Контрольные вопросы для самоподготовки студентов к экзамену

(для групп 4405, 4406)

1. Современная ситуация и проблемы в области информационной безопасности. Предмет и задачи курса.
2. Основные понятия защиты информации и информационной безопасности компьютерных систем и сетей.
3. Определяющие факторы и классификация угроз.
4. Базовая классификация уязвимостей. Основные классы злоупотреблений в компьютерных сетях.
5. Уязвимость компонентов распределенных АС. Типовая структура компьютерных сетей. Структура MAC-адреса. Структура IP-адреса.
6. Модель OSI/ISO. Распределение функций между различными элементами сети.
7. Стек протоколов TCP/IP.
8. Сетевые уязвимости, угрозы и атаки. Основные причины уязвимости компьютерных сетей
9. Примеры уязвимостей по уровням модели OSI
10. Основные проблемы стека протоколов TCP/IP: Протокол IP, Протоколы TCP и UDP, Протоколы маршрутизации, Протокол ICMP, Протокол DNS.
11. Классификация атак и их основные виды. Отказ в обслуживании. Спуфинг. Внедрение вредоносных программ. Кража личности. Фишинг. Сетевая разведка. Подслушивание. Посредничество. Парольные атаки. Атаки на уровне приложений.
12. Примеры сетевых атак. Прослушивание сетевого трафика. Способы защиты от снифферов и их выявление. Спуфинг. Перенаправление трафика (ICMP-атака). Защита от ARP-спуффинга. Методы посредничества (подделка TCP-сегмента, повторение TCP-сегментов, сброс TCP-соединения). Атаки типа «отказ в доступе» (атаки, основанные на насыщении полосы пропускания, основанные на недостатке ресурсов жертвы, основанные на ошибках в программном коде, основанные на маршрутизации и атаки DNS-серверы). Способы защиты от DoS-атак. Проникновение в компьютерные сети (парольные атаки, использование уязвимостей программных кодов, эксплойты, внедрение вредоносных программ, скрытые коммуникации и скрытые каналы, программные закладки, аппаратные закладки, SQL инъекция). Сканирование компьютерных сетей.
13. Технологии защиты информации в сетях. Сеть как объект защиты. Способы безопасности информационных сетей. Системный подход к управлению безопасностью. Пути решения проблем защиты информации в сетях.
14. Модель OSI. Механизмы защиты информации, применяемые на разных уровнях: физический уровень, канальный уровень, сетевой уровень, транспортный уровень, сеансовый уровень, прикладной уровень.
15. Средства защиты информации в компьютерных сетях. Базовые средства защиты в компьютерных сетях.
16. Межсетевые экраны. Правила фильтрации МЭ. Классификация МЭ. Фильтрация трафика на нижнем слое модели OSI. Межсетевые экраны сеансового уровня. Межсетевые экраны прикладного уровня. Гибридные технологии межсетевых экранов. Персональные МЭ. Файерволы с функцией NAT. Схемы подключения МЭ.
17. Системы обнаружения атак (вторжений). Необходимость СОВ. Отличие СОВ И МЭ. Обнаружение вторжений. Классификация IDS по типу идентификации атак. Классификация IDS. Архитектура системы выявления атак. Пример размещения СОВ. Пассивные и активные СОВ. Классификация IPS.
18. Виртуальные частные сети (VPN). Концепция построения защищенных виртуальных частных сетей. Функции и компоненты сети VPN. Основные задачи, решаемые VPN. Классификация VPN. Классификация VPN по протоколам туннелирования и уровням эталонных моделей (VPN канального уровня, VPN сетевого уровня, VPN верхнего слоя). Классификация VPN по способу технической реализации.
19. Сканеры уязвимостей. Механизмы работы сканеров безопасности. Классы сканеров безопасности. Методика использования сканеров.