DOI 10.37882/2223-2966.2024.12-2.05

БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ В КОРПОРАТИВНЫХ ЦИФРОВЫХ КОММУНИКАЦИЯХ

DATA SECURITY AND CONFIDENTIALITY IN CORPORATE DIGITAL COMMUNICATIONS

V. Voronin
O. Romashkova

Summary. This paper identifies effective strategies and technologies for protecting data in a corporate environment, including the implementation of modern technologies such as encryption and multi-factor authentication. Particular attention is paid to the analysis of threats related to cyberterrorism and social engineering, which have recently become increasingly sophisticated. The study aims to study and develop strategies to help reduce risks and ensure the security of corporate systems.

Keywords: security, data, communication, data protection, encryption, enterprise systems.

Воронин Владимир Алексеевич
Аспирант, ГАОУ ВО «Московский городской педагогический университет»
mgvoron@gmail.com
Ромашкова Оксана Николаевна
Доктор технических наук, профессор, профессор, Российская академия народного хозяйства и государственной службы при Президенте РФ (РАНХиГС)» г. Москва
ox-rom@yandex.ru

Аннотация. В статье были выявлены эффективные стратегии и технологии защиты данных в корпоративной среде, включая внедрение современных технологий, таких как шифрование и многофакторная аутентификация. Особое внимание уделяется анализу угроз, связанных с кибертерроризмом и социальной инженерией, которые в последнее время приобретают всё более изощренные формы. Исследование направлено на изучение и разработку стратегий, способствующих снижению рисков и обеспечению безопасности корпоративных систем.

Ключевые слова: безопасность, данные, коммуникация, защита данных, шифрование, корпоративные системы.

Введение

Современная корпоративная среда неизменно связана с необходимостью обеспечения безопасности цифровых коммуникаций, которые подвергаются возрастающим киберугрозам. В условиях растущей цифровизации бизнеса, обеспечение защиты данных становится ключевой задачей для организаций, независимо от их уровня и масштаба. Взаимодействие в цифровой среде подвержено многочисленным угрозам, включая кибертерроризм и социальную инженерию, что предъявляет высокие требования к системам безопасности. Такое положение отражает актуальность темы настоящего исследования, посвященного изучению всех аспектов угроз, которым подвергаются корпоративные информационные системы и методы их противодействия.

Целью данной работы является выявление эффективных стратегий и технологий защиты корпоративных данных с акцентом на внедрение современных решений, таких как шифрование и многофакторная аутентификация. Особое внимание уделяется анализу таких угроз, как кибертерроризм и социальная инженерия, которые становятся все более изощренными. Исследование направлено на изучение и разработку стратегий, которые помогают снизить риски и обеспечить безопасность корпоративных систем.

Важность данной темы обусловлена не только возрастанием числа и уровня угроз, но и необходимостью соблюдения правовых требований в области защиты данных. Внедрение передовых технологических решений и соответствие законодательным требованиям становятся неотъемлемой частью эффективной политики информационной безопасности. Существующие правовые нормы устанавливают стандарты и обязательства, которые компании должны соблюдать для обеспечения надежной защиты информации и минимизации рисков, связанных с утечками данных.

Таким образом, для успешного функционирования современных корпоративных систем важным аспектом является комплексный подход, включающий как технологические, так и организационные меры безопасности. Работа направлена на обоснование целесообразности использования многофакторной аутентификации, шифрования данных, а также внедрения смарт-контрактов, что способствует формированию многоуровневой защиты в условиях увеличивающихся цифровых угроз. Эффективное управление данными и защита информационных ресурсов позволяют предприятиям не только минимизировать риски, но и укреплять свою стратегическую стабильность в условиях интенсивного изменения технологической среды.

Анализ современных угроз безопасности в цифровых коммуникациях

Типы угроз и уязвимости в корпоративных системах

Современные цифровые коммуникации в корпоративной среде подвержены различным типам угроз, что требует от организаций постоянной бдительности и применения передовых мер безопасности. Кибертерроризм, например, представляет собой преднамеренные атаки на информационные системы, которые преследуют определенные политически мотивированные цели и могут создавать угрозу государственной безопасности и обществу. Эти атаки могут вызывать значительные перебои в работе как государственных структур, так и частных организаций, что обуславливает необходимость создания устойчивых механизмов противодействия и быстрой реакции на возможные инциденты.

Одной из значительных угроз в цифровой среде также являются атаки социальной инженерии. В современном информационном мире они представляют собой серьезную угрозу для безопасности данных и конфиденциальности, так как злоумышленники используют психологические приемы для обмана сотрудников и получения доступа к конфиденциальной информации. Эти атаки становятся всё более изощренными, что требует от организаций внедрения комплексных стратегий, включающих технические и процедурные меры безопасности, а также обучения персонала способам выявления таких угроз.

Для эффективной защиты корпоративных данных необходимо внедрение современных технологий и разработка четкой политики безопасности. Технологические решения, такие как шифрование и многофакторная аутентификация, обеспечивают высокую степень защиты от несанкционированного доступа, а надлежащее законодательное регулирование и следование лучшим практикам, таким как модель Zero Trust, помогают минимизировать риски. Таким образом, реализация комплексного подхода в цифровой безопасности становится неотъемлемой частью устойчивого функционирования корпоративных систем.

Атаки на данные и их последствия для бизнеса

Современные корпоративные системы чрезвычайно уязвимы перед угрозами, связанными с кибертерроризмом и атаками социальной инженерии. Эти угрозы не только способны нанести серьезный вред безопасной и конфиденциальной обработке данных, но и угрожают общей устойчивости организаций. Кибертерроризм включает в себя умышленные политически мотивированные нападения на информационные системы, что может поставить под угрозу государственную безопасность и общество в целом. Эти атаки часто приводят к нарушению работы критически важных инфраструктур, требуя от компаний готовности к быстрому реагированию и созданию адаптивных оборонительных механизмов.

В довершение к кибертерроризму, атаки социальной инженерии вошли в ранг серьезных угроз для корпоративных систем. В современном информационном мире такие атаки представляют собой серьезную угрозу для безопасности данных и конфиденциальности. Злоумышленники, используя психологические методы манипуляции, часто добиваются доступа к закрытым данным сотрудников, становясь ключевыми факторами таких угроз. Это требует от организаций разработки комплексных стратегий, которые включают как технологические, так и процедурные меры безопасности.

Для успешной защиты и укрепления обороны своих систем, компании должны внедрять передовые технологии и разрабатывать четкую политику безопасности. Использование методов шифрования и многофакторной аутентификации становится важными мерами предосторожности против несанкционированного доступа. Организации также необходимо учитывать актуальные правовые нормы и применять лучшие практики, способствующие минимизации рисков, связанных с утечками данных. Внедрение комплексного подхода становится важным аспектом для обеспечения надежной работы и устойчивости корпоративных систем в условиях постоянно эволюционирующих цифровых угроз.

Методы защиты информации в корпоративной среде

Технологические решения для обеспечения безопасности данных

В условиях роста цифровых коммуникаций обеспечение защиты данных в корпоративной среде становится приоритетной задачей для большинства организаций. Технологические решения, включая шифрование и использование многофакторной аутентификации, представляют собой эффективные методы противодействия киберугрозам. Шифрование данных не только защищает их целостность, но и оказывается незаменимым инструментом для предотвращения несанкционированного доступа, поскольку шифрование используется для предотвращения просмотра истинного содержания сообщения, будь то текст или файл.

Существует несколько основных способов шифрования данных:

Симметричное шифрование:

- AES (Advanced Encryption Standard): Широко используемый алгоритм, обеспечивающий высокий уровень безопасности и быструю обработку.
- DES (Data Encryption Standard): Более старый алгоритм, считается неэффективным из-за малой длины ключа (56 бит).
- 3DES (Triple DES): Удлинённая версия DES, использующая три итерации шифрования, но всё ещё не устарела.

Асимметричное шифрование:
- RSA (Rivest–Shamir–Adleman): Один из первых и наиболее известных алгоритмов асимметричного шифрования, использующий пару ключей (публичный и приватный).
- ECC (Elliptic Curve Cryptography): Более современный подход, безопасный при меньшей длине ключа, что делает его эффективным.

Гибридное шифрование — сочетание симметричного и асимметричного шифрования, используя асимметрию для обмена симметричным ключом.

Транспортное шифрование — TLS (Transport Layer Security) — способ шифрования данных для обеспечения безопасной передачи данных по сети.

Таким образом, организациям необходимо уделять особое внимание использованию современных технологий для поддержания высокого уровня безопасности и защиты своих информационных ресурсов.

Многофакторная аутентификация, в свою очередь, представляет собой один из ключевых подходов для защиты от атак социальной инженерии. Это позволяет не только обеспечить дополнительную безопасность данных, но и минимизировать риски утечки конфиденциальной информации. Согласно исследованию, одним из ключевых методов защиты от атак социальной инженерии является внедрение многофакторной аутентификации, что позволяет дополнительно обеспечить безопасность доступа к системам и данным. Актуальность этого метода обуславливается сложностью современных угроз и постоянным развитием технологий, которые используются злоумышленниками для проникновения в корпоративные сети.

Однако технологические решения не могут обеспечивать достаточный уровень защиты без поддержки со стороны организационных мер по безопасности. Регулярное обновление программного обеспечения, политика управления доступом, а также создание резервных копий данных должны быть важной частью комплексного подхода к информационной безопасности. Подобные меры не только дополняют технологические решения, но и создают многоуровневую защиту, способную противостоять современным киберугрозам. В условиях, когда растет количество атак и уязвимостей в корпоративных системах, только интеграция технологических и процедурных мер может обеспечить эффективную защиту данных и минимизировать риски информационной безопасности.

Процедурные меры и политика безопасности в организациях

Процедурные меры и политики безопасности в организациях также играют немаловажную роль в защите данных. Базовой мерой безопасности данных можно назвать документирование, то есть создание чёткой и доступной политики безопасности, которая подробно объясняет основные принципы защиты данных, обязанности сотрудников, а также действия в случае инцидентов. Помимо документирования, необходимо проводить регулярные тренинги по вопросам безопасности данных и повышению осведомлённости о рисках, связанных с киберугрозами. Также важно проводить ведение логов для отслеживания доступов и действий пользователей с целью выявления несанкционированной активности. Ко всему этому относится и анализ системы безопасности для выявления уязвимостей, и оценки эффективности текущих мер.

Правовые аспекты в обеспечении конфиденциальности и безопасности данных

В современных организациях обеспечение безопасности данных является критически важным аспектом, поскольку нарушение конфиденциальности может привести к значительным юридическим и финансовым рискам. С данным аспектом связано и законодательное регулирование, которое установило стандарты и требования для поддерживания защиты конфиденциальной информации, гарантируя, что компании соблюдают все необходимые юридические обязательства.

Современные ключевые аспекты можно поделить на несколько пунктов, а именно:

1. **Правовые акты.** Главными правовыми актами по безопасности данных являются — Федеральный закон «О персональных данных» (№ 152-ФЗ), регулирующий сбор, обработку и хранение персональных данных; Федеральные закон «О коммерческой тайне» (№ 98-ФЗ), регулирующий защиту конфиденциальной информации, касающейся коммерческих интересов субъектов бизнеса; Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» (№ 187-ФЗ), определяющий требования к обеспечению безопасности данных в рамках критической информационной инфраструктуры.

2. **Основные принципы обработки данных.** Законность и добросовестность — обработка данных должна осуществляться на законных основаниях и добросовестно; Целевое использование — данные могут использоваться только для заранее определённых законных целей; Минимизация данных — сбор и обработка данных должны ограничиваться той информацией, которая необходима для достижения поставленных целей; Достоверность и актуальность — данные должны быть актуальны и точны.

Заключение

Обеспечение надежной защиты данных в корпоративной среде становится неотъемлемой частью стратегии устойчивого функционирования организаций. Внедрение смешанных подходов, сочетая технологические и процедурные меры, устраняет слабые места систем безопасности и позволяет противостоять угрозам в условиях быстрого роста цифровых коммуникаций. Дальнейшие исследования могут сосредоточиться на развитии адаптивных механизмов и политик, которые соответствуют усложняющимся киберугрозам, и на разработке комплексных решений, которые смогут защитить корпоративные системы от постоянно эволюционирующих опасностей.

ЛИТЕРАТУРА

1. Алехин Р.В. Облачные сервисы. принцип работы, классификация и модели обслуживания / Р.В. Алехин, А.В. Красов, А.Д. Макарова и др. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИ-НО 2022). XI Международная научно-техническая и научно-методическая конференция. — Санкт-Петербург, 2022. — С. 70–74.
2. Кутовенко, А.А., Сидорик. В.В. Облачные и сетевые технологии в учебном процессе: учебное-методическое пособие для студентов и слушателей системы повышения квалификации и переподготовки. — М.: Минск: БНТУ. 2020. — 57с.
3. Кривоносова А.Д. Коммуникации в условиях цифровой трансформации: сборник материалов VI Международной научно-практической конференции, Санкт-Петербург, 29–30 ноября 2022 г. — СПб.: Изд-во СПбГЭУ, 2022. — 310 с.
4. Лисица Н.В. Инновационные подходы к оценке эффективности средств безопасности против киберугроз // Cifra. Компьютерные науки и информатика. — СПб, 2024 — 8 с.
5. Лапыгин Д.Ю. Обеспечение экономической безопасности инструментами информационных технологий / Д.Ю. Лапыгин, К.С. Караман // Экономическая безопасность. — 2023. — Т. 6. — № 1. — С. 429–442
6. Лебедь С.В. Инновационные технологии в сфере кибербезопасности / С.В. Лебедь // Современные информационные технологии и ИТ-образование. — 2022. — №2.
7. Родивилин И.П. социальная инженерия как угроза информационной безопасности: тенденции и защита // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. — 2023. — №4. — С. 12–24
8. Рыжова Н.И., Громова О.Н. Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности // Вестник РУДН. Серия: Информатизация образования. — 2020. — Т. 17. — № 3. — С. 254–268
9. Косов Н.А. Способы защиты от инсайдерских атак / Н.А. Косов, Н.А. Голубов // Инновационные решения социальных, экономических и технологических проблем современного общества. Сборник научных статей по итогам круглого стола со всероссийским и международным участием. — Москва, 2021. — С. 149–151.
10. Штеренберг С.И. Анализ безопасности доменных систем / С.И. Штеренберг, Г.С. Бударный, И.В. Чумаков // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. — Санкт-Петербург, 2022. — С. 587–588.

Журнал «Современная наука: актуальные проблемы теории и практики»