УДК 631

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ ЛЮБОГО ПРОФИЛЯ

Исмагилов Тимур Ленарович
- студент 2 курса
Алексеева Анна Александровна
– кандидат технических наук, доцент
Казанский национальный исследовательский технологический университет, Казань

Аннотация: Научная статья посвящена важной проблеме обеспечения комплексной информационной безопасности на предприятиях различных профилей деятельности. В статье рассматриваются ключевые аспекты информационной безопасности, воздействие угроз на компании, а также предлагаются рекомендации по эффективному обеспечению безопасности информации на предприятии.
Ключевые слова: предприятия, безопасность, профиль, информация.

ENSURING COMPREHENSIVE INFORMATION SECURITY AT AN ENTERPRISE OF ANY PROFILE

Timur Ismagilov Lenarovich
- 2nd year student
Alekseeva Anna Alexandrovna
– Candidate of Technical Sciences, Associate Professor
Kazan National Research Technological University, Kazan

Abstract: The scientific article is devoted to the important problem of ensuring integrated information security at enterprises of various business profiles. The article examines the key aspects of information security, the impact of threats on companies, and also offers recommendations on effective information security in the enterprise.
Keywords: enterprises, security, profile, information.

В современном мире, где информационные технологии играют все более значимую роль, обеспечение комплексной информационной безопасности (ИБ) становится неотъемлемым элементом успешного функционирования любого предприятия, независимо от его профиля деятельности. Потери от киберугроз постоянно растут, и неспособность обеспечить адекватную защиту может привести к серьезным финансовым и репутационным потерям, а также нарушению нормальной работы бизнеса.

Данная статья посвящена комплексному подходу к обеспечению информационной безопасности на предприятиях различного профиля. Мы рассмотрим ключевые аспекты построения системы ИБ, современные угрозы и методы защиты, а также законодательную базу, регламентирующую деятельность в сфере информационной безопасности.

Основные понятия и терминология

-Информационная безопасность (ИБ) – это комплекс мер, направленных на защиту информации от несанкционированного доступа, изменения, уничтожения, а также на обеспечение ее целостности, конфиденциальности и доступности.

-Информационные активы – это любая информация, которая имеет для предприятия ценность, например, финансовая документация, персональные данные сотрудников, коммерческие секреты, интеллектуальная собственность.

-Киберугрозы – это действия или события, которые могут привести к нарушению информационной безопасности, например, хакерские атаки, вирусы, шпионские программы, DDoS-атаки, утечки информации.

-Система информационной безопасности (СИБ) – это совокупность организационных, технических и правовых мер, направленных на обеспечение информационной безопасности предприятия.

Этапы построения системы информационной безопасности.Построение эффективной системы информационной безопасности является многоэтапным процессом, который включает в себя:

Анализ рисков и уязвимостей.

-Определение информационных активов: выявление всех ценных информационных ресурсов, находящихся в распоряжении предприятия.

-Оценка угроз: анализ существующих и потенциальных угроз для информационных активов, исходя из специфики деятельности предприятия и внешних факторов.

-Оценка уязвимостей: выявление слабых мест в информационной системе, которые могут быть использованы злоумышленниками.

Формирование политики информационной безопасности.

-Разработка политики: создание комплексного документа, определяющего основные принципы и правила обеспечения ИБ на предприятии.

-Внедрение политики: доведение политики до сведения всех сотрудников, обучение и контроль за ее соблюдением.

Выбор и внедрение средств защиты

-Технические средства: антивирусные программы, межсетевые экраны, системы обнаружения вторжений, системы управления доступом, шифрование данных.

-Организационные меры: разработка и внедрение внутренних регламентов, обучение сотрудников правилам ИБ, контроль за использованием информационных систем.

-Правовые меры: заключение договоров о неразглашении конфиденциальной информации, соблюдение законодательства о защите персональных данных.

Мониторинг и реагирование на инциденты.

-Мониторинг: постоянный контроль за состоянием информационной системы, выявление и анализ подозрительных событий.

-Реагирование на инциденты: разработка плана действий в случае возникновения угроз, восстановление работоспособности системы, расследование инцидентов.

Основные угрозы информационной безопасности.Современный киберландшафт характеризуется высоким уровнем сложности и разнообразием угроз. Основные типы угроз:

Внутренние угрозы

-Неосторожные действия сотрудников: несоблюдение правил ИБ, использование личных устройств для работы, передача конфиденциальной информации по незащищенным каналам.

-Злонамеренные действия сотрудников: кража конфиденциальных данных, саботаж, мошенничество.

Внешние угрозы

-Хакерские атаки: взлом информационных систем, кража данных, DDoS-атаки.

-Вирусы и вредоносные программы: заражение компьютеров, кража данных, блокировка работы системы.

-Фишинговые атаки: мошеннические действия, направленные на получение конфиденциальных данных пользователей, например, логинов и паролей.

-Социальная инженерия: психологическое воздействие на пользователей с целью получения доступа к информационным ресурсам.

Методы защиты информационной безопасности

-Антивирусное ПО: блокировка вредоносных программ, обнаружение и удаление вирусов.

-Межсетевые экраны: блокировка несанкционированного доступа к информационным ресурсам.

-Системы обнаружения вторжений: выявление подозрительной активности в сети.

-Системы управления доступом: контроль за доступом пользователей к информационным ресурсам.

-Шифрование данных: преобразование данных в нечитаемый формат для защиты от несанкционированного доступа.

-Разработка и внедрение политики ИБ: определение правил и процедур обеспечения безопасности.

-Обучение сотрудников: повышение осведомленности сотрудников о киберугрозах, обучение правилам работы с информационными системами.

-Разработка плана реагирования на инциденты: определение действий в случае возникновения угроз.

-Законодательство о защите персональных данных: соблюдение правил обработки и хранения личной информации.

-Договоры о неразглашении конфиденциальной информации: защита коммерческих секретов.

Роль информационных технологий в обеспечении комплексной информационной безопасностиСовременные информационные технологии играют ключевую роль в обеспечении комплексной информационной безопасности.

-Системы управления информационной безопасностью (СУИБ): централизованные системы для управления процессами ИБ, мониторинга, реагирования на инциденты, аудита.

-Сетевые технологии: использование VPN, защищенных протоколов.

-Облачные технологии: использование облачных сервисов для хранения данных, резервного копирования, обеспечения доступности.

-Big Data: анализ больших объемов данных для выявления аномалий и прогнозирования угроз.

-Искусственный интеллект: автоматизация процессов ИБ, выявление аномалий, реагирование на инциденты.

Правовая база обеспечения информационной безопасности.

-Федеральный закон "Об информации, информационных технологиях и о защите информации" (№ 149-ФЗ от 27.07.2006 г.): устанавливает основные положения о защите информации, включая конфиденциальную информацию, персональные данные, государственную тайну.

-Федеральный закон "О персональных данных" (№ 152-ФЗ от 27.07.2006 г.): устанавливает правила обработки и защиты персональных данных.

-Постановление Правительства РФ "Об утверждении Положения о требованиях к защите информации, обрабатываемой в информационных системах персональных данных" (№ 1119 от 15.09.2008 г.): устанавливает требования к защите персональных данных, обрабатываемых в информационных системах.

-ГОСТы и стандарты в сфере информационной безопасности.

-Инструкции и приказы ФСБ России, МВД России, ФСО России, Роскомнадзора.

Кейсы и примеры практического применения.

-Банковская сфера: использование многофакторной аутентификации, шифрования данных, систем мониторинга и реагирования на инциденты.

-Компании электронной коммерции: использование антивирусного ПО, межсетевых экранов, систем предотвращения мошенничества.

-Производственные предприятия: использование систем управления доступом, контроля за промышленными объектами, систем безопасности для промышленных сетей.

Тенденции развития информационной безопасности.

-Увеличение сложности киберугроз: новые типы атак, использование искусственного интеллекта, распространение ботнетов.

-Рост использования облачных технологий:
повышение требований к защите данных в облаке, обеспечение безопасности при работе с облачными сервисами.

-Развитие технологий ИБ: новые методы шифрования, системы анализа больших данных, средства обнаружения и реагирования на атаки.

-Увеличение роли человеческого фактора: повышение осведомленности сотрудников, обучение правилам ИБ, создание культуры безопасности.

Подводим итог: обеспечение комплексной информационной безопасности является важнейшей задачей для любого предприятия, желающего успешно функционировать в современном мире. Построение системы ИБ – это непрерывный процесс, необходимо постоянно анализировать риски, совершенствовать методы защиты, адаптироваться к новым угрозам.Информационная безопасность – это не только техническая проблема: ключевую роль играют организационные меры, обучение сотрудников, создание культуры безопасности.Совместные усилия, необходима тесная координация между ИТ-отделом, службой безопасности, руководством, всеми сотрудниками.

Литература

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон от 27.07.2006 г. № 152-ФЗ "О персональных данных"
3. Постановление Правительства РФ от 15.09.2008 г. № 1119 "Об утверждении Положения о требованиях к защите информации, обрабатываемой в информационных системах персональных данных"
4. ГОСТ Р 56939-2016 "Информационная безопасность. Защита информации. Общие положения"
5. ГОСТ Р 57580.3-2017 "Информационная безопасность. Системы защиты информации. Комплексная система защиты информации. Требования и рекомендации"
6. "Information Security Management Systems - Requirements" (ISO/IEC 27001:2013)
7. "Guide for the Management of IT Security" (ISO/IEC 27002:2013)
8. "The CIS Controls v8" (Center for Internet Security)
9. "NIST Cybersecurity Framework" (National Institute of Standards and Technology)
10. "Security and Privacy for Cloud Computing" by Michael W. Allen and William A. Wulf.