1. Виды угроз информационной безопасности

2. Источники угроз информационной безопасности

3. Задачи обеспечения информационной безопасности в различных сферах деятельности

4. Методы обеспечения информационной безопасности Российской Федерации в различных сферах

5. Функции и структура государственной системы обеспечения информационной безопасности

6. Общая характеристика организационных методов защиты информации

7. Требования к построению систем безопасности предприятия

8. Концептуальная модель информационной безопасности

12. Виды объектов защиты

13. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии.

14. Основные направления организационной защиты информации на предприятии

15. Характеристика защитных действий

16. Разглашение защищаемой информации

17. Способы пресечения разглашения защищаемой информации

18. Противодействие несанкционированному доступу к информации

19. Государственная тайна и порядок отнесения к ней информации

20. Защита государственной тайны

21. Организация режима секретности, его особенности и содержание

22. Коммерческая тайна и порядок её определения

23. Организация работ с информацией, составляющей коммерческую тайну

24. Организационная структура службы безопасности

25. Организация внутриобъектового режима на предприятия

26. Организация охраны объектов предприятия

27. Организация и обеспечение защиты коммерческой тайны на предприятии

28. Организация инженерно-технической безопасности

29. Организация безопасности функционирования информационных систем

30. Проведение аналитико-разведывательной работы. Цели и задачи информационно-аналитической работы

31. Направления и методы аналитической работы

32. Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения

аналитических исследований

33. Защита информации при проведении совещаний и переговоров. Защита информации при работе с посетителями

34. Организация защиты информации в кадровой службе. Организация работы с документами

35. Подбор и подготовка кадров. Проверка персонала на благонадежность

36. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих

конфиденциальной информацией

37. Правовая основа системы лицензирования и сертификации в РФ

38. Лицензирование деятельности по защите информации. Сертификация средств защиты информации.

**1. Виды угроз информационной безопасности**

* **Классификация угроз:**
  1. **По природе возникновения:**
     + Природные (наводнения, пожары, землетрясения).
     + Техногенные (сбои в оборудовании, аварии на объектах).
     + Антропогенные (ошибки сотрудников, вредоносные действия).
  2. **По направлению воздействия:**
     + Утечка информации.
     + Нарушение целостности данных.
     + Блокировка доступа.
     + Неавторизованное использование ресурсов.
  3. **По источнику:**
     + Внутренние (сотрудники компании).
     + Внешние (хакеры, конкуренты).

**2. Источники угроз информационной безопасности**

* **Внутренние:**
  + Ошибки персонала.
  + Злоупотребление полномочиями.
  + Незнание или несоблюдение правил.
* **Внешние:**
  + Хакеры и киберпреступники.
  + Конкуренты.
  + Государственные структуры.
  + Природные катаклизмы.
  + Технические сбои.

**3. Задачи обеспечения информационной безопасности в различных сферах деятельности**

* **Для бизнеса:**
  + Защита коммерческой тайны.
  + Обеспечение конфиденциальности данных клиентов.
  + Сохранение конкурентных преимуществ.
* **Для государственных органов:**
  + Защита государственной тайны.
  + Обеспечение кибербезопасности.
  + Поддержание национальной безопасности.
* **Для образовательных учреждений:**
  + Защита персональных данных студентов и сотрудников.
  + Обеспечение доступа к образовательным ресурсам.

**4. Методы обеспечения информационной безопасности Российской Федерации в различных сферах**

* **Технические методы:**
  + Шифрование данных.
  + Использование межсетевых экранов (фаерволов).
  + Установка систем обнаружения вторжений.
* **Организационные методы:**
  + Создание политики информационной безопасности.
  + Проведение регулярных обучений сотрудников.
  + Разработка процедур управления доступом.
* **Правовые методы:**
  + Законодательное регулирование (например, законы о персональных данных).
  + Лицензирование и сертификация средств защиты.
* **Программные методы:**
  + Антивирусное программное обеспечение.
  + Средства для защиты от DDoS-атак.
* **Физические методы:**
  + Охрана объектов.
  + Контроль доступа в помещения.
  + Видеонаблюдение.

**5. Функции и структура государственной системы обеспечения информационной безопасности**

* **Функции:**
  + Контроль за соблюдением законодательства в области информационной безопасности.
  + Обеспечение защиты критической информационной инфраструктуры.
  + Предотвращение утечек государственной тайны.
  + Противодействие киберугрозам.
* **Структура:**
  + Федеральные органы власти (например, ФСБ, ФСТЭК, Минцифры).
  + Специализированные подразделения (Центры мониторинга и реагирования на компьютерные инциденты).
  + Органы по сертификации и лицензированию.

**6. Общая характеристика организационных методов защиты информации**

* **Составляющие:**
  + Разработка политики информационной безопасности.
  + Установление режима доступа к ресурсам.
  + Проведение аудитов безопасности.
  + Регулярное обучение и инструктаж сотрудников.
  + Контроль работы с конфиденциальной информацией.
* **Цель:**
  + Создание системы мер, направленных на предотвращение угроз утечки, модификации или уничтожения информации.

**7. Требования к построению систем безопасности предприятия**

* **Обеспечение конфиденциальности, целостности и доступности информации.**
* **Комплексный подход:**
  + Внедрение технических, организационных и правовых мер.
  + Учет возможных внутренних и внешних угроз.
* **Соответствие нормативным актам (ГОСТ, ISO/IEC 27001).**
* **Постоянный мониторинг и анализ рисков.**

**8. Концептуальная модель информационной безопасности**

* **Основные компоненты:**
  + **Активы:** информация, технологии, персонал.
  + **Угрозы:** потенциальные источники вреда.
  + **Уязвимости:** слабости в системе.
  + **Контрмеры:** защитные действия (технические, организационные, правовые).
* **Цели:**
  + Минимизация рисков.
  + Повышение устойчивости системы.
  + Поддержание доверия к системе.

**12. Виды объектов защиты**

* **Физические:**
  + Помещения, серверы, оборудование.
* **Цифровые:**
  + Программное обеспечение, базы данных.
* **Информационные:**
  + Документы, данные, интеллектуальная собственность.
* **Человеческие:**
  + Сотрудники, их знания и навыки.

**13. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии**

**Классификация угроз:**

1. **По типу воздействия:**
   * Утечка информации.
   * Нарушение целостности данных.
   * Блокировка доступа.
   * Неправомерное использование ресурсов.
2. **По источнику:**
   * Внутренние (действия сотрудников).
   * Внешние (хакеры, конкуренты).
3. **По способу реализации:**
   * Технические (вредоносное ПО, сбои оборудования).
   * Социальные (фишинг, социальная инженерия).
   * Физические (уничтожение носителей).
4. **По степени целенаправленности:**
   * Случайные (ошибки, аварии).
   * Преднамеренные (вредоносные действия).

**Каналы утечки информации:**

1. **Технические:**
   * Электромагнитные излучения (побочные сигналы).
   * Сетевые коммуникации (перехват данных в сети).
   * Неавторизованный доступ к носителям.
2. **Организационные:**
   * Неразграниченные права доступа.
   * Отсутствие контроля за действиями сотрудников.
3. **Физические:**
   * Кража документов, оборудования.
   * Прослушивание переговоров.
4. **Социальные:**
   * Манипуляции с сотрудниками (фишинг, обман).

**14. Основные направления организационной защиты информации на предприятии**

1. **Разработка политики безопасности:**
   * Установление правил и стандартов работы с данными.
   * Определение ответственности сотрудников.
2. **Контроль доступа:**
   * Регламентация доступа к информации.
   * Аутентификация и авторизация пользователей.
3. **Проведение обучения:**
   * Инструктаж по правилам работы с данными.
   * Повышение осведомленности о киберугрозах.
4. **Регулярные проверки и аудиты:**
   * Тестирование уязвимостей.
   * Анализ инцидентов безопасности.
5. **Установление внутриобъектового режима:**
   * Контроль доступа в помещения.
   * Организация охраны.

**15. Характеристика защитных действий**

1. **Превентивные действия:**
   * Внедрение систем мониторинга.
   * Установление ограничений доступа.
   * Обучение сотрудников.
2. **Реактивные действия:**
   * Реагирование на инциденты (локализация, устранение последствий).
   * Проведение расследований.
3. **Технические меры:**
   * Установка межсетевых экранов, антивирусов.
   * Шифрование данных.
4. **Организационные меры:**
   * Регламентация документооборота.
   * Разработка инструкций.

**16. Разглашение защищаемой информации**

* **Причины:**
  + Неправомерные действия сотрудников (небрежность, предательство).
  + Недостаточные меры защиты (технические или организационные).
  + Успешные атаки со стороны злоумышленников.
* **Последствия:**
  + Финансовые потери.
  + Утрата конкурентных преимуществ.
  + Уголовная ответственность.

**17. Способы пресечения разглашения защищаемой информации**

1. **Технические:**
   * Установка систем обнаружения утечек (DLP).
   * Шифрование и ограничение копирования данных.
2. **Организационные:**
   * Контроль за работой сотрудников.
   * Проведение проверок и аудитов.
3. **Юридические:**
   * Введение соглашений о неразглашении (NDA).
   * Привлечение к ответственности за разглашение.
4. **Обучение персонала:**
   * Проведение тренингов.
   * Создание культуры осведомленности о безопасности.

**18. Противодействие несанкционированному доступу к информации**

**Основные меры:**

1. **Технические:**
   * Использование сложных паролей.
   * Внедрение двухфакторной аутентификации.
   * Установка межсетевых экранов и систем мониторинга.
2. **Организационные:**
   * Разграничение прав доступа к информации.
   * Контроль действий пользователей.
   * Введение политики безопасности.
3. **Программные:**
   * Антивирусное ПО и системы обнаружения вторжений.
   * Шифрование данных.
4. **Физические:**
   * Контроль доступа в помещения.
   * Использование сейфов, замков и видеонаблюдения.
5. **Юридические:**
   * Применение соглашений о конфиденциальности.
   * Закрепление ответственности за несанкционированный доступ.

**19. Государственная тайна и порядок отнесения к ней информации**

**Государственная тайна:**

* Это сведения, охраняемые государством и связанные с:
  + Военной, экономической или внешнеполитической деятельностью.
  + Разработкой, производством и использованием вооружений.
  + Обеспечением безопасности государства.

**Порядок отнесения:**

1. **Определение степени секретности:**
   * Совершенно секретно.
   * Секретно.
   * Для служебного пользования.
2. **Нормативное регулирование:**
   * Закон "О государственной тайне" (№5485-1).
3. **Утверждение списка сведений:**
   * Составляется органами власти.

**20. Защита государственной тайны**

1. **Технические меры:**
   * Шифрование данных.
   * Установка специальных систем защиты.
2. **Организационные меры:**
   * Ограничение круга лиц, допущенных к информации.
   * Проведение инструктажей и проверок.
3. **Юридические меры:**
   * Привлечение к ответственности за разглашение.
   * Введение санкций за нарушение режима секретности.

**21. Организация режима секретности, его особенности и содержание**

1. **Особенности:**
   * Включает меры по предотвращению утечек.
   * Требует строгого контроля действий сотрудников.
2. **Содержание:**
   * Разработка внутренней документации.
   * Установление порядка доступа к секретным сведениям.
   * Организация охраны объектов.
   * Введение систем учёта носителей информации.

**22. Коммерческая тайна и порядок её определения**

**Коммерческая тайна:**

* Это конфиденциальные сведения, связанные с хозяйственной деятельностью организации.

**Порядок определения:**

1. **Формирование перечня сведений, составляющих тайну.**
2. **Разработка политики защиты коммерческой тайны.**
3. **Юридическое закрепление:**
   * Заключение договоров с сотрудниками.
   * Уведомление персонала о тайне.

**23. Организация работ с информацией, составляющей коммерческую тайну**

1. **Разграничение доступа:**
   * Назначение ответственных лиц.
   * Установление уровня доступа.
2. **Обучение персонала:**
   * Проведение инструктажей и тренингов.
3. **Технические меры:**
   * Шифрование данных.
   * Установка систем мониторинга.
4. **Контроль за соблюдением правил:**
   * Проведение проверок и аудитов.

**24. Организационная структура службы безопасности**

1. **Основные подразделения:**
   * Аналитическое отделение.
   * Инженерно-технический отдел.
   * Отдел охраны объектов.
   * Отдел кадровой безопасности.
2. **Функции:**
   * Обеспечение безопасности данных.
   * Организация охраны объектов.
   * Проверка сотрудников на благонадёжность.
   * Реагирование на инциденты.

**25. Организация внутриобъектового режима на предприятии**

1. **Меры контроля:**
   * Регистрация посетителей.
   * Ограничение доступа в определённые зоны.
2. **Обеспечение безопасности:**
   * Использование пропускной системы.
   * Установка видеонаблюдения.
3. **Инструктаж персонала:**
   * Ознакомление с правилами режима.
   * Проверка соблюдения инструкций.

**26. Организация охраны объектов предприятия**

1. **Физическая охрана:**
   * Посты охраны на ключевых точках.
   * Организация патрулирования территории.
   * Установка системы видеонаблюдения.
2. **Технические меры:**
   * Сигнализация.
   * Контроль доступа с помощью электронных систем.
   * Использование датчиков движения.
3. **Организационные меры:**
   * Разработка плана охраны.
   * Обучение сотрудников службы безопасности.
   * Проведение регулярных проверок безопасности.
4. **Правовые аспекты:**
   * Договор с лицензированной охранной организацией.
   * Регламентация обязанностей службы охраны.

**27. Организация и обеспечение защиты коммерческой тайны на предприятии**

1. **Создание политики защиты:**
   * Определение перечня коммерческой тайны.
   * Закрепление правил работы с конфиденциальной информацией.
2. **Технические меры:**
   * Ограничение доступа к данным.
   * Использование шифрования и защиты от копирования.
3. **Организационные меры:**
   * Введение системы уровней доступа.
   * Регистрация носителей информации.
   * Назначение ответственных лиц.
4. **Юридическое обеспечение:**
   * Заключение соглашений о неразглашении (NDA).
   * Контроль выполнения договорных обязательств.

**28. Организация инженерно-технической безопасности**

1. **Системы контроля и управления доступом (СКУД):**
   * Автоматические турникеты.
   * Электронные пропускные системы.
2. **Видеонаблюдение:**
   * Камеры с широким охватом.
   * Архивирование записей для анализа.
3. **Сигнализация:**
   * Противопожарные системы.
   * Датчики вторжения.
4. **Инженерные барьеры:**
   * Укреплённые двери, заборы.
   * Установка замков с повышенной защитой.

**29. Организация безопасности функционирования информационных систем**

1. **Аудит безопасности:**
   * Оценка уязвимостей.
   * Анализ рисков.
2. **Технические меры:**
   * Антивирусное ПО.
   * Системы обнаружения и предотвращения вторжений.
3. **Политики безопасности:**
   * Разграничение доступа.
   * Введение ограничений на использование личных устройств.
4. **Резервирование данных:**
   * Создание резервных копий.
   * Использование облачных хранилищ.
5. **Мониторинг:**
   * Постоянное отслеживание работы системы.
   * Уведомления о подозрительных действиях.

**30. Проведение аналитико-разведывательной работы. Цели и задачи информационно-аналитической работы**

1. **Цели:**
   * Выявление потенциальных угроз.
   * Оценка конкурентной среды.
   * Обеспечение безопасности решений.
2. **Задачи:**
   * Сбор и анализ данных.
   * Прогнозирование рисков.
   * Выработка рекомендаций по защите информации.

**31. Направления и методы аналитической работы**

1. **Направления:**
   * Конкурентная разведка.
   * Мониторинг угроз.
   * Анализ внутренней безопасности.
2. **Методы:**
   * Сбор открытой информации (OSINT).
   * Интервьюирование и опросы.
   * Анализ статистических данных.
   * Использование специализированного программного обеспечения.

**32. Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения аналитических исследований**

1. **Этапы:**
   * Постановка цели.
   * Сбор информации.
   * Анализ данных.
   * Выводы и рекомендации.
2. **Методы:**
   * SWOT-анализ.
   * Метод сценариев.
   * Экспертные оценки.
   * Моделирование ситуаций.

**33. Защита информации при проведении совещаний и переговоров. Защита информации при работе с посетителями**

1. **Меры на совещаниях:**
   * Запрет на использование личных устройств.
   * Проведение совещаний в защищённых помещениях.
   * Шифрование записи переговоров.
2. **Меры при работе с посетителями:**
   * Проверка личности посетителя.
   * Сопровождение внутри объекта.
   * Ограничение доступа к важным зонам.

**34. Организация защиты информации в кадровой службе. Организация работы с документами**

1. **Кадровая служба:**
   * Защита персональных данных сотрудников.
   * Ограничение доступа к кадровым документам.
   * Ведение электронных реестров с контролем доступа.
2. **Работа с документами:**
   * Хранение в защищённых архивах.
   * Регламентация уничтожения устаревших документов.
   * Использование электронных систем документооборота.

**35. Подбор и подготовка кадров. Проверка персонала на благонадёжность**

1. **Подбор:**
   * Проведение собеседований.
   * Проверка резюме и рекомендаций.
   * Оценка психологической устойчивости.
2. **Проверка на благонадёжность:**
   * Запросы в правоохранительные органы.
   * Анализ социальных сетей.
   * Тестирование на знание политики безопасности.

**36. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией**

1. **Контракты и соглашения:**
   * Введение пунктов о неразглашении информации.
   * Регистрация согласий на обработку данных.
2. **Увольнение сотрудников:**
   * Аннулирование прав доступа.
   * Изъятие устройств и ключей.
   * Проведение финального инструктажа.

**37. Правовая основа системы лицензирования и сертификации в РФ**

1. **Основные законы:**
   * Закон «О лицензировании отдельных видов деятельности» (№99-ФЗ).
   * Закон «Об информации, информационных технологиях и о защите информации» (№149-ФЗ).
2. **Цель:**
   * Установление требований к деятельности по защите информации.
   * Контроль за соблюдением стандартов.
3. **Ключевые нормативные акты:**
   * Постановления Правительства РФ о лицензировании.
   * Требования ФСТЭК и ФСБ к системам защиты информации.

**38. Лицензирование деятельности по защите информации. Сертификация средств защиты информации**

1. **Лицензирование:**
   * Осуществляется ФСТЭК, ФСБ, Роскомнадзором.
   * Требуется для деятельности, связанной с:
     + Технической защитой информации.
     + Шифровальными средствами.
     + Обеспечением безопасности персональных данных.
   * Этапы:
     + Подача заявки.
     + Проверка соответствия требованиям.
     + Выдача лицензии.
2. **Сертификация средств защиты:**
   * Проводится для подтверждения соответствия ГОСТам и стандартам.
   * Включает:
     + Испытания на безопасность.
     + Проверку на отсутствие уязвимостей.
   * Обеспечивает доверие к используемым технологиям.