Шаханова М.В., Швец Е.Е., Шаханова Э.С. Защита конфиденциальных сведений от несанкционированного доступа // Международный журнал информационных технологий и энергоэффективности. – 2025. –Т. 10 № 2(52) с. 166–171

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

[1]Шаханова М.В., Швец Е.Е., Шаханова Э.С.
ФГБОУ ВО «ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Защита конфиденциальных сведений от несанкционированного доступа является актуальной в свете возрастающих угроз кибербезопасности и необходимости обеспечения конфиденциальности информации в цифровую эпоху. Роль информационной составляющей в любом бизнесе с каждым днем возрастает. Защита конфиденциальных сведений охватывает множество аспектов, включая технические меры, организационные протоколы и правовые нормы. В статье рассматриваются вопросы обеспечения защиты конфиденциальных данных, виды информационных угроз. А также будут рассмотрены методы и рекомендации по защите от несанкционированного доступа.

Ключевые слова: Несанкционированный доступ, защита конфиденциальных данных.

PROTECTING CONFIDENTIAL INFORMATION FROM UNAUTHORIZED ACCESS

[1]Shakhanova M. V., Shvets E.E., Shakhanova E.S.
MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

Protecting confidential information from unauthorized access is relevant in light of increasing cybersecurity threats and the need to ensure information privacy in the digital age. The role of the information component in any business is increasing every day. Protecting confidential information covers many aspects, including technical measures, organizational protocols and legal norms. The article discusses issues of ensuring the protection of confidential data, types of information threats. And methods and recommendations for protection from unauthorized access will also be considered.

Keywords: Unauthorized access, protection of confidential data.

В современном мире, где информация становится одним из самых ценных ресурсов, защита конфиденциальных сведений от несанкционированного доступа выходит на передний план. В условиях жесткой конкуренции компании стремятся защитить свою информацию, так как это напрямую влияет на их конкурентоспособность. При этом возрастающая роль законодательства в области защиты данных, такого как Общий регламент по защите данных (GDPR) в Европе, усиливает требования к обработке и хранению личной информации.

Несанкционированный доступ к информации возможен в любой системе – от небольших организаций до крупных государственных структур. Угрозы могут исходить как от внешних злоумышленников, так и от внутренних источников – недобросовестных сотрудников или даже случайных ошибок. Понимание актуальности темы и применение комплексных мер безопасности могут существенно снизить риски, связанные с киберугрозами.

Проблема

Согласно последним данным в области кибербезопасности, число инцидентов, связанных с утечками данных, неуклонно растет. Например, за девять месяцев с начала 2024 года зафиксировано 569 сообщений об утечках баз данных российских компаний, что на 80% больше показателей аналогичного периода прошлого года и на 35% больше, чем за весь 2023 год [1]. Утечки, кражи данных и их подмена могут привести к серьезным последствиям как для организаций, так и для частных лиц: от финансовых потерь до потери репутации. Основные причины утечек часто связаны с недостаточными мерами безопасности: неправильной конфигурацией систем, использованием устаревшего программного обеспечения и слабыми паролями.

Чем более привлекательна информация для злоумышленников, тем настойчивее и изобретательнее становятся их попытки взломов. Чтобы хоть на шаг опередить киберпреступников в этом бесконечном соревновании, компании и госорганы вынуждены тратить колоссальные средства на создание систем ИБ, стремясь максимально защитить свои ресурсы.

Угрозы несанкционированного доступа к конфиденциальным сведениям

На сегодняшний день конфиденциальность информации находится под угрозой из-за ряда факторов, среди которых кибератаки занимают ключевое место. Современные атаки, такие как фишинг, вирусные проникновения и DDoS, представляют собой серьезную угрозу для данных. Например, исследования 2023 года показывают, что фишинг используется в 80% успешных атак для извлечения конфиденциальной информации [2]. Не менее значительными являются внутренние угрозы, возникающие из-за действий сотрудников. Около 60% утечек данных происходит по причине случайных ошибок или умышленных действий персонала [3]. Это подчеркивает необходимость строгого контроля доступа и регулярного обучения сотрудников.

С распространением облачных технологий увеличились риски, связанные с безопасностью данных в удаленных хранилищах. Ненадежные меры защиты на уровне облачных платформ могут стать причиной компрометации информации. В 2024 году доля утечек данных, связанных с облачными хранилищами, составляет около 25% [2]. Кроме того, социальная инженерия остается мощным инструментом злоумышленников. Манипуляции с использованием доверия, например, через поддельные звонки или письма, обеспечивают доступ к закрытой информации. Этот метод в последние годы стал причиной 30% всех инцидентов утечки данных [3].

Законодательные и правовые аспекты защиты данных

Защита конфиденциальной информации не только является вопросом технологий и внутренних практик безопасности, но и подразумевает соблюдение множества законодательных норм. С каждым годом правительства различных стран принимают законы, направленные на защиту личных данных и установление стандартов безопасности. Невыполнение этих норм может привести не только к утечке данных, но и к серьезным юридическим последствиям для организаций.

Основные законы и регуляции

Общий регламент по защите данных (GDPR), принятый в Европейском Союзе в 2018 году, устанавливает строгие требования к обработке и хранению персональных данных. Компании обязаны получить четкое согласие пользователей на обработку их данных, обеспечить право на доступ к информации и её удаление. Штрафы за нарушение GDPR могут достигать 4% от годового мирового оборота компании, что делает соблюдение этого регламента критически важным для бизнеса. Например, в 2023 году средний размер штрафов составил около 1,3 млн евро, отражая усиление контроля за соблюдением норм [2].

В России действует Федеральный закон № 152 «О персональных данных», который регулирует обработку информации граждан. Он предоставляет гражданам право на доступ и корректировку данных, а также предписывает организациям внедрение комплексных мер защиты. Закон требует, чтобы обработка персональных данных происходила только на территории России, что особенно актуально в условиях глобальной цифровизации. За нарушение закона предусмотрены штрафы до 18 млн рублей, а также репутационные потери, которые могут повлиять на доверие клиентов и партнеров.

Законодательные инициативы создают основу для разработки эффективных практик безопасности и формируют культуру ответственности в отношении конфиденциальной информации. Организации, которые серьезно относятся к соблюдению законов о защите данных, не только снижают риски, связанные с утечками, но и укрепляют доверие своих клиентов.

Методы защиты от несанкционированного доступа

Для повышения уровня защиты конфиденциальной информации организациям важно сосредоточиться на ключевых аспектах, обеспечивающих надежную информационную безопасность, особенно в условиях увеличения числа кибератак, которых в 2024 году стало на 25% больше по сравнению с предыдущими годами. Первым шагом является обучение сотрудников. Согласно исследованиям, до 70% утечек данных происходят по причине человеческих ошибок. [8] Регулярное обучение персонала методам защиты и распознавания угроз, таким как фишинг, позволяет существенно снизить вероятность инцидентов. Это особенно важно для сотрудников, работающих с конфиденциальной информацией. Политики безопасности, разработанные службой ИБ, должны четко регулировать доступ сотрудников к информации. Применение принципа "минимально необходимого доступа" может уменьшить риски неправомерного использования данных. Каждое подразделение и каждый сотрудник должны иметь доступ только к тем данным, которые требуются для выполнения их конкретных задач.

Аудит и мониторинг - важный инструмент для своевременного обнаружения угроз. Использование UAM-систем (User Activity Monitoring) для анализа пользовательской активности позволяет выявлять аномалии и предотвращать утечки данных на ранних стадиях. Подобные системы сокращают риск утечек за счет анализа журналов и поведенческой аналитики. Шифрование данных остается основой защиты конфиденциальной информации. Применение шифрования как при передаче данных, так и в состоянии покоя снижает вероятность несанкционированного доступа в большинстве случаев. Многофакторная аутентификация также является обязательным элементом защиты. Внедрение этой технологии делает несанкционированный доступ к системам практически невозможным, увеличивая уровень безопасности учетных записей. Инвестиции в современные технологии, такие как

системы защиты от утечек данных (DLP) и управления доступом (IAM), становятся необходимыми. Например, внедрение DLP-систем позволяет снизить риск потери данных, а IAM-решения обеспечивают эффективное управление правами доступа, защищая системы от внутренних и внешних угроз.

Комплексный подход к защите конфиденциальных сведений

Обеспечение защиты конфиденциальных сведений от несанкционированного доступа требует комплексного и многоуровневого подхода. Однажды внедренные меры безопасности не могут оставаться статичными – их необходимо регулярно пересматривать и адаптировать к новым угрозам и технологическим изменениям. Комплексный подход подразумевает интеграцию технологий, процессов, людей и культуры безопасности в единую стратегию защиты данных.

В современных условиях обеспечения информационной безопасности компании обязаны внедрять передовые технологии и программные решения. Антивирусные системы, межсетевые экраны, инструменты для обнаружения вторжений и шифрование данных становятся стандартом. Важными элементами также являются использование многофакторной аутентификации и регулярное обновление ПО. Эти меры позволяют снизить вероятность успешных кибератак, что особенно актуально в 2024 году, когда количество угроз продолжает расти. Контроль доступа к конфиденциальной информации играет ключевую роль в защите данных. Внедрение принципа "минимально необходимого доступа" и строгих политик управления правами доступа значительно сокращает риски утечек. Такой подход обеспечивает защиту как от ошибок сотрудников, так и от целенаправленных действий злоумышленников.

Однако даже самые продвинутые технологии будут бесполезны без обучения сотрудников. Исследования показывают, что до 70% утечек данных связаны с человеческим фактором. [8] Поэтому компании должны регулярно проводить тренинги для своих сотрудников, обучая их методам распознавания кибератак, включая фишинговые схемы. Создание культуры осведомленности помогает формировать безопасную рабочую среду. Не менее важным аспектом является готовность компании к инцидентам. Четко прописанный план реагирования на утечки данных, включающий конкретные шаги и механизмы, позволяет минимизировать ущерб. Регулярные тестирования и симуляции подобных ситуаций позволяют отработать действия на практике, чтобы при реальной угрозе сократить время реакции и уменьшить последствия.

Следующим аспектом в организации информационной безопасности является анализ рисков. Современные компании должны проводить регулярный анализ рисков, чтобы определить уязвимости своих систем. Это включает в себя оценку текущих мер безопасности, идентификацию критических ресурсов и внедрение политики по защите данных. Важно отметить, что даже самые современные технологии не смогут гарантировать полную защиту без должного контроля и мониторинга.

Защита конфиденциальных сведений от несанкционированного доступа - это вопрос не только технологий, но и ответственного подхода организаций к своей деятельности. Инвестиции в безопасность, обучение сотрудников, соблюдение законодательства и комплексный подход к защите данных позволят существенно снизить риски и защитить как

бизнес, так и персональные данные пользователей. Создавая культуры безопасности, мы можем обеспечить надежное будущее для конфиденциальной информации.

Заключение

Защита конфиденциальных сведений от несанкционированного доступа является комплексной задачей, требующей интеграции технологий, повышения осведомленности сотрудников и соблюдения правовых норм. Внедрение эффективных мер безопасности и соблюдение законодательства не только обеспечивает защиту данных, но и укрепляет доверие клиентов, что в свою очередь способствует успешному развитию бизнеса.

Для создания действенной системы защиты компании необходимо определить степень важности различных типов данных, знать, где они хранятся, как обрабатываются, круг лиц, имеющих доступ, а также как уничтожаются в конце жизненного цикла. Без такого структурированного подхода будет сложно предотвратить утечку конфиденциальных данных и обосновать финансовые затраты на защиту информации.

Список литературы

1. ГК «Солар»: число инцидентов, связанных с утечками данных, с начала года выросло на 80%. [Электронный ресурс]. Режим доступа: https://rt-solar.ru/events/news/4836/.
2. Фишинг Phishing. [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/index.php/Статья:Фишинг_(phishing).
3. Утечки данных. [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/index.php/Статья:Утечки_данных.
4. Богданова А.М. Вопросы студенческой науки Защита конфиденциальных данных, как способ поддержания информационной безопасности / А.М. Богданова, Путилов А.О. - Выпуск №5 (45), май 2020
5. Л.Р. Сафина Обеспечение безопасности конфиденциального документа Российский государственный профессионально-педагогический университет
6. INFOWATCH Аналитика Новые отчеты по кибербезопасности компании Cyble 2024 год
7. Информационная безопасность и защита персональных данных 2023 года [Электронный ресурс]. URL: https://rt-solar.ru/products/solar_dozor/blog/3321/
8. Утечки персональных данных. 20224 год. [Электронный ресурс]. URL: https://gendalf.ru/news/zpdn/chelovecheskiy-faktor-68-utechek-dannykh/

References

1. Solar Group: the number of incidents related to data leaks has increased by 80% since the beginning of the year. [electronic resource]. Access mode: https://rt-solar.ru/events/news/4836/.
2. Phishing Phishing. [electronic resource]. Access mode: https://www.tadviser.ru/index.php/Статья:Phishing_(phishing).
3. Data leaks. [electronic resource]. Access mode: https://www.tadviser.ru/index.php/Статья:Leake_data.
4. Bogdanova A.M. Issues of student science Protection of confidential data as a way to maintain information security / A.M. Bogdanova, Putilov A.O. - Issue No. 5 (45), May 2020

5. L.R. Safina Ensuring the security of a confidential document Russian State Vocational Pedagogical University
6. INFOWATCH Analytics New Cybersecurity Reports from Cyble 2024
7. Information security and personal data protection in 2023 [Electronic resource]. URL:https://rt-solar.ru/products/solar_dozor/blog/3321/
8. Leakage of personal data. The year is 20224. [electronic resource]. URL: https://gendalf.ru/news/zpdn/chelovecheskiy-faktor-68-utechek-dannykh/