Вопросы к контрольной работе 3

1. Приведите и объясните определение защищенной информационной системы
2. Основные свойства информационной системы 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 иженерно-технические 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. Методы предотвращения компрометации DNS
35. Приведите классификацию сетевых атак
36. Опишите основные стадии развития сетевой атаки
37. Перечислите комплекс мер по борьбе с атаками
38. Опишите действия локального сканера безопасности
39. Опишите действия сетевого сканера безопасности
40. Что такое fix-script и что делать, если его применение не приводит к желаемому результату?
41. Какие меры предосторожности следует принимать при сканировании безопасности собственных сетей?
42. Почему применение сканера безопасности к “чужим» компьютерам может повлечь уголовную ответственность по ст. 273 УК РФ?
43. За какие упущения при выполнении процедуры применения сканера безопасности администратора сети могут привлечь к ответственности по ст. 274 УК РФ?
44. Укажите взаимные достоинства и недостатки локальных и сетевых сканеров безопасности.
45. Перечислите и вкратце охарактеризуйте типы IDS по месту их установки
46. Перечислите и вкратце охарактеризуйте методы обнаружения атак, используемые в системах IDS.
47. Принципы работы, достоинства и недостатки сигнатурных IDS
48. Принципы работы, достоинства и недостатки поведенческих (статистических) IDS
49. Какие действия могут выполняться IDS всех типов при обнаружении факта атаки?
50. Назначение и принципы работы межсетевых экранов.
51. Понятие о межсетевых экранах сеансового и прикладного уровня.
52. Понятие демилитаризованной зоны и принципы включения компьютеров в эту зону
53. Возможные способы технической реализации межсетевого экрана, их достоинства и недостатки.
54. Обзор систем, частично реализующих функции межсетевого экрана

55. Что такое wrapper'ы и какие проверки устанавливаемых соединений они могут выполнять?
56. Принципы работы систем аудита и краткая характеристика разновидностей таких систем.
57. Общая организация системных средств аудита ОС UNIX.
58. Криптозащита. Понятие о симметричных и несимметричных схемах шифрования и областях их применимости.
59. Схема организации работы защищенных сетевых протоколов.
60. Схема организации криптозащиты электронной подписи.
61. Какой была цель создания системы Биткоин?
62. Каковы основные недостатки централизованной платёжной системы?
63. Какие 2 революции произвело создание системы Биткоин?
64. Для чего предназначена технология блокчейн?
65. Что такое реестр транзакций, как он организован и где хранится?
66. Что Вы знаете о Сатоси Накамото
67. Что Вы знаете о системе Эфириум и её создателе?
68. Что Вам известно об истории создания, назначении и особенностям системы Мастерчейн?
69. Какова топологическая структура сети Биткоин на сетевом уровне и какова её виртуальная топология?
70. Какие функции выполняет полный узел майнера?
71. Какие три значения хранятся в криптокошельке Биткоин, «откуда они берутся» где и как они используются
72. Какие способы хранения криптокошелька Вам известны?
73. Опишите структуру записи транзакции и назначение её полей
74. Для чего нужны транзакции с несколькими входами или выходами?
75. Что происходит, если сумма выходов транзакции с несколькими выходами меньше суммы её входа. Для чего могут использоваться такие транзакции?
76. Что такое цепочки транзакций и для чего они используются?
77. Опишите 2 основные проверки корректности транзакции
78. Какова организация реестра транзакций? Как и для чего устроен блокчейн? Что такое Genezis-блок?
79. Какая информация и для чего заносится в начало каждого блока перед занесением в него записей транзакций по переводу средств между участниками системы?
80. Как вычисляется криптоподпись блока и что такое PoW?
81. Каким свойствам должна удовлетворять криптоподпись блока и как эти свойства обеспечиваются?

82. Как узлы сети Биткоин приходят к консенсусу (консенсуса PoW) о признаваемом всеми ими значениям криптоподписи и подписанного ею блока (описать в крупных чертах)?
83. Что нужно сделать злоумышленнику для подмены некоторого блока блокчейна? Что такое «атака 51%»?
84. Что такое консенсус BFT (вкратце с упоминанием автора соответствующего алгоритма), его основные недостатки по сравнению с консенсусом PoW?
85. Что такое консенсус PoS, его основные достоинства и недостатки по сравнению с консенсусом PoW? В каких блокчейн-системах он применяется?