1. Основные понятия защиты информации и информационной безопасности:
Защита информации - это комплексный процесс обеспечения конфиденциальности, целостности и доступности информации. Информационная безопасность - это состояние защищенности информационных ресурсов от неблагоприятных факторов внутренней и внешней среды, которые могут привести к утрате или нарушению конфиденциальности, целостности и доступности информации.

2. Актуальность проблемы обеспечения. Классификация уязвимостей. Классификация атак:
Актуальность проблемы информационной безопасности возрастает в связи с ростом числа компьютерных угроз и сетевых атак. Классификация уязвимостей включает в себя программные и аппаратные уязвимости, а также человеческий фактор. Классификация атак представляет атаки на уровнях прикладного, транспортного, сетевого и канального уровней.

3. Основные механизмы защиты компьютерной информации:
Основные механизмы защиты компьютерной информации включают в себя физическую защиту, логическую защиту, контроль доступа, шифрование, целостность и проверку подлинности.

4. Управление механизмами защиты:
Управление механизмами защиты включает в себя управление политиками безопасности, регулирование доступа, мониторинг и аудит безопасности, управление инцидентами и управление рисками.

5. Сетевые анализаторы и «снифферы»:
Сетевые анализаторы и «снифферы» используются для мониторинга и анализа сетевого трафика, что может помочь обнаружить уязвимости и атаки на сетевом уровне, транспортном уровне и уровне приложений.

6. Защита на канальном уровне. Протокол PPTP:
Протокол PPTP (Point-to-Point Tunneling Protocol) используется для создания защищенного канала передачи данных между двумя узлами сети на канальном уровне. Он обеспечивает шифрование, аутентификацию и целостность данных.

7. Защита на канальном уровне. Протоколы L2F, L2TP:
Протоколы L2F (Layer 2 Forwarding Protocol) и L2TP (Layer 2 Tunneling Protocol) также используются для создания защищенного канала передачи данных между двумя узлами сети на канальном уровне. Они обеспечивают шифрование, аутентификацию и целостность данных.

8. Протокол IPSec. Структура протокола (протоколы AH, ESP, IKE):
Протокол IPSec (Internet Protocol Security) используется для создания защищенного канала передачи данных между двумя узлами сети на сетевом уровне. Он обеспечивает шифрование, аутентификацию и целостность данных. IPSec включает протоколы AH (Authentication Header), ESP (Encapsulating Security Payload) и IKE (Internet Key Exchange).

9. Режимы работа IPSec:
Режимы работы протокола IPSec включают туннельный режим, в котором весь пакет защищается, и транспортный режим, в котором защитой покрывается только полезный заголовок данных.

10. Виртуальные частные сети. Типы VPN-устройств:
Виртуальная частная сеть (VPN) позволяет создавать защищенную сеть между двумя удаленными узлами через открытую сеть. Типы VPN-устройств включают в себя VPN-сервер, VPN-клиент, VPN-маршрутизатор, VPN-концентратор и VPN-фаервол.

11. Проблемы безопасности протоколов прикладного уровня. Меры защиты прикладного уровня:
Проблемы безопасности протоколов прикладного уровня могут включать в себя небезопасное кодирование, взломы сессий, межсайтовый скриптинг, SQL-инъекции и другие. Меры защиты прикладного уровня могут включать в себя кодирование данных, использование SSL/TLS протоколов, фильтрацию пользовательского ввода и т.д.

12. Криптография. Основные понятия. Оценка надежности криптоалгоритмов:
Криптография - это наука о методах обеспечения конфиденциальности информации. Основные понятия включают в себя шифрование, разрешение криптоанализа, ключи шифрования и атаки на криптографические методы. Оценка надежности криптоалгоритмов включает в себя оценку его выводимой сводимости, вычислительной и информационной сложности.

13. Классификация методов шифрования информации. Блочные шифры. Поточные шифры:
Классификация методов шифрования информации включает в себя симметричное шифрование, асимметричное шифрование и хеш-функции. Блочные шифры и поточные шифры - это две разновидности симметричного шифрования. Блочные шифры шифруют блоки данных определенного размера, а поточные шифры шифруют данные бит за битом.

14. Криптосистема с открытым ключом. Криптосистема с закрытым ключом:
Криптосистема с открытым ключом использует два ключа - открытый и закрытый для шифрования и дешифрования информации. Криптосистема с закрытым ключом использует только один ключ для обеих операций.

15. Модель безопасности ОС. Компоненты системы безопасности. Пользовательские бюджеты:
Модель безопасности ОС включает в себя компоненты системы безопасности, такие как система управления доступом, протоколы шифрования, межсетевой экран и система аудита. Пользовательские бюджеты - это механизм управления ресурсами пользователями в системе.

16. Обеспечение комплексной безопасности:

Обеспечение комплексной безопасности включает в себя применение различных мер безопасности, таких как механизмы защиты корпоративной сети, аутентификация пользователя и управление утечками данных.

17. Защита базы данных:
Защита базы данных включает в себя меры для обеспечения конфиденциальности, целостности и доступности данных в базе данных. Меры включают в себя шифрование данных, резервное копирование данных, управление доступом и мониторинг.

18. Понятие МЭ:
МЭ (магнитоэлектрическое излучение) - это электромагнитные волны, которые испускаются электрическими устройствами при выполнении операций обработки информации. Они могут помешать работе электронного оборудования и привести к ослаблению компонентов.

19. Схемы подключения электромагнитных полей (МЭ) могут быть использованы для защиты информации в компьютерных системах. Они основаны на том, что электромагнитные поля могут замешать передачу информации, если они попадают на канал связи или провод, по которому передается информация. Соответственно, схемы подключения МЭ используют электромагнитное поле, чтобы создать помехи и затруднить или невозможным сделать подслушивание или перехват информации.

Существуют разные схемы подключения МЭ, включая:

1. Установка экранированных кабелей и переходов: такие кабели содержат внутренний экран, который защищает их от воздействия внешних электромагнитных полей.

2. Использование электромагнитных завес: производят электромагнитные поля в некоторой области вокруг канала передачи информации, чтобы создать помехи для записи информации.

3. Использование ЭМИ-фильтров: ЭМИ-фильтры уменьшают уровень шума и помех, которые могут повлиять на передачу информации.

4. Использование методов оптической связи: данный метод передачи информации использует луч света, что делает его крайне малочувствительным к МЭ помехам.

Схемы подключения МЭ могут использоваться во многих различных областях, таких как финансы, медицина, правительство и многое другое. Они пригодны для защиты любого типа информации, будь то личные данные, бизнес-секреты или государственные секреты.