УДК 004.6

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ: МЕТОДЫ ЗАЩИТЫ ОТ КИБЕРАТАК, ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ, УПРАВЛЕНИЕ ДОСТУПОМ

Сергеев Александр Эдуардович
доцент, канд. физ.-мат. наук
e-mail galua1979@yandex.ru
ФГБОУ ВО Кубанский государственный аграрный университет имени И. Т. Трубилина, г. Краснодар, РФ

Неженцев Максим Витальевич
Студент
maks.negentsev@mail.ru
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Балаев Кияс Самандович
студент
balaevkiyas@mail.ru
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

В статье рассматриваются ключевые аспекты безопасности корпоративных сетей, включая защиту от кибератак, обеспечение конфиденциальности данных и управление доступом. Анализируются современные угрозы, такие как фишинг, DDoS-атаки и утечки данных, а также методы их предотвращения с помощью шифрования, фаерволов и систем IDS/IPS. Особое внимание уделяется стратегиям управления доступом, включая многофакторную аутентификацию и ролевое управление (RBAC). Также даются рекомендации по обучению сотрудников и внедрению проактивных мер защиты. Статья подчеркивает важность комплексного подхода к кибербезопасности для минимизации рисков в корпоративных сетях

Ключевые слова: КИБЕРБЕЗОПАСНОСТЬ, КОРПОРАТИВНЫЕ СЕТИ, ЗАЩИТА ОТ КИБЕРАТАК, КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ, УПРАВЛЕНИЕ ДОСТУПОМ, ШИФРОВАНИЕ, АУТЕНТИФИКАЦИЯ, ФАЕРВОЛЫ, IDS/IPS, МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ, РОЛЕВОЕ УПРАВЛЕНИЕ ДОСТУПОМ (RBAC)

http://dx.doi.org/10.21515/1990-4665-212-020

UDC 004.6

2.3.6. Information protection methods and systems, information security (technical sciences)

CORPORATE NETWORK SECURITY: METHODS OF PROTECTION AGAINST CYBERATTACKS, ENSURING DATA CONFIDENTIALITY, ACCESS MANAGEMENT

Sergeev Aleksandr Eduardovich
Senior lecturer
e-mail galua1979@yandex.ru
FSAU HE Kuban State Agrarian University named after I.T. Trubilin, Krasnodar, Russia

Nezhentsev Maxim Vitalievich
student
maks.negentsev@mail.ru
"Kuban State Agrarian University named after I.T. Trubilin", Krasnodar 350044, Kalinina 13, Russia

Balaev Kiyas Samandovich
student
balaevkiyas@mail.ru
"Kuban State Agrarian University named after I.T. Trubilin", Krasnodar 350044, Kalinina 13, Russia

The article examines key aspects of corporate network security, including protection against cyberattacks, ensuring data privacy, and access management. It analyzes modern threats such as phishing, DDoS attacks, and data leaks, as well as methods for preventing them using encryption, firewalls, and IDS/IPS systems. Particular attention is paid to access management strategies, including multi-factor authentication and role-based access control (RBAC). Recommendations for employee training and the implementation of proactive security measures are also given. The article emphasizes the importance of a comprehensive approach to cybersecurity to minimize risks in corporate networks

Keywords: CYBERSECURITY, CORPORATE NETWORKS, PROTECTION AGAINST CYBERATTACKS, DATA CONFIDENTIALITY, ACCESS MANAGEMENT, ENCRYPTION, AUTHENTICATION, FIREWALLS, IDS/IPS, MULTI-FACTOR AUTHENTICATION, ROLE-BASED ACCESS CONTROL (RBAC)

Введение

В эпоху цифровизации и стремительного развития информационных технологий корпоративные сети стали критически важными элементами для успешного функционирования любой компании. Они обеспечивают не только внутреннюю коммуникацию, но и взаимодействие с внешними партнёрами и клиентами. Однако по мере роста их значимости увеличивается и число угроз, связанных с кибербезопасностью. Каждая организация, владеющая или работающая с ценными данными, неизбежно сталкивается с рисками, начиная от утечек конфиденциальной информации и заканчивая масштабными кибератаками.

Кибератаки могут принимать различные формы: от известных фишинговых атак до комплексных угроз, таких как Advanced Persistent Threats (APT). Задача по защите корпоративных сетей усложняется, так как атакующие постоянно совершенствуют свои технологии и стратегии.

Кроме угроз извне, корпоративные сети сталкиваются с внутренними рисками, которые часто недооцениваются. Небрежность сотрудников, их недостаточная осведомлённость в области ИТ-безопасности или даже преднамеренные злонамеренные действия могут привести к серьёзным последствиям.

Ключевыми аспектами обеспечения безопасности корпоративных сетей являются использование современных методов защиты от кибератак, обеспечение конфиденциальности и целостности данных, а также управление доступом к информационным ресурсам. Компании должны стремиться к созданию многоуровневых систем безопасности, которые могут противостоять разнообразным угрозам и гибко адаптироваться к новым вызовам.

В этой статье мы подробно рассмотрим методы, которые помогут защитить корпоративные сети. Мы обсудим, как современные технологии

и лучшие практики помогают минимизировать риски и поддерживать высочайший уровень защищённости данных.

Также сравним энергоэффективные протоколы по отдельности и друг с другом. Проведём формульное сравнение для выявления лучшего.

Методы защиты от кибератак

В современном цифровом мире кибератаки становятся всё более изощрёнными и масштабными, что делает их серьёзной угрозой для корпоративных сетей. В этой главе мы рассмотрим основные методы защиты, которые могут помочь организациям минимизировать эти риски.

Первый шаг в защите от кибератак — это понимание угроз. Атаки могут включать в себя различного рода вредоносные действия, такие как DDoS-атаки, вирусные и фишинговые атаки. DDoS-атаки направлены на перегрузку сервера, делая его недоступным для пользователей. В то же время фишинговые атаки нацелены на похищение персональных данных посредством обмана сотрудников.

Одним из ключевых инструментов в предотвращении кибератак являются фаерволы. Фаерволы служат «защитной стеной» между внутренними сетями организации и внешними угрозами, фильтруя входящий и исходящий трафик на основе предварительно заданных правил. Они играют важную роль в блокировке несанкционированного доступа и защите корпоративных ресурсов.

Системы обнаружения и предотвращения вторжений (IDS/IPS) дополняют фаерволы, анализируя потоки данных на предмет подозрительной активности и предпринимая меры в случае обнаружения потенциальных угроз. Эти системы могут автоматически блокировать нарушителей и отправлять уведомления администратору для дальнейшего расследования.

Антивирусные программы также являются важным элементом в стратегии защиты от угроз. Они обеспечивают обнаружение и удаление

вредоносного ПО, уведомления о признанных угрозах и преактивную защиту от неизвестных вирусов путем мониторинга поведения программ.

Не менее важным являются и реактивные меры, такие как развитие планов реагирования на инциденты. Оперативная реакция и фиксация действий в случае инцидента помогают минимизировать ущерб, ограничивая распространение атаки и восстанавливая системные функции. Регулярное резервное копирование данных обеспечивает возможность быстрого восстановления информации в случае серьезной атаки.

В целом, комплексный подход к защите от кибератак требует интеграции разнообразных технологий и мер безопасности, которые способствуют эффективному противодействию внутренним и внешним угрозам. Организациям важно постоянно совершенствовать свои методики, оставаться в курсе новых типов атак и адаптировать свои стратегии в соответствии с изменяющейся киберугрозой.

Обеспечение конфиденциальности данных

Конфиденциальность данных остаётся одним из ключевых компонентов кибербезопасности и важнейшей задачей для любой организации, работающей с чувствительной информацией. Однако поддержание конфиденциальности требует не только технических средств, но и правильно выстроенной политики управления данными.

Одним из наиболее надёжных методов защиты данных является их шифрование. Шифрование превращает информацию в нечитаемый формат, который может быть расшифрован только теми, кто имеет соответствующий ключ. Существуют два основных вида шифрования: симметричное и асимметричное. Симметричное шифрование использует один и тот же ключ для шифрования и дешифрования данных, что требует заботы о безопасности этого ключа. Асимметричное шифрование, напротив, использует пару ключей — открытый и закрытый — что делает процесс управления ключами более безопасным и гибким.

SSL/TLS протоколы широко применяются для обеспечения безопасности во время передач данных по интернету, создавая защищённый канал связи между клиентом и сервером. Это особенно важно для онлайн-транзакций, где конфиденциальность и целостность данных являются критически важными.

Помимо технических решений, успешное управление конфиденциальностью зависит от внутренней политики компании. Все данные должны быть классифицированы в зависимости от их уровня конфиденциальности. Это классификация служит основой для определения доступа и защиты данных. Например, информация, содержащая персональные данные клиентов, должна иметь более строгие ограничения по сравнению с обычной рабочей документацией.

Еще один аспект — обеспечение безопасности информационных носителей. Предприятия должны иметь ясные процедуры уничтожения и обезвреживания данных на устаревших и избыточных устройствах. Многие утечки данных происходят именно из-за неправильно удаленной информации.

Современные угрозы кибербезопасности требуют комплексного подхода к обеспечению конфиденциальности данных. Включив в него передовые технологии шифрования и надежные корпоративные политики, компании смогут лучше защитить свои важные активы от несанкционированного доступа и утечки. Тем самым они сохранят доверие своих клиентов и успешность бизнес-операций в долгосрочной перспективе.

Управление доступом

Эффективное управление доступом к корпоративным ресурсам является краеугольным камнем безопасности информационных систем. Оно не только предотвращает несанкционированный доступ, но и обеспечивает, чтобы только необходимые лица имели доступ к

соответствующим данным, минимизируя риск внутреннего злоупотребления.

Одним из первых шагов в управлении доступом является внедрение надёжных механизмов аутентификации. Пароли по-прежнему являются наиболее распространённым методом аутентификации, однако их использование связано с определёнными рисками. Слабые пароли, использование одних и тех же паролей для разных учётных записей и недостаточная их сложность делают системы уязвимыми для атак. В этой связи многие организации переходят к более безопасной многофакторной аутентификации (MFA), которая требует от пользователей подтверждения своей личности посредством различных факторов, таких как SMS-коды, аппаратные ключи или биометрические данные.

Биометрическая аутентификация, такая как сканирование отпечатков пальцев или распознавание лиц, предоставляет дополнительный уровень безопасности и удобства использования. Однако она также требует ответственного подхода к обработке и хранению биометрических данных, чтобы защитить их от потенциальных утечек.

Контроль доступа подразумевает более широкий подход, чем просто аутентификация. Ролевое управление доступом (RBAC) позволяет организациям предоставлять доступ к ресурсам на основании ролей, которые выполняет тот или иной сотрудник в компании. Это значительно упрощает управление, поскольку вместо того, чтобы управлять доступом каждого пользователя отдельно, администраторы могут определять права доступа на уровне ролей. Принцип минимальных привилегий дополняет данный подход, обеспечивая, чтобы пользователи имели доступ только к тем ресурсам, которые необходимы им для выполнения своих обязанностей и не более того.

Ещё один важный аспект — это обеспечение надзора и мониторинга доступов. Создание журналов событий и их регулярный анализ позволяют

быстро выявлять подозрительные действия и предпринимать необходимые меры.

Эффективное управление доступом требует постоянного пересмотра и обновления политик безопасности. В результате компании получают не только более защищенные информационные системы, но и повышенную адаптивность к новым угрозам, сохраняя конкурентоспособность и доверие клиентов.

Обучение и повышение осведомлённости сотрудников

Никакие технические меры безопасности не смогут обеспечить полную защиту данных, если сотрудники компании не обладают достаточными знаниями и осведомлённостью в области информационной безопасности. Человеческий фактор часто становится слабым звеном в защите корпоративных сетей, поэтому систематическое обучение сотрудников — это неотъемлемая часть стратегии кибербезопасности.

Первым шагом к созданию культуры безопасности является проведение регулярных тренингов и семинаров для всех уровней сотрудников. Эти мероприятия поднимают осведомлённость о современных угрозах, методах их предотвращения и реакций на инциденты. Важно, чтобы такие тренинги включали практические примеры и кейсы из реальной жизни, что помогает сотрудникам лучше понять потенциальные угрозы и эффективные способы их избежания.

Специализированные входные программы для новых сотрудников являются ещё одним важным элементом обучения. Они обеспечивают свежих работников основами информационной безопасности и правилами безопасного использования корпоративных сетей и оборудования.

Кроме того, компании должны проводить регулярные оценки осведомлённости сотрудников не только для оценки эффективности обучения, но и для выявления слабых мест, требующих дополнительного внимания. Одним из эффективных методов повышения бдительности

среди сотрудников являются симуляции атак, например, фишинг-тесты. Такие симуляции выявляют, как персонал справляется с потенциальными угрозами, и становятся основой для последующих образовательных мероприятий.

Руководители и ИТ-отделы должны также поддерживать открытое и доверительное отношение к сообщениям о подозрительных действиях или потенциальных угрозах. Люди должны быть уверены, что могут сообщить о своих ошибках или замеченных уязвимостях без страха наказания. Это способствует формированию корпоративной культуры, где кибербезопасность воспринимается как общая ответственность.

Обучающие инициативы и повышение уровня осведомлённости сотрудников — это инвестиция в будущее компании. Благодаря обучению сотрудники становятся не только первой линией обороны от кибератак, но и активными участниками укрепления общей безопасности организации. Это позволяет значительно снизить риски и обеспечивает более устойчивую защиту корпоративных данных.

Сравнение энергоэффективных протоколов

1. DTLS (Datagram Transport Layer Security)

Назначение и использование:

DTLS предоставляет безопасность для соединений, использующих протокол передачи дейтаграмм (UDP). Это делает его идеальным выбором для приложений, где важна задержка и быстродействие, например, для видеоконференций или IoT-устройств.

Энергоэффективность:

DTLS специально разработан для работы в условиях ограниченных ресурсов. Он минимизирует энергопотребление благодаря сниженной сложности протокола и меньшему числу передаваемых данных по сравнению с TCP.

Безопасность:

DTLS обеспечивает аутентификацию, целостность и конфиденциальность, заимствуя многие механизмы из TLS. Несмотря на энергоэффективность, он предоставляет надежную защиту данных в корпоративных сетях.

2. TLS (Transport Layer Security)

Назначение и использование:

TLS используется для обеспечения безопасного обмена данными через интернет. Он обеспечивает конфиденциальность и целостность данных, будучи основой для HTTPS.

Энергоэффективность:

Стандартный TLS может быть довольно энергозатратным. Однако существуют оптимизированные реализации, которые уменьшают нагрузку на процессор и энергопотребление, что особенно актуально для мобильных устройств и корпоративной инфраструктуры.

Безопасность:

TLS считается одним из самых надежных протоколов безопасности, предохраняя данные от перехвата и модификации. Его широкое принятие и поддержка делают его стандартом де-факто в вопросах безопасности.

3. CoAP (Constrained Application Protocol)

Назначение и использование:

CoAP разработан для IoT-устройств с ограниченными ресурсами. Это легкий протокол, специально созданный для передачи данных между узлами с низкой мощностью.

Энергоэффективность:

CoAP минимизирует использование ресурсов за счет использования простого, текстово ориентированного формата сообщений и поддержки multicast-сообщений. Это снижает затраты на энергопотребление и передачу данных.

Безопасность:

CoAP поддерживает одноуровневую безопасность через DTLS, обеспечивая аутентификацию и шифрование данных. Это позволяет поддерживать достаточный уровень защиты в условиях ограниченных ресурсов.

4. MQTT (Message Queuing Telemetry Transport)

Назначение и использование:

MQTT — это протокол обмена сообщениями, ориентированный на ресурсоэкономичность, часто применяемый в IoT-системах для сбора и передачи данных от датчиков к серверу.

Энергоэффективность:

MQTT разрабатывался с прицелом на низкое потребление мощности и высокую производительность. Он использует механизм "publish-subscribe", минимизируя объем трафика и необходимость постоянного соединения, что особенно полезно для батарейных устройств.

Безопасность:

MQTT поддерживает TLS/SSL для шифрования, а также различные уровни аутентификации и авторизации. Это позволяет достичь надежной защиты данных в корпоративных и IoT-сетях.

Итоги

Выбрав эти четыре протокола для сравнения, мы можем увидеть баланс между энергоэффективностью и уровнем защищенности данных. DTLS и CoAP прекрасно подходят для ограниченных ресурсов и IoT-решений, тогда как TLS и MQTT обеспечивают более традиционный и многогранный подход к защите данных в более сложных корпоративных средах. Правильный выбор протокола зависит от конкретных нужд компании, используемых устройств и требуемого уровня безопасности.

Формульное сравнение

Для формульного сравнения данных протоколов мы можем проанализировать их по следующим ключевым параметрам:

1. Энергоэффективность (EE): Общая эффективность по потреблению энергии, измеряется в потребляемых ватт-часах за передачу одного килобайта данных.

2. Задержка (D): Время, необходимое для передачи и получения данных, измеряется в миллисекундах.

3. Защищенность (S): Уровень безопасности, который определяется количеством шифрованных данных (битов).

4. Нагрузка (L): Нагрузка на сеть или сервер в процессе использования, измеряется в процентах от используемой мощности.

Теперь проведем формульное описание и сравнительный анализ каждого протокола на основе этих параметров:

1. DTLS

$$EE_{DTLS} = k_1 * \frac{\text{Обработка сообщения}}{\text{Энергоресурсы}}$$

$$D_{DTLS} = f_1\,(\text{Размер данных, Скорость канала})$$

$$S_{DTLS} = 256 - \text{битное шифрование}$$

$$L_{DTLS} = f_2(\text{Число соединений})$$

2. TLS

$$EE_{TLS} = k_2 * \frac{\text{Обработка сообщения}}{\text{Энергоресурсы с оптимизацией}}$$

$$D_{TLS} = f_3\,(\text{Процесс установления соединения, Размер данных})$$

$$S_{TLS} = 256 - \text{битное шифрование или выше}$$

$$L_{TLS} = f_4(\text{Количество потока})$$

3. CoAP

$$EE_{CoAP} = k_3 * \frac{\text{Минимальная обработка}}{\text{Энергоресурсы}}$$

$$D_{CoAP} = f_5\,(\text{Тип сообщения, Скорость сети})$$

$$S_{CoAP} = 128 - \text{битное или больше через } DTLS$$

$$L_{CoAP} = f_6(\text{Объем запросов})$$

4. MQTT

$$EE_{MQTT} = k_4 * \frac{\text{Публикация/подписка}}{\text{Энергоресурсы}}$$

$$D_{MQTT} = f_7\ (QoS\ \text{уровень}, \text{Размер сообщения})$$

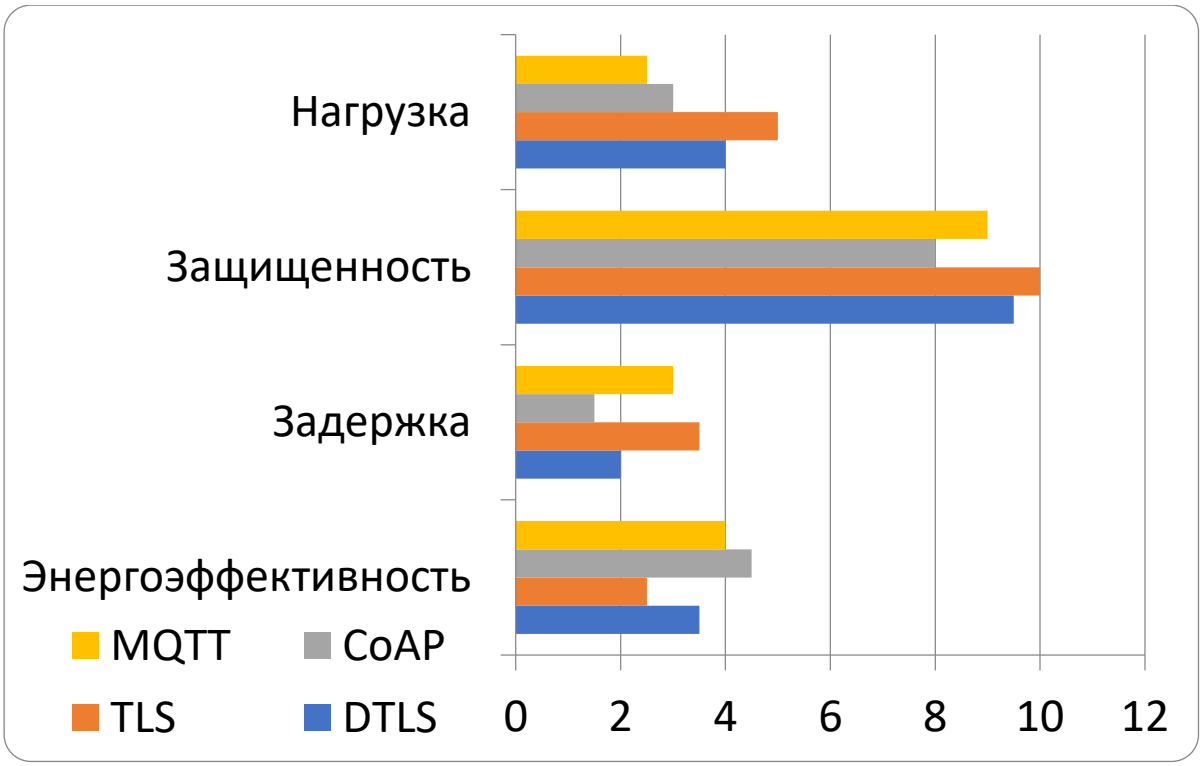
$$S_{MQTT} = 256 - \text{битное шифрование через } TLS$$

$$L_{MQTT} = f_8(\text{Количество клиентов})$$

Сравнение:

- Энергоэффективность (EE): CoAP и MQTT специально оптимизированы для низкого потребления энергии, что делает их более энергоэффективными для IoT-сетей.
- Задержка (D): DTLS и CoAP имеют низкую задержку за счет использования UDP, тогда как TLS и MQTT могут демонстрировать большую задержку из-за более сложных процедур установления соединения.
- Защищенность (S): TLS обеспечивает наивысший уровень безопасности, следуемый DMTS и MQTT, которые тоже поддерживают высокие стандарты шифрования.
- Нагрузка (L): CoAP и MQTT поддерживают более низкую нагрузку на сеть благодаря своей структуре взаимодействия и способности работать с ограниченными ресурсами.

Такая формульная модель позволяет структурировать и понять различные аспекты рассмотренных протоколов, помогая выбрать наиболее подходящий под конкретные задачи в рамках безопасности корпоративных сетей.



Заключение

Современные вызовы в области кибербезопасности требуют комплексного подхода и постоянного совершенствования мер защиты корпоративных сетей. Организации сталкиваются с беспрецедентным количеством угроз, и ни одна из них не может позволить себе оставаться уязвимой в этой стремительно меняющейся цифровой среде. В этом контексте защита от кибератак, обеспечение конфиденциальности данных и эффективное управление доступом становятся критически важными элементами общей стратегии безопасности.

Как было рассмотрено в статье, проактивные и реактивные меры, такие как использование фаерволов, систем IDS/IPS, шифрования, многофакторной аутентификации и ролевого управления доступом, составляют фундамент комплексной защиты. Планы по быстрому реагированию на инциденты и регулярное резервное копирование данных добавляют дополнительный уровень безопасности и готовности к непредвиденным обстоятельствам.

Кроме технических решений, крайне важной составляющей успешной стратегии кибербезопасности является человеческий фактор. Регулярные тренинги и повышение осведомлённости сотрудников создают культуру безопасности и облегчают внедрение лучших практик на всех уровнях организации. Систематическое обучение и тестирование позволяют адаптироваться к новым угрозам и реагировать на них более эффективно.

Не менее важно оставаться в курсе новых тенденций и технологий в области кибербезопасности. Внедрение искусственного интеллекта, машинного обучения и автоматизации в процессы безопасности уже приносит ощутимые результаты, улучшая предсказуемость и точность обнаружения угроз. Благодаря этому компании могут сосредоточиться на своей основной деятельности, имея уверенность в защите своих информационных систем.

В конечном счёте, комплексный подход к обеспечению безопасности корпоративных сетей не только предотвращает инциденты, но и поддерживает долгосрочную устойчивость и успешность бизнеса. Эффективная кибербезопасность — это не просто соблюдение обязательных требований, но и стратегический актив, способствующий усилению доверия со стороны клиентов и партнёров. Таким образом, инвестиции в кибербезопасность становятся залогом устойчивого развития компаний в цифровую эпоху.

Список литературы

1. Андресон, Р. «Инженерия безопасности». — М.: Вильямс, 2008. Основное пособие по вопросам проектирования и реализации системы безопасности с акцентом на различные аспекты киберугроз.

2. Голубев, А. Ю. «Кибербезопасность: учебное пособие для вузов». — М.: ИНФРА-М, 2017. Учебное пособие, предоставляющее комплексный обзор подходов и методов обеспечения безопасности в информационных системах.

3. Кузнецов, С. Б., Иванов, В. И. «Информационная безопасность: новые вызовы и угрозы». — СПб.: Питер, 2019. Книга, раскрывающая актуальные угрозы кибербезопасности и стратегии противодействия современным атакам.

4. Мельников, И. В. «Основы безопасности информационных систем и технологий». — М.: Форум, 2016. Основной учебник по вопросам фундаментальных принципов защиты информации и методов управления безопасностью в условиях современных угроз.

5. Смирнов, А. В., Петров, Н. С. «Защита информации и кибербезопасность». — М.: Юрайт, 2018. Практическое руководство по внедрению безопасных систем и технологий защиты информации.

6. Соловьев, В. В. «Энциклопедия кибербезопасности». — М.: Эксмо, 2020. Энциклопедическое издание, охватывающее широкий спектр вопросов кибербезопасности, включая техники и методы защиты данных.

7. Тимофеев, Ю. Н. «Противодействие кибератакам и информационным угрозам». — Новосибирск: Сибирское универсальное издательство, 2015. Обзорные материалы по современным методам защиты от различных типов кибератак и подходам к управлению рисками.

8. Харитонов, Л. Л. «Комплексные системы защиты информации». — М.: Альфа-Пресс, 2014. Практическое руководство по созданию комплексных систем защиты информации в организациях.

References

1. Andreson, R. «Inzhenerija bezopasnosti». — M.: Vil'jams, 2008. Osnovnoe posobie po voprosam proektirovanija i realizacii sistemy bezopasnosti s akcentom na razlichnye aspekty kiberugroz.

2. Golubev, A. Ju. «Kiberbezopasnost': uchebnoe posobie dlja vuzov». — M.: INFRA-M, 2017. Uchebnoe posobie, predostavljajushhee kompleksnyj obzor podhodov i metodov obespechenija bezopasnosti v informacionnyh sistemah.

3. Kuznecov, S. B., Ivanov, V. I. «Informacionnaja bezopasnost': novye vyzovy i ugrozy». — SPb.: Piter, 2019. Kniga, raskryvajushhaja aktual'nye ugrozy kiberbezopasnosti i strategii protivodejstvija sovremennym atakam.

4. Mel'nikov, I. V. «Osnovy bezopasnosti informacionnyh sistem i tehnologij». — M.: Forum, 2016. Osnovnoj uchebnik po voprosam fundamental'nyh principov zashhity informacii i metodov upravlenija bezopasnost'ju v uslovijah sovremennyh ugroz.

5. Smirnov, A. V., Petrov, N. S. «Zashhita informacii i kiberbezopasnost'». — M.: Jurajt, 2018. Prakticheskoe rukovodstvo po vnedreniju bezopasnyh sistem i tehnologij zashhity informacii.

6. Solov'ev, V. V. «Jenciklopedija kiberbezopasnosti». — M.: Jeksmo, 2020. Jenciklopedicheskoe izdanie, ohvatyvajushhee shirokij spektr voprosov kiberbezopasnosti, vkljuchaja tehniki i metody zashhity dannyh.

7. Timofeev, Ju. N. «Protivodejstvie kiberatakam i informacionnym ugrozam». — Novosibirsk: Sibirskoe universal'noe izdatel'stvo, 2015. Obzornye materialy po sovremennym metodam zashhity ot razlichnyh tipov kiberatak i podhodam k upravleniju riskami.

8. Haritonov, L. L. «Kompleksnye sistemy zashhity informacii». — M.: Al'fa-Press, 2014. Prakticheskoe rukovodstvo po sozdaniju kompleksnyh sistem zashhity informacii v organizacijah.