Шаханова М.В., Забелина В.Д., Шаханова Э.С. Актуальность проблемы и методы защиты конфиденциальных данных от утечки в системах российских организаций // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 2(52) с. 80–84

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ И МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОТ УТЕЧКИ В СИСТЕМАХ РОССИЙСКИХ ОРГАНИЗАЦИЙ

[1]Шаханова М.В., Забелина В.Д., 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

Одной из наиболее актуальных проблем в обеспечении системы информационной безопасности организации является утечка информации. Автором настоящей статьи акцентируется внимание на актуальности вопроса и методах защиты конфиденциальных данных в информационных системах. Целью работы является обоснование необходимости развития существующих технологий и методов на фоне увеличивающегося числа успешных кибератак и колоссального объема утечки информации. В результате статьи подтверждается острая актуальность данной проблемы, а также представлены наиболее эффективные и требующие своего внедрение методы защиты конфиденциальных данных. Автором также ставится вопрос о необходимости применения комплексных систем и подходов, обеспечивающих защиту в различных направлениях.

Ключевые слова: Информационная безопасность, защита, конфиденциальные данные, утечка, информация, организация, информационная система.

THE RELEVANCE OF THE PROBLEM AND METHODS OF PROTECTING CONFIDENTIAL DATA FROM LEAKAGE IN THE SYSTEMS OF RUSSIAN ORGANIZATIONS

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

One of the most pressing problems in ensuring an organization's information security system is information leakage. The author of this article focuses on the relevance of the issue and methods of protecting confidential data in information systems. The purpose of the work is to substantiate the need to develop existing technologies and methods against the background of an increasing number of successful cyber-attacks and a huge amount of information leakage. Because of the article, the acute relevance of this problem is confirmed, and the most effective and demanding methods of protecting confidential data are presented. The author also raises the question of the need to apply integrated systems and approaches that provide protection in various directions.

Keywords: Information security, protection, confidential data, leakage, information, organization, information system.

Актуальность проблемы утечки конфиденциальных данных в российских информационных системах с каждым годом становится все более острой. Современные информационные технологии (далее – ИТ) активно внедряются во все сферы жизни, однако вместе с их развитием увеличивается объем обрабатываемой и хранимой информации, включая персональные данные, коммерческие тайны и государственную информацию, что порождает риски информационной безопасности (далее – ИБ). Однако эта тенденция

сопровождается ростом рисков несанкционированного доступа и утечек данных, что приводит к серьезным экономическим, репутационным и правовым последствиям для организаций и общества в целом [1]. Ситуация в 2023 году демонстрирует тревожную динамику. Средний объем утечки данных в России увеличился вдвое и составил 1,7 миллиона записей персональных данных. За год было зафиксировано 95 утечек крупных баз данных, что на 28% больше, чем в 2022 году. Эти цифры свидетельствуют о растущем масштабе проблемы и увеличении целенаправленных атак на информационные системы российских организаций. Особую тревогу вызывает тот факт, что более 80% утечек произошли в результате кибератак, что подтверждает высокий уровень угрозы со стороны киберпреступников.

Данные тенденции подчеркивают необходимость комплексного подхода к обеспечению ИБ. Устранение рисков утечек требует усиления мер защиты, внедрения современных технологий кибербезопасности, повышения осведомленности сотрудников и разработки надежных механизмов мониторинга и предотвращения инцидентов [2]. Эти вопросы также регулируются ФЗ № 152 «О персональных данных» от 27.07.2006 [3]. В условиях увеличивающегося количества утечек защита конфиденциальной информации становится одной из ключевых задач для российских организаций и государства. Для решения проблем утечки конфиденциальных данных необходимо применять специальные методы защиты, которые обеспечивают комплексный подход к информационной безопасности [4]. В 2024 году существует множество таких методов и подходов, каждый из которых направлен на устранение различных угроз и повышение уровня защищенности информации. В табл. 1 автором представлены результаты систематизации наиболее актуальных и эффективных методов защиты, включая антивирусы, межсетевые экраны, системы предотвращения вторжений (IPS), системы обнаружения вторжений (IDS), и системы предотвращения утечек (DLP).

Таблица 1 - Методы защиты конфиденциальных данных

№	Метод	Описание и состав	Возможности
1	Антивирусы	Программное обеспечение для обнаружения и устранения вредоносного кода (вирусов, троянов, шпионских программ).	Защита от вредоносного ПО, автоматическое сканирование файлов, карантин для подозрительных объектов.
2	Межсетевые Экраны (МЭ)	Сетевые устройства или программы, фильтрующие входящий и исходящий трафик на основе заданных правил.	Предотвращение несанкционированного доступа, контроль трафика между сегментами сети.
3	Системы предотвращения вторжений (IPS)	Активные системы, блокирующие подозрительную активность в реальном времени.	Оперативное реагирование на атаки, защита от попыток эксплуатации уязвимостей.

4	Системы обнаружения вторжений (IDS)	Пассивные системы, отслеживающие и фиксирующие подозрительные действия в сети.	Мониторинг активности, выявление потенциальных угроз, анализ инцидентов.
5	Системы предотвращения утечек (DLP)	Комплекс программных решений, предотвращающих несанкционированную передачу конфиденциальной информации.	Контроль перемещения данных, защита на уровне пользователей, предотвращение отправки данных за пределы сети.

Применение данных методов позволяет минимизировать риски утечек, повысить устойчивость систем к кибератакам и обеспечить соответствие современным требованиям информационной безопасности. Учитывая непрекращаемую динамику роста числа кибератак и объемов утечек в период последних лет до 2023 года, автором рекомендуется применение комплексных систем безопасности, включающих несколько методов из табл. 1. Такой подход позволяет обеспечить многоуровневую защиту, которая снижает вероятность успешной реализации угроз, минимизирует последствия кибератак и утечек данных. В комплексе целесообразно использовать следующие методы:

1. Антивирусы и МЭ обеспечивают базовый уровень защиты, предотвращая проникновение вредоносного программного обеспечения и ограничивая несанкционированный доступ к сети [5]. Они действуют как первая линия обороны, отсекая известные угрозы и фильтруя подозрительный трафик;

2. Системы предотвращения вторжений (IPS) и обнаружения вторжений (IDS) дополняют этот уровень, отслеживая подозрительную активность и оперативно блокируя угрозы в реальном времени. Их синергия позволяет не только фиксировать атаки, но и предпринимать превентивные меры, что особенно важно в условиях высоких скоростей современных атак;

3. Системы предотвращения утечек (DLP) интегрируются для защиты критически важных данных на уровне пользователя [6]. Они предотвращают передачу конфиденциальной информации за пределы корпоративной сети и обеспечивают контроль над действиями сотрудников, снижая риски утечек по вине внутренних угроз.

Использование этих методов в комплексе создаст надежный защитный периметр, охватывающий все этапы работы с информацией: от предотвращения внешних вторжений до защиты внутренних процессов. Такой подход особенно актуален в условиях российской информационной среды, в которой число кибератак продолжает расти, а объемы утечек персональных данных увеличиваются ежегодно, исходя из открытых данных до 2023 года. Ожидается, что применение комплексного подхода к защите конфиденциальных данных, включающего использование нескольких методов из табл. 1, позволит повысить эффективность системы защиты до 40-70%. Это будет достигнуто за счет реализации многоуровневой защиты, которая снизит вероятность успешных атак, охватывая как

внутренние, так и внешние угрозы, а также обеспечивающая своевременное выявление и предотвращение инцидентов [7]. Интеграция различных инструментов позволит устранить уязвимости, которые могут быть свойственны отдельным методам, создавая единый эффективный механизм защиты информации.

Целью настоящей статьи являлось обоснование необходимости внедрения комплексных систем защиты конфиденциальных данных, включающих наиболее эффективные современные методы, а также анализ их значимости для противодействия растущим киберугрозам и предотвращения утечек информации в российских информационных системах. В рамках работы проанализирована актуальность проблемы утечки конфиденциальных данных в условиях роста числа кибератак, увеличения объема утечек персональных данных и значительного ущерба, наносимого российским организациям. Представлена систематизация современных методов защиты конфиденциальной информации. Обоснована необходимость применения комплексных подходов, которые обеспечивают многоуровневую защиту за счет комбинации различных методов, что позволяет устранить уязвимости отдельных решений и обеспечить высокий уровень безопасности. Проведенный анализ демонстрирует, что комплексный подход способен существенно повысить эффективность защиты конфиденциальных данных благодаря устранению внутренних и внешних угроз, своевременному реагированию на инциденты и улучшению мониторинга состояния информационных систем. Практическая ценность статьи заключается в том, что представленные материалы могут быть использованы организациями для формирования эффективных стратегий обеспечения информационной безопасности, минимизации рисков утечек данных и повышения устойчивости к киберугрозам.

Список литературы

1. Хаджаев С.И. Актуальность проблемы защиты информационных систем малого и среднего бизнеса от кибератак // Al-Farg’oniy avlodlari. 2023. №4. С. 212-217.
2. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. №91. С. 226-241.
3. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция).
4. Губенко Н.Е., Потреба Е.Ю. Анализ методов и средств предотвращения утечек конфиденциальных данных // Проблемы искусственного интеллекта. 2023. №3 (30). С. 55-64.
5. Митюшин Д.А. Правовые вопросы применения систем защиты от утечки конфиденциальной информации на объектах информатизации // Вестник Московского университета МВД России. 2020. №5. С. 163-168.
6. Богданова А. М., Путилов А. О. Защита конфиденциальных данных, как способ поддержания информационной безопасности // Скиф. 2020. №5-1 (45). С. 102-106.
7. Афанасьева С. А., Терешкина О. С. Стратегии защиты от утечек информации в целях обеспечения экономической безопасности организации // Вестник науки. 2024. №11 (80). С. 50-59.

References

1. Khadzhaev S.I. The relevance of the problem of protecting information systems of small and medium-sized businesses from cyber attacks // Al-Farg'oniy avlodlari. 2023. No. 4. pp. 212-217.
2. Shvyryaev P.S. Confidential data leaks: the main enemy inside // State Administration. Electronic bulletin. 2022. No. 91. pp. 226-241.
3. Federal Law "On Personal Data" dated 27.07.2006 N 152-FZ (latest edition).
4. Gubenko N.E., Ubera E.Y. Analysis of methods and means of preventing confidential data leaks // Problems of artificial intelligence. 2023. No. 3 (30). pp. 55-64.
5. Mityushin D.A. Legal issues of the use of protection systems against leakage of confidential information at informatization facilities // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. No. 5. pp. 163-168.
6. Bogdanova A.M., Putilov A. O. Protection of confidential data as a way to maintain information security // Skif. 2020. No.5-1 (45). pp. 102-106.
7. Afanasyeva S. A., Tereshkina O. S. Strategies to protect against information leaks in order to ensure economic security organizations // Bulletin of Science. 2024. No. 11 (80). pp. 50-59.