Список экзаменационных вопросов по курсу
«Управление и защита информации в компьютерных сетях»

1. Альтернативные архитектуры КС. Архитектура сетей Novell.
2. Альтернативные архитектуры КС. Архитектура DNA.
3. Альтернативные архитектуры КС. Архитектура AppleTalk.
4. Недостатки протокола IPv4. Семейство протоколов IPv6. Основные особенности.
5. Протокол IPv6. Адресация в сетях IPv6.
6. Семейство протоколов IPv6. Сетевой уровень.
7. Семейство протоколов IPv6. Маршрутизация, DNS, транспортные механизмы IPv6.
8. Безопасность в IPv6. Способы совместного сосуществования сетей IPv4 и IPv6. Механизмы перехода на IPv6.
9. Конфигурирование компьютерных сетей. Протоколы RARP, BOOTP, DHCP. Утилиты контроля и диагностики.
10. Управление учетом использования ресурсов. Управление неисправностями. Сетевые анализаторы.
11. Управление доставкой. Доступ к ресурсам с помощью серверов-посредников. Шлюзы уровня приложения (ALG).
12. Управление доставкой. Протокол SOCKS.
13. Управление доставкой. Технология трансляции адресов (NAT). Прозрачные серверы-посредники (transparent proxy).
14. Туннелирование
15. Управление в компьютерных сетях. Модель систем управления ISO. Архитектуры систем управления
16. Протокол SNMP. Объекты SNMP, их параметры.
17. Протокол SNMP. Управляющая база MIB. Безопасность SNMP.
18. Групповая маршрутизация. Алгоритмы построения дерева доставки.
19. Групповая маршрутизация. Протоколы динамической групповой маршрутизации.
20. Управление доставкой. Коммутация 3-го уровня.
21. Качество обслуживание. Классификация приложений. Параметры качества обслуживания.
22. Архитектура службы QOS. Средства QoS. Протоколы сигнализации. Централизованные функции политики, управления и учета QoS.
23. Защита информации в компьютерных сетях. Виды нарушения защиты. Классификация сетевых атак. Механизмы защиты информации.
24. Криптографическая защита информации. Общие принципы симметричных систем шифрования. Алгоритмы замены и перестановки.
25. Криптографическая защита информации. Алгоритмы взбивания. Схема Фейстеля.
26. Криптографическая защита информации. Алгоритм DES. Режимы работы.
27. Криптографическая защита информации. Асимметричные системы шифрования. Понятие открытых и секретных ключей. Алгоритмы RSA и Эль-Гамаля.
28. Хэширование. Электронная цифровая подпись.
29. Механизмы защиты информации. Идентификация. Аутентификация.
30. Аутентификация на основе паролей. Аутентификация в ОС. Аудит.
31. Авторизация. Модели управления доступом.
32. Организация аутентификации на основе системы PAM.
33. Протоколы аутентификации и авторизации. PAP, CHAP, RADIUS, TACACS.
34. Архитектура системы Kerberos.
35. Криптографические файловые системы. Механизмы очистки «мусора».
36. Ограничение доступа к компьютерным сетям на основе межсетевых экранов (firewall). Типы экранов и их функции.
37. Виртуальные частные сети. (VPN). Архитектура IPSec.
38. Сертификация. Сертификаты. Удостоверяющие центры.