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

1. Именование ресурсов в сетях TCP/IP. Доменная система имен.
2. Архитектура DNS. Рекурсивные и нерекурсивные серверы имен. Ретрансляторы.
3. База данных DNS. Ресурсные записи DNS. Адресные записи, записи о сервере имен, псевдонимах.
4. База данных DNS. Ресурсные записи DNS. Главная ресурсная запись. Маршрутизация электронной почты.
5. Доменная система имен. Динамические обновления.
6. Доменная система имен. Нотификации об изменениях; инкрементальные обновления
7. Прикладные протоколы. Протоколы удаленных терминалов.
8. Электронная почта. Механизм работы. Система MIME
9. Электронная почта. Протокол передачи электронной почты SMTP.
10. Электронная почта. Маршрутизация почты. Борьба со спамом.
11. Электронная почта. Протокол доступа к почтовым ящикам POP3.
12. Электронная почта. Протокол доступа к почтовым ящикам IMAP4.
13. Протоколы прикладного уровня. Протоколы передачи файлов FTP и TFTP.
14. Протоколы прикладного уровня. Протокол HTTP.
15. Альтернативные архитектуры КС. Архитектура сетей Novell.
16. Альтернативные архитектуры КС. Архитектура DNA.
17. Альтернативные архитектуры КС. Архитектура AppleTalk.
18. Недостатки протокола IPv4. Семейство протоколов IPv6. Основные особенности.
19. Протокол IPv6. Адресация в сетях IPv6.
20. Семейство протоколов IPv6. Сетевой уровень.
21. Семейство протоколов IPv6. Маршрутизация, DNS, транспортные механизмы IPv6.
22. Безопасность в IPv6. Способы совместного сосуществования сетей IPv4 и IPv6. Механизмы перехода на IPv6.
23. Управление в компьютерных сетях. Модель систем управления ISO. Архитектуры систем управления.
24. Управления конфигурацией. Протоколы RARP, BOOTP, DHCP. Утилиты контроля и диагностики.
25. Протокол SNMP. Объекты SNMP, их параметры.
26. Протокол SNMP. Управляющая база MIB. Безопасность SNMP.
27. Управление учетом использования ресурсов. Управление неисправностями. Сетевые анализаторы.
28. Управление доставкой. Доступ к ресурсам с помощью серверов-посредников. Шлюзы уровня приложения (ALG).
29. Управление доставкой. Протокол SOCKS.
30. Управление доставкой. Технология трансляции адресов (NAT). Прозрачные серверы-посредники (transparent proxy).
31. Туннелирование
32. Групповая маршрутизация. Алгоритмы построения дерева доставки.

33. Групповая маршрутизация. Протоколы динамической групповой маршрутизации.
34. Управление доставкой. Коммутация 3-го уровня.
35. Качество обслуживание. Классификация приложений. Параметры качества обслуживания.
36. Архитектура службы QOS. Средства QoS. Протоколы сигнализации. Централизованные функции политики, управления и учета QoS.
37. Защита информации в компьютерных сетях. Виды нарушения защиты. Классификация сетевых атак. Механизмы защиты информации.
38. Криптографическая защита информации. Общие принципы симметричных систем шифрования. Алгоритмы замены и перестановки.
39. Криптографическая защита информации. Алгоритмы взбивания. Схема Фейстеля.
40. Криптографическая защита информации. Алгоритм DES. Режимы работы.
41. Криптографическая защита информации. Асимметричные системы шифрования. Понятие открытых и секретных ключей. Алгоритмы RSA и Эль-Гамаля.
42. Хэширование. Электронная цифровая подпись.
43. Механизмы защиты информации. Идентификация. Аутентификация.
44. Аутентификация на основе паролей. Аутентификация в ОС. Аудит.
45. Авторизация. Модели управления доступом.
46. Организация аутентификации на основе системы PAM.
47. Протоколы аутентификации и авторизации. PAP, CHAP, RADIUS, TACACS.
48. Архитектура системы Kerberos.
49. Криптографические файловые системы. Механизмы очистки «мусора».
50. Ограничение доступа к компьютерным сетям на основе межсетевых экранов (firewall). Типы экранов и их функции.
51. Виртуальные частные сети. (VPN). Архитектура IPSec.
52. Сертификация. Сертификаты. Центры сертификации.