МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__8__»__08__ 2023 г.

Организация работ по обеспечению безопасности в информационных системах

Методические указания по выполнению практических работ по дисциплине «Организация работ по обеспечению безопасности в информационных системах» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Организация работ по обеспечению безопасности в информационных системах: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 41 с.: Библиогр.: с. 40.

Содержат сведения по вопросам изучения технологий, методов и средств организации работ по обеспечению безопасности в информационных системах для успешной профессиональной деятельности, а также развития в процессе обучения системного мышления, необходимого для решения задач управления в области информационной безопасности.

Методические указания по выполнению практических работ по дисциплине «Организация работ по обеспечению безопасности в информационных системах» предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60х84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

Введение

Организация работ по обеспечению безопасности в информационных системах является критическим аспектом для любого предприятия или организации. Для эффективного обеспечения безопасности информационных систем необходимо учитывать ряд ключевых подразделов, таких как система анализа рисков и проверки политики информационной безопасности, моделирование объектов защиты, организационная культура и управление конфликтами, работа с нормативно-правовыми документами, разработка организационных и технических мер по технической защите информации, а также разработка модели угроз информационной безопасности.

1. Система анализа рисков и проверки политики информационной безопасности предприятия:

Система анализа рисков позволяет определить потенциальные угрозы и уязвимости информационных систем организации. Анализ рисков помогает выявить возможные последствия нарушений безопасности и определить вероятность их возникновения. После анализа рисков проводится проверка политики информационной безопасности предприятия, чтобы убедиться в ее соответствии требованиям безопасности и эффективности.

2. Моделирование объектов защиты:

Моделирование объектов защиты представляет собой процесс создания моделей информационных систем с целью анализа и определения мер по обеспечению их безопасности. Моделирование помогает идентифицировать уязвимости, провести анализ возможных угроз и разработать соответствующие меры по защите информации.

3. Организационная культура и управление конфликтами:

Организационная культура играет важную роль в обеспечении безопасности информационных систем. Культура безопасности должна быть прочно внедрена во все уровни организации и быть поддерживаемой руководством. Управление конфликтами также является важным аспектом, поскольку конфликты внутри организации могут негативно повлиять на безопасность информационных систем.

4. Работа с нормативно-правовыми документами:

Работа с нормативно-правовыми документами включает в себя изучение и применение действующих законов, стандартов и регуляторных требований в области информационной безопасности. Правильное понимание нормативного регулирования позволяет организации соответствовать требованиям безопасности и защитить свою информацию от возможных угроз.

5. Разработка организационных и технических мер по технической защите информации:

Разработка организационных и технических мер по технической защите

информации включает в себя создание политик, процедур, инструкций и технических решений, направленных на обеспечение безопасности информационных систем. Эти меры могут включать контроль доступа, шифрование данных, мониторинг сетевой активности и другие техники защиты информации.

6. Разработка модели угроз информационной безопасности:

Разработка модели угроз информационной безопасности представляет собой процесс идентификации потенциальных угроз, которые могут нанести вред информационным системам организации. Модель угроз позволяет определить вероятность возникновения и воздействия угроз на систему, а также разработать соответствующие меры по защите информации.

В целом, эти подразделы являются ключевыми элементами организации работ по обеспечению безопасности в информационных системах предприятия. Учет всех этих аспектов позволяет создать надежную систему защиты информации и свести к минимуму возможные риски и угрозы.

Работа №1.

Тема: Система анализа рисков и проверки политики информационной безопасности предприятия.

Цель и содержание

Целью занятий является теоретическая и практическая подготовка студентов в области изучения задач по разработке системы анализа рисков и проверки политики информационной безопасности предприятия.

Основные этапы работ при выполнении задания по разработке системы анализа рисков и проверки политики информационной безопасности предприятия:

1. Понимание требований: В первую очередь, вам необходимо установить четкое понимание требований заказчика. Встретитесь с представителями предприятия, чтобы обсудить их потребности и ожидания от системы анализа рисков и проверки политики информационной безопасности. Уточните основные цели, ограничения, бизнес-процессы и возможные угрозы.
2. Идентификация активов: Определите все информационные активы, которые необходимо защитить. Это может включать данные клиентов, финансовую информацию, интеллектуальную собственность, программное обеспечение и техническое оборудование.
3. Идентификация угроз: Определите потенциальные угрозы для информационной безопасности предприятия. Это могут быть внешние угрозы, такие как хакеры или кибератаки, а также внутренние угрозы, такие как небрежность сотрудников или несанкционированный доступ к данным.
4. Оценка уязвимостей: Проанализируйте систему и процессы предприятия, чтобы выявить возможные уязвимости. Это могут быть слабые места в сетевой инфраструктуре, устаревшее программное обеспечение или отсутствие политик безопасности.
5. Оценка рисков: Оцените вероятность возникновения угроз и потенциальный ущерб, который они могут причинить предприятию. Разработайте матрицу рисков, чтобы классифицировать угрозы по их серьезности и приоритетности для дальнейших действий.
6. Разработка политики безопасности: Создайте политику информационной безопасности, которая будет определять правила и рекомендации по защите активов предприятия. Убедитесь, что политика ясна, понятна и соответствует требованиям заказчика.
7. Разработка мер безопасности: На основе выявленных уязвимостей и рисков разработайте конкретные меры безопасности, которые помогут снизить риски и улучшить безопасность предприятия. Это может включать установку

брандмауэров, шифрование данных, контроль доступа и обучение сотрудников.

8. Реализация системы анализа рисков: Создайте систему, которая будет использоваться для непрерывного мониторинга и анализа рисков информационной безопасности. Это может быть программное обеспечение, специально разработанное для этих целей, или интегрированная система, использующая существующие инструменты.

9. Тестирование и проверка: Перед внедрением системы проведите тестирование ее функциональности и эффективности. Убедитесь, что система работает должным образом и способна выявлять и предотвращать угрозы безопасности.

10. Внедрение и обучение: Опишите этапы внедрения системы анализа рисков и проверки политики информационной безопасности на предприятии. Опишите план обучения сотрудников работе с новой системой.

11. Мониторинг и обновление: Разработайте план мониторинга системы на первый год после ее внедрения.

Этапы выполнения работы и ожидаемые результаты.

1. Понимание требований:

Проведите встречу с представителями предприятия ООО ЦСБ "ЩИТ-ИНФОРМ" для обсуждения их потребностей и ожиданий от системы анализа рисков и проверки политики информационной безопасности и сведений о предприятии, для которого ООО ЦСБ "ЩИТ-ИНФОРМ" будет разрабатывать данную систему. Уточните основные цели, ограничения, бизнес-процессы и возможные угрозы.

Результат: Четкое понимание требований заказчика.

Пример: Заказчик является крупной финансовой организацией и хочет разработать систему, которая поможет им идентифицировать и управлять рисками в области информационной безопасности, основываясь на их политике безопасности.

2. Идентификация активов:

Определите все информационные активы, которые необходимо защитить, например, данные клиентов, финансовую информацию, интеллектуальную собственность, программное обеспечение и техническое оборудование.

Результат: Список и описание всех идентифицированных информационных активов.

Пример: Информационные активы включают данные клиентов, финансовые отчеты, торговые секреты, интеллектуальную собственность и сервисы,

предоставляемые предприятием.

3. Идентификация угроз:

Определите потенциальные угрозы информационной безопасности предприятия, как внешние (например, хакеры, кибератаки) так и внутренние (например, небрежность сотрудников, несанкционированный доступ).

Результат: Список и описание всех идентифицированных угроз безопасности.

Пример: Угрозы могут быть кибератаки, физические доступы к серверам, утечка конфиденциальных данных сотрудниками или вредоносное программное обеспечение.

4. Оценка уязвимостей:

Проанализируйте систему и процессы предприятия для выявления возможных уязвимостей, таких как слабые места в сетевой инфраструктуре, устаревшее программное обеспечение или отсутствие политик безопасности.

Результат: Список и описание всех выявленных уязвимостей.

Пример: Уязвимости могут включать отсутствие обновлений программного обеспечения, слабые пароли, открытые порты на сетевых устройствах или отсутствие физической безопасности для серверных комнат.

5. Оценка рисков:

Оцените вероятность возникновения угроз и потенциальный ущерб, который они могут причинить предприятию.

Разработайте матрицу рисков для классификации угроз по серьезности и приоритетности.

Результат: Матрица рисков, определяющая приоритеты для дальнейших действий.

Пример: Например, оценка рисков может показать, что кибератаки имеют высокую вероятность и могут привести к значительным финансовым потерям и ущербу репутации.

6. Разработка политики безопасности:

Создайте политику информационной безопасности, которая будет содержать правила и рекомендации по защите активов предприятия. Убедитесь, что политика ясна, понятна и соответствует требованиям заказчика.

Результат: Разработанная и утвержденная политика информационной безопасности.

Пример: Политика может включать требования к использованию сильных паролей, доступа только для авторизованных сотрудников, регулярное обновление программного обеспечения и шифрование конфиденциальных данных.

7. Разработка мер безопасности:

Разработайте конкретные меры безопасности для устранения или снижения выявленных уязвимостей и рисков. Это может включать установку брандмауэров, шифрование данных, контроль доступа и обучение сотрудников.

Результат: Список и описание разработанных мер безопасности.

Пример: Меры безопасности могут включать установку брандмауэров, использование системы обнаружения вторжений, резервное копирование данных, проведение регулярных аудитов безопасности и обучение сотрудников по основам информационной безопасности.

8. Реализация системы анализа рисков:

Создайте систему для непрерывного мониторинга и анализа рисков информационной безопасности.

Это может быть специальное программное обеспечение или интегрированная система, использующая существующие инструменты.

Результат: Реализованная система анализа рисков.

Пример: Система может включать использование специализированного программного обеспечения для сканирования уязвимостей, мониторинга событий безопасности и генерации отчетов о рисках.

9. Тестирование и проверка:

Проведите тестирование функциональности и эффективности системы перед ее внедрением.

Убедитесь, что система работает должным образом и способна выявлять и предотвращать угрозы безопасности.

Результат: Подтверждение работоспособности системы на основе результатов тестирования.

Пример: Проведите пенетрационное тестирование сети, чтобы проверить наличие уязвимостей и эффективность мер безопасности.

10. Внедрение и обучение:

После успешного тестирования опишите этапы внедрения системы анализа рисков и проверки политики информационной безопасности на предприятии.

Опишите план обучения сотрудников работе с новой системой.

Результат: Презентация, содержащая описание этапов внедрения, план обучения сотрудников.

Пример: Проведите обучающую сессию на практическом занятии, где объясните новую систему, ее цели и важность соблюдения политики безопасности.

11. Мониторинг и обновление:

Разработайте план мониторинга системы на первый год после ее внедрения.

Результат: План мониторинга системы на первый год после ее внедрения.

Пример плана мониторинга системы на первый год после ее внедрения:

Месяц 1:

- Установить основные метрики и показатели производительности, которые будут измеряться и отслеживаться.
- Назначить ответственных лиц за мониторинг каждого показателя.
- Настроить систему автоматического сбора данных и регулярные отчеты.

Месяцы 2-3:

- Отслеживать и анализировать ключевые метрики производительности, такие как время отклика системы, загрузка серверов и количество ошибок.
- Провести первую оценку эффективности системы по сравнению с предыдущей системой или целевыми показателями.
- Провести пользовательский опрос или интервью для получения обратной связи от пользователей системы.

Месяцы 4-6:

- Продолжить мониторинг ключевых метрик и провести сравнительный анализ с начальными данными.
- Выявить любые проблемы или узкие места в системе и разработать план действий для их устранения.
- Провести аудит безопасности системы и реализовать необходимые корректирующие меры.

Месяцы 7-9:

- Провести серию нагрузочных тестов для проверки производительности системы при пиковых нагрузках.
- Проанализировать результаты тестов и определить, требуется ли масштабирование системы или оптимизация ресурсов.
- Предоставить финальные отчеты о производительности системы за первый год внедрения.

Месяцы 10-12:

- Продолжить мониторинг системы и сравнивать текущие показатели с

начальными данными.

- Оценить удовлетворенность пользователей системы через опросы или обратную связь.
- Подготовить детальный отчет о производительности системы за первый год и предложить рекомендации по ее улучшению в будущем.

Контрольные вопросы:

1. Какие методы и инструменты используются для анализа рисков информационной безопасности на предприятии?
2. Каков процесс оценки и классификации рисков информационной безопасности?
3. Какие шаги необходимо предпринять для определения приоритетов в управлении рисками информационной безопасности?
4. Как проводится анализ уязвимостей информационной системы предприятия?
5. Каким образом реализуется контроль изменений в политике информационной безопасности предприятия?
6. Каким образом осуществляется мониторинг и обновление политики информационной безопасности предприятия?
7. Какие средства используются для обнаружения и предотвращения инцидентов информационной безопасности на предприятии?
8. Каким образом осуществляется аудит информационной безопасности на предприятии?
9. Какие меры принимаются для защиты конфиденциальных данных и персональной информации сотрудников на предприятии?
10. Как происходит обучение сотрудников предприятия в области информационной безопасности?
11. Какие критерии и метрики используются для оценки эффективности политики информационной безопасности на предприятии?
12. Какие меры принимаются для обеспечения бизнес-продолжительности при возникновении инцидентов информационной безопасности?
13. Как осуществляется управление доступом к информационным ресурсам на предприятии?
14. Какие методы и процедуры используются для резервного копирования и восстановления данных на предприятии?
15. Какие требования и стандарты информационной безопасности соблюдаются на предприятии?

Работа №2.
Тем: Моделирование объектов защиты

Цель и содержание

Цель работы "Моделирование объектов защиты" может быть описана как разработка и анализ моделей, которые представляют системы или объекты, используемые для обеспечения безопасности.

Эта работа включает в себя создание математических или компьютерных моделей, которые отражают различные аспекты объектов защиты, такие как физическая инфраструктура, технические системы, процессы контроля доступа, мониторинг и др. Эти модели могут быть использованы для проведения анализа уязвимостей, оценки эффективности систем безопасности, прогнозирования рисков и разработки стратегий улучшения безопасности.

Цель моделирования объектов защиты заключается в том, чтобы предоставить инструменты для понимания и оптимизации системы безопасности. Моделирование позволяет исследовать различные сценарии и условия, выявлять слабые места и находить наилучшие решения для повышения уровня безопасности объекта.

Конкретные задачи, связанные с моделированием объектов защиты, могут включать:

1. Создание трехмерных моделей физической инфраструктуры для анализа уязвимостей и определения наилучшего размещения систем безопасности.
2. Разработка математических моделей, которые описывают потоки людей или транспортных средств в системе безопасности, чтобы исследовать эффективность контрольных мер и процессов.
3. Изучение поведения и взаимодействия технических систем, таких как видеонаблюдение, системы контроля доступа или датчики, с помощью компьютерного моделирования.
4. Анализ данных и симуляция различных сценариев, чтобы выявить уязвимости и разработать стратегии реагирования на аварийные ситуации.

В целом, моделирование объектов защиты направлено на создание виртуальной среды, которая позволяет анализировать и оптимизировать системы безопасности, предотвращать возникновение угроз и минимизировать возможные последствия инцидентов.

Ход работы:

1. Создание трехмерных моделей физической инфраструктуры для анализа уязвимостей и определения наилучшего размещения систем безопасности.

Сбор данных:

Первый этап заключается в сборе всех необходимых данных о физической инфраструктуре, которую вы планируете анализировать. Это может включать планы помещений, чертежи зданий, расположение существующих систем безопасности (например, камер наблюдения или датчиков), данные о сетевой инфраструктуре и другие соответствующие информационные ресурсы.

Пример: Если вы хотите проанализировать уязвимости в системе безопасности торгового центра, вы будете собирать данные о его планах этажей, местоположении существующих камер наблюдения, точках доступа Wi-Fi, периметре объекта и других сведениях, которые могут быть важными для оценки безопасности.

Ожидаемые результаты: Полный комплект данных о физической инфраструктуре, включая планы, чертежи и другие релевантные сведения.

Создание трехмерной модели:

На этом этапе используются специализированные программы для создания трехмерной модели физической инфраструктуры. Вы можете использовать программы DesignSpark Mechanical (бесплатную обучающую версию можно получить по ссылке https://www.rs-online.com/designspark/mechanical-software) или SketchUP (бесплатную обучающую версию можно получить по ссылке https://www.sketchup.com/try-sketchup), которые позволяют создавать детальные трехмерные модели зданий, помещений, систем безопасности и других компонентов инфраструктуры.

Пример создания трехмерной модели физической инфраструктуры в программе SketchUp:

1. Запустите программу SketchUp и создайте новый проект.
2. Выберите инструмент "Прямоугольник" на панели инструментов или используйте сочетание клавиш "R". Нарисуйте прямоугольник, представляющий основание здания или структуры.

3. Используйте инструмент "Толщина" (Push/Pull), выбрав его на панели инструментов или нажав клавишу "P". Вытяните прямоугольник вверх или вниз, чтобы создать объем здания.

4. Продолжайте добавлять дополнительные элементы, такие как окна, двери и другие детали, используя инструменты "Прямоугольник", "Окружность" и т.д.

5. Для создания более сложных форм и деталей можно использовать инструменты "Смещение" (Offset), "Масштабирование" (Scale), "Перемещение" (Move) и т.д.

6. Чтобы придать модели реалистичный вид, вы можете добавить текстуры и материалы. Используйте инструмент "Заливка" (Paint Bucket) для изменения цвета поверхностей или применения текстур из библиотеки материалов SketchUp.

7. Для создания окружающей инфраструктуры, такой как дороги, парковки или зеленые насаждения, можно использовать инструмент "Линия" (Line) и инструмент "Возвышение" (Extrude).

8. Если вы хотите добавить дополнительные детали и объекты, такие как автомобили, люди или другие элементы, вы можете воспользоваться 3D-моделями из онлайн-библиотек или создать их самостоятельно с помощью инструментов SketchUp.

Ожидаемые результаты: Трехмерная модель физической инфраструктуры, включающая все соответствующие элементы, такие как стены, полы, потолки, системы безопасности, электрические точки доступа и прочее.

Анализ уязвимостей:

Следующий этап заключается в проведении анализа уязвимостей на основе созданной трехмерной модели. Здесь вы исследуете потенциальные слабые места и недостатки в системах безопасности и инфраструктуре в целом. Это может включать оценку физической защищенности, выявление слабых мест в системах контроля доступа или обнаружение уязвимостей в сетевой инфраструктуре.

Пример: Вы можете провести анализ уязвимостей, чтобы определить, какие области здания наиболее подвержены несанкционированному доступу, например, площадки парковки или задние выходы, и предложить соответствующие меры безопасности для устранения этих уязвимостей.

Ожидаемые результаты: Список выявленных уязвимостей и рекомендации по их исправлению.

Размещение систем безопасности:

На этапе размещения систем безопасности вы используете трехмерную модель для определения наилучшего расположения систем безопасности, таких как камеры наблюдения, датчики движения, автоматические ворота и прочее. Это позволяет оптимизировать охват и эффективность систем безопасности в пределах физической инфраструктуры.

Пример: Для рисования камер наблюдения, датчиков движения и автоматических ворот на плане здания с использованием программы SketchUp, следуйте этим шагам:

1. Загрузите и установите пробную 30-ти дневную версию программы SketchUp. Она доступна для загрузки на официальном сайте SketchUp или по ссылке, представленной выше.
2. Откройте программу SketchUp и создайте новый проект, выбрав опцию "Новый файл" или используя сочетание клавиш Ctrl+N.
3. Нажмите кнопку "Линия" на панели инструментов или выберите инструмент "Линия" из меню "Инструменты". Используйте этот инструмент, чтобы рисовать контуры здания на плане, включая расположение дверей, окон и других основных элементов.
4. Чтобы добавить камеры наблюдения, выберите инструмент "Компоненты" на панели инструментов или выберите его из меню "Окно". Затем щелкните правой кнопкой мыши по плоскости здания, где вы хотите разместить камеру, и выберите "Вставить компонент". В открывшемся окне найдите модель камеры наблюдения или импортируйте собственную модель. Щелкните "Вставить", чтобы добавить камеру на план здания.
5. Для добавления датчиков движения повторите шаг 4, но выберите модель датчика движения вместо камеры наблюдения.
6. Аналогично, для добавления автоматических ворот используйте инструмент "Компоненты" и вставьте модель автоматических ворот на план здания.
7. После того, как вы разместили все элементы на плане здания, вы можете использовать инструменты SketchUp для редактирования, масштабирования и перемещения элементов по необходимости.
8. Также вы можете применить текстуры и цвета к элементам для улучшения визуального представления.
9. Когда закончите работу над проектом, сохраните его, выбрав "Сохранить" или "Сохранить как" в меню "Файл".

Ожидаемые результаты: План размещения систем безопасности, указывающий оптимальные места для установки каждой системы.

2. Разработка математических моделей, которые описывают потоки людей или транспортных средств в системе безопасности, чтобы исследовать эффективность контрольных мер и процессов.

Определение целей и требований:

Цель: Оптимизация размещения контрольных точек для обеспечения эффективности системы безопасности.

Требования: Ограничения на количество доступного персонала, время, затраченное на проверку каждого человека.

Сбор данных:

Сбор информации о количестве людей, проходящих через каждую контрольную точку в определенный период времени.

Сбор данных о времени, затраченном на проверку каждого человека.

Выбор математической модели:

Модель массового обслуживания: Модель, учитывающая потоки клиентов (в данном случае людей) и процессы обслуживания (проверку).

Стохастическая модель: Модель, основанная на вероятностных расчетах и учете случайных факторов.

ПРИМЕР:

Пример формализации модели математической модели для описания потоков людей в системе безопасности с использованием Python:

```
import numpy as np
import matplotlib.pyplot as plt

# Генерация случайных данных о потоках людей
num_people = 1000
mean_arrival_rate = 10  # Среднее количество прибывающих людей в единицу времени
std_deviation = 2  # Стандартное отклонение

arrival_times = np.cumsum(np.random.exponential(scale=1/mean_arrival_rate, size=num_people))
departure_times = arrival_times + np.random.normal(loc=5, scale=2, size=num_people)

# Анализ данных

# Вычисление общего количества людей в системе
total_people = len(arrival_times)

# Вычисление среднего времени пребывания
mean_stay_time = np.mean(departure_times - arrival_times)

# Разработка математической модели

# Модель M/M/1 - модель массового обслуживания с одним каналом
arrival_rate = 1 / mean_arrival_rate
service_rate = 1 / mean_stay_time

# Оценка модели

# Проверка условия стационарности
```

```
utilization = arrival_rate / service_rate
if utilization >= 1:
    print("Условие стационарности не выполняется. Увеличьте пропускную способность системы.")
else:
    print("Условие стационарности выполняется.")

# Визуализация результатов

# График потока прибытия и ухода людей
plt.step(arrival_times, range(total_people), label='Прибытие')
plt.step(departure_times, range(total_people), label='Уход')
plt.xlabel('Время')
plt.ylabel('Количество людей')
plt.legend()
plt.show()
```

В этом примере мы генерируем случайные данные о прибытии и уходе людей в системе безопасности. Затем мы анализируем данные, разрабатываем модель M/M/1 для описания потоков людей и оцениваем модель с помощью условий стационарности. Наконец, мы визуализируем результаты на графике.

Анализ и интерпретация результатов:

Определение узких мест или проблемных зон в системе безопасности.

Предложение улучшений или оптимизации системы безопасности.

3. Изучение поведения и взаимодействия технических систем, таких как видеонаблюдение, системы контроля доступа или датчики, с помощью компьютерного моделирования.

Описание задания:

Вам необходимо создать компьютерную модель системы видеонаблюдения, которая будет включать в себя различные параметры, такие как расположение камер, угол обзора, разрешение изображения и т. д. Задача состоит в том, чтобы определить оптимальное расположение камер для максимального охвата и эффективности наблюдения. Используйте компьютерное моделирование для варьирования параметров и сравнения различных конфигураций системы.

Шаги выполнения задания:

1. Определите основные параметры модели системы видеонаблюдения, такие как количество камер, их расположение, угол обзора и разрешение.
2. Создайте компьютерную модель, используя специализированное программное обеспечение или язык программирования для моделирования.
3. Задайте различные конфигурации системы, меняя параметры, такие как расположение камер, угол обзора и разрешение.

4. Запустите моделирование и оцените эффективность каждой конфигурации, например, по количеству обнаруженных объектов или покрытию зоны наблюдения.

5. Сравните результаты различных конфигураций и определите оптимальную конфигурацию системы видеонаблюдения.

ПРИМЕР:

Для решения данной задачи с помощью Python можно использовать библиотеку для компьютерного зрения OpenCV. OpenCV предоставляет мощные инструменты для обработки изображений и анализа видео.

Вот пример того, как можно создать компьютерную модель системы видеонаблюдения с использованием Python и OpenCV:

1. Установите библиотеку OpenCV, если она еще не установлена, с помощью команды `pip install opencv-python`.

2. Импортируйте необходимые модули:

cv2 - это модуль для работы с компьютерным зрением, который предоставляет функции для обработки изображений и видео. Он содержит различные методы и алгоритмы для выполнения операций, таких как загрузка изображений, обнаружение объектов, фильтрация и преобразование изображений.

numpy (Numerical Python) - это библиотека для работы с многомерными массивами данных. В контексте OpenCV, numpy часто используется для представления изображений и выполнения математических операций над пикселями изображений.

```
pythonCopy Code

import cv2
import numpy as np
```

3. Загрузите изображение или видео, на котором вы хотите определить расположение камер:

```
pythonCopy Code

image = cv2.imread('path/to/image.jpg')
# или
video = cv2.VideoCapture('path/to/video.mp4')
```

4. Определите параметры камеры, такие как расположение, угол обзора, разрешение и другие:

```
pythonCopy Code

camera_params = {
    'location': (x, y),
    'angle_of_view': angle,
    'resolution': (width, height)
}
```

5. Создайте функцию, которая будет обрабатывать изображение или кадр видео и определять, какие области покрываются конкретной камерой:

```
pythonCopy Code

def process_frame(frame, camera_params):
    # Примените необходимую обработку кадра для определения областей покрытия камерой
    # Например, можно использовать алгоритмы компьютерного зрения, такие как сегментация, детекция объектов и т. д.

    # Верните результат обработки кадра
    return processed_frame
```

6. Примените функцию обработки кадров ко всем кадрам видео или изображению:

```
pythonCopy Code

if video.isOpened():
    while True:
        ret, frame = video.read()

        if not ret:
            break

        processed_frame = process_frame(frame, camera_params)

        cv2.imshow('Camera View', processed_frame)

        if cv2.waitKey(1) & 0xFF == ord('q'):
            break

    video.release()
else:
    processed_frame = process_frame(image, camera_params)
    cv2.imshow('Camera View', processed_frame)
    cv2.waitKey(0)

cv2.destroyAllWindows()
```

7. Вы можете использовать циклы и условные выражения для варьирования параметров камер и сравнения различных конфигураций системы.

4. Анализ данных и симуляция различных сценариев, чтобы выявить уязвимости и разработать стратегии реагирования на аварийные ситуации.

Задание:

Провести анализ данных и симуляцию различных сценариев с целью выявления уязвимостей в системе и разработки эффективных стратегий реагирования на аварийные ситуации. Задача заключается в определении потенциальных угроз, оценке их воздействия на систему, а также создании планов действий для предотвращения или минимизации возможных негативных последствий.

Шаги выполнения:

Сбор данных:

Определить необходимые данные для анализа и симуляции.

Собрать данные, связанные с функционированием системы и ее компонентами.

Включить данные, отражающие прошлые аварийные ситуации и извлечь из них уроки и паттерны.

Проектирование сценариев:

Идентифицировать различные сценарии, которые могут привести к аварийным ситуациям.

Учесть разнообразные факторы, включая технические, природные и человеческие аспекты.

Определить параметры и условия для каждого сценария.

Анализ данных:

Проанализировать собранные данные с использованием методов статистики и машинного обучения.

Выявить корреляции, тренды и аномалии, которые могут указывать на потенциальные уязвимости.

Определить критические точки и слабые места в системе.

Симуляция сценариев:

Разработать модели и симуляторы для воссоздания различных сценариев.

Используйте полученные данные для создания виртуальных сред, где можно воспроизводить аварийные ситуации.

Испытать различные стратегии реагирования на каждый сценарий и оценить их эффективность.

Разработка стратегий реагирования:

Исследовать результаты симуляций и анализа данных для выявления оптимальных стратегий реагирования на аварийные ситуации.

Разработать планы действий, которые позволят предотвратить или минимизировать негативные последствия аварий.

Учесть потенциальные ограничения и риски при разработке стратегий.

Тестирование и оценка:

Протестируйте разработанные стратегии на виртуальных симуляторах или с использованием исторических данных.

Оцените эффективность стратегий и проведите анализ результатов.

Внесите необходимые корректировки и усовершенствования в стратегии реагирования.

Подготовка отчета:

Подготовьте детальный отчет, содержащий все выполненные шаги и полученные результаты.

Опишите выявленные уязвимости, предложенные стратегии реагирования и рекомендации для повышения безопасности и эффективности системы.

Предоставьте графики, таблицы и другие визуализации для наглядного представления результатов.

ПРИМЕР:

Решение задачи "Анализ данных и симуляция различных сценариев для выявления уязвимостей и разработки стратегий реагирования на аварийные ситуации" в Python может быть выполнено следующим образом:

1. Сбор данных:

- Загрузите данные о транзакциях клиентов, системных логах и других необходимых источниках данных. Используйте библиотеку Pandas для работы с табличными данными. Можно воспользоваться публичными репозиториями данных, такими как Kaggle, UCI Machine Learning Repository или другими открытыми источниками данных, чтобы найти подходящий набор данных о транзакциях или системных логах для вашего проекта.

```
Copy Code

import pandas as pd

# Загрузка данных о транзакциях
transactions_data = pd.read_csv('transactions.csv')

# Загрузка системных логов
logs_data = pd.read_csv('system_logs.csv')
```

2. Проектирование сценариев:

- Определите сценарии, которые вы хотите проанализировать, и их параметры. Например, сценарии мошенничества, технических сбоев и кибератак.

```
Copy Code

# Пример определения сценария мошенничества
fraud_scenario = {
    'frequency': 0.05,  # Частота возникновения
    'intensity': 0.2    # Интенсивность
}
```

3. Анализ данных:

- Проанализируйте данные, используя методы статистического анализа и машинного обучения. Используйте библиотеки Pandas, NumPy и Scikit-learn.

```
Copy Code

# Пример анализа данных и обнаружения аномалий
import numpy as np
from sklearn.ensemble import IsolationForest

# Обработка и анализ данных о транзакциях
transactions_processed = preprocess_transactions(transactions_data)
anomaly_detector = IsolationForest()
anomalies = anomaly_detector.fit_predict(transactions_processed)

# Анализ системных логов
log_patterns = analyze_logs(logs_data)
```

4. Симуляция сценариев:

- Разработайте моделирование событий для каждого сценария, используя данные и параметры. Используйте библиотеку SimPy для дискретно-событийного моделирования.

```
Copy Code

# Пример симуляции сценария мошенничества
import simpy

def fraud_simulation(env):
    while True:
        if np.random.rand() < fraud_scenario['frequency']:
            perform_fraud_action()

        yield env.timeout(1 / fraud_scenario['intensity'])

env = simpy.Environment()
env.process(fraud_simulation(env))
env.run(until=100)
```

5. Разработка стратегий реагирования:

- Исследуйте результаты анализа данных и симуляций, чтобы разработать эффективные стратегии реагирования на каждый сценарий.

```
Copy Code

# Пример разработки стратегии реагирования на мошенничество
def fraud_detection(transaction):
    if is_anomaly(transaction):
        send_alert()

transactions_data.apply(fraud_detection, axis=1)
```

6. Тестирование и оценка:

- Проведите тестирование разработанных стратегий, используя виртуальные симуляторы или исторические данные. Оцените эффективность стратегий с помощью метрик.

```
Copy Code

# Пример оценки эффективности стратегий противодействия мошенничеству
true_positives = count_true_positives()
false_positives = count_false_positives()

precision = true_positives / (true_positives + false_positives)
recall = true_positives / total_fraud_cases

print('Precision:', precision)
print('Recall:', recall)
```

7. Подготовка отчета:

- Напишите детальный отчет, содержащий все выполненные шаги, методологии, результаты анализа и симуляций. Используйте библиотеки для генерации графиков и визуализации данных, такие как Matplotlib и Seaborn.

```
Copy Code

import matplotlib.pyplot as plt

# Пример визуализации результатов анализа данных
plt.plot(transactions_processed['timestamp'], transactions_processed['amount'])
plt.xlabel('Timestamp')
plt.ylabel('Amount')
plt.title('Transaction Amount over Time')
plt.show()
```

Контрольные вопросы

1. Что такое моделирование объектов защиты?

2. Какие основные цели преследует моделирование объектов защиты?
3. Какие методы используются для моделирования объектов защиты?
4. Какие типы объектов защиты могут быть подвержены моделированию?
5. Какие данные и параметры учитываются при моделировании объектов защиты?
6. Какой роль играет математическое моделирование в области защиты объектов?
7. Какие программные инструменты используются для моделирования объектов защиты?
8. Какие преимущества может предоставить моделирование объектов защиты?
9. Каковы основные вызовы, связанные с моделированием объектов защиты?
10. Какие факторы необходимо учитывать при разработке моделей объектов защиты?
11. Каким образом моделирование объектов защиты помогает в анализе уязвимостей и рисков?
12. Какие методы анализа данных могут применяться после моделирования объектов защиты?
13. Как моделирование объектов защиты влияет на процесс разработки систем безопасности?
14. Каковы основные принципы и подходы к моделированию объектов защиты?
15. Какие будущие тенденции и развитие можно ожидать в области моделирования объектов защиты?

Работа №3.

Тема: Организационная культура и управление конфликтами.

1. Цель и содержание

Цель работы "Организационная культура и управление конфликтами" заключается в изучении и понимании роли организационной культуры в управлении конфликтами внутри организации. Она направлена на разработку стратегий и методов, которые помогут создать и поддерживать здоровую организационную культуру, способствующую снижению конфликтов и повышению эффективности работы.

2. Теоретическое обоснование

Организационная культура оказывает значительное влияние на управление конфликтами внутри организации. Конфликты могут возникать из-за различий в ценностях, убеждениях, нормах и поведении людей в организации. Они могут возникать как между отдельными сотрудниками, так и между группами или отделами.

Организационная культура является совокупностью общепринятых ценностей, убеждений, норм и традиций, которые формируются со временем и влияют на поведение и отношения между сотрудниками. Культура организации определяет, какие типы поведения поощряются и одобряются, а какие являются неприемлемыми. Она создает основу для взаимодействия и коммуникации между сотрудниками и влияет на то, как они решают возникающие конфликты.

Основные аспекты организационной культуры:

1. Значение ценностей и норм: Организационная культура формирует общие ценности и нормы, которые влияют на поведение сотрудников. Если организация ставит акцент на сотрудничество, уважение и поддержку, это может способствовать решению конфликтов путем поиска компромиссов и сотрудничества.

2. Поддержка открытой коммуникации: Здоровая организационная культура поощряет открытую и эффективную коммуникацию между сотрудниками. Это создает возможность для выражения мнений и обеспечивает пространство для разрешения конфликтов через открытые диалоги и обмен идеями.

3. Развитие навыков управления конфликтами: Организация может предоставить своим сотрудникам необходимые знания и навыки управления конфликтами. Это может включать тренинги, семинары и программы развития лидерства, которые помогут сотрудникам эффективно управлять конфликтами и находить конструктивные решения.

4. Лидерство и роль моделирования: Руководители организации играют важную роль в создании и поддержании здоровой организационной культуры. Они должны демонстрировать положительные навыки управления конфликтами, быть готовыми выслушать стороны, поощрять сотрудничество и принимать конструктивные решения.

5. Создание системы поддержки: Организация может создать систему, которая обеспечивает поддержку сотрудникам в управлении конфликтами. Это может включать наличие специалистов по управлению конфликтами или механизмы для представления жалоб и разрешения споров.

Таким образом, понимание и активное использование организационной культуры в управлении конфликтами может помочь создать благоприятную рабочую среду, в которой конфликты рассматриваются как возможность для роста и улучшения, а не как проблема.

3. Ситуационная задача

Тема: Управление конфликтами

Цель: Практика навыков посредничества и разрешения конфликтов

Вы работаете в IT-компании, где возник серьезный конфликт между отделом маркетинга и отделом разработки. Отдел маркетинга отвечает за продвижение и рекламу продуктов компании, а отдел разработки занимается созданием программного обеспечения.

В последнее время отдел маркетинга столкнулся с проблемой. Они утверждают, что продукты, которые выпускает отдел разработки, содержат множество ошибок и недоработок. Клиенты жалуются на нестабильную работу программ и высокий уровень ошибок, что негативно сказывается на репутации компании и объеме продаж. Отдел маркетинга возмущен тем, что отдел разработки не выполняет свои обязательства в срок и не предоставляет качественные продукты для рекламы.

Отдел разработки утверждает, что основная причина возникновения ошибок заключается в постоянных изменениях требований со стороны отдела маркетинга. Они отмечают, что сроки разработки часто сжимаются, а требования не всегда ясно и полно описываются. Отдел разработки также жалуется на то, что отдел маркетинга не учитывает технические ограничения и неразумные требования, что

создает большое давление на команду разработчиков.

Ваша цель состоит в том, чтобы помочь обоим отделам найти компромиссное решение и восстановить работоспособность команды. Вам предстоит провести серию встреч и действий для разрешения данного конфликта.

Примеры шагов, которые можно предпринять:

1. Организация встречи с представителями обоих отделов: Пригласите руководителей и ключевых сотрудников обоих отделов на совместную встречу. Создайте атмосферу доверия и объективности, чтобы каждая сторона могла выразить свои претензии и точку зрения.
2. Анализ конкретных случаев: Попросите представителей отделов подготовить конкретные примеры, где возникли проблемы или недоразумения. Рассмотрите эти примеры и попытайтесь выявить корни проблемы, а также найти возможные решения.
3. Установление единого языка: Помогите отделам понять и описать свои требования и ограничения. При необходимости проведите обучение или семинары для персонала, чтобы улучшить понимание процессов работы друг друга.
4. Разработка процедур и коммуникационных каналов: Совместно с отделами создайте процессы и процедуры, которые помогут улучшить коммуникацию между отделами. Это может включать регулярные встречи для обсуждения текущих задач, использование специализированных программ для учета требований и изменений, а также установление ответственных лиц за координацию работы между отделами.
5. Регулярный мониторинг и оценка: После введения новых процедур и коммуникационных каналов, следите за их эффективностью и собирайте обратную связь от сотрудников обоих отделов. Проводите периодические встречи для обсуждения возникших проблем и предложения дополнительных улучшений.

Важно помнить, что разрешение конфликта может потребовать времени и терпения. Ваша роль состоит в том, чтобы быть нейтральным посредником и помочь обоим отделам найти справедливое и удовлетворительное решение.

4. Контрольные вопросы

1. Какие основные элементы организационной культуры существуют?
2. Как организационная культура влияет на эффективность работы команды?
3. Какие преимущества может предоставить разнообразие в организационной культуре?
4. Какие факторы могут способствовать возникновению конфликтов в рамках организационной культуры?
5. Какие методы управления конфликтами широко используются в организациях?
6. Какие стратегии разрешения конфликтов могут быть эффективными?
7. Какое влияние оказывает лидерская роль на организационную культуру и управление конфликтами?
8. Каковы основные принципы выстраивания конструктивного диалога в случае конфликта?
9. Как можно предупредить конфликты в рамках организационной культуры?
10. Какие типы конфликтов могут возникнуть в организации?
11. Какие негативные последствия могут возникнуть при неэффективном управлении конфликтами?
12. Какие роли и ответственности лежат на руководителях при управлении конфликтами?
13. Какие методы медиации можно использовать для разрешения конфликтов в организации?
14. Каким образом организационная культура может способствовать устойчивому разрешению конфликтов?
15. Как измерить эффективность управления конфликтами в организации?

Работа №4.

Тема: Работа с нормативно-правовыми документами

1. Цель и содержание

Цель работы с нормативно-правовыми документами в сфере информационной безопасности состоит в обеспечении защиты информации путем правильного применения и соблюдения соответствующих норм и правил. Основные задачи работы с нормативно-правовыми документами в сфере информационной безопасности включают:

- Изучение и анализ действующего законодательства и нормативных актов, регулирующих информационную безопасность. Это включает изучение международных, национальных и отраслевых стандартов, законов, постановлений, указов и других регуляторных документов.

- Интерпретация и применение норм и требований, содержащихся в нормативно-правовых документах. Работник в области информационной безопасности должен разбираться в том, какие меры необходимо предпринять для обеспечения безопасности информации, и какие требования должны быть учтены при разработке и внедрении систем и технологий.

- Разработка и внедрение политик, процедур и практик в соответствии с требованиями нормативно-правовых документов. Это включает разработку политик безопасности, стандартов, регламентов, инструкций и других документов, определяющих правила и процедуры работы с информацией.

- Обеспечение соответствия организации требованиям нормативно-правовых документов. Работник должен контролировать выполнение установленных требований и проводить аудиты для проверки соответствия системы информационной безопасности законодательству и регуляторным нормам.

- Участие в процессе разработки новых нормативно-правовых документов в области информационной безопасности. Работник может принимать активное участие в работе экспертных групп, комитетов и форумов по разработке и совершенствованию законодательства и стандартов в области информационной безопасности.

Таким образом, основная цель работы с нормативно-правовыми документами в сфере информационной безопасности заключается в обеспечении защиты конфиденциальности, целостности и доступности информации, а также защите от несанкционированного доступа, использования и распространения информации.

2. Задание

Подготовьте презентацию на тему "Работа с нормативно-правовыми документами в сфере информационной безопасности".

Презентация должна включать следующие пункты:

- Введение в тему: объясните, что такое нормативно-правовые документы в контексте информационной безопасности и почему они важны.

- Обзор основных законодательных и нормативных актов в области информационной безопасности, как на международном, так и национальном уровне.

- Описание процесса работы с нормативно-правовыми документами: как найти актуальные версии документов, как они структурированы и какие разделы и положения следует особо учитывать.

- Роль нормативно-правовых документов в обеспечении информационной безопасности: как они помогают предотвратить утечки данных, защитить системы от несанкционированного доступа и реагировать на инциденты.

- Примеры случаев, когда нормативно-правовые документы в сфере информационной безопасности играли важную роль и помогли предотвратить угрозы или минимизировать последствия инцидентов.

- Рекомендации по работе с нормативно-правовыми документами: какие процедуры и практики следует внедрить в организации для эффективного соблюдения требований информационной безопасности.

Презентация должна быть логически структурированной, содержать понятные иллюстрации и примеры, а также предоставлять релевантные источники информации для дальнейшего изучения темы.

Контрольные вопросы

1. Какие нормативно-правовые документы регулируют работу в сфере информационной безопасности?
2. Что такое ГОСТ Р и какую роль он играет в работе с нормативно-правовыми документами в сфере информационной безопасности?
3. Какие основные принципы работы с нормативно-правовыми документами в информационной безопасности следует учитывать?
4. Какие требования обычно предъявляются к оформлению нормативно-правовых документов в сфере информационной безопасности?
5. Какие действия должны быть предприняты в случае изменений в нормативно-правовой базе по информационной безопасности?
6. Какова роль Роскомнадзора в работе с нормативно-правовыми документами в сфере информационной безопасности?
7. Какие требования обычно предъявляются к защите персональных данных в нормативно-правовых документах?
8. Какие ответственности могут быть наложены на организации в случае нарушения нормативно-правовых требований по информационной безопасности?
9. Какие международные стандарты информационной безопасности существуют и как они связаны с российскими нормативно-правовыми документами?
10. Какие основные этапы проходит нормативно-правовой документ в процессе его разработки и принятия?
11. Какие специалисты должны быть вовлечены в работу с нормативно-правовыми документами по информационной безопасности?
12. Какие требования предъявляются к процедуре аутентификации и авторизации пользователей в нормативно-правовых документах?
13. Какие полномочия имеет Федеральная служба безопасности (ФСБ) в сфере информационной безопасности и как они отражены в нормативно-правовых документах?
14. Какие меры обеспечения информационной безопасности предусмотрены в нормативно-правовых документах для предотвращения утечек конфиденциальных данных?
15. Какие требования предъявляются к хранению и передаче информации в нормативно-правовых документах по информационной безопасности?

Работа №5.

Тема: Разработка организационных и технических мер по технической защите информации

1. Цель и содержание

Цель работы "Разработка организационных и технических мер по технической защите информации" заключается в создании системы и механизмов, которые обеспечат безопасность информации в организации или предприятии. Эта работа имеет несколько аспектов:

Организационные меры: Цель организационных мер состоит в разработке политик, процедур и правил, которые определяют, как должна быть обрабатываться и защищаться информация в организации. Включает в себя разработку политики доступа к информации, процедур управления паролями, обучение персонала по вопросам информационной безопасности и контроль соответствия сотрудников установленным правилам.

Технические меры: Цель технических мер заключается в применении технологий и инструментов для защиты информации от несанкционированного доступа, изменений или уничтожения. Примерами таких мер являются установка физических барьеров (например, замки и системы видеонаблюдения), использование антивирусных программ и брандмауэров для обнаружения и предотвращения вторжений, шифрование данных для защиты конфиденциальности и резервное копирование информации для обеспечения ее целостности.

Результатом работы по разработке организационных и технических мер по технической защите информации должна быть эффективная система, которая минимизирует угрозы безопасности информации и обеспечивает защиту конфиденциальности, целостности и доступности данных.

2. Задание

Разработайте план организационных и технических мер по технической защите информации для организации, включающий следующие этапы:

- Анализ угроз и рисков: Проведите анализ возможных угроз безопасности информации, которым подвергается ваша организация. Определите существующие риски и потенциальные последствия инцидентов.

- Разработка политики безопасности информации: Сформулируйте политику безопасности информации, которая будет служить основой для разработки всех последующих мер по технической защите. Укажите цели, принципы и правила, которые должны быть соблюдены всеми сотрудниками.

- Защита сети: Разработайте меры для защиты сетевой инфраструктуры организации. Включите в план использование брандмауэров, систем обнаружения вторжений (Intrusion Detection System – IDS) и систем предотвращения вторжений (Intrusion Prevention System – IPS).

- Защита данных: Определите методы шифрования данных, которые будут использоваться для защиты конфиденциальной информации. Разработайте план резервного копирования данных и обеспечения их целостности.

- Управление учетными записями: Создайте стратегию управления учетными записями, включающую разграничение прав доступа, установку сложных паролей, периодическое обновление паролей и мониторинг активности пользователей.

- Физическая безопасность: Определите организационные меры для обеспечения физической защиты серверных комнат, центров обработки данных и других важных объектов. Рассмотрите использование систем видеонаблюдения, контроля доступа и ограничения зоны доступа.

- Обучение персонала: Разработайте программу обучения и осведомленности сотрудников о правилах информационной безопасности.

- Мониторинг и аудит: Разработайте процедуры для анализа журналов событий и реагирования на инциденты.

Ваша задача состоит в том, чтобы разработать подробный план с описанием каждого этапа и соответствующими мерами по технической защите информации. Обоснуйте выбор конкретных мер и инструментов на основе анализа угроз и рисков, а также целей организации в области безопасности информации.

Контрольные вопросы

1. Какие организационные меры обеспечивают техническую защиту информации?
2. Какой роль играет политика безопасности в разработке мер по технической защите информации?

3. Какими методами можно обеспечить контроль доступа к конфиденциальной информации?

4. Какие технические меры используются для защиты информации от несанкционированного доступа?

5. Что такое аутентификация и какие методы аутентификации могут быть применены для технической защиты информации?

6. Каковы основные принципы шифрования информации и какие шифровальные алгоритмы можно использовать?

7. Какие меры могут быть предприняты для предотвращения атак по перехвату данных, например, через сетевые протоколы?

8. Какие меры обеспечивают сохранность данных при их хранении и передаче?

9. Как влияют физические меры безопасности на техническую защиту информации?

10. Какие меры предусмотрены для защиты информации от вредоносного программного обеспечения (вирусы, трояны и т.д.)?

11. Каковы основные этапы разработки системы технической защиты информации?

12. Какие меры могут быть предприняты для обеспечения надежности и целостности хранения информации?

13. Какие меры предусмотрены для защиты информации от несанкционированного копирования или распространения?

14. Какова роль мониторинга и аудита в обеспечении технической защиты информации?

15. Какие требования и стандарты следует учитывать при разработке организационных и технических мер по технической защите информации?

Работа №6.

Тема: Разработка модели угроз информационной безопасности

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

1. Составить список всех возможных угроз физической безопасности для заданного объекта. При этом использовать перечень угроз, данный в таблице 1.

Таблица 1 - Основные угрозы физической безопасности

Угроза	Тип источника угроз
1	2
Несанкционированное проникновение в КЗ	Антропогенный
Совершение диверсии в КЗ	Антропогенный
Совершение террористических актов	Антропогенный
Несанкционированные действия, приводящие к нарушению производственных технологических процессов	Антропогенный
Несанкционированный доступ к компьютерам	Антропогенный
Кража технических средств с хранящейся в них информацией	Антропогенный
Кража носителей информации	Антропогенный
Кража материальных и финансовых ценностей	Антропогенный
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств	Антропогенный
Прослушивание телефонных и радиопереговоров	Антропогенный
Внедрение «закладок»	Антропогенный
Воздействие на технические средства в целях нарушения их работоспособности	Техногенный
Воздействие на программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации	Техногенный
Воздействие на средства защиты информации	Техногенный

Продолжение таблицы 1

1	2
Побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации	Техногенный
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ	Техногенный
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств	Техногенный
Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом	Техногенный
Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	Техногенный
Угроза пожара	Стихийный
Угроза наводнения	Стихийный
Отказы и сбои в работе инженерно-технических средств охраны	Техногенный
Отказы и сбои в работе системы электроснабжения	Техногенный
Незапланированная потеря каналов связи, невозможность управления системой ОПС и видеонаблюдения на объектах с пульта централизованного наблюдения	Техногенный
выход из строя системы видеонаблюдения	Техногенный
выход из строя СКУД	Техногенный
Непреднамеренные (ошибочные, случайные, без корыстных целей) нарушения установленных требований при работе с материальными ценностями, финансовыми ресурсами, информацией, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный
Преднамеренные (в корыстных целях, по принуждению, со злым умыслом, т.п.) действия сотрудников, допущенных к материальным, финансовым и информационным ресурсам, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный

2. Вычислить все необходимые показатели угроз.

Для построения модели угроз безопасности можно применить руководящие документы ФСТЭК, разработанные для защиты персональных данных. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Частота реализации угроз безопасности определяется экспертным методом в соответствии с и на основании результатов обследования объекта.

Оценка вероятности реализации угрозы (Y2) определяется по четырем вербальным градациям:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны (5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты (10).

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_i + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 < Y < 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y < 0{,}6$, то возможность реализации угрозы средняя;
- если $0{,}6 < Y < 0{,}8$, то возможность реализации угрозы высокая;
- если $Y > 0{,}8$, то возможность реализации угрозы очень высокая.

Определение опасности угроз проводится экспертным методом с учетом результатов обследования объекта. Y1=5 для среднего уровня исходной защищенности.

Показателем опасности, имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям;

- средняя опасность - если реализация угрозы может привести к негативным последствиям;

- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям.

Определение актуальных угроз безопасности.

Актуальная угроза - угроза, которая может быть реализована и представляет опасность. Правила определения актуальности УБСКХ приведены в таблице 2.

Таблица 2 - Правила определения актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

3. Построить модель угроз по примеру таблицы 3.

Таблица 3 - Модель угроз безопасности защищаемого объекта

Угроза	Вероят-ность реализаци и угрозы	Возмож-ность реализации угрозы	Показатель опасности угрозы	Актуаль-ность угрозы
Несанкционированный доступ к компьютерам	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная
Кража технических средств с хранящейся в них информацией	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная
Кража носителей информации	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальн ая
Кража материальных и финансовых ценностей	Средняя вероят-ность (5)	0,5 (средняя)	Высокая	Актуальная

Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероят-ность (5)	0, 6 (средняя)	Высокая	Актуальная
Прослушивание телефонных и радиопереговоров	Средняя вероят-ность(5)	0,5 (средняя)	Высокая	Актуальная
Внедрение «закладок»	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная

Выписать из таблицы только актуальные угрозы безопасности.

Контрольные вопросы

1. Что такое модель угроз информационной безопасности?
2. Какие основные компоненты включает модель угроз?
3. Каким образом модель угроз помогает в обеспечении информационной безопасности?
4. Какие этапы включает процесс разработки модели угроз?
5. Какие методы и подходы используются при разработке модели угроз информационной безопасности?
6. Какие типы угроз могут быть учтены в модели угроз?
7. Какие инструменты и технологии могут быть применены для разработки модели угроз информационной безопасности?
8. Какие роли могут быть назначены при разработке модели угроз?
9. Какие факторы следует учитывать при оценке уровня риска в модели угроз?
10. Какие методы анализа используются для оценки уровня угрозы в модели угроз?
11. Какая роль уязвимостей в модели угроз информационной безопасности?
12. Какие меры предосторожности можно предпринять для снижения уровня угрозы на основе модели угроз?
13. Какие преимущества имеет использование модели угроз информационной безопасности?
14. Какие ограничения могут быть связаны с применением модели угроз?
15. Какой подход может быть использован для непрерывного обновления и совершенствования модели угроз информационной безопасности?

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ, Об информации, информационных технологиях и о защите информации
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ О персональных данных
3. «Порядок проведения классификации информационных систем персональных данных», утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №. 55/86/20
4. Приказ ФСТЭК от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
5. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 г. № 996 Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России от 15.02.2008 г.
7. Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 20.07.2013) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"
8. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
9. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996, утвержденные 13.12.2013 г. Руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
10. «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн». Статья, август 2013. Код безопасности
11. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от «18» февраля 2013 г. № 21.// Официальный сайт ФСТЭК России. URL: http://fstec.ru/component/attachments/download/562 (дата обращения: 15.09.2014).

12. «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн». Статья, август 2013. Код безопасности http://www.securitycode.ru/upload/iblock/8e9/algoritm-deystviy-operatora-pdn-po-sozdaniyu- si stemy-zashchity-ispdn.pdf

13. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

14. Аверченков, В. И. Аудит информационной безопасности : учебное пособие / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. – Воронеж : Воронежский государственный университет инженерных технологий, 2012. – 172 с. – URL: https://biblioclub.ru/index.php?page=book&id=141626 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

4. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 222 с. – URL: https://biblioclub.ru/index.php?page=book&id=458204 (дата обращения: 22.05.2023). - Режим доступа: по подписке. – Текст : электронный.

5. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.