Вопросы к контрольной работе 4

1. Приведите определение защищенной информационной системы
2. Основные свойства информации как объекта защиты и их краткая характеристика
3. Что такое средства аудита уровня С2?
4. Приведите классификацию угроз информационной безопасности
5. В чем может состоять ненадежность персонала и каковы основные меры по повышению его надежности?
6. Какие угрозы могут быть реализованы техническими способами?
7. Какие конкретные угрозы могут возникать при непосредственном доступе злоумышленника к информационной системе?
8. Перечислите комплексы мер по предотвращению реализации угроз безопасности.
9. Назовите известные Вам статьи УК РФ, предусматривающие уголовную ответственность за различные виды деятельности, связанные с нарушениями ИБ
10. Назовите основные организационные меры по повышению уровня информационной безопасности.
11. Какие административные меры по повышению уровня ИБ вы знаете?
12. Каким образом вырабатывается политика информационной безопасности
13. Назовите основные виды разрушающих программных воздействий и вредоносных программ и дайте их краткую характеристику
14. Перечислите возможные эффекты разрушающих программных воздействий
15. Чем хакерство отличается от крэкерства?
16. Что такое вирус? Классификация вирусов.
17. Что такое сетевые черви и троянские кони?
18. Каковы основные источники появления вредоносных программ
19. Каковы основные методы борьбы (предотвращения и избавления) с вредоносными программами?
20. Как еще называются вирусы-невидимки и полиморфные вирусы, какими способами они затрудняют их обнаружение?
21. Как за 20 секунд доступа к терминалу, открытому с правами суперпользователя злоумышленник может предоставить себе такие права?
22. Механизм и оценка временн'ой сложности взлома паролей методом «грубой силы».
23. Меры по предотвращению доступа к файлам зашифрованных паролей
24. В чем состоит опасность командных SetUId файлов?
25. Дайте общее определение бреши в системе ИБ программы
26. Опишите механизм бреши, использующей системный вызов gets()
27. Как защитить информацию от суперпользователя?
28. Основные меры борьбы с внутренними атаками
29. Какие основные угрозы ИБ существуют на физическом и канальном уровнях сетевых протоколов?
30. Какие основные угрозы ИБ существуют на IP-уровне?
31. Какие основные угрозы ИБ существуют на уровне протокола TCP?
32. Какие основные угрозы ИБ существуют на прикладном уровне?
33. В чем состоит компрометация DNS и как ее обнаружить?
34. Приведите классификацию сетевых атак
35. Опишите основные стадии развития сетевой атаки
36. Перечислите комплекс мер по борьбе с атаками
37. Опишите действия локального сканера безопасности
38. Опишите действия сетевого сканера безопасности
39. Какие меры предосторожности следует принимать при сканировании безопасности собственных сетей?

40. Почему применение сканера безопасности к “чужим» компьютерам может повлечь уголовную ответственность по ст. 273 УК РФ?
41. Укажите взаимные достоинства и недостатки локальных и сетевых сканеров безопасности.
42. Перечислите и вкратце охарактеризуйте методы обнаружения атак, используемые в системах IDS.
43. Принципы работы, достоинства и недостатки сигнатурных IDS
44. Принципы работы, достоинства и недостатки поведенческих (статистических) IDS
45. Назначение и принципы работы межсетевых экранов.
46. Понятие о межсетевых экранах сеансового и прикладного уровня.
47. Понятие демилитаризованной зоны и принципы включения компьютеров в эту зону
48. Возможные способы технической реализации межсетевого экрана, их достоинства и недостатки.
49. Обзор систем, частично реализующих функции межсетевого экрана
50. Что такое wrapper'ы и какие проверки устанавливаемых соединений они могут выполнять?
51. Принципы работы систем аудита и краткая характеристика разновидностей таких систем.
52. Общая организация системных средств аудита ОС UNIX
53. Криптозащита. Понятие о симметричных и несимметричных схемах шифрования и областям их применимости.
54. Схема организации работы защищенных сетевых протоколов.
55. Схема организации криптозащиты электронной подписи.