Вопросы к контрольной работе 3

1. Что обеспечивают протоколы внутренней маршрутизации? Укажите основные классы этих протоколов.
2. Опишите алгоритм Беллмана-Форда (его первоначальный вариант в RIP 1).
3. Опишите ситуации некорректной работы (отсутствия сходимости) в RIP 1 и способы преодоления этой некорректности.
4. Перечислите основные недостатки протокола RIP
5. Какие демоны используются для поддержки протоколов управления маршрутизацией? Какие протоколы поддерживает каждый демон?
6. Почему значение «бесконечности» метрики RIP равное 32 достаточно, несмотря на существование в интернете более длинных маршрутов?
7. Объясните смысл названия протокола OSPF. К каким классам относится этот протокол?
8. Опишите основные типы метрик протокола OSPF.
9. Опишите алгоритм работы протокола OSPF.
10. Перечислите основные достоинства протокола OSPF.
11. Что такое зонная организация сети OSPF маршрутизаторов и для чего она нужна?
12. Что такое автономная система и где она регистрируется?
13. В чем отличие между протоколами внутренней и внешней маршрутизации, какова основная особенность внешней маршрутизации?
14. Что такое политика маршрутизации AS и что означает анонсирование маршрутов автономной системой?
15. Для чего предназначены протоколы EBGP и IBGP?
16. Общая организация управления сетью на базе протокола SNMP
17. Что такое MIB и как она связана с ядром ОС управляемого по SMTP устройства?
18. Почему для SMTP построен над UDP? Обмен какими пакетами выполняется между агентом и управляющей станцией?
19. Какие пакеты (какие данные, каких команд) пересылаются с управляющей станции на агенты SNMP?
20. Какие пакеты (какие данные, каких команд) пересылаются с агентов SNMP на управляющую станцию?
21. Возможности команды snmpstat
22. Определение защищенной информационной системы
23. Типы угроз информационной безопасности
24. Типы мер по предотвращению угроз информационной безопасности
25. Какова суть статей 272, 273 и 274 УК РФ?
26. Понятие о политике информационной безопасности
27. Основные программно-технические угрозы безопасности и их краткая характеристик.
28. Типы вредоносных программ и меры по борьбе с ними
29. Методы реализации внутренних атак (бреши в программах)
30. Основные типы уязвимостей сетевых протоколов
31. Состав комплекса мер по обеспечению информационной безопасности
32. Понятие об аудите уровня С2
33. Понятие о методах криптозащиты

34. Принципы работы межсетевого экрана и разновидности межсетевых экранов
35. Принципы работы сканера безопасности
36. Принципы работы систем обнаружения вторжений (IDS).