УДК 004

Набиева А.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В условиях постоянного роста объемов данных увеличения числа киберугроз, защита информации стала одной из главных задач для организаций. В данной работе рассмотрены основы технической защиты информации, проведен анализ современных методов и технологий защиты данных, а также разработаны рекомендации по совершенствованию системы технической защиты информации организации. Особое внимание уделено комплексному подходу, включающему аппаратные, программные и организационные меры.

Ключевые слова: техническая защита информации, уязвимости, киберугрозы, системы обнаружения вторжений, аудит безопасности.

Комплексная система защиты информации (КСЗИ) – совокупность организационных, правовых, инженерно-технических (физических), программно-аппаратных, криптографических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа [1].

Система технической защиты информации (СТЗИ) – это совокупность специальных технических средств, персонала его эксплуатирующего и их использование для защиты информации. Выбор технических средств защиты зависит от выбранного уровня защищенности информации, который необходимо обеспечить.

Мероприятия, проводимые для технической защиты информационной инфраструктуры организации, могут включать в себя: использование защищенных подключений и межсетевых экранов, средств шифрования и защиты от несанкционированного доступа, а также разграничение потоков информации между сегментами сети. При этом они неразрывно связаны с инженерно-техническими (физическими) – установкой систем контроля управления доступом (СКУД), средствами видеонаблюдения, датчиков охранной сигнализации, металлических ворот и др. Отдельные помещения также могут быть оборудованы средствами защиты от утечки акустической (речевой) информации.

В целом, многие организации сталкиваются с угрозами информационной безопасности, которые можно классифицировать на

четыре категории: внешние кибератаки, внутренние угрозы, технические уязвимости и методы социальной инженерии [2].

К внешним угрозам относятся: фишинг, DDoS-атаки, эксплуатация уязвимостей программного обеспечения. Внутренние угрозы включают в себя как умышленные действия инсайдеров (злоупотребление доступом), так и непреднамеренные нарушения (ошибочные отправки конфиденциальной информации). Технические уязвимости проявляются в слабом шифровании данных (использование устаревших алгоритмов), ошибках конфигурации облачных сервисов.

Опасность представляют методы социальной инженерии, позволяющие злоумышленникам обходить технические средства защиты через манипуляции с персоналом. Последствия перечисленных угроз представляют комплексный характер: от прямых финансовых потерь, до репутационного ущерба и юридических рисков, что подтверждает необходимость внедрения многоуровневой системы защиты, включающей регулярный аудит уязвимостей, сочетание технологических решений и обучение сотрудников [3].

В цифровой среде защита информации требует особого подхода, сочетающего несколько взаимодополняющих технологий. Основой являются криптографические методы: передаваемые данные защищаются протоколами SSL/TLS, которые обеспечивают безопасное соединение, а для хранения конфиденциальной информации применяются алгоритмы шифрования (AES-256 для симметричного шифрования и PGP для асимметричного).

Одним из главных элементов защиты являются системы обнаружения и предотвращения вторжений (IDS/IPS), которые анализируют сетевой трафик, используя сигнатурный анализ для выявления известных угроз и поведенческий анализ для обнаружения аномальной активности, автоматически блокируя потенциально опасные действия. Для предотвращения утечек данных применяются DLP-системы, которые производят глубокий контент-анализ и мониторинг всех каналов передачи информации (электронная почта, мессенджеры, съемные носители), а также отслеживающие поведение пользователей для выявления подозрительных действий. Доступ к критическим системам защищается многофакторной аутентификацией, требующей не только пароль, но и дополнительное подтверждение через SMS-коды или биометрические данные. Систематическое обновление программного обеспечения помогает своевременно закрывать уязвимости, а стратегия резервного копирования по принципу 3-2-1 (три копии данных на двух разных типах носителей, одна из которых хранится географически обособленно) дает возможность быстрого восстановления после инцидентов [4].

В целях совершенствования СТЗИ организации необходимо произвести комплекс взаимосвязанных мер, основанных на современных подходах к информационной безопасности. Главной задачей является проведение

регулярного комплексного аудита безопасности, включающего анализ уязвимостей и оценку соответствия международным стандартам (ISO 27001, PCI DSS). Основным элементом модернизации СТЗИ должно стать внедрение SOC (Security Operations Center) с использованием платформ SIEM (например, IBM QRadar или Splunk), обеспечивающего оперативное выявление инцидентов и координацию реагирования. Также необходимо реализовать программу непрерывного обучения сотрудников, где будут не только базовые тренинги по кибергигиене, но и специализированные курсы по распознаванию фишинга и социальной инженерии [5]. Архитектурные улучшения должны включать в себя логическую сегментацию сети с применением технологий микросегментации, что позволит минимизировать зону поражения при компрометации. Обязательным требованием является разработка детальных политик безопасности, регламентирующих все аспекты работы с данными – от классификации информации, до процедур реагирования на инциденты. В качестве технологической основы рекомендовано использовать защищенные облачные решения, такие как Microsoft Azure Sentinel для мониторинга угроз или Kaspersky Endpoint Security для защиты рабочих станций, которые обеспечивают масштабируемость и доступ к современным средствам защиты. Реализация данных мер поможет создать адаптивную СТЗИ, которая качественно противостоит современным киберугрозам.

В заключение необходимо выделить, что разработка эффективной СТЗИ подразумевает комплексный подход, умещающий современные технологические решения (криптографическую защиту, системы обнаружения вторжений, DLP-системы, многофакторную аутентификацию) с организационными мерами (регулярный аудит безопасности, создание SOC, обучение персонала, разработку регламентирующих документов). Одним из главных является принцип многоуровневой защиты, предполагающий не только внедрение отдельных средств защиты, но и их системную интеграцию, обеспечивающую синергетический эффект. Соблюдение предложенных рекомендаций поможет организациям создать адаптивную систему информационной безопасности, которая сможет противостоять киберугрозам, минимизировать риски утечек данных и обеспечить непрерывность бизнес-процессов.

Список использованных источников:

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. Электрон. версия. URL: https://books.ifmo.ru/file/pdf/2006.pdf /.

2. Николаева К.А, Шабурова А.В. Совершенствование политики информационной безопасности в организации. Электрон. версия. URL:https://cyberleninka.ru/article/n/sovershenstvovanie-politiki-informatsionnoy-bezopasnosti-v-organizatsii /.

3. Солодянников А.В. Информационная безопасность автоматизированных систем: учебное пособие. Электрон. версия. URL: https://infosec.spb.ru/wp-content/uploads/2020/08/solodjannikov.pdf /.

4. Исмагилова А.С. Количественная оценка рекомпозиционной системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 8(116). С. 273–281.

5. Ахмадиева В.Ф. Обучение персонала с использованием платформы по осуществлению симуляции кибератак / В.Ф. Ахмадиева, В.Ф. Ахмадиева // Вопросы эффективного применения научного потенциала общества: сборник статей по итогам Международной научно-практической конференции, Екатеринбург, 09 апреля 2025 г. Стерлитамак: Агентство международных исследований, 2025. С. 110–114.

Nabieva A.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF IMPROVING THE SYSTEM OF TECHNICAL PROTECTION OF INFORMATION

Abstract. With the constant growth of data volumes and the increasing number of cyber threats, information protection has become one of the main tasks for organizations. In this paper, the basics of technical information protection are considered, an analysis of modern methods and technologies of data protection is carried out, and recommendations for improving the system of technical information protection (TPI) of organizations are developed. Special attention is paid to an integrated approach, including hardware, software and organizational measures.

Keywords: technical information protection, vulnerabilities, cyber threats, intrusion detection systems, security audit.