**Часть 1.**

1. Что такое система физической защиты объекта?

2. Какие требования предъявляются к комплексной системе безопасности объекта?

3. Аналоговый, дискретный сигнал.

4. Спектр. Спектр аналогового и дискретного сигнала.

5. Скремблер. Принцип действия скремблера.

6. Условие для выбора n (число мелких интервалов в пределах Т).

7. Виды скремблирования. Достоинства и недостатки.

8. Полосовой фильтр. Как он используется при скремблировании, в каком из видов скрембли-рования.

9. Инверсия частотного спектра сообщения. Для чего применяется.

10. Какие модели доступа Вам известны? Раскройте их сущность.

**1. Что такое система физической защиты объекта?**

Система физической защиты объекта — это совокупность технических, организационных, и инженерных мер, направленных на предотвращение несанкционированного доступа, вандализма, краж и других угроз безопасности.

**Основные элементы системы:**

* **Физические барьеры:** заборы, двери, замки, окна с решетками.
* **Системы контроля доступа:** пропускные пункты, СКУД.
* **Системы обнаружения:** датчики движения, охранная сигнализация.
* **Системы видеонаблюдения.**
* **Охрана объекта:** патрулирование, дежурные посты.

**2. Какие требования предъявляются к комплексной системе безопасности объекта?**

1. **Надежность:**
   * Устойчивость к сбоям и внешним воздействиям.
2. **Комплексность:**
   * Включение различных видов защиты (физической, информационной, технической).
3. **Совместимость:**
   * Интеграция всех элементов системы.
4. **Гибкость:**
   * Возможность адаптации под изменяющиеся условия.
5. **Доступность:**
   * Быстрый доступ для уполномоченных лиц.
6. **Юридическая обоснованность:**
   * Соответствие законодательству.
7. **Эффективность:**
   * Способность предотвращать угрозы с минимальными затратами.

**3. Аналоговый, дискретный сигнал**

* **Аналоговый сигнал:** имеет непрерывный характер. Значения сигнала изменяются плавно во времени (пример: звук, изображение).
* **Дискретный сигнал:** представляет собой набор отдельных значений (цифровые данные).

**4. Спектр. Спектр аналогового и дискретного сигнала**

* **Спектр:** распределение энергии сигнала по частотам.
* **Спектр аналогового сигнала:** непрерывный, охватывает диапазон частот, содержащих всю информацию о сигнале.
* **Спектр дискретного сигнала:** дискретен, состоит из отдельных частотных составляющих.

**5. Скремблер. Принцип действия скремблера**

Скремблер — устройство или программа, изменяющее структуру сигнала, чтобы сделать его нечитаемым для неавторизованных пользователей.

**Принцип действия:**

* Перестановка или замена битов/символов сигнала.
* Шифрование или маскирование данных.
* Обратное преобразование (дескремблирование) возможно только с использованием ключа.

**6. Условие для выбора n (число мелких интервалов в пределах T)**

Для точного представления сигнала необходимо:

* **n ≥ 2 × f\_max × T,**  
  где fmaxf\_{max}fmax​ — максимальная частота сигнала, TTT — период.  
  Это условие соответствует теореме Котельникова о дискретизации.

**7. Виды скремблирования. Достоинства и недостатки**

**Виды:**

1. **Перестановка битов:**
   * Простая реализация.
   * Низкая устойчивость к взлому.
2. **Шифрование:**
   * Высокая степень защиты.
   * Требует значительных вычислительных ресурсов.
3. **Инверсия частот:**
   * Легко реализуется в аналоговых системах.
   * Меньшая защита в сравнении с цифровыми методами.

**8. Полосовой фильтр. Как он используется при скремблировании, в каком из видов скремблирования**

Полосовой фильтр используется для выбора определённого диапазона частот сигнала.

* Применяется в **частотном скремблировании**, где спектр сигнала инвертируется, а затем фильтруется для подавления лишних частот.

**9. Инверсия частотного спектра сообщения. Для чего применяется**

* **Суть:** Меняет местами высокие и низкие частоты сигнала.
* **Цель:** Скрыть содержание сообщения, сделать его неразборчивым без обратного преобразования.

**10. Какие модели доступа Вам известны? Раскройте их сущность**

1. **Мандатная модель (MAC):**
   * Доступ определяется уровнем секретности пользователя и ресурса.
   * Пример: армейские системы.
2. **Дискреционная модель (DAC):**
   * Доступ контролируется владельцем ресурса.
   * Пример: файлы в операционных системах.
3. **Ролевая модель (RBAC):**
   * Доступ предоставляется на основе роли пользователя.
   * Пример: корпоративные системы.
4. **Атрибутивная модель (ABAC):**
   * Доступ определяется на основе свойств (атрибутов) пользователя и объекта.
   * Пример: современные облачные сервисы.

**Часть 2.**

**1. Основные термины и определения**

* **Информация** — это данные, которые имеют значение для получателя и могут быть использованы для принятия решений.
* **Информационные отношения** — взаимодействие субъектов, которые обмениваются, обрабатывают, хранят и передают информацию.
* **Субъекты информационных отношений** — это участники процесса обработки информации, включая пользователей, организации и системы.
* **Автоматизированная система обработки информации (АСОИ)** — система, которая выполняет обработку, хранение, передачу и защиту информации с использованием вычислительных средств.
* **Информационная безопасность АС** — совокупность мер по защите информации от несанкционированного доступа, утрат и искажений в рамках автоматизированных систем.

**2. Базовые свойства защищаемой информации и систем ее обработки**

* **Свойства информации как предмета защиты:** конфиденциальность, целостность, доступность, подлинность.
* **Способы нанесения ущерба субъектам информационных отношений:**
  + Нарушение конфиденциальности (несанкционированный доступ).
  + Нарушение целостности (изменение или уничтожение информации).
  + Нарушение доступности (блокировка доступа).

**3. Определение требований к защищаемой информации. Информационные пакеты.**

* **Требования к защищаемой информации** — обеспечение конфиденциальности, целостности и доступности.
* **Информационные пакеты** — совокупности данных, передаваемых через систему, которые могут включать как текстовую информацию, так и управляющие данные для обработки.

**4. Особенности автоматизированной системы (АС) как объекта защиты**

* **Уязвимость АС:** каждый элемент системы (программное обеспечение, аппаратные средства, сеть) может быть подвержен угрозам.
* **Угрозы безопасности:** это события или действия, которые могут привести к ущербу в области конфиденциальности, целостности и доступности информации.

**5. Классификация угроз безопасности информации**

* **По источникам:** внешние (вредоносные программы, хакеры), внутренние (ошибки сотрудников, недобросовестные действия).
* **По типу воздействия:** физические угрозы, программные угрозы, человеческий фактор.
* **Методы перечисления угроз:** анализ уязвимостей, сценарные подходы, классификация по типам атак.

**6. Основные искусственные угрозы информационной безопасности**

* **Преднамеренные угрозы:** умышленные действия (хакерские атаки, вредоносное ПО).
* **Случайные угрозы:** ошибки пользователей или систем, которые могут вызвать ущерб без злого умысла (например, удаление данных).

**7. Классификация каналов проникновения в систему и утечки информации**

* **Каналы проникновения:** сетевая связь, физический доступ, социальная инженерия.
* **Каналы утечки:** каналы передачи данных, несанкционированный доступ через уязвимости.

**8. Неформальная модель нарушителя в автоматизированных системах обработки информации**

* **Модель нарушителя:** включает оценку мотивов (например, финансовая выгода), навыков (умение использовать уязвимости), а также возможности доступа (физический или сетевой доступ).

**9. Основные меры противодействия угрозам безопасности**

* **Методы защиты информации:**
  + Шифрование данных.
  + Контроль доступа.
  + Защита сети (межсетевые экраны, IDS).
  + Аудит безопасности.
  + Физическая защита.

**10. Взаимосвязь различных методов обеспечения информационной безопасности**

* **Достоинства:** комплексный подход обеспечивает более высокий уровень защиты, позволяя устранить уязвимости на разных уровнях (сеть, приложения, физическая защита).
* **Недостатки:** высокий ресурсозатратный характер, сложности в интеграции различных систем защиты.
* **Задачи системы информационной безопасности:** защита данных, предотвращение атак, восстановление после инцидентов.

**11. Основные принципы обеспечения безопасности автоматизированных систем обработки информации**

* **Конфиденциальность:** информация должна быть доступна только уполномоченным пользователям.
* **Целостность:** защита данных от несанкционированных изменений.
* **Доступность:** информация должна быть доступна в нужное время и в нужном месте.
* **Подотчетность:** учет всех действий с данными.

**12. Основные механизмы защиты автоматизированных систем**

* **Термины и определения:** защита данных, системы контроля доступа, криптография, резервное копирование, фаерволы, системы обнаружения вторжений (IDS).

**13. Построение систем защиты от угроз нарушения конфиденциальности информации**

* **Модель системы защиты:** состоит из защиты каналов передачи данных, защиты информации в хранилищах, политики безопасности для доступа.
* **Идентификация и аутентификация:** процедуры, направленные на проверку личности пользователя и его полномочий для доступа.

**14. Особенности парольных систем аутентификации**

* **Особенности:** пароли должны быть уникальными, сложными и храниться в зашифрованном виде.
* **Типы паролей:** однофакторная аутентификация (пароль) и двухфакторная (помимо пароля требуется код с устройства).

**15. Рекомендации по практической реализации парольных систем аутентификации**

* **Рекомендации:** использовать длинные пароли, избегать использования общеизвестных слов, регулярная смена паролей, хранение в зашифрованном виде.

**16. Оценка стойкости парольных систем аутентификации. Методы хранения паролей**

* **Стойкость:** определяется длиной и сложностью пароля.
* **Методы хранения паролей:** хэширование с солью, использование ключей для усиления защиты.

**17. Два основных метода разграничения доступа**

1. **Ролевой доступ:** доступ к данным на основе роли пользователя в организации.
2. **Мандатный доступ:** доступ определен политикой безопасности и требованиями безопасности данных.

**18. Типы моделей управления доступом**

1. **DAC (Дискреционная модель управления доступом):** доступ контролируется владельцем ресурса.
2. **MAC (Мандатная модель):** доступ ограничивается на основе политики безопасности.
3. **RBAC (Ролевая модель):** доступ назначается на основе роли пользователя.
4. **ABAC (Атрибутивная модель):** доступ определяется на основе атрибутов пользователей и объектов.

**19. Криптографические методы обеспечения конфиденциальности информации**

* **Симметричные криптосистемы:** один и тот же ключ используется для шифрования и дешифрования (например, AES).
* **Асимметричные криптосистемы:** используется пара ключей — открытый и закрытый (например, RSA).

**20. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов**

* **Межсетевое экранирование:** использование фаерволов для фильтрации трафика между различными сетями.
* **Классы межсетевых экранов:**
  + **Пакетные фильтры:** проверка пакетов на основе их заголовков.
  + **Прокси-серверы:** проверка и фильтрация данных на уровне приложений.
  + **Сетевые экраны нового поколения:** использование анализа трафика, детекции вторжений и фильтрации по содержимому.