# Вопросы к аттестации

1. Основные понятия и терминология информационных сетей, понятия сетевого узла, ресурса, клиента, сервера, трафика, пропускной способности.
2. Классификация информационных сетей. Понятия и терминология информационной безопасности.
3. Классификация локальных сетей. Топологии локальных сетей: физическая и логическая. Достоинства и недостатки. Выбор топологии.
4. Среда передачи: проводная и беспроводная. Коаксиальный кабель, витая пара, оптоволокно. Радиоволны, микроволны, инфракрасное излучение.
5. Методы доступа к среде передачи: конфликтные и бесконфликтные. Модель взаимодействия открытых систем. Стеки протоколов.
6. Базовые технологии локальных сетей. Объединения сетей и глобальные сети. Принципы межсетевого взаимодействия. Глобальные сети и перспективные сетевые технологии. Глобальная сеть Интернет
7. Простейшие шифры. Симметричная криптография.
8. Криптография с открытым ключом
9. Аутентификация сообщений. Электронная цифровая подпись. Идентификация и аутентификация пользователей
10. Многоуровневые модели. Модель OSI. Физический уровень. Канальный уровень. Протокол Ethernet. Сетевой уровень. Протокол IP. Транспортный уровень. Протокол TCP. Протокол UDP. Сеансовый уровень. Уровень представления. Прикладной уровень. Протокол HTTP.
11. Классификация атак. Классификация методов и средств защиты.
12. Атака типа ложный ARP-сервер. Ложный DNS-сервер. Подмена одного из субъектов TCP-соединения в сети Internet.
13. Методы удаленного сканирования портов. Защита от удаленных атак в сети Internet. Функции межсетевого экранирования.
14. Методы обнаружения анализаторов сетевого трафика. Защищенные сетевые протоколы. Протоколы SSL, IPsec, SET.
15. Защита электронных банковских платежных систем. Защита конфиденциальности информации в мобильных устройствах.
16. Классификация угроз. Классификация методов и средств защиты.
17. Средства защиты от несанкционированного использования.
18. Средства защиты ПО от обратного проектирования.
19. Средства защиты от модификации.
20. Атаки на переполнение буфера. Переполнение стека. Переполнение кучи. Целочисленное переполнение. Защита от переполнения буфера.
21. Внедрение SQL-кода (SQL-injection). Защита от атак типа SQL-injection. Проверка входных данных. Защита от атак, основанных на изменении входных данных.
22. Биометрические системы контроля доступа. Водяные знаки. Активное измерение. Применение физически неклонируемых функций