МИНОБРНАУКИ РОССИИ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ

ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)

Кафедра Систем автоматизированного проектирования

ИДЗ №1

по дисциплине «Экономика»

Тема: «Информационная безопасность – понятие и направления деятельности»

Студент гр. 1302 _____ Новиков Г.В.

Преподаватель _____ Скрынская О.А.

Санкт-Петербург

2022

Содержание

Введение

Информационная безопасность — это практика сохранения и защиты информации путем снижения информационных рисков. Предотвращается несанкционированный доступ, использование, модификация, запись или уничтожение информации, а также включаются действия, направленные на уменьшение неблагоприятных последствий.

В информационной безопасности необходимо учитывать все текущие и вероятные угрозы и уязвимости, обеспечивать непрерывный мониторинг в режиме реального времени и отслеживать весь жизненный цикл информации (с момента создания до ее уничтожения или потери актуальности).

В современном мире, где данные компаний и людей находятся в относительном информационном доступе, необходимо защищать эти данные, поскольку в случае их утери могут быть утеряны персональные данные человека, а бизнес может потерять значительные суммы и т.д.

Модель системы безопасности

Информация защищена, если соблюдаются эти 3 свойства:

1. Целостность – обеспечение надежности и корректного отображения защищенных данных, независимо от того, какие системы безопасности и методы защиты используются в компании. Целостность также гарантирует предотвращение искажения информации.

2. Конфиденциальность – доступ к просмотру и редактированию корпоративных данных, информации и активов предоставляется исключительно авторизованным пользователям системы защиты на определенных этапах бизнес-операций.

3. Доступность – все авторизованные пользователи должны иметь надежный и эффективный доступ к конфиденциальной информации. Доступность также включает в себя восстановление системы из-за сбоя.

Элементы управления безопасности

Правильный выбор соответствующих типов контроля безопасности необходим для правильного обеспечения информационной безопасности:

Административный. Административный тип контроля состоит из утвержденных процедур, стандартов и принципов. Это формирует основу для ведения бизнеса и управления людьми. Законы и подзаконные акты, создаваемые государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают корпоративные политики безопасности, пароли, прием на работу и дисциплинарные меры.

Логический. Логические средства контроля (также называемые техническими средствами контроля) основаны на защите доступа к информационным системам, программному обеспечению, паролям, брандмауэрам, информации для мониторинга и контроля доступа к информационным системам.

Физический. Это контроль рабочей среды и вычислительных средств (отопление и кондиционирование воздуха, дымовая и пожарная сигнализации, системы противопожарной защиты, камеры, баррикады, заборы, замки, двери и т.д.).

Виды конфиденциальных данных

Личные конфиденциальные данные: персональные данные граждан, право на неприкосновенность частной жизни, переписка, сокрытие личности. Единственным исключением является информация, которая распространяется в средствах массовой информации.

Официальные конфиденциальные данные: информация, доступ к которой может ограничить только государство (органы государственной власти).

Судебные конфиденциальные данные: тайна следствия и судебного разбирательства.

Коммерческие конфиденциальные данные: все виды информации, связанной с коммерцией (прибылью) и доступ к которой ограничен законом или предприятием (секретные разработки, производственные технологии и т.д.).

Профессиональные конфиденциальные данные: данные, связанные с деятельностью граждан, например, медицинская, нотариальная или адвокатская тайна, разглашение которой преследуется по закону.

Угрозы информационной безопасности

Природные (катаклизмы, не зависящие от человека: пожары, ураганы, наводнения, удары молнии и т.д.).

Искусственные, которые также делятся на:

- непреднамеренные (совершенный людьми по небрежности или невежеству);

- преднамеренные (хакерские атаки, незаконные действия конкурентов, месть сотрудников и т.д.).

- внутренние (источники угроз, которые находятся внутри системы).

- внешние (источники угроз вне системы).

Они также делятся на пассивные (не изменяют структуру и содержание информации) и активные (изменяют структуру и содержание системы).

Средства защиты информационной безопасности

Организационные: это совокупность организационно-технических (предоставление компьютерных средств, настройка кабельной системы и т.д.) и организационно-правовых (законодательная база, устав конкретной организации) средств.

Программное обеспечение: те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.

Технические (аппаратные средства): это технические типы устройств, которые защищают информацию от проникновения и утечки.

Смешанное аппаратное и программное обеспечение: выполняет функции как аппаратного, так и программного обеспечения.

Типы средств информационной безопасности: антивирусы, криптографические системы, предотвращение утечки данных (DLP), брандмауэры, виртуальные частные сети (VPN), прокси-серверы, системы мониторинга и управления информационной безопасностью.

Направления развития информационной безопасности

• Безопасность критически важных объектов:

1. системы управления государственными и правоохранительными органами, Министерством по чрезвычайным ситуациям, системами пожарной и военной безопасности;

2. информационная инфраструктура кредитно-финансовых учреждений;

3. системы связи, спутниковые, географические, навигационные системы;

4. системы управления ресурсоснабжающими организациями (электростанции, водоканалы);

5. системы управления транспортом;

6. системы управления опасными объектами.

• Разработка кибероружия;

• Облачная безопасность:

Нерешенные вопросы: нормативно-правовое регулирование,

техническая поддержка, разработка новых средств защиты информации, организационное взаимодействие.

• Противодействие мошенничеству в финансово-кредитной сфере:

1. защита каналов удаленного доступа, трафика передачи финансовой конфиденциальной информации;

2. Создание доверенной среды на оборудовании клиента с использованием токенов TrustScreen или Mac;

3. разработка и внедрение процессов борьбы с мошенничеством, направленных на хищение денежных средств;

4. мониторинг всех транзакций, который может выявить мошеннические транзакции среди сотен тысяч транзакций, проходящих через банковскую систему.

• Информационная безопасность криптовалют;

• Защита персональных данных;

• Безопасность медицинских систем;

• Безопасность мобильных устройств;

• Защита от виртуализации;

Заключение

Информация очень важна для успешного развития бизнеса, поэтому она нуждается в соответствующей защите. Это стало особенно актуальным в бизнес-среде, где информационные технологии вышли на первый план. Поскольку мы живем в эпоху цифровой экономики, рост компании без них просто невозможен.

Обеспечение информационной безопасности становится все более сложным и актуальным по мере развития цифрового мира. Информация в настоящее время подвергается хакерским атакам, перехватам данных по сети, воздействию вирусного программного обеспечения и другим угрозам, которые становятся все более изощренными и набирают огромные темпы. Следовательно, существует необходимость во внедрении систем информационной безопасности, которые могли бы защитить данные компании.

На выбор подходящих средств информационной безопасности влияют многие факторы, в том числе сфера деятельности компании, ее размер, техническая сторона, а также знания сотрудников в области информационной безопасности.

Список используемых источников:

1. Информационная безопасность (википедия – англ.): https://en.wikipedia.org/wiki/Information_security#Security_controls

2. Информационная безопасность: https://searchinform.ru/informatsionnaya-bezopasnost/

3. Информационная безопасность: https://pirit.biz/reshenija/informacionnaja-bezopasnost

4. Направления информационной безопасности: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/napravleniya-informatsionnoj-bezopasnosti/