Интернету Вещей. Собранные данные анализируются для передачи важной информации при помощи приложений. Эти данные могут быть используемы для прогнозирования различных проблем до их возникновения, выявления закономерностей и формирования оптимальных рекомендаций. Информация поступает в режиме реального времени, что помогает экономить время и деньги. Общая модель IoT показана на рисунке 1.

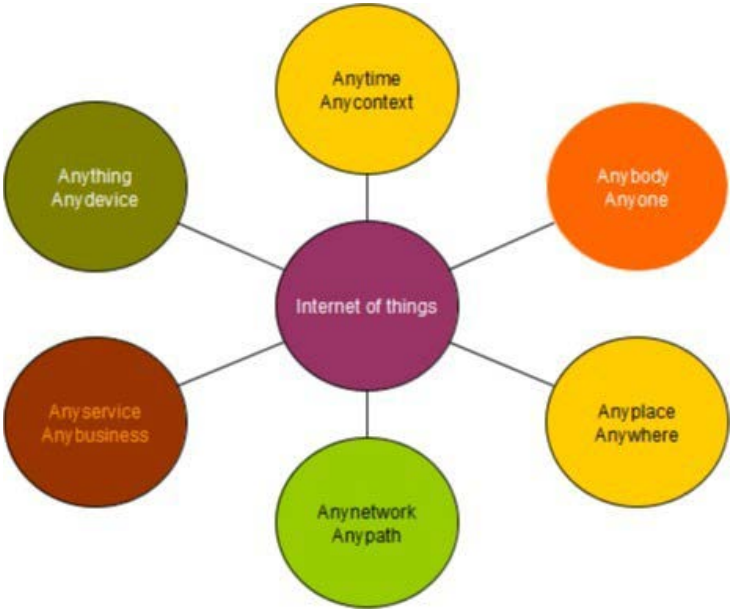

Рисунок 1. **Обобщённая модель Интернета Вещей**

Параметры безопасности в Интернете Вещей

Безопасность данных, собранных в облачных сетях в Интернете вещей, становится большой проблемой, а управление конфиденциальностью данных — сложной задачей. К сожалению, мобильные устройства и их программное обеспечение обычно разрабатываются так, что они не могут защититься от атак на безопасность. Безопасность и конфиденциальность данных, собранных устройствами в Интернете вещей, сложно контролировать. Количество устройств и атак увеличивается каждый день. Исследования показывают, что около 70% устройств в Интернете вещей легко взломать. Поэтому необходим эффективный механизм защиты облачных данных устройств на базе IoT. Ниже приведены некоторые ключевые параметры безопасности в IoT:

Конфиденциальность: передача данных между отправителем и получателем может быть легко взломана хакером. Безопасность в IoT для конечного пользователя обязательна. Конфиденциальность можно обеспечить с помощью шифрования и дешифрования.

Совместимость: в настоящее время не существует международного стандарта совместимости оборудования для маркировки и мониторинга. Производители этого оборудования должны договориться о стандарте, например, Bluetooth, USB и т.д.

Целостность: передача данных между источником и местом назначения происходит на разных этапах и без изменения данных. Злоумышленники проводят атаки в этот период. Необходимо использовать эффективные методы защиты передачи данных, чтобы злоумышленники не могли изменять или повреждать данные.

Доступность: необходимо гарантировать связь между проверенными пользователями. Для этого устройства в Интернете вещей должны иметь возможность проводить процедуру аутентификации.

Интеграция облачных вычислений и Интернета Вещей

В последние годы технология облачных вычислений оказывает значительное влияние на развитие интеллектуальных услуг. Основная цель облачных вычислений — обеспечить доступ к данным и информации через

интернет, что позволяет минимизировать или ограничить использование аппаратного оборудования. Структура Интернета Вещей может быть разной, и многие исследователи предложили различные архитектуры. Для работы Интернета Вещей необходимы четыре типа взаимосвязанных систем: пользовательские устройства, сетевые маршрутизаторы, инфраструктура сети и облачный сервер.

Облачные вычисления — это относительно новая область, которая позволяет получать доступ к данным и информации в любом месте и в любое время без необходимости в аппаратном оборудовании. Интернет Вещей и облачные вычисления имеют ряд общих характеристик, таких как хранение данных, обеспечение сервисов и приложений через интернет, и при этом требуют меньше вычислительных ресурсов, как показано в таблице 1.

Таблица 1. **Общие черты IoT и облачных вычислений**

Характеристика	Интернет Вещей	Облачные вычисления
Хранение данных в интернете	Да	Да
Услуги в интернете	Да	Да
Доступ к приложению	Да	Да
Без привязки к месту	Да	Да
Энергоэффективность	Да	Да
Вычислительные возможности	Да	Да

Интернет Вещей: существует множество устройств, включая датчики, смартфоны, транспортные средства и другие, которые взаимодействуют между собой по беспроводной связи. Для Интернета Вещей требуется умная система, способная управлять и обрабатывать данные. Примерами использования IoT являются охранная сигнализация, мобильные телефоны, GPS-навигаторы, умные устройства и датчики.

Сетевые маршрутизаторы: сетевые маршрутизаторы используются для подключения устройств, которые не могут напрямую взаимодействовать с интернетом. В телекоммуникациях термин «шлюз» относится к оборудованию, которое обеспечивает взаимодействие с другой сетью, использующей разные протоколы.

Инфраструктура сети: интернет представляет собой глобальную связь устройств через IP-сети. Инфраструктура сети включает в себя программные и аппаратные ресурсы, которые обеспечивают подключение устройств, передачу данных, операции и управление сетью. Структура сети включает маршрутизаторы, коммутаторы, сетевые карты и беспроводные маршрутизаторы для управления трафиком данных.

Облачный сервер: облачные вычисления представляют собой парадигму IT, которая обеспечивает универсальный доступ к общим ресурсам конфигурируемых систем с минимальными затратами на управление. Облако состоит из множества серверов, связанных между собой. Облачные системы выполняют различные типы приложений для анализа данных, полученных от разных объектов, для создания точных прогнозов, которые поддерживают экосистему Интернета Вещей. В облачной и IoT-среде данные с устройств могут храниться в облачном хранилище и доступ к ним можно получить в любой момент.

Общие сведения о методах обеспечения безопасности

Криптография: Криптография — это широко используемая и мощная техника обеспечения безопасности. Она применяется для защиты компьютерных паролей с использованием хэш-функции, а также для безопасной отправки электронной почты с помощью метода SSL. Криптография обеспечивает конфиденциальность (только авторизованный пользователь может получить доступ к данным), целостность (данные не могут быть изменены или подделаны) и доступность (данные доступны в любой необходимый момент). В криптографии данные сохраняются и передаются в форме, понятной только отправителю и получателю. Сторонние лица не могут понять или получить доступ к этим данным. Шифрование и дешифрование — два основных термина в криптографии. Криптография имеет два основных типа: симметричная и асимметричная.

Симметричная криптография: В симметричной криптографии один и тот же ключ используется для шифрования и дешифрования данных. Отправитель шифрует данные ключом и передает их получателю, который затем дешифрует их тем же ключом. Существуют различные алгоритмы симме-

тричной криптографии, такие как DES (Data Encryption Standard), AES (Advanced Encryption Standard), Block Cipher, Caesar Cipher и Stream Cipher.

Стандарт шифрования данных (DES): DES — это тип симметричной криптографии, основанный на блочном шифре, разработанном Хорстом Фейстелем. В DES один и тот же ключ используется для шифрования и дешифрования. DES шифрует блоки данных размером 64 бита. Длина ключа в DES составляет 56 бит, но 8 из 64 бит не используются для шифрования.

Стандарт расширенного шифрования (AES): AES — это популярный и широко используемый метод шифрования для защиты информации. AES работает быстрее, чем DES и 3DES. Для шифрования в AES используются ключи длиной 128, 192 и 256 бит. [1]

Асимметричное шифрование: Асимметричная криптография, или шифрование с открытым ключом, использует два разных ключа для шифрования и дешифрования данных. Отправитель и получатель используют свои собственные открытый и закрытый ключи. Открытый ключ используется для шифрования, а закрытый — для дешифрования. Существуют различные алгоритмы асимметричной криптографии, такие как ECC (Elliptic Curve Cryptography), Diffie-Hellman и RSA (Rivest-Shamir-Adleman).

Криптография Ривеста-Шамира-Адлемана (RSA): RSA — это тип асимметричной криптографии, названный по именам ее создателей: Рональда Линна Ривеста, Ади Шамира и Леонарда Макса Адлемана. RSA чаще всего используется для шифрования с открытым ключом. Данные шифруются с помощью открытого ключа, который передается другим пользователям, а закрытый ключ используется только для расшифровки данных. В облачных вычислениях RSA используется для шифрования данных и их хранения в облаке, чтобы защитить данные от несанкционированного доступа. Пользователь получает доступ к данным после проверки его подлинности.

Легкая криптография: Интернет Вещей представляет собой совокупность подключенных машин и людей для связи и передачи данных. Умные устройства в IoT потребляют меньше энергии и имеют низкую вычислительную стоимость, поэтому для защиты данных необходимо использовать легкую криптографию. Это форма криптографии, которая используется в ограниченных условиях, например, на датчиках, медицинских устройствах, бесконтактных смарт-картах, RFID-метках и так далее. При

разработке методов легкой криптографии необходимо учитывать как программные, так и аппаратные характеристики: время шифрования/дешифровки, потребляемую энергию и объем оперативной памяти для компиляции. Легкая криптография предполагает меньшие вычислительные затраты, но это не означает, что она ухудшает безопасность.

Стеганография: термин «стеганография» происходит от греческого слова «steganos», что означает «скрытый», и «graphein», что означает «рисунок» или «письмо». Стеганография буквально означает «скрытое письмо». Греки использовали эту технику около 2000 лет назад для передачи секретной информации. Стеганография — это способ сокрытия секретной информации в другой информации. Файл или данные, которые используются для сокрытия секретной информации, называются носителем. Информация скрывается внутри носителя так, что он выглядит как оригинал. Изображения, аудио и видео являются лучшими носителями для такой информации. В сущности, стеганография — это сокрытие информации без ее шифрования.

В таблице 2 представлен сравнительный анализ некоторых из самых популярных алгоритмов шифрования.

Таблица 2. **Сравнение некоторых алгоритмов шифрования**

Информация	DES	AES	RSA	ECC
Дата разработки	1977	2000	1978	1985
Размер ключа (биты)	56	128, 192 и 256	Минимум 1024	Максимум 1024
Размер блоков (биты)	64	128	512	–
Техника	Симметричный	Симметричный	Асимметричный	Асимметричный
Ключ для шифрования и дешифрования	Один ключ	Один ключ	Разные ключи	Разные ключи
Масштабируемость	Масштабируемый	–	–	–
Потребление энергии	Низкий	Низкий	Высокий	Низкий

Таблица 2 **(продолжение)**

Шифрование и дешифрование	Быстрое	Быстрое	Медленное	Медленное
Реализация	Быстро	Быстро	Медленно	Быстро
Встроенные уязвимости	Атака грубой силы, различные крипто аналитические и линейные атаки	Атака грубой силы	Атака грубой силы	Атака грубой силы, атака по сторонним каналам

Проблемы интеграции Интернета Вещей и облачных вычислений

Безопасность интеграции является ключевой проблемой, особенно когда развитие критически важных приложений Интернета Вещей смещается в сторону применения технологий облачных вычислений. Это вызывает вопросы о доверии к поставщику услуг, особенно когда речь идет о физическом местоположении данных. Нельзя применять криптографию с открытым ключом на всех уровнях из-за ограниченной вычислительной мощности устройств Интернета Вещей. [2] Проблемы, которые необходимо решить при интеграции этих технологий, включают:

Неоднородность: это ключевая проблема интеграции облачных вычислений и IoT, связанная с разнообразием устройств, операционных систем, платформ и услуг.

Производительность: интеграция облачных вычислений и IoT часто требует специфических требований к производительности и качеству обслуживания технологических платформ, которые некоторые сценарии интеграции могут не выполнить.

Надежность: при интеграции облачных вычислений и IoT для критически важных приложений возникают проблемы надежности, особенно при использовании в условиях интеллектуальной мобильности. Уровень соединения для движущихся транспортных средств часто бывает низким, а развертывание приложений с ограниченными ресурсами может привести к отказу в обслуживании или невозможности связи с устройствами.

Большие данные: с учетом около 13 млрд устройств в Интернете Вещей, транспортировка, хранение, доступ и обработка огромного количества данных, которые они производят, требуют особого внимания. Масштабируемость вычислительных платформ становится основной потребностью из-за повсеместности мобильных устройств и распространенности сенсоров. [3]

Мониторинг: в облачных средах мониторинг является важным видом профилактической деятельности для своевременного планирования и управления ресурсами, производительностью и безопасностью, а также для оперативного реагирования на возникающие проблемы и их устранения.

В таблице 3 обобщены проблемы интеграции этих технологий, связанные в основном с безопасностью. Среди них две основные общие проблемы — производительность и большие данные.

Таблица 3. **Проблемы безопасности в Интернете Вещей и облачных вычислениях**

Проблемы безопасности	**Разнородность**	**Производительность**	**Надежность**	**Большие данные**	**Мониторинг**
Интернет Вещей	Нет	Да	Да	Да	Да
Облачные вычисления	Да	Да	Нет	Да	Нет

Заключение

Интернет Вещей предоставляет решения для управления устройствами, включая использование мобильных приложений. Технология облачных вычислений, с одной стороны, предлагает множество возможностей, с другой — накладывает определенные ограничения. Облачные вычисления представляют собой инфраструктурное решение, где обработка и хранение данных происходят вне мобильного устройства.

Интеграция IoT и облачных вычислений может уменьшить вычислительные затраты, так как эти системы имеют связанные особенности, включая хранение данных, сервисы, приложения через Интернет, а также энергетическую и вычислительную эффективность. Кроме того, различные криптографические методы могут быть использованы для обеспечения доступности, целостности и конфиденциальности данных.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
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. 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.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
5. 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.

УДК 004.7

Эволюция программно-аппаратных средств защиты информации: современные тренды и вызовы

Заозерский Александр Александрович

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

***Аннотация**: Статья рассматривает современные тренды и вызовы в области программно-аппаратных средств защиты информации. С увеличением объемов цифровой информации и постоянно меняющейся обстановкой эволюция таких средств становится необходимостью. Обсуждаются такие аспекты, как использование искусственного интеллекта, защита в облаке, квантовая криптография, а также автоматизация и оркестрация процессов безопасности.*

***Abstract**: This article examines the current trends and challenges in the field of hardware and software-based information security. With the increasing amount of digital information and the ever-changing environment, the evolution of such tools becomes a necessity. Aspects such as the use of artificial intelligence, protection in the cloud, quantum cryptography, and automation and orchestration of security processes are discussed.*

***Ключевые слова**: программно-аппаратные средства защиты информации, искусственный интеллект, защита в облаке, квантовая криптография, автоматизация, безопасность данных.*

***Keywords**: software and hardware means of information protection, artificial intelligence, protection in the cloud, quantum cryptography, automation, data security.*

Введение

В эпоху цифровизации и столь быстрого развития технологий обеспечение безопасности информации становится одним из наиболее важных аспектов в современном мире. С увеличением объемов цифровых данных и разнообразия угроз информационной безопасности программно-аппаратные средства защиты информации играют ключевую роль в обеспечении конфиденциальности, целостности и доступности данных. Однако, с течением времени, ситуация на поле информационной безопасности неуклонно меняется, и появляются новые угрозы и вызовы.

Современный цифровой ландшафт характеризуется постоянным развитием технологий, расширением киберугроз и усилением кибератак. Это создает потребность в постоянном совершенствовании программно-аппаратных средств защиты информации для эффективного противодействия современным угрозам.

В данной статье мы обратим внимание на современные тренды и вызовы, с которыми сталкиваются программно-аппаратные средства защиты информации. Мы рассмотрим влияние искусственного интеллекта, защиту в облаке, квантовую криптографию, а также важность автоматизации и оркестрации процессов безопасности в современной цифровой экосистеме. Понимание этих трендов и вызовов не только поможет в эффективной борьбе с киберугрозами, но и обеспечит повышение уровня безопасности данных в цифровой эпохе.

Исторический обзор

С момента, когда человек впервые осознал необходимость защиты своих данных, начался исторический путь развития методов обеспечения информационной безопасности. В его основе лежит эволюция криптографии, антивирусной защиты и других средств, направленных на сохранение конфиденциальности и целостности информации.

Ранние методы криптографии

Шифр Цезаря: Один из самых простых и ранних методов шифрования, где каждая буква заменяется на другую букву алфавита с фиксированным сдвигом.

Шифр Атбаш: Еще один простой метод, где каждая буква заменяется на противоположную в алфавите.

Шифр Виженера: Впервые использовал ключевое слово для создания повторяющегося ключа для шифрования текста. Этот метод считается первым примером полиалфавитного шифра и представляет собой существенное улучшение по сравнению с моноалфавитными шифрами.

Криптография во время Второй мировой войны

Энигма: Немецкая шифровальная машина, использовавшаяся для шифрования сообщений во время Второй мировой войны. Расшифровка Энигмы английскими кодировщиками стала одним из ключевых моментов в ходе войны, что дало альянсу союзников существенное преимущество в разведке.

Улучшение криптографических методов: В результате Второй мировой войны криптографы начали разрабатывать более сложные методы шифрования и разгадывания шифров, открывая новые направления в науке о криптографии.

Развитие криптографии в эпоху компьютеров

Шифрование с открытым ключом: Изобретенное в 1970-х годах, шифрование с открытым ключом стало революционным методом шифрования, который позволяет безопасно обмениваться ключами через открытые каналы.

Стандарты шифрования: Развитие стандартов шифрования, таких как DES (Data Encryption Standard), AES (Advanced Encryption Standard) и RSA (Rivest-Shamir-Adleman), способствовало повышению уровня безопасности в информационных системах.

Развитие средств защиты от вирусов и кибератак

Первые антивирусные программы: В начале 1980-х годов появились первые антивирусные программы, которые помогали обнаруживать и удалять вредоносные программы с компьютеров.

Фаерволы: Развитие средств контроля и фильтрации сетевого трафика, таких как фаерволы, стало ключевым шагом в обеспечении безопасности сетей.

Системы обнаружения вторжений: В конце 1990-х годов начали активно разрабатываться системы обнаружения вторжений (IDS), которые помогали выявлять аномальное поведение в сети и реагировать на потенциальные угрозы.

Этот обзор демонстрирует, как криптография и средства защиты информации эволюционировали от простых методов шифрования до сложных систем безопасности, адаптируясь к изменяющимся угрозам в сфере информационной безопасности.

В современном мире, где угрозы информационной безопасности становятся все более сложными и утонченными, развитие программно-аппаратных средств защиты информации играет ключевую роль в обеспечении безопасности данных. Новейшие технологии и подходы отражают стремление к непрерывному улучшению защиты и адаптации к постоянно меняющейся среде. В рамках темы «Эволюция программно-аппаратных средств защиты информации: современные тренды и вызовы» можно выделить несколько ключевых направлений развития:

Развитие искусственного интеллекта (ИИ)

Современные системы защиты информации все чаще внедряют технологии искусственного интеллекта для более точного обнаружения и пред-

отвращения угроз. Методы машинного обучения и анализа больших данных позволяют создавать интеллектуальные системы, способные быстро адаптироваться к новым видам атак и выявлять аномальное поведение в реальном времени.

Использование блокчейн технологий

Блокчейн технологии нашли свое применение не только в области криптовалют, но и в обеспечении безопасности информации. За счет своей децентрализованной и прозрачной природы блокчейн может быть использован для создания надежных систем хранения и передачи данных, исключающих возможность подделки или изменения информации.

Интеграция квантовой криптографии

Квантовая криптография представляет собой новую фронтальную область в обеспечении безопасности информации. Она основана на принципах квантовой механики и предлагает методы шифрования, устойчивые к атакам с использованием квантовых компьютеров. Интеграция квантовой криптографии может стать перспективным решением для обеспечения надежной защиты данных в будущем.

Улучшение аутентификации и управления доступом

Безопасность информации также зависит от эффективных методов аутентификации и управления доступом. Современные технологии включают в себя биометрическую идентификацию, многофакторную аутентификацию и интеллектуальные системы управления доступом, которые помогают предотвратить несанкционированный доступ к данным.

Развитие квантово-стойкой криптографии

Учитывая потенциальные угрозы, связанные с развитием квантовых компьютеров и их способности ломать существующие криптографические

алгоритмы, активно ведется исследование и разработка квантово-стойких алгоритмов шифрования, которые будут устойчивы к атакам как современных, так и квантовых компьютеров.

Эти направления развития являются лишь частью широкого спектра инноваций в области программно-аппаратных средств защиты информации. Вместе они стремятся к созданию более надежных, эффективных и адаптивных систем обеспечения безопасности, способных противостоять все более сложным и усовершенствованным угрозам.

Искусственный интеллект в защите данных

С развитием искусственного интеллекта (ИИ) и машинного обучения (МО) наблюдается переход от традиционных методов обнаружения угроз к более эффективным и автоматизированным системам защиты. Системы ИИ могут обнаруживать необычное поведение в сетях и приложениях, выявлять аномальные активности и предсказывать потенциальные угрозы, что значительно повышает уровень безопасности.

Защита в облаке

С развитием облачных технологий возникают новые вызовы в области безопасности данных. Концепции Zero Trust и микросегментация используются для обеспечения безопасного доступа к облачным сервисам и контроля трафика в облаке. Программно-аппаратные решения должны адаптироваться к особенностям облачных сред и обеспечивать защиту данных в условиях динамичной инфраструктуры.

Квантовая криптография

С развитием квантовых технологий становится необходимым разработка квантовоустойчивых алгоритмов шифрования и аутентификации. Программно-аппаратные средства защиты информации должны быть способны обеспечить защиту данных от квантовых атак, что требует пересмотра традиционных методов криптографии и разработки новых подходов.

Автоматизация и оркестрация

Для эффективного реагирования на угрозы необходима автоматизация процессов обнаружения, анализа и реагирования. Программно-аппаратные средства защиты информации должны интегрироваться с системами автоматизации и оркестрации, обеспечивая быструю и координированную реакцию на инциденты безопасности.

Заключение

Прогресс и постоянные изменения в области информационных технологий непрерывно подталкивают нас к эволюции программно-аппаратных средств защиты информации. Современные тренды, такие как использование искусственного интеллекта для обнаружения угроз, защита данных в облаке для адаптации к облачным средам, квантовая криптография для повышения степени защиты, и автоматизация процессов безопасности для более оперативного реагирования на инциденты, создают новые вызовы и возможности в сфере безопасности информации.

Развитие инновационных программно-аппаратных средств защиты данных становится неотъемлемым элементом обеспечения надежной защиты в нашем цифровом мире. Но для того, чтобы успешно справляться с современными угрозами, необходимо постоянно улучшать технологии и адаптироваться к изменяющейся среде. Только так мы сможем гарантировать безопасность данных в условиях быстро развивающегося цифрового ландшафта и сохранять доверие пользователей к информационным технологиям.

Безопасность информации является ключевым фактором успеха в современном мире, и только путем постоянного совершенствования и адаптации мы сможем обеспечить ее надежность и целостность данных в будущем.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика” РИ-2018”.— 2018. — С. 149–149.

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. 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.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018".— 2018. — С. 149–149.
5. 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.

УДК 004.7

Роль человеческого фактора в информационной безопасности

Заозерский Александр Александрович

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

***Аннотация**: Статья рассматривает роль человеческого фактора в обеспечении информационной безопасности. Освещаются угрозы, такие как социальная инженерия и недостаточная осведомленность сотрудников, а также предлагаются стратегии и технологические инновации для их преодоления. Работа будет полезна специалистам и руководителям, заинтересованным в защите данных организации.*

***Abstract**: The article considers the role of human factor in ensuring information security. Threats such as social engineering and lack of employee awareness are highlighted, and strategies and technological innovations to overcome them are proposed. The paper will be useful to professionals and managers interested in protecting organizational data.*

***Ключевые слова**: человеческий фактор, защита данных, социальная инженерия, многоуровневая защита, множественная аутентификация, машинное обучение, стратегии безопасности.*

***Keywords**: human factor, data protection, social engineering, layered security, multiple authentication, machine learning, security strategies.*

Введение

В современном мире безопасности информации, управление человеческим фактором становится ключевым элементом. Недостаточная осведомленность сотрудников и их возможная уязвимость перед социальной инженерией оставляют организации открытыми для атак. Это подчеркивает необходимость балансирования технических мер безопасности с обучением и образованием персонала. Осознание этой проблемы и принятие соответствующих мер позволят компаниям эффективно справиться с угрозами информационной безопасности в современном цифровом мире.

В данной статье мы глубже рассмотрим роль человеческого фактора в обеспечении информационной безопасности, выявим основные угрозы, связанные с ним, а также предложим стратегии и инновации, направленные на укрепление защиты от этих угроз. Осознание важности человеческого фактора и принятие соответствующих мер по его управлению помогут организациям сделать свои данные более защищенными в эпоху все возрастающих киберугроз.

Человеческий фактор как слабое звено

Человеческий фактор играет ключевую роль в обеспечении информационной безопасности организации. Однако, часто это является слабым звеном из-за неосведомленности, непреднамеренных ошибок или действий под воздействием манипуляций.

Социальная инженерия: Это метод атаки, когда злоумышленники используют психологические механизмы, чтобы убедить сотрудника выполнить определенные действия, такие как предоставление доступа к системам или раскрытие конфиденциальной информации.

Фишинг: Этот вид атаки подразумевает маскировку под легитимные источники (например, электронные письма или веб-сайты), чтобы обма-

нуть пользователей и получить от них конфиденциальные данные, такие как пароли или номера кредитных карт.

Недостаточная осведомленность: Многие сотрудники не обладают достаточным пониманием рисков информационной безопасности или правилами обращения с конфиденциальной информацией. Это может привести к непреднамеренным нарушениям безопасности, таким как слабые пароли или открытие вредоносных вложений в электронных письмах.

Стратегии для преодоления угроз

Обучение и осведомленность: Регулярные тренинги и обучающие сессии помогут сотрудникам лучше понять угрозы информационной безопасности и научат их правильным практикам, таким как создание надежных паролей и распознавание фишинговых попыток.

Многоуровневая защита: Внедрение нескольких уровней защиты, таких как антивирусное программное обеспечение, брандмауэры и системы обнаружения вторжений, поможет уменьшить вероятность успешной атаки, даже если человеческий фактор был компрометирован.

Создание культуры безопасности: Организации должны поощрять культуру безопасности, в которой безопасность данных признается как общая ответственность всех сотрудников, а не только ИТ-отдела.

Технологические инновации в поддержку человеческого фактора:

Множественная аутентификация (MFA): Эта технология требует от пользователя предоставить дополнительные данные для подтверждения своей личности, помогая защитить учетные записи от компрометации даже в случае утечки пароля.

Машинное обучение и искусственный интеллект

Машинное обучение (МО) и искусственный интеллект (ИИ) становятся все более важными инструментами в обеспечении информационной безопасности, особенно в контексте борьбы с внутренними угрозами, такими как действия инсайдеров. Эти технологии позволяют организациям

автоматизировать процессы обнаружения аномалий, идентифицировать подозрительное поведение сотрудников и своевременно реагировать на потенциальные угрозы.

Одним из основных преимуществ МО и ИИ является их способность анализировать большие объемы данных в реальном времени и выявлять скрытые паттерны, которые могут указывать на потенциальные угрозы безопасности. Например, системы машинного обучения могут анализировать доступ к файлам и ресурсам, типичное поведение пользователей и транзакционные данные, чтобы выявить аномалии, указывающие на возможные намеренные или ненамеренные нарушения безопасности.

Таким образом, МО и ИИ представляют собой мощные инструменты для обеспечения безопасности организации путем обнаружения и предотвращения внутренних угроз. Их использование позволяет организациям быстро адаптироваться к постоянно изменяющимся сценариям атак и обеспечивать непрерывную защиту информации.

Проактивный мониторинг и аналитика

Этот подход включает в себя несколько ключевых шагов:

Сбор данных: Специализированные инструменты собирают информацию о сетевой активности, журналах событий, а также другие данные, которые могут быть связаны с безопасностью.

Анализ данных: Полученные данные анализируются с использованием алгоритмов машинного обучения, статистических методов и других аналитических техник для выявления аномальных паттернов или подозрительной активности.

Обнаружение угроз: На основе результатов анализа выявляются потенциальные угрозы и рассматриваются как объекты для дальнейшего расследования.

Реагирование и предотвращение: В случае обнаружения угрозы принимаются меры по ее нейтрализации и предотвращению ущерба. Это может включать в себя блокировку доступа, изоляцию уязвимых устройств или систем, а также восстановление данных, если это необходимо.

Постоянное совершенствование стратегий безопасности

Развитие стратегий безопасности должно быть постоянным процессом. Организации должны регулярно анализировать свои политики безопасности и внедрять обновления, учитывая новые методы атак и опыт предыдущих инцидентов. Это включает в себя как технические, так и организационные аспекты, такие как обучение сотрудников и улучшение процессов реагирования на инциденты.

Заключение

В заключение, стоит подчеркнуть, что человеческий фактор играет критическую роль в обеспечении информационной безопасности организаций. Недооценка этого аспекта может привести к серьезным последствиям, включая утечку конфиденциальных данных, финансовые потери и ущерб репутации. Однако, при правильном подходе, человеческий фактор может стать не проблемой, а частью решения.

Обучение сотрудников, создание культуры безопасности и внедрение технологических решений, таких как множественная аутентификация и системы машинного обучения, помогают укрепить защиту от угроз, связанных с человеческим фактором. Кроме того, постоянное совершенствование стратегий безопасности и адаптация к новым методам атак помогают организациям оставаться на шаг впереди потенциальных угроз.

Только интегрированный подход, объединяющий технические меры безопасности, обучение персонала и применение передовых технологий, позволит организациям минимизировать риски и обеспечить эффективную защиту информации в современном цифровом мире.

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. 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.
3. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 563–568.
4. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании.— 2015. — С. 193–197.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 406–411.

УДК 004

Роль обновлений программного обеспечения (ПО) в обеспечении безопасности информационных систем

Макшанский Анатолий Романович

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

***Аннотация**: Обновления ПО критически важны для безопасности систем. Они исправляют уязвимости, внедряют новые механизмы защиты и минимизируют риски. Регулярные обновления обеспечивают надежную защиту данных. Установка обновлений вовремя — ключевой шаг для безопасности систем.*

***Abstract**: Software updates are critical to the security of systems. They patch vulnerabilities, implement new security mechanisms, and minimize risks. Regular updates ensure reliable data protection. Installing updates on time is a key step to secure systems.*

***Ключевые слова**: обновления ПО, безопасность, уязвимости, защита данных, риски, механизмы защиты, регулярные обновления, надежность.*

***Keywords**: software updates, security, vulnerabilities, data protection, risks, protection mechanisms, regular updates, reliability.*

В контексте изощрённости киберугроз в сфере цифровой информационной безопасности, императив безопасной эксплуатации информационных систем (ИС) для корпоративных структур и индивидуальных пользователей набирает первостепенную значимость. Одним из ведущих методологических инструментов, направленных на минимизацию рисков проникновения в систему и потенциальных утечек данных, является последовательное применение обновлений программного обеспечения (ПО).

Рассмотрим ключевые аспекты, обосновывающие значимость обновлений ПО в контексте обеспечения кибербезопасности:

1. Ликвидация уязвимостей и программных дефектов: Программное обеспечение по своей сути представляет собой подверженную ошибкам структуру, где каждая отдельная уязвимость может стать точкой входа для злоумышленников. Систематическое обновление ПО обеспечивает разработчиков механизмом оперативного устранения выявленных слабостей и недоработок кода, тем самым существенно снижая вероятность кибер-инцидентов и компрометации данных. Пренебрежение регулярными обновлениями ПО оставляет информационную систему уязвимой к эксплойтам, повышая риски деструктивных последствий.
2. Интеграция передовых защитных механизмов: Обновления ПО часто сопровождаются внедрением усовершенствованных функций и механизмов защиты, предназначенных для повышения уровня секьюрности ИС. Данное улучшение может охватывать обновления алгоритмов криптографической защиты, реализацию продвинутых методик обнаружения вредоносных программ, а также совершенствование механизмов контроля доступа. Эволютивное обновление ПО способствует поддержанию системы в состоянии готовности к противостоянию с актуальными и потенциальными киберугрозами, эффективно оберегая пользовательские данные.

Однако многие организации и пользователи часто пренебрегают обновлениями ПО из-за неудобств или недостатка времени. Это ошибка,

которая может привести к серьезным последствиям. Например, необновленное ПО может стать легкой добычей для хакеров, которые могут использовать известные уязвимости для взлома системы или кражи конфиденциальных данных.

Поэтому важно осознавать что, регулярные обновления программного обеспечения являются неотъемлемой частью стратегии обеспечения безопасности информационных систем. Они помогают устранять уязвимости, улучшать механизмы защиты и минимизировать риски кибератак. Поэтому важно следить за доступными обновлениями и устанавливать их своевременно, чтобы обеспечить надежную защиту своей системы и данных

Иногда корпорации и отдельные пользователи пренебрегают процедурой обновления ПО, исходя из соображений временных издержек или неудобства процедуры, что категорически недопустимо в условиях острых киберугроз. Игнорирование обновлений может привести к легкому доступу хакерских атак через известные уязвимости, что потенциально влечёт за собой кражу конфиденциальных данных. Таким образом, регулярные обновления ПО являются существенным элементом стратегии по обеспечению информационной безопасности, функционируя как ключевой механизм для нейтрализации уязвимостей, улучшения механизмов защиты и минимизации рисков цифровых угроз. Актуализация ПО должна рассматриваться как приоритетная задача, обеспечивающая защиту информационной системы и данных.

Вывод заключается в том, что регулярное и своевременное обновление программного обеспечения становится корнерстоуном в концепции кибербезопасности информационных систем. Это обеспечивает прочный фундамент для защиты от киберугроз и гарантирует конфиденциальность и целостность данных. Следовательно, важность своевременной апдейт-процедуры не может быть недооценена в современной цифровой эпохе.

Список литературы

1. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей Красов А.В., Штеренберг С.И., Голузина Д. Р. Электросвязь. 2019. № 11. С. 39–47.

2. Уязвимости программно-определяемых сетей Волкогонов В.Н., Преображенский А.И., Ушаков И.А. В сборнике: 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.
3. Метрика защищенности интернет вещей Крылов А.В., Ушаков И.А. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 622–626.
4. Анализ механизмов разграничения доступа в системах специального назначения Катасонов А.И., Цветков А.Ю. В сборнике: 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.
5. Общая методика обнаружения инсайдера компьютерной сети на основе технологий больших данных Котенко И.В., Пелёвин Д.В., Ушаков И.А. В сборнике: 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. 572–576.

УДК 004

Протоколы шифрования и аутентификации в беспроводных сетях: особенности и рекомендации по использованию

Макшанский Анатолий Романович

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

***Аннотация**: Статья об особенностях протоколов шифрования и аутентификации в беспроводных сетях, рекомендации по обеспечению безопасности передачи данных. Обсуждаются протоколы WPA, WPA2, WPA3, EAP, RADIUS, методы повыше-*

ния безопасности. Рекомендации: использование современных протоколов, избегание устаревших, внедрение двухфакторной аутентификации, регулярное обновление ПО. Правильный выбор и настройка протоколов важны для минимизации рисков утечки данных и несанкционированного доступа.

***Abstract**: The article is about the peculiarities of encryption and authentication protocols in wireless networks. It provides recommendations to ensure the security of data transmission. WPA, WPA2, WPA3, EAP, RADIUS protocols and methods of security enhancement are discussed. Recommendations are as follows: use modern protocols, avoid obsolete ones, implement two-factor authentication, regularly update software. Proper selection and configuration of protocols are important to minimize the risks of data leakage and unauthorized access.*

***Ключевые слова**: Протоколы шифрования, аутентификации, беспроводные сети, WPA, WPA2, WPA3, EAP, RADIUS, безопасность данных, утечка информации, несанкционированный доступ, современные протоколы, двухфакторная аутентификация, обновление ПО.*

***Keywords**: Encryption protocols, authentication, wireless networks, WPA, WPA2, WPA3, EAP, RADIUS, data security, information leakage, unauthorized access, modern protocols, two-factor authentication, software update.*

Беспроводные коммуникационные сети образуют фундаментальную инфраструктуру в современных информационно-коммуникационных системах, ориентированных на обеспечение мобильности и доступности данных в реальном времени. В контексте сохранения конфиденциальности и целостности передаваемых данных, применение адекватных механизмов криптографической защиты и аутентификации является критическим.

Один из базовых протоколов безопасности — WPA (Wi-Fi Protected Access) — был разработан для устранения уязвимостей WEP (Wired Equivalent Privacy), используя алгоритм TKIP (Temporal Key Integrity Protocol) для динамического ключевого управления и шифрования на пакетном уровне. Несмотря на значительные улучшения, эксплуатация криптографических слабостей TKIP показала необходимость перехода к более совершенным стандартам.

В реализации WPA2 применяется алгоритм AES (Advanced Encryption Standard) в режиме CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), который предлагает высокую степень

защиты от атак, сопряженных с перехватом данных, благодаря механизму обеспечения целостности и конфиденциальности информации. WPA3, развивая концепцию предшественника, вводит дополнительные методы, такие как защита от атак подбора пароля через оффлайн-методы, и улучшенную криптографическую защиту данных в сетевом взаимодействии.

Использование более современных версий протоколов шифрования, таких как WPA2 или WPA3, рекомендуется для обеспечения наивысшего уровня безопасности в беспроводных сетях. Эти версии протоколов обладают более сильными механизмами защиты и помогают предотвратить возможные атаки на данные, передаваемые по беспроводной сети. Таким образом, переход на более современные версии протоколов шифрования является важным шагом для обеспечения безопасности вашей беспроводной сети..

Для аутентификации субъектов в беспроводных сетях широко используются протоколы на базе EAP (Extensible Authentication Protocol), который поддерживает множество механизмов проверки подлинности, включая цифровые сертификаты, одноразовые пароли и биометрию, обеспечивая гибкость и расширяемость процесса аутентификации. Протокол RADIUS (Remote Authentication Dial-In User Service) служит в качестве централизованного диспетчера аутентификации, облегчая управление доступом пользователей и наделяя систему возможностью учета и мониторинга активности сетевых сессий.

В контексте разработки и эксплуатации беспроводных сетевых инфраструктур, настоятельно рекомендуется придерживаться следующих рекомендаций:

1. Интеграция современных стандартов шифрования, таких как WPA3, для максимизации уровня защиты данных.
2. Исключение использования устаревших и компрометированных протоколов типа WEP, уязвимых к взломам.
3. Реализация принципа многофакторной аутентификации для укрепления системы контроля доступа.
4. Систематическое обновление программного обеспечения аппаратных средств, включенных в сеть, для исправления известных уязвимостей и повышения резистентности к новым угрозам безопасности.

Применение продвинутых протоколов и алгоритмов в сфере шифрования и аутентификации лежит в основе обеспечения защищенности беспроводных сетей, предотвращая несанкционированный доступ и утечку конфиденциальных данных, тем самым поддерживая целостность и доступность информационных ресурсов.

В целом, правильный выбор и настройка протоколов шифрования и аутентификации играют ключевую роль в обеспечении безопасности беспроводных сетей. Следуя рекомендациям по использованию современных протоколов и дополнительным мерам безопасности, можно минимизировать риски утечки данных и несанкционированного доступа, обеспечивая защиту конфиденциальности информации в беспроводных сетях.

Список литературы

1. Построение доверенной вычислительной среды 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. Санкт-Петербург, 2019.
2. Построение защищенных сетевых соединений на основе отечественного оборудования Кравцова В.А., Ушаков И.А. В сборнике: 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. 702–706.
3. Анализ защищенности современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера raspberry pi Габуев А.Г., Красов А.В., Ощенков Ф.Д., Тарасов Н.М. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 295–298.
4. Результаты анализа функционирования механизмов защиты в беспроводных сетях передачи данных Подшибякин А.С., Ушаков И.А., Шинкаренко А. Ф. Труды Военно-космической академии имени А.Ф.Можайского. 2021. № 678. С. 163–174.

5. Исследование методов обнаружения бэкдоров, основанных на пассивном мониторинге каналов доступа Батин Е.А., Катасонов А.И. В сборнике: 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. 127–131.

УДК 004

Основные принципы стеганографии и её отличие от криптографии

Макшанский Анатолий Романович

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

***Аннотация**: Стеганография и криптография — разные области информационной безопасности. Стеганография скрывает факт сообщения, а криптография — содержание. Обе могут комбинироваться для безопасности данных.*

***Abstract**: Steganography and cryptography are different areas of information security. Steganography hides the fact of a message, while cryptography hides the content. Both can be combined for data security.*

***Ключевые слова**: Стеганография, криптография, информационная безопасность, конфиденциальность данных, скрытие сообщения, шифрование, алгоритмы, ключ, извлечение информации, носитель, шифрованные данные, обмен сообщениями, конфиденциальность, целостность данных, комбинация технологий.*

***Keywords**: Steganography, cryptography, information security, data confidentiality, message hiding, encryption, algorithms, key, information extraction, carrier, encrypted data, messaging, confidentiality, data integrity, combination of technologies.*

Стеганография и криптография — две разные области информационной безопасности, хотя и обе направлены на защиту конфиденциальности данных. Основным отличием между ними является то, что стеганография

скрывает сам факт существования сообщения, в то время как криптография скрывает содержание сообщения.

Основные принципы стеганографии включают в себя следующие:

1. Скрытность: основной принцип стеганографии заключается в том, чтобы скрыть наличие самого сообщения или информации. Это означает, что стеганографическое сообщение должно быть невидимым для посторонних наблюдателей.
2. Невозможность обнаружения: стеганографические методы должны быть разработаны таким образом, чтобы скрытую информацию было практически невозможно обнаружить без знания специальных ключей или методов.
3. Устойчивость к атакам: стеганографические методы должны быть устойчивы к различным видам атак, направленных на раскрытие скрытой информации, таких как статистический анализ или атаки на изображения.
4. Емкость: стеганографические методы должны обеспечивать возможность скрыть достаточное количество информации в носителе без существенного ухудшения качества или визуальной целостности.
5. Невозможность подделки: стеганографические методы должны предотвращать возможность подделки или изменения скрытой информации без правильного ключа или метода извлечения.

Основные принципы стеганографии заключаются в том, что информация скрывается в другом носителе, таком как изображение, аудиофайл или текстовый документ. Скрытая информация может быть встроена в носитель таким образом, чтобы она была незаметна для посторонних наблюдателей. Для извлечения скрытой информации необходимо знать специальный ключ или метод.

Для успешного использования стеганографии необходимо учитывать не только методы скрытия информации, но и методы извлечения этой информации. Важно также помнить, что стеганография не обеспечивает шифрование данных, поэтому для полной защиты конфиденциальности информации может потребоваться комбинация стеганографии и криптографии.

Основные принципы криптографии включают в себя следующие:

1. Конфиденциальность (секретность): гарантирует, что информация остается скрытой от несанкционированных лиц и может быть прочитана только теми, у кого есть правильный ключ для расшифровки.

2. Целостность: обеспечивает защиту данных от несанкционированных изменений или повреждений в процессе передачи, таким образом гарантируя, что информация остается неизменной.
3. Аутентификация: подтверждает идентичность отправителя и/или получателя данных, чтобы убедиться, что информация передается между правильными сторонами.
4. Неотказуемость: предотвращает возможность отрицания отправления или получения сообщения, обеспечивая доказательства о том, что обмен информацией действительно произошел.
5. Доступность: гарантирует доступность информации для правильных пользователей в нужное время и место, предотвращая блокировку или отказ в доступе к данным.

В отличие от криптографии, стеганография скрывает сам факт обмена сообщениями, встраивая информацию в другие носители, такие как изображения, аудиофайлы или текстовые документы. Это позволяет передавать информацию незаметно для посторонних лиц, что делает стеганографию более скрытной и менее заметной, чем криптография. Однако стеганография не обеспечивает защиту данных от прямого доступа, так как скрытая информация может быть обнаружена при наличии специальных инструментов и методов извлечения.

Таким образом, криптография и стеганография могут использоваться в комбинации для обеспечения полной защиты информации: криптография защищает данные от несанкционированного доступа, а стеганография скрывает сам факт обмена сообщениями.

Список литературы

1. Метод обнаружения сетевой стеганографии на основе машинного обучения Красов А. В. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 3. С. 100–108.
2. Методы выявления сетевой стеганографии Красов А. В. Методы и технические средства обеспечения безопасности информации. 2023. № 32. С. 52–54.

3. Цифровая стеганография Коржик В.И., Красов А.В. учебник / Москва, 2023.
4. Криптография и криптоанализ Казанцев А.А. В книге: Школьная секция: информационные технологии. Материалы 57-й Международной научной студенческой конференции. 2019. С. 18.
5. Криптографические средства защиты информации Красов А.В., Земцов Д. С. Инновации. Наука. Образование. 2021. № 48. С. 1629–1632.

УДК 004

Последствия эксплуатации уязвимостей для пользователей и организаций

Макшанский Анатолий Романович

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

***Аннотация**: Статья об уязвимостях в компьютерных системах и их влиянии на репутацию. Обсуждение последствий эксплуатации уязвимостей, таких как потеря доверия клиентов, ущерб репутации, потеря партнеров и инвесторов, юридические последствия. Подчеркивается важность безопасности информационных систем и регулярного обновления ПО для минимизации рисков и защиты репутации.*

***Abstract**: Article on vulnerabilities in computer systems and their impact on reputation. Discusses the consequences of exploiting vulnerabilities, such as loss of customer trust, damage to reputation, loss of partners and investors, and legal implications. Emphasizes the importance of information systems security and regular software updates to minimize risks and protect reputation.*

***Ключевые слова**: уязвимости, компьютерные системы, репутация, доверие клиентов, потеря партнеров, безопасность информационных систем, обновление ПО, риски, защита данных.*

***Keywords**: vulnerabilities, computer systems, reputation, customer trust, loss of partners, information system security, software updates, risks, data protection.*

Эксплуатация уязвимостей в компьютерных системах и программном обеспечении может привести к серьезным последствиям для как инди-

видуальных пользователей, так и корпоративных субъектов. Возможные последствия включают в себя несанкционированный доступ к данным, нарушение конфиденциальности, кражу персональной информации, реализацию кибератак и иных малварных операций. Настоящий обзор описывает принципиальные риски, связанные с эксплуатацией уязвимостей, и предлагает меры по их предотвращению.

1. Потеря конфиденциальности данных: Эксплуатация уязвимостей может приводить к несанкционированному доступу к защищаемым данным, включая личные данные (как имена, адреса, контактная информация), финансовую информацию (номера счетов, пароли к онлайн-банкам), а также коммерческую тайну, что нарушает приватность информации и может вызвать финансовые убытки, юридические претензии и потерю доверия со стороны клиентов и партнеров.
   - Утечка личных данных пользователей: Злоумышленники могут получить доступ к личным данным пользователей, таким как имена, адреса, номера телефонов, адреса электронной почты, данные о месте работы и другие конфиденциальные сведения. Эти данные могут быть использованы для мошенничества, кражи личности, фишинга и других преступных действий.
   - Утечка финансовых сведений: Злоумышленники могут получить доступ к финансовым данным пользователей, таким как номера банковских карт, пароли к онлайн-банкам, данные о транзакциях и другие финансовые сведения. Это может привести к краже денежных средств, мошенничеству с банковскими картами и другим финансовым преступлениям.
   - Утечка коммерческой тайны: Для организаций утечка коммерческой тайны может иметь катастрофические последствия. Злоумышленники могут получить доступ к секретным технологиям, планам разработки продуктов, стратегическим партнерствам и другой конфиденциальной информации, что может привести к утрате конкурентного преимущества и финансовым потерям.
   - Финансовые потери: Потеря конфиденциальности данных может привести к финансовым потерям как для отдельных пользователей, так и для организаций. Например, клиенты могут столкнуться с не-

законными транзакциями на своих банковских счетах или кредитных картах, а компании могут потерять прибыль из-за утечки коммерческой информации.

- Утрата доверия: Когда происходит утечка конфиденциальных данных, пользователи теряют доверие к организации или сервису, который не смог обеспечить безопасность и защиту их информации. Это может привести к оттоку клиентов, падению репутации компании и другим негативным последствиям.
- Юридические проблемы: Утечка конфиденциальных данных может привести к юридическим проблемам для организации. Нарушение законодательства о защите персональных данных или утечка коммерческой тайны может привести к штрафам, судебным искам со стороны пострадавших сторон и другим юридическим последствиям.

2. Нарушение целостности данных: Злоумышленники могут модифицировать или уничтожать данные, что подвергает риск ценную информацию (финансовые отчеты, клиентская база, проектная документация), вызывает функциональные нарушения системы или даже полную ее неработоспособность, что нарушает бесперебойность бизнес-процессов и требует значительных ресурсов на восстановление.
   - Потеря ценной информации: Когда данные подвергаются изменениям или уничтожению, это может привести к потере ценной информации, такой как финансовые отчеты, клиентские данные, документы о проектах и другие важные файлы. Это может нанести ущерб бизнесу, вызвать потерю доверия со стороны клиентов и партнеров, а также привести к финансовым потерям.
   - Ошибки в работе системы: Если злоумышленники изменят данные в системе, это может привести к ошибкам в работе программного обеспечения, неправильной обработке информации, некорректному выводу результатов и другим проблемам. Это может сказаться на эффективности работы системы и привести к сбоям в работе бизнес-процессов.
   - Полная неработоспособность системы: В некоторых случаях нарушение целостности данных может привести к полной неработо-

способности системы. Например, если злоумышленники уничтожат критические данные, необходимые для запуска операционной системы или приложений, это может привести к тому, что система перестанет функционировать полностью. Это может вызвать значительные проблемы для пользователей и организации, а также потребовать времени и ресурсов для восстановления работы системы.

3. Риск финансовых потерь: Эксплуатация уязвимостей может стать причиной прямых финансовых убытков за счет неавторизованных транзакций, мошенничества с использованием банковских карт и манипуляций с финансовыми операциями, что негативно сказывается на экономической стабильности как отдельных лиц, так и организаций.
   - Кража денежных средств: Злоумышленники могут использовать уязвимости в системе для доступа к банковским счетам, электронным кошелькам или другим финансовым активам пользователей. Они могут осуществлять транзакции без разрешения владельца счета, переводить деньги на свои счета или использовать украденные данные для получения доступа к финансовым ресурсам.
   - Мошенничество с банковскими картами: Уязвимости в системе могут привести к утечке данных банковских карт, что позволит злоумышленникам осуществлять незаконные транзакции, снимать деньги с банкоматов или совершать покупки онлайн от имени жертвы. Это может привести к финансовым потерям как для отдельных пользователей, так и для банков.
   - Манипуляции с финансовыми операциями: Злоумышленники могут использовать уязвимости в финансовых системах для проведения манипуляций с финансовыми операциями, такими как изменение цен на акции, валютные курсы или другие финансовые инструменты. Это может привести к финансовым потерям для инвесторов, компаний и других участников финансовых рынков.
4. Угроза безопасности: Несанкционированный доступ к системам может быть использован для проведения кибератак на другие цели, распространения вредоносного ПО, а также для осуществления шпионских операций, что подрывает общую кибербезопасность и может привести к масштабным последствиям.

- Кибератаки: Злоумышленники могут использовать доступ к уязвимой системе для проведения кибератак на другие цели. Например, они могут использовать систему в качестве платформы для запуска DDoS-атак, фишинга, внедрения вредоносных программ или других видов кибератак. Это может привести к нарушению работы других систем, утечке конфиденциальной информации или другим негативным последствиям.
- Распространение вредоносных программ: Злоумышленники могут использовать доступ к уязвимой системе для распространения вредоносных программ, таких как вирусы, троянские кони, шпионские программы и другие. Эти программы могут нанести ущерб как самой системе, так и другим пользователям или организациям, а также привести к утечке чувствительной информации.
- Шпионаж: Злоумышленники могут использовать доступ к уязвимой системе для сбора конфиденциальной информации, шпионажа или слежки за пользователями. Это может привести к утечке персональных данных, бизнес-секретов или другой чувствительной информации, что может нанести серьезный ущерб как отдельным пользователям, так и организациям.

5. Потеря репутации: Инциденты, связанные с нарушением безопасности, могут серьезно подорвать репутацию пользователя или организации, привести к потере доверия со стороны клиентов и партнеров, а также оттоку инвестиций, что негативно сказывается на долгосрочной перспективе развития.
   - Потеря доверия клиентов: Когда данные клиентов становятся уязвимыми из-за нарушения безопасности, это может привести к потере доверия со стороны клиентов. Клиенты могут перестать использовать услуги или продукты пользователя или организации из-за опасений по поводу безопасности и конфиденциальности своих данных.
   - Ущерб репутации: Публичные утечки данных или финансовые потери из-за эксплуатации уязвимостей могут привести к ухудшению репутации пользователя или организации. Негативные новости о нарушениях безопасности могут быстро распространиться и навсегда повлиять на восприятие общественностью.

- Потеря партнеров и инвесторов: Потеря доверия со стороны партнеров, инвесторов и других стейкхолдеров также может быть серьезным последствием эксплуатации уязвимостей. Партнеры могут отказаться от сотрудничества, а инвесторы могут потерять интерес к инвестированию в пользователя или организацию из-за риска безопасности.
- Юридические последствия: В случае утечки конфиденциальной информации из-за уязвимости, пользователь или организация также могут столкнуться с юридическими последствиями. Это может включать в себя штрафы, судебные иски, утрату лицензий или другие правовые последствия, что дополнительно ухудшит их репутацию.

Для минимизации рисков, связанных с эксплуатацией уязвимостей, целесообразно принятие комплексных мер безопасности, которые включают регулярное обновление программного обеспечения, применение систем защиты информации, организацию обучения сотрудников основам информационной безопасности и непрерывный мониторинг систем на предмет новых уязвимостей. Эффективное использование кибербезопасностных практик позволяет снизить вероятность эксплуатации уязвимостей и обеспечить устойчивость информационных систем в условиях постоянно развивающихся угроз.

Список литературы

1. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей Красов А.В., Штеренберг С.И., Голузина Д. Р. Электросвязь. 2019. № 11. С. 39–47.
2. Уязвимости программно-определяемых сетей Волкогонов В.Н., Преображенский А.И., Ушаков И.А. В сборнике: 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.
3. Метрика защищенности интернет вещей Крылов А.В., Ушаков И.А. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке

и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 622–626.
4. Анализ механизмов разграничения доступа в системах специального назначения Катасонов А.И., Цветков А.Ю. В сборнике: 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.
5. Общая методика обнаружения инсайдера компьютерной сети на основе технологий больших данных Котенко И.В., Пелёвин Д.В., Ушаков И.А. В сборнике: 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. 572–576.

УДК 004

Лучшие практики по обеспечению безопасности IP в организации

Макшанский Анатолий Романович

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

***Аннотация**: Обеспечение безопасности IP-адресов важно для организаций. Лучшие практики включают использование брандмауэров, шифрование данных, обновление ПО, мониторинг трафика и управление доступом. Эти меры помогут защитить сеть от угроз.*

***Abstract**: Securing IP addresses is important for organizations. Best practices include the use of firewalls, data encryption, software updates, traffic monitoring, and access control. These measures will help protect the network from threats.*

***Ключевые слова**: сетевые брандмауэры, шифрование данных, обновление ПО, мониторинг трафика, управление доступом.*

***Keywords**: network firewalls, data encryption, software updates, traffic monitoring, access control.*

В современном мире информационные технологии играют ключевую роль в деятельности организаций. С развитием цифровых технологий и увеличением объема передаваемой информации, безопасность IP-адресов становится все более важной задачей для компаний. IP-адрес — это уникальный идентификатор, который используется для идентификации устройств в сети. Нарушение безопасности IP-адресов может привести к утечке конфиденциальной информации, взлому системы и другим серьезным последствиям.

Для обеспечения безопасности IP-адресов в организации необходимо следовать определенным лучшим практикам. В данной статье мы рассмотрим некоторые из них.

1. Использование сетевых брандмауэров является одним из ключевых аспектов обеспечения безопасности сети. Сетевой брандмауэр — это специальное устройство или программное обеспечение, которое контролирует и фильтрует трафик, проходящий через сеть. Он может блокировать вредоносные пакеты данных, предотвращать несанкционированный доступ к сети и защищать сеть от внешних атак.

Настройка сетевого брандмауэра позволяет определить правила доступа к сети для различных пользователей и устройств. Это позволяет ограничить доступ к сети только авторизованным пользователям и устройствам, что повышает уровень безопасности сети. Брандмауэр также может контролировать и регулировать трафик в соответствии с заданными политиками безопасности.

2. Шифрование данных является одним из наиболее эффективных способов обеспечения безопасности передаваемой информации по сети. Шифрование позволяет преобразовать данные в непонятный для посторонних вид, что делает их недоступными для несанкционированного доступа.

Протоколы шифрования, такие как SSL (Secure Sockets Layer) и IPSec (Internet Protocol Security), обеспечивают защиту данных путем создания зашифрованного туннеля для передачи информации между устройствами. SSL шифрует данные, передаваемые через веб-сайты, обеспечивая безопасное соединение между браузером пользователя и сервером. IPSec обеспечивает шифрование данных на уровне сетевого соединения, защищая информацию, передаваемую между сетями или устройствами.

3. Обновление программного обеспечения на всех устройствах в сети играет ключевую роль в обеспечении безопасности информации. Постоянное обновление программных продуктов помогает закрыть уязвимости, которые могут быть использованы злоумышленниками для атак на систему.

В процессе разработки программного обеспечения обнаруживаются новые уязвимости и ошибки, которые могут быть использованы для несанкционированного доступа к данным или вредоносной активности. Производители выпускают обновления и патчи, исправляющие эти уязвимости и улучшающие безопасность системы.

4. Мониторинг сетевого трафика играет важную роль в обеспечении безопасности информации и выявлении потенциальных угроз. Постоянное отслеживание сетевого трафика позволяет оперативно реагировать на аномальные активности, атаки и несанкционированный доступ к данным.

С помощью мониторинга сетевого трафика можно обнаружить следующие угрозы и аномалии:

- DDoS-атаки: Мониторинг трафика позволяет выявить атаки на сеть, направленные на перегрузку ее ресурсов и отказ в обслуживании.
- Внутренние угрозы: Мониторинг сетевого трафика помогает выявить аномальные активности сотрудников, которые могут указывать на утечку данных или другие нежелательные действия.
- Малварные атаки: Обнаружение подозрительного трафика может указывать на наличие вредоносных программ на устройствах в сети.
- Отправка конфиденциальной информации: Мониторинг трафика позволяет выявить случаи отправки конфиденциальных данных через незащищенные каналы.

5. Управление доступом к сети играет ключевую роль в обеспечении безопасности информации и предотвращении несанкционированного доступа к ресурсам. Реализация строгой политики управления доступом помогает ограничить права доступа пользователей, устройств и сервисов к сети и ресурсам, что снижает риск возможных угроз и атак.

Соблюдение вышеуказанных лучших практик по обеспечению безопасности IP-адресов в организации поможет защитить ее от потенциальных угроз и обеспечить безопасную работу сети. Внедрение комплексных мер

безопасности и постоянное обновление системы защиты помогут предотвратить возможные атаки и сохранить целостность информации.

Список литературы

1. Разработка защищенной системы мгновенного обмена сообщениями. Алиметов К.С., Цветков А.Ю. В сборнике: 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. 56–59.
2. Криптографические средства защиты информации Красов А.В., Земцов Д. С. Инновации. Наука. Образование. 2021. № 48. С. 1629–1632.
3. Анализ безопасности WI-FI сетей Волкогонов В.Н., Казанцев А.А., Катасонов А.И., Орлов Г.А. В сборнике: 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. Построение защищенных сетевых соединений на основе отечественного оборудования Кравцова В.А., Ушаков И.А. В сборнике: 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. 702–706.
5. Защита для распределенных отказов в обслуживании в облачных вычислениях Гельфанд А.М., Косов Н.А., Красов А.В., Орлов Г.А. В сборнике: 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. 329–334.

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