 **Санкт-Петербургское государственное бюджетное**

**профессиональное образовательное учреждение**

**«Радиотехнический колледж»**

**ОТЧЕТ**

**по практической работе № 14**

**на тему**: **«Разработка требований безопасности информационной системы»**

**по дисциплине МДК.05.01 наименование:**

**Проектирование и дизайн информационных систем.**

**специальность 09.02.07 наименование:**

**Информационные системы и программирование.**

Выполнил: студент группы

№ ИВ1-2-22

Сметанин Максим Дмитриевич

Проверил: преподаватель

Юрченко А.М.

Санкт-Петербург

Вариант 20

**Задание 1: Основные цели и задачи защиты информации**

**Цели:**

1. **Конфиденциальность:** Гарантировать, что информация доступна только тем, кто имеет к ней право.
2. **Целостность:** Обеспечить, чтобы информация не подвергалась несанкционированным изменениям.
3. **Доступность:** Гарантировать доступ к информации для тех, кто имеет на это право, в любое удобное время.
4. **Аутентификация:** Удостоверить личность пользователей и устройств для предотвращения несанкционированного доступа.
5. **Невозможность отказа:** Предотвратить возможность отказа от признания своих действий в системе.

Задачи

1. **Разработка политики безопасности:** Установление правил и стандартов для защиты информации.
2. **Использование шифрования:** Защита данных от несанкционированного доступа путем применения криптографических методов.
3. **Управление доступом:** Контроль доступа к ресурсам и информации на основе принципа наименьших привилегий.
4. **Обучение сотрудников:** Повышение осведомленности персонала по вопросам безопасности и защиты от социальной инженерии.
5. **Мониторинг и аудит безопасности:** Слежение за событиями в системе для выявления аномалий и несанкционированных действий.

**Задание 2: Факторы, влияющие на организацию системы защиты информации**

1. **Типы данных:** Чувствительность данных определяет уровень защиты, необходимый для их безопасного хранения и передачи.
2. **Типы угроз:** Различные виды угроз требуют разных методов защиты. Например, защита от вирусов отличается от защиты от кибератак.
3. **Пользователи и персонал:** Уровень обученности и осведомленности пользователей существенно влияет на успешность системы защиты.
4. **Технологии:** Используемые технологии (программное и аппаратное обеспечение) имеют свои собственные уровни уязвимости и требований к защите.
5. **Физическая безопасность:** Защита от несанкционированного доступа к физическим ресурсам (серверам, оборудованию).
6. **Законодательство и нормативы:** Соблюдение законодательства и стандартов в области безопасности информации.
7. **Бюджет и ресурсы:** Доступные финансовые и человеческие ресурсы определяют возможности в области информационной безопасности.

**Задание 3: Дестабилизирующие воздействия и их нейтрализация**

**Дестабилизирующие воздействия:**

1. **Кибератаки:** Атаки на информационные системы с целью получения несанкционированного доступа, уничтожения данных или нарушения их целостности.
2. **Мальвара и вредоносные программы:** Вирусы, троянские программы и другие виды вредоносных приложений, нарушающих работу системы.
3. **Социальная инженерия:** Обман пользователей для получения конфиденциальной информации.
4. **Недостатки в программном обеспечении:** Уязвимости в коде программ могут быть использованы для несанкционированного доступа.

**Способы нейтрализации:**

1. **Использование антивирусного программного обеспечения:** Для обнаружения и удаления вредоносных программ.
2. **Обучение пользователей:** Повышение осведомленности о методах социальной инженерии и безопасных практиках.
3. **Регулярные аудиты и тестирование на проникновение:** Выявление уязвимостей в системе и их устранение.
4. **Обновление программного обеспечения:** Регулярное внесение изменений для устранения известных уязвимостей.

**Задание 4: Требования безопасности для "Информационные системы управления. Системы, ускоряющие потоки товаров"**

1. **Контроль доступа:** Реализация строгого контроля доступа к данным, обеспечивающего отображение информации только авторизованным пользователям.
2. **Шифрование данных:** Использование современных алгоритмов шифрования для защиты конфиденциальности данных при передаче и хранении.
3. **Резервное копирование и восстановление:** Регулярное создание резервных копий данных и обеспечение возможности быстрого восстановления системы после сбоев или атак.
4. **Мониторинг и аудит безопасности:** Системы логирования и мониторинга для выявления необычной активности и проведения аудита безопасности.
5. **Физическая безопасность:** Защита физического оборудования от несанкционированного доступа.

**Задание 5: Методы и средства защиты информации**

1. **Файерволы и интранет-шлюзы:** Контроль и фильтрация сетевого трафика для предотвращения несанкционированного доступа.
2. **Антивирусное программное обеспечение:** Защита от вредоносных программ и вирусов.
3. **Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS):** Раннее обнаружение и предотвращение попыток вторжения.
4. **Шифрование:** Защита конфиденциальных данных в пути и в покое.
5. **Многоуровневая аутентификация:** Усиление контроля доступа с использованием нескольких методов аутентификации.
6. **Обновление и патчи:** Регулярное обновление программного обеспечения и применение патчей для закрытия уязвимостей.
7. **Обучение пользователей:** Проведение регулярных тренингов по безопасности для сотрудников.