1602 р/с Защита информации

1) Протокол FTP предназначен для...
a) загрузки сообщений из новостных групп
b) просмотра Web-страниц
c) общения в чатах
d)) передачи файлов

2) Протокол POP3 работает на _____ уровне.
a) Физическом;
b) Транспортном;
c) Сетевом;
d)) Прикладном.

3) Поток сообщений в сети передачи данных определяется:
a) Треком;
b)) Трафиком;
c) Объемом памяти канала передачи сообщений;
d) Скоростью передачи данных.

4) Протокол SMTP предназначен для…
a) Общения в чате;
b)) Отправки электронной почты;
c) Просмотра веб-страниц;
d) Приема электронной почты.

5) Адрес веб-страницы для просмотра в браузере начинается с...
a) ftp;
b)) http;
c) www;
d) smpt

.
6) Системой, автоматически устанавливающей связь между IP-адресами в сети Интернет и текстовыми именами, является ...
a) Доменная система имен (DNS);
b)) Система URL-адресации;
c) Интернет-протокол;
d) Протокол передачи гипертекста.

7) Укажите правильно записанный IP-адрес в компьютерной сети
a) 192.154.144.270;
b) www.50.50.10;
c)) 10.172.122.26;
d) 193.264.255.10;
e) www.alfa193.com.

8) Домен .ru является _____ доменом.
a)) Зональным;
b) Основным;
c) Надежным;
d) Первичным.

9) Любой узел сети Интернет имеет свой уникальный IP-адрес, который состоит из _____ чисел в диапазоне от 0 до 255.
a) Пяти;
b) Трех;
c)) Четырех;
d) Двух.

10) Для правильной, полной и безошибочной передачи данных необходимо придерживаться согласованных и установленных правил, которые оговорены в _____ передачи данных.
a)) Протокол;
b) Канал;
c) Порт;
d) Описание.

11) Формой написания IP - адреса является запись вида:

xxx.xxx.xxx.xxx ,
где xxx - это…
a)) Десятичные числа от 0 до 255;
b) Десятичные числа от 0 до 999;
c) Двоичный код;
d) Буквы латинского алфавита.

12) Для безопасного использования ресурсов в сети Интернет предназначен протокол…
a)) HTTPS;
b) NNTP;
c) IRC;
d) FTP.

13) Сетевым протоколом является...
a)) Набор программ;
b) Инструкция;
c) Набор правил;
d) Программа.

14. Основные угрозы доступности информации:
a) непреднамеренные ошибки пользователей
b) злонамеренное изменение данных

))хакерская атака
c) отказ программного и аппаратно обеспечения
d) разрушение или повреждение помещений

15. Суть компрометации информации
a) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

))несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

b) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

16. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

))с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

a) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
b) способна противостоять только информационным угрозам, как внешним так и внутренним
c) способна противостоять только внешним информационным угрозам

17. Методы повышения достоверности входных данных

a) Замена процесса ввода значения процессом выбора значения из предлагаемого множества
b) Отказ от использования данных
c) Проведение комплекса регламентных работ
d))Использование вместо ввода значения его считывание с машиночитаемого носителя
e) Введение избыточности в документ первоисточник
f) Многократный ввод данных и сличение введенных значений

18. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)

a) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
b) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
c) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

19. Сервисы безопасности:

))идентификация и аутентификация

a) шифрование
b) инверсия паролей
c) контроль целостности
d) регулирование конфликтов
e) экранирование
f) обеспечение безопасного восстановления
g) кэширование записей

20. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

e))несанкционированного управления удаленным компьютером

a) внедрения агрессивного программного кода в рамках активных объектов Web-страниц
b) перехвата или подмены данных на путях транспортировки
c) вмешательства в личную жизнь
d) поставки неприемлемого содержания

21. Причины возникновения ошибки в данных

a) Погрешность измерений
b) Ошибка при записи результатов измерений в промежуточный документ

a))Неверная интерпретация данных

c) Ошибки при переносе данных с промежуточного документа в компьютер
d) Использование недопустимых методов анализа данных
e) Неустранимые причины природного характера
f) Преднамеренное искажение данных
g) Ошибки при идентификации объекта или субъекта хозяйственной деятельности

22. К формам защиты информации не относится…

))аналитическая

a) правовая
b) организационно-техническая
c) страховая

23. Наиболее эффективное средство для защиты от сетевых атак

a) использование сетевых экранов или «firewall»
b) использование антивирусных программ
c) посещение только «надёжных» Интернет-узлов
d))использование только сертифицированных программ-броузеров при доступе к сети Интернет

24. Информация, составляющая государственную тайну не может иметь гриф…

a))«для служебного пользования»

a) «секретно»
b) «совершенно секретно»
c) «особой важности»

25. Разделы современной криптографии:

d))Симметричные криптосистемы

a) Криптосистемы с открытым ключом
b) Криптосистемы с дублированием защиты
c) Системы электронной подписи

d) Управление паролями
e) Управление передачей данных
f) Управление ключами

26. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности
a) рекомендации X.800
b) Оранжевая книга

))Закону «Об информации, информационных технологиях и о защите информации»

27. Утечка информации – это …
))несанкционированный процесс переноса информации от источника к злоумышленнику
a) процесс раскрытия секретной информации
b) процесс уничтожения информации
c) непреднамеренная утрата носителя информации

28. Основные угрозы конфиденциальности информации:
a) маскарад
b) карнавал
c) переадресовка
d) перехват данных
e) блокирование

))злоупотребления полномочиями

29. Элементы знака охраны авторского права:
a) буквы С в окружности или круглых скобках

))буквы Р в окружности или круглых скобках
b) наименования (имени) правообладателя
c) наименование охраняемого объекта
d) года первого выпуска программы

30. Защита информации обеспечивается применением антивирусных средств
a) да
b) нет

))не всегда

31. Средства защиты объектов файловой системы основаны на…
))определении прав пользователя на операции с файлами и каталогами
a) задании атрибутов файлов и каталогов, независящих от прав пользователей

32. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза

a) активная
b))пассивная

32. Преднамеренная угроза безопасности информации

))кража

a) наводнение
b) повреждение кабеля, по которому идет передача, в связи с погодными условиями
c) ошибка разработчика

33. Концепция системы защиты от информационного оружия не должна включать…

a) средства нанесения контратаки с помощью информационного оружия
b) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
c) признаки, сигнализирующие о возможном нападении

))процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

34. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

a))обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
b) реализацию права на доступ к информации»
c) соблюдение норм международного права в сфере информационной безопасности
d) выявление нарушителей и привлечение их к ответственности
e) соблюдение конфиденциальности информации ограниченного доступа
f) разработку методов и усовершенствование средств информационной безопасности

35. Выберите правильный ответ из предложенных вариантов. Что такое компьютерный вирус?

a) Прикладная программа.
b) Системная программа.

)) Программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.

c) База данных.

36. Выберите правильный ответ из предложенных вариантов. Какие существуют основные средства защиты?

a)) Резервное копирование наиболее ценных данных.
b) Аппаратные средства.
c) Программные средства
d) Все перечисленное

37. Выберите правильный ответ из предложенных вариантов. Какие существуют вспомогательные средства защиты?

a) Аппаратные средства.
b) Программные средства
c)) Аппаратные средства и антивирусные программы.
d) Все перечисленное

38. Выберите правильный ответ из предложенных вариантов. На чем основано действие антивирусной программы?

a) На ожидании начала вирусной атаки.
b)) На сравнение программных кодов с известными вирусами.
c) На удалении зараженных файлов.
d) На всех перечисленных

39. Выберите правильный ответ из предложенных вариантов. Какие программы относятся к антивирусным?

a)) AVP, DrWeb, Norton AntiVirus.
b) MS-DOS, MS Word, AVP.
c) MS Word, MS Excel, Norton Commander.
d) MS Word, MS Excel, Paint

40. Выберите правильный ответ из предложенных вариантов. Определите тип антивирусной программы. DrWeb относится

a)) Полифаги
b) Ревизоры.
c) Блокировщики.
d) Сторожа

41. По предложенному описанию определите тип вируса.Заражают файлы документов Word и Excel. Являются фактически макрокомандами, которые встраиваются в документ

a) Бутовый
b) Червь
c) Троян
d)) Макровирус

"

42. Заражение компьютерными вирусами может произойти в процессе ...

a)) работы с файлами
b) форматирования диска
c) выключения компьютера

d) печати на принтере

43. Что необходимо иметь для проверки на вирус жесткого диска?

a) защищенную программу

b) загрузочную программу

c) файл с антивирусной программой

d)) антивирусную программу, установленную на компьютер

44. Какая программа не является антивирусной?

a) AVP

b)) Defrag

c) Norton Antivirus

d) Dr Web

45. Какие программы не относятся к антивирусным?

a) программы-фаги

b) программы сканирования

c) программы-ревизоры

d) программы-детекторы

46. Как вирус может появиться в компьютере?

a)) при работе компьютера в сети

b) при решении математической задачи

c) при работе с макросами

d) самопроизвольно

47. Как происходит заражение «почтовым» вирусом?

a)) при открытии зараженного файла, присланного с письмом по e-mail

b) при подключении к почтовому серверу

c) при подключении к web-серверу, зараженному «почтовым» вирусом

d) при получении с письмом, присланном по e-mail, зараженного файла

48. Как обнаруживает вирус программа-ревизор?

a) контролирует важные функции компьютера и пути возможного заражения

b) отслеживает изменения загрузочных секторов дисков

c)) при открытии файла подсчитывает контрольные суммы и сравнивает их с данными, хранящимися в базе данных

d) периодически проверяет все имеющиеся на дисках файлы

49. Компьютерным вирусом является ...

a) программа проверки и лечения дисков

b) любая программа, созданная на языках низкого уровня

c) программа, скопированная с плохо отформатированной дискеты

d)) специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться"

50. категории компьютерных вирусов НЕ относятся

a) загрузочные вирусы
b)) type-вирусы
c) сетевые вирусы
d) файловые вирусы

51. Найдите правильные слова: компьютерные вирусы ...

a) возникают в связи со сбоями в аппаратных средствах компьютера
b)) пишутся людьми специально для нанесения ущерба пользователям персональных компьютеров
c) зарождаются при работе неверно написанных программных продуктов
d) являются следствием ошибок в операционной системе компьютера

52. Найдите отличительные особенности компьютерного вируса:

a) он обладает значительным объемом программного кода и ловкостью действий
b) компьютерный вирус легко распознать и просто удалить
c) вирус имеет способности к повышению помехоустойчивости операционной системы и к расширению объема оперативной памяти компьютера
d)) он обладает маленьким объемом, способностью к самостоятельному запуску и многократному копированию кода, к созданию помех корректной работе компьютера

53. Создание компьютерных вирусов является

a) последствием сбоев операционной системы
b) необходимым компонентом подготовки программистов
c) побочным эффектом при разработке программного обеспечения
d)) преступлением

54. Загрузочные вирусы характеризуются тем, что ...

a)) поражают загрузочные секторы дисков
b) поражают программы в начале их работы
c) запускаются при загрузке компьютера
d) изменяют весь код заражаемого файла

55. Файловый вирус ...

a) поражает загрузочные сектора дисков
b)) всегда изменяет код заражаемого файла
c) всегда меняет длину имени файла
d) всегда меняет начало и длину файла

56. Назначение антивирусных программ, называемых детекторами:

a) обнаружение и уничтожение вирусов
b)) контроль возможных путей распространения компьютерных вирусов
c) обнаружение компьютерных вирусов
d) уничтожение зараженных файлов

57. К антивирусным программам не относятся:

a) фаги
b) ревизоры
c)) интерпретаторы
d) мониторы

58. Назовите метод защиты от компьютерных вирусов:

a) отключение комптютера от электросети при малейшем подозрении на вирус
b) перезагрузка компьютера
c) вызов специалиста по борьбе с вирусами
d) установка на компьютер программы-монитора

59. Выберите правильное утверждение: сетевые вирусы ...

a) существуют и размножаются в среде локальных и глобальных сетей
b) поражают и паразитируют в файлах, в основном исполняемых файлах типов *.COM или *.EXE
c) поражают загрузочные области диска и остаются в оперативной памяти, готовые к заражению новых файлов вплоть до выключения или перезагрузки компьютера
d) существуют в среде Linux и могут поражать файлы, созданные ее приложениями

60. Какие файлы могут быть испорчены компьютерным вирусом?

a) исполняемые
b) любые
c) графические
d) загрузчик ОС, исполняемые, файлы типа *.DOC

61. Сетевые черви - это...
a) Программы, которые не изменяют файлы на дисках, а распространяются в компьютерной сети, проникают в операционную систему компьютера, находят адреса других компьютеров или пользователей и рассылают по этим адресам свои копии;
b) Вредоносные программы, действие которых заключается в создании сбоев при питании компьютера от электрической сети;
c) Программы, распространяющиеся только при помощи электронной почты;
d) Программы, которые изменяют файлы на дисках и распространяются в пределах компьютера.

62. Наиболее эффективным средством для защиты от сетевых атак является...
a) Использование сетевых экранов, или Firewall;
b) Посещение только "надёжных" Интернет-узлов;
c) Использование антивирусных программ;
d) Использование только сертифицированных программ-браузеров при доступе к сети Интернет.

63. Сжатый образ исходного текста обычно используется ...
a) В качестве ключа для шифрования текста;
b) Для создания электронно-цифровой подписи;

c) Как открытый ключ в симметричных алгоритмах;
d) Как результат шифрования текста для его отправки по незащищенному каналу.

64. Из перечисленного:
1) пароли доступа,
2) дескрипторы,
3) шифрование,
4) хеширование,
5) установление прав доступа,
6) запрет печати,
к средствам компьютерной защиты информации относятся:
a)) 1, 3, 5;
b) 1, 4, 6;
c) 2, 4, 6;
d) 4, 5, 6.

65. Принципиальным отличием межсетевых экранов (МЭ) от систем обнаружения атак (СОА) является то, что...
a) МЭ работают только на сетевом уровне, а СОА - еще и на физическом;
b) МЭ были разработаны для активной или пассивной защиты, а СОА - для активного или пассивного обнаружения;
c) МЭ были разработаны для активного или пассивного обнаружения, а СОА - для активной или пассивной защиты;
d) Отличий МЭ от СОА нет.

66. Заражение компьютерным вирусом не может произойти…
a) При открытии файла, прикрепленного к почте;
b)) При включении и выключении компьютера;
c) При копировании файлов;
d) При запуске на выполнение программного файла.

67. Электронная цифровая подпись документа позволяет решить вопрос о ____ документа(у).
a) Режиме доступа к;
b) Ценности;
c)) Подлинности;
d) Секретности.

68. Результатом реализации угроз информационной безопасности может быть…
a) Уничтожение устройств ввода/вывода;
b) Изменение конфигурации периферийных устройств;
c) Уничтожение каналов связи;
d)) Внедрение дезинформации.

69. Электронная цифровая подпись устанавливает _____ информации
a) Непротиворечивость;
b) Подлинность;
c) Объем;
d) Противоречивость.

70. Программными средствами для защиты информации в компьютерной сети являются:
1) Firewall,

2) Brandmauer,
3) Sniffer,
4) Backup.
a)) 1 и 4;
b) 2 и 3;
c) 3 и 4;
d) 1 и 2.

71. Под утечкой информации понимается...
a)) Несанкционированный процесс переноса информации от источника к злоумышленнику;
b) Процесс уничтожения информации;
c) Непреднамеренная утрата носителя информации;
d) Процесс раскрытия секретной информации.

72. Вирусы могут быть:
а) загрузочными,
б) мутантами,
в) невидимками,
г) дефектными,
д) логическими.
a) б, г, д;
b) в, г, д;
c)) а, б, в;
d) а, в, г;

73. Концепция системы защиты от информационного оружия не должна включать...
a) Признаки, сигнализирующие о возможном нападении;
b) Процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей;
c) Средства нанесения контратаки с помощью информационного оружия;
d) Механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры.

74. Троянской программой является...
a)) Программа, вредоносное действие которой выражается в удалении и/или модификации системных файлов компьютера;
b) Программа, заражающая компьютер независимо от действий пользователя;
c) Программа, проникающая на компьютер пользователя через Интернет.
d) Вредоносная программа, которая сама не размножается, а выдает себя за что-то полезное, тем самым пытаясь побудить пользователя переписать и установить на свой компьютер программу самостоятельно.

75. Программа для архивации файлов - это:
a) программа для создания резервных копий файлов

b))программа для уменьшения (сжатия) исходного объема файлов
c) программа для просмотра архивных файлов

76. Сжатый файл представляет собой:

a) файл, упакованный с помощью архиватора
b) файл, защищенный от копирования
c) файл, защищенный от несанкционированного доступа

77.Какое из названных действий можно произвести со сжатым файлом:
a) запустить на выполнение
b)) распаковать
c) просмотреть

78. Компьютерные вирусы:
a) зарождаются при работе неверно написанных программных продуктов
b)) создаются людьми специально для нанесения ущерба ПК
c) являются следствием ошибок в операционной системе

79. Отличительными особенностями компьютерного вируса являются:
a) значительный объем программного кода
b)) маленький объем и способность к самостоятельному запуску и созданию
c) помехи корректной работе компьютера
d) необходимость запуска со стороны пользователя

80. Загрузочные вирусы:
a) изменяют весь код заражаемого файла
b)) поражают загрузочные сектора дисков
c) запускаются при запуске компьютера

81. Файловые вирусы:
a) запускаются при запуске компьютера
b) поражают программы в начале их работы
c) поражают загрузочные сектора дисков
d)) изменяют весь код заражаемого файла

82. Какого типа файлы лучше всего сжимаются:
a) текстовые
b)) графические
c) исполняемые

83. Чему равен коэффициент сжатия, если начальный объем составлял 250 Кбайт, после сжатия 50 Кбайт
a) 50%
b)) 20%
c) 25%

84. Какие мероприятия не являются административными при обеспечении мер безопасности:
a) пропускной режим
b) контроль журналов работы
c) контроль смены паролей
d)) выявление уязвимостей в системе защиты
e) порядок хранения документов

85. Сигнатурный метод антивирусной проверки заключается в …
a))анализе поведения файла в разных условиях

b) сравнении файла с известными образцами вирусов
c) отправке файлов на экспертизу в компанию-производителя антивирусного средства
d) анализе кода на предмет наличия подозрительных команд

86. Косвенное проявление наличия вредоносной программы на компьютере
a))неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
b) неожиданно появляющееся всплывающее окно с текстом порнографического содержания
c) неожиданное отключение электроэнергии
d) неожиданное уведомление антивирусной программы об обнаружении вируса
e) неожиданное самопроизвольное завершение работы почтового агента

87. Антиспамовая программа, установленная на домашнем компьютере, служит для …
a) корректной установки и удаления прикладных программ
b) обеспечения регулярной доставки антивирусной программе новых антивирусных баз
c) защиты компьютера от хакерских атак
d))защиты компьютера от нежелательной и/или незапрошенной корреспонденции

88. Положения, которые целесообразно вынести в инструкцию по работе за компьютером, разрабатываемую для компьютерного класса средней школы
a) не открывать почтовые сообщения от незнакомых отправителей
b))перед работой (копированием, открытие, запуском) с файлами, размещенными на внешнем носителе (компакт-диск, дискета, флеш-накопитель) нужно проверить их на отсутствие вирусов
c) перед работой с любым объектом, загруженным из Интернета, его следует проверить на вирусы
d) при работе в Интернет не соглашаться на предложения загрузить и/или установить неизвестную программу
e) не открывать почтовые сообщения, содержащие вложения
f) не пользоваться определенными видами браузеров

89. Цель создания анонимного SMTP-сервера – для …
a) размещения на них сайтов с порнографической или другой запрещенной информацией
b))рассылки спама
c) создания ботнета
d) распределенных вычислений сложных математических задач

90. Метаморфизм – это …
a))метод маскировки от антивирусов с помощью шифрования
b) метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки

c) создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд
d) создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд

91. Деятельность клавиатурных шпионов
a) находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают своему хозяину
b))находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором
c) находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими
d) передают хозяину марку и тип используемой пользователем клавиатуры

92. Обязательные свойства любого современного антивирусного комплекса
a) не мешать выполнению основных функций компьютера
b) не занимать много системных ресурсов
c) не занимать канал Интернет
d) надежно защищать от вирусов
e))быть кроссплатформенным (работать под управлением любой операционной системы)
f) интегрироваться в браузер

93. Задача, выполняющая модуль планирования, входящий в антивирусный комплекс
a))настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)
b) определения параметров взаимодействия различных компонентов антивирусного комплекса
c) определения областей работы различных задач поиска вирусов
d) настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса

94. Логические бомбы относятся к классу …
a) файловых вирусов
b) макровирусов
c) сетевых червей
d) троянов
e))условно опасных программ

95. К какому типу Использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести к … методам антивирусной защиты.

a) теоретическим
b))практическим
c) организационным
d) техническим

96. Использование брандмауэров относят к … методам антивирусной защиты.

a) теоретическим
b) практическим
c))организационным
d) техническим

97. Свойство вируса, позволяющее называться ему загрузочным – способность …

a))заражать загрузочные сектора жестких дисков
b) заражать загрузочные дискеты и компакт-диски
c) вызывать перезагрузку компьютера-жертвы
d) подсвечивать кнопку Пуск на системном блоке

98. К классу условно опасных относятся программы …

a) о которых нельзя однозначно сказать, что они вредоносны
b) последствия выполнения которых нельзя предугадать
c) которые можно выполнять только при наличии установленного антивирусного программного обеспечения
d))характеризующиеся способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов. В остальное время они безвредны

99. Типы методов антивирусной защиты

a) теоретические
b) практические
c) организационные
d) технические
e))программные

100. Главное преимущество встроенного в Microsoft Windows XP (с установленным Service Pack 2) брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами

a))более ясный и интуитивно понятный интерфейс
b) отсутствие необходимости отдельно покупать его и устанавливать
c) наличие более полного функционала
d) возможность более точно задавать исключения

101. Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет

a) трудности с регулярным автоматическим получением новых антивирусных баз
b) невозможность использовать антиспамовую программу в режиме реального времени
c) ложные срабатывания в работе персонального брандмауэра
d))невозможность запуска антивирусной проверки в режиме реального времени

102. Брандмауэр (firewall) – это программа, …

a))которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
b) которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
c) на основе которой строится система кэширования загружаемых веб-страниц
d) реализующая простейший антивирус для скриптов и прочих использующихся в Интернет активных элементов

103. Преимущества сигнатурного метода антивирусной проверки над эвристическим

a) более надежный
b) существенно менее требователен к ресурсам
c) не требует регулярного обновления антивирусных баз
d))позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

104. Типы троянов:

a) клавиатурные шпионы
b) похитители паролей
c) дефрагментаторы дисков
d))утилиты скрытого удаленного управления
e) логические бомбы
f) шутки
g) вирусные мистификации

105. Вирус – это программа, способная…

a))создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению
b) нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети
c) нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

106. Стадии жизненного цикла классического трояна

a))проникновение на чужой компьютер
b) активация
c) поиск объектов для заражения
d) подготовка копий
e) внедрение копий
f) выполнение вредоносных действий

107. Трояны классифицируются по …
a) методу размножения
b))методу распространения
c) методу маскировки
d) типу вредоносной нагрузки

108. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности
a))уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer
b) уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer
c) возможность установить отличную от www.msn.com стартовую страницу
d) возможность одновременно работать в нескольких окнах

109. Преимущества эвристического метода антивирусной проверки над сигнатурным
a) более надежный
b) существенно менее требователен к ресурсам
c))не требует регулярного обновления антивирусных баз
d) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

110. Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает …
a))явные проявления
b) косвенные проявления
c) материальные проявления
d) скрытые проявления

111. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.
a))да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы
b) да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы,

которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

c) нет

112. Скрытые проявлениям вирусного заражения:

a) наличие на рабочем столе подозрительных ярлыков
b))наличие в оперативной памяти подозрительных процессов
c) наличие на компьютере подозрительных файлов
d) подозрительная сетевая активность
e) неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
f) неожиданное уведомление антивирусной программы об обнаружении вируса

113. Основная задача, которую решает антивирусная проверка в режиме реального времени

a))обеспечение непрерывности антивирусной проверки
b) обеспечение невмешательства в процесс деятельности других программ
c) обеспечение взаимодействия между пользователем и антивирусной программой
d) предоставление возможности глубокой проверки заданных объектов

114. Подозрительная сетевая активность может быть вызвана …

a) сетевым червем
b))P2P-червем
c) трояном
d) логической бомбой

115. Необходимость модуля обновления для любого современного антивирусного средства – для …

a) доставки сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу
b) взаимодействия антивирусной программы с сайтом компании-производителя
c))подключения антивирусных баз к антивирусной программе
d) обеспечения взаимодействия операционной системы с антивирусным комплексом

116. Сколько процентов электронных писем являются Спамом?

a))10;
b) 30;
c) 50;
d) 70;
e) 90.

117. К каким ежегодным убыткам приводят спамы (млрд. долл. США)?

a))20;

b) 40;
c) 60;
d) 80;
e) 100.

118. В 2003 году ФСБ пресечено попыток проникновения в информационные ресурсы органов государственной власти России около (раз):

a) 10;

b) 100;
c) 1 000;
d) 10 000;
e) 100 000.

119. Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?

a) 2;

b) 3;
c) 4;
d) 5;
e) 6.

120. Активный перехват информации это перехват, который:

a))заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

121. Пассивный перехват информации это перехват, который:

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d))осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

122. Аудиоперехват перехват информации это перехват, который:

a))заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

123. Просмотр мусора это перехват информации, который:
a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c))неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

124. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
a) активный перехват;

b) пассивный перехват;
c))аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

125. Перехват, который осуществляется путем использования оптической техники называется:
a) активный перехват;

b) пассивный перехват;
c) аудиоперехват;
d))видеоперехват;
e) просмотр мусора.

126. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
a) активный перехват;

b))пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

127. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:
a) активный перехват;

b) пассивный перехват;
c) аудиоперехват;

d))видеоперехват;
e) просмотр мусора.

128. Перехват, который неправомерно использует технологические отходы информационного процесса называется:

a) активный перехват;

b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e))просмотр мусора.

129. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?

a) “За дураком”;

b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

130. Как называется способ несанкционированного доступа к информации, который заключается в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме?

a) “За дураком”;

b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

131. Как называется способ несанкционированного доступа к информации, который заключается в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе?

a) “За дураком”;

b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

132. Как называется способ несанкционированного доступа к информации, который заключается в отыскании участков программ, имеющих ошибку или неудачную логику построения?

a) “За дураком”;

b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

133. Как называется способ несанкционированного доступа к информации, который заключается в нахождении злоумышленником уязвимых мест в ее защите?

a) “За дураком”;

b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

134. Способ несанкционированного доступа к информации “За дураком” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;

b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

135. Способ несанкционированного доступа к информации “Брешь” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;

b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

136. Способ несанкционированного доступа к информации “Компьютерный абордаж” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;

b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;

e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

137. Способ несанкционированного доступа к информации “За хвост” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;

b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

138. Способ несанкционированного доступа к информации “Неспешный выбор” заключается в:

a))отыскании участков программ, имеющих ошибку или неудачную логику построения;

b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

139. Хакер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;

b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c))Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохого игрока в гольф, дилетанта;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

140. Фракер?

a))Это лицо, которое взламывает интрасеть в познавательных целях;

b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

141. Кракер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;

b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e)))Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

142. Фишер?

a))Это лицо, которое взламывает интрасеть в познавательных целях;

b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

143. Скамер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;

b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d)))Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

144. Спамер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;

b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d))Это тот, от кого приходят в наши почтовые ящики не запрошенные рассылки;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

145. Лицо, которое взламывает интрасеть в познавательных целях это:

a) скамер;

b) хакер;
c)))фишер;
d) фракер;
e) кракер.

146. Мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных это:
a) скамер;

b) хакер;
c) фишер;
d) фракер;
e))кракер.

147. Лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО это:
a) скамер;

b) хакер;
c) фишер;
d) фракер;
e) кракер.

148. Так в XIX веке называли плохих игроков в гольф, дилетантов это:
a) скамер;

b) хакер;
c) фишер;
d))фракер;
e) кракер.

149. Мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию это:
a) скамер;

b))хакер;
c) фишер;
d) фракер;
e) кракер.

150. От них приходят в наши почтовые ящики не запрошенные рассылки это:
a) скамер;

b) хакер;
c))спамер;
d) фракер;
e) кракер.

151. Защита информации это:
a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b))преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

152. Информационные процессы это:
a))процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

153. Шифрование информации это:
a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b))преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

154. Доступ к информации это:
a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d))совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

155. Защита информации от утечки это деятельность по предотвращению:
a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником,

владельцем информации прав или правил доступа к защищаемой информации;

b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d))неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

156. Защита информации от несанкционированного воздействия это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b))воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

157. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:

a))получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

158. Защита информации от разглашения это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

159. Защита информации от несанкционированного доступа это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d))неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

160. Субъект доступа к информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c))субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

161. Носитель информации это:
    a))физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
    b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
    c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
    d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
    e) участник правоотношений в информационных процессах.

162. Собственник информации это:
    a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
    b))субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
    c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
    d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
    e) участник правоотношений в информационных процессах.

163. Владелец информации это:
    a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
    b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
    c))субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
    d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
    e) участник правоотношений в информационных процессах.

164. Пользователь (потребитель) информации это:
    a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d))субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

165. Естественные угрозы безопасности информации вызваны:
a) деятельностью человека;

b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
c))воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d) корыстными устремлениями злоумышленников;
e) ошибками при действиях персонала.

166. Искусственные угрозы безопасности информации вызваны:
a) деятельностью человека;

b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d))корыстными устремлениями злоумышленников;
e) ошибками при действиях персонала.

167. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) физическое разрушение системы путем взрыва, поджога и т.п.;

b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e))неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

168. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) физическое разрушение системы путем взрыва, поджога и т.п.;

b) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
c))изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

169. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) неумышленная порча носителей информации;
e))перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

170. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) физическое разрушение системы путем взрыва, поджога и т.п.;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

171. К основным непреднамеренным искусственным угрозам АСОИ относится:
a))физическое разрушение системы путем взрыва, поджога и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

172. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d))неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

173. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) физическое разрушение системы путем взрыва, поджога и т.п.;

b))разглашение, передача или утрата атрибутов разграничения доступа;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

174. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) физическое разрушение системы путем взрыва, поджога и т.п.;

b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e))проектирование архитектуры системы, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

175. К основным непреднамеренным искусственным угрозам АСОИ относится:
a))игнорирование организационных ограничений при работе в системе;

b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) физическое разрушение системы путем взрыва, поджога и т.п..

176. К основным непреднамеренным искусственным угрозам АСОИ относится:
a))изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) вход в систему в обход средств защиты;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) физическое разрушение системы путем взрыва, поджога и т.п..

177. К основным непреднамеренным искусственным угрозам АСОИ относится:
a) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

b) некомпетентное использование, настройка или отключение средств защиты;
c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

e) физическое разрушение системы путем взрыва, поджога и т.п..

178. К основным непреднамеренным искусственным угрозам АСОИ относится:
   a))изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
   b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
   c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
   d) пересылка данных по ошибочному адресу абонента;
   e) физическое разрушение системы путем взрыва, поджога и т.п..

179. К основным непреднамеренным искусственным угрозам АСОИ относится:
   a))ввод ошибочных данных;
   b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
   c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
   d) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
   e) физическое разрушение системы путем взрыва, поджога и т.п..

180. К основным непреднамеренным искусственным угрозам АСОИ относится:
   a))перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
   b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
   c) неумышленное повреждение каналов связи;
   d) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
   e) физическое разрушение системы путем взрыва, поджога и т.п..

181. К основным преднамеренным искусственным угрозам АСОИ относится:
   a))неправомерное отключение оборудования или изменение режимов работы устройств и программ;
   b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
   c) физическое разрушение системы путем взрыва, поджога и т.п.;
   d) игнорирование организационных ограничений (установленных правил) при работе в системе;
   e) пересылка данных по ошибочному адресу абонента.

182. К основным преднамеренным искусственным угрозам АСОИ относится:
   a))отключение или вывод из строя систем электропитания, охлаждения и вентиляции, линий связи и т.п.;

b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) пересылка данных по ошибочному адресу абонента.

183. К основным преднамеренным искусственным угрозам АСОИ относится:
a))пересылка данных по ошибочному адресу абонента;

b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) действия по дезорганизации функционирования системы (изменение режимов работы, забастовка, саботаж персонала, и т.п.).

184. К основным преднамеренным искусственным угрозам АСОИ относится:
a))пересылка данных по ошибочному адресу абонента;

b) внедрение агентов в число персонала системы, в том числе в административную группу, отвечающую за безопасность;
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

185. К основным преднамеренным искусственным угрозам АСОИ относится:
a))пересылка данных по ошибочному адресу абонента;

b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) вербовка персонала или отдельных пользователей, имеющих необходимые полномочия;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

186. К основным преднамеренным искусственным угрозам АСОИ относится:
a))пересылка данных по ошибочному адресу абонента;

b) игнорирование организационных ограничений (установленных правил) при работе в системе;

c) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

187. К основным преднамеренным искусственным угрозам АСОИ относится:
a))пересылка данных по ошибочному адресу абонента;

b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

188. К основным преднамеренным искусственным угрозам АСОИ относится:
a))перехват данных, передаваемых по каналам связи;

b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) пересылка данных по ошибочному адресу абонента;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

189. К основным преднамеренным искусственным угрозам АСОИ относится:
a))разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) пересылка данных по ошибочному адресу абонента;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) хищение носителей информации.

190. К основным преднамеренным искусственным угрозам АСОИ относится:
a))разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

b))игнорирование организационных ограничений (установленных правил) при работе в системе;
c) несанкционированное копирование носителей информации;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

e) пересылка данных по ошибочному адресу абонента.

191. К основным преднамеренным искусственным угрозам АСОИ относится:
   a))разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
   b))хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
   c) игнорирование организационных ограничений (установленных правил) при работе в системе;
   d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
   e) пересылка данных по ошибочному адресу абонента.

192. К основным преднамеренным искусственным угрозам АСОИ относится:
   a))чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
   b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
   c) игнорирование организационных ограничений (установленных правил) при работе в системе;
   d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
   e) пересылка данных по ошибочному адресу абонента.

193. К основным преднамеренным искусственным угрозам АСОИ относится:
   a))неправомерное отключение оборудования или изменение режимов работы устройств и программ;
   b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
   c) игнорирование организационных ограничений (установленных правил) при работе в системе;
   d) незаконное получение паролей и других реквизитов разграничения доступа;
   e) пересылка данных по ошибочному адресу абонента.

194. К основным преднамеренным искусственным угрозам АСОИ относится:
   a))неправомерное отключение оборудования или изменение режимов работы устройств и программ;
   b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
   c) игнорирование организационных ограничений (установленных правил) при работе в системе;
   d) пересылка данных по ошибочному адресу абонента;
   e) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики.

195. К основным преднамеренным искусственным угрозам АСОИ относится:
    a))неправомерное отключение оборудования или изменение режимов работы устройств и программ;
    b))вскрытие шифров криптозащиты информации;
    c) игнорирование организационных ограничений (установленных правил) при работе в системе;
    d) пересылка данных по ошибочному адресу абонента;
    e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

196. К основным преднамеренным искусственным угрозам АСОИ относится:
    a))неправомерное отключение оборудования или изменение режимов работы устройств и программ;
    b) пересылка данных по ошибочному адресу абонента;
    c) игнорирование организационных ограничений (установленных правил) при работе в системе;
    d))внедрение аппаратных спецвложений, программных "закладок" и "вирусов";
    e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

197. К основным преднамеренным искусственным угрозам АСОИ относится:
    a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
    b))незаконное подключение к линиям связи с целью работы "между строк";
    c) игнорирование организационных ограничений (установленных правил) при работе в системе;
    d) пересылка данных по ошибочному адресу абонента;
    e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

198. К основным преднамеренным искусственным угрозам АСОИ относится:
    a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
    b) игнорирование организационных ограничений (установленных правил) при работе в системе;
    c))незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему;
    d) пересылка данных по ошибочному адресу абонента;
    e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

199. К внутренним нарушителям информационной безопасности относится:

a) клиенты;

b))пользователи системы;
c) посетители;
d) любые лица, находящиеся внутри контролируемой территории;
e) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.

200. К внутренним нарушителям информационной безопасности относится:
a) клиенты;

b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) посетители;
d) любые лица, находящиеся внутри контролируемой территории;
e))персонал, обслуживающий технические средства.

201. К внутренним нарушителям информационной безопасности относится:
a))сотрудники отделов разработки и сопровождения ПО;

b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) посетители;
d) любые лица, находящиеся внутри контролируемой территории;
e) клиенты.

202. К внутренним нарушителям информационной безопасности относится:
a))посетители;

b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) технический персонал, обслуживающий здание;
d) любые лица, находящиеся внутри контролируемой территории;
e) клиенты.

203. К внутренним нарушителям информационной безопасности относится:
a) посетители;

b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) любые лица, находящиеся внутри контролируемой территории;
d))сотрудники службы безопасности;
e) клиенты.

204. К внутренним нарушителям информационной безопасности относится:
a) посетители;

b))руководители различных уровней;
c) любые лица, находящиеся внутри контролируемой территории;
d) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
e) клиенты.

205. К посторонним лицам нарушителям информационной безопасности относится:

a) пользователи;

b) персонал, обслуживающий технические средства;
c))клиенты;
d) технический персонал, обслуживающий здание;
e) сотрудники службы безопасности.

206. К посторонним лицам нарушителям информационной безопасности относится:

a))пользователи;

b) персонал, обслуживающий технические средства;
c) технический персонал, обслуживающий здание;
d) посетители;
e) сотрудники службы безопасности.

207. К посторонним лицам нарушителям информационной безопасности относится:

a))представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

b) персонал, обслуживающий технические средства;
c) технический персонал, обслуживающий здание;
d) пользователи;
e) сотрудники службы безопасности.

208. К посторонним лицам нарушителям информационной безопасности относится:

a))сотрудники службы безопасности;

b) персонал, обслуживающий технические средства;
c) технический персонал, обслуживающий здание;
d) пользователи;
e) представители конкурирующих организаций.

209. К посторонним лицам нарушителям информационной безопасности относится:

a) сотрудники службы безопасности;

b))лица, нарушившие пропускной режим;
c) технический персонал, обслуживающий здание;
d) пользователи;
e) персонал, обслуживающий технические средства.

210. По характеру воздействия удаленные атаки делятся на:

a))условные и безусловные;

b) атаки с обратной связью и без обратной связи;
c) внутрисегментные и межсегментные;
d) пассивные и активные;
e) атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном.

211. По цели воздействия удаленные атаки делятся на:

a) условные и безусловные;

b) атаки с обратной связью и без обратной связи;
c))внутрисегментные и межсегментные;
d) пассивные и активные;
e) атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

212. По условию начала осуществления воздействия удаленные атаки делятся на:
a) условные и безусловные;

b))атаки с обратной связью и без обратной связи;
c) внутрисегментные и межсегментные;
d) пассивные и активные;
e) атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

213. По наличию обратной связи с атакуемым объектом удаленные атаки делятся на:
a) условные и безусловные;

b) атаки с обратной связью и без обратной связи;
c) внутрисегментные и межсегментные;
d) пассивные и активные;
e) атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

214. По расположению субъекта атаки относительно атакуемого объекта удаленные атаки делятся на:
a) условные и безусловные;

b) атаки с обратной связью и без обратной связи;
c) внутрисегментные и межсегментные;
d) пассивные и активные;
e))атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

215. По уровню эталонной модели взаимосвязи открытых систем OSI Международной организации стандартизации (ISO) удаленные атаки делятся на:
a) условные и безусловные;

b) атаки с обратной связью и без обратной связи;
c) внутрисегментные и межсегментные;
d) пассивные и активные;
e))атаки, которые могут реализовываться на всех семи уровнях.

216. Атака, которая позволяет изучить логику работы сети:
a))подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

217. Атака позволяющая перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c))анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

218. Атака эффективно реализующаяся в системах, где применяются нестойкие алгоритмы идентификации/аутентификации хостов, пользователей:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

219. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

220. Атака, которая использует недостатки алгоритмов удаленного поиска (SAP(NetWare), и DNS (Internet)…):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

221. Атака, которая позволяет воздействовать на перехваченную информацию (проводить селекцию потока информации):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c))анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

222. Атака, которая позволяет воздействовать на перехваченную информацию (модифицировать информацию):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

223. Атака, которая позволяет воздействовать на перехваченную информацию (подменять информацию):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

224. Атака, результатом осуществления которой может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

225. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

226. Атака, которая заключается в передаче с одного адреса такого количества запросов на подключение к атакуемому хосту, какое максимально может "вместить" трафик:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

227. Атака, которая заключается в запуске на атакуемом компьютере программы "сетевого шпиона":

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

228. Атака, которая заключается в запуске на атакуемом компьютере программы "сетевого шпиона":

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

229. По среде обитания классические вирусы разделяются на:

a) паразитические;

b) компаньоны;
c) файловые;
d) ссылки;
e) перезаписывающие.

230. По среде обитания классические вирусы разделяются на:

a) загрузочные;

b) компаньоны;
c) паразитические;
d) ссылки;
e) перезаписывающие.

231. По среде обитания классические вирусы разделяются на:

a) ссылки;

b) компаньоны;
c) паразитические;
d) макровирусы;
e) перезаписывающие.

232. По среде обитания классические вирусы разделяются на:

a) ссылки;

b) компаньоны;
c) скриптовые;
d) паразитические;
e) перезаписывающие.

233. По способу заражения классические вирусы разделяются на:

a) файловые;

b) загрузочные;
c) макровирусы;
d) скриптовые;
e) перезаписывающие.

234. По способу заражения классические вирусы разделяются на:
a) файловые;

b) паразитические;
c) макровирусы;
d) скриптовые;
e) загрузочные.

235. По способу заражения классические вирусы разделяются на:
a) компаньоны;

b) файловые;
c) макровирусы;
d) скриптовые;
e) загрузочные.

236. По способу заражения классические вирусы разделяются на:
a) скриптовые;

b) файловые;
c) макровирусы;
d) ссылки;
e) загрузочные.

237. Сетевой червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе:
a) IM-Worm;

b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

238. Сетевые черви используют способ распространения – рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL на файл, расположенный на каком-либо веб-сервере:
a) IM-Worm;

b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

239. Сетевые черви распространяются двумя способами по IRC-каналам. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть:
a) IM-Worm;

b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

240. Сетевой червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись, при этом червь или перебирает доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищет компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ:

a) IM-Worm;

b) IRC-Worm;
c) Net-Worm;
d))P2P-Worm;
e) Email-Worm.

241. Сетевые черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос, в результате чего код червя проникает на компьютер-жертву:

a))IM-Worm;

b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

242. Для внедрения в сеть сетевому червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальном компьютере. Всю остальную работу по распространению вируса сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера:

1. IM-Worm;
2. IRC-Worm;
3.)Net-Worm;
4. P2P-Worm;
5. Email-Worm.

243. Сетевой червь имитирует сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечает положительно – при этом червь предлагает для скачивания свою копию:

a) IM-Worm;

b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

244. Троянские утилиты удаленного администрирования:

a))Trojan-PSW;

b) Trojan-Clicker;
c) Backdoor;

d) Trojan-Downloader;
e) Trojan-Dropper.

245. Троянские программы для воровства паролей:
a) Trojan-PSW;

b) Trojan-Clicker;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

246. Троянские программы для доставки вредоносных программ:
a) Trojan-PSW;

b) Trojan-Clicker;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

247. Троянские программы инсталляторы вредоносных программ:
a) Trojan-PSW;

b) Trojan-Clicker;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

248. Троянские шпионские программы:
a) Trojan-PSW;

b) Trojan-Spy;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

249. Троянские программы, применяемые для организации несанкционированных обращений к интернет-ресурсам:
a) Trojan-PSW;

b) Trojan-Spy;
c) Trojan-Clicker;
d) Trojan-Downloader;
e) Trojan-Dropper.

250. Троянские программы, скрытно осуществляющие анонимный доступ к различным интернет-ресурсам, обычно используются для рассылки спама:
a) Trojan-PSW;

b) Trojan-Spy;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

251. Троянские программы, предназначенные для оповещение об успешной атаке:

a) Trojan-PSW;

b) Trojan-Spy;
c) Trojan-Proxy;
d) Trojan-Notifier;
e) Trojan-Dropper.

252. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

a) черный пиар;

b))фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

253. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

a))черный пиар;

b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

254. Спам, написанный от имени реальных или вымышленных лиц, обычно граждан стран с нестабильной экономической ситуацией, воспринимаемых публикой как рассадник коррупции:

a) черный пиар;

b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

255. Спам инициирует письма, содержащие сведения о потенциальной опасности или просьбы о помощи жертвам стихийных бедствий:

a) черный пиар;

b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

256. Спам периодически проводит рассылки нерекламных сообщений:

a) черный пиар;

b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

257. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

a))детектор;

b) доктор;
c) сканер;
d) ревизор;
e) сторож.

258. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

a) детектор;

b) доктор;
c) сканер;
d))ревизор;
e) сторож.

259. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

a) детектор;

b) доктор;
c))сканер;
d) ревизор;
e) сторож.

260. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

a) детектор;

b) доктор;
c) сканер;
d) ревизор;
e) сторож.

261. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

a) детектор;

b) доктор;
c) сканер;
d) ревизор;
e) сторож.

262. Антивирус модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся:

a) детектор;

b) доктор;
c) сканер;

d) ревизор;
e) иммунизатор.

263. Антивирусный сканер:
a) обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
b) находит зараженные вирусами файлы, "лечит" их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;
c) запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
d) просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
e) обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

264. Антивирусный детектор:
a) обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
b) находит зараженные вирусами файлы, "лечит" их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;
c) запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
d) просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
e) обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

265. Антивирусный доктор:
a) обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
b) находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
c) запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
d) просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
e) обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

266. Антивирусный ревизор:
a) обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
b) находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
c) запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
d) просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;

e) обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

267. Антивирусный сторож:

a) обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;

b) находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
c) запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
d) просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
e) обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

268. Антивирусный иммунизатор:

a) обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;

b) находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
c) модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся;
d) просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
e) обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

269. Метод защиты информации ограничение доступа заключается в:

a))контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

b) создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
c) разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
d) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
e) проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

270. Метод защиты информации контроль доступа к аппаратуре заключается в:

a))контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

b) создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;

c) разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
d) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
e) проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

271. Метод защиты информации разграничение и контроль доступа к информации заключается в:

a) контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

b) создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
c) разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
d) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
e) проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

272. Метод защиты информации предоставление привилегий на доступ заключается в:

a) контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

b) создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
c) разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
d) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
e) проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

273. Метод защиты информации идентификация и установление подлинности заключается в:

a) контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

b) создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
c) разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;

d) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
e) проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

274. Шифрование методом подстановки:
a))символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;

b) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
c) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
d) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
e) замена слов и предложений исходной информации шифрованными.

275. Шифрование методом перестановки:
a) символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;

b) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
c) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
d) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
e) замена слов и предложений исходной информации шифрованными.

276. Шифрование методом гаммирования:
a) символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;

b) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
c) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
d) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
e) замена слов и предложений исходной информации шифрованными.

277. Шифрование методом аналитических преобразований:
a) символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;

b) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
c) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
d) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;

e) замена слов и предложений исходной информации шифрованными.

278. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

a) гаммирования;

b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

280. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

a) гаммирования;

b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

281. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

a) гаммирования;

b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

282. Шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор, это метод:

a) гаммирования;

b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

283. Шифр DES это:

a) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;

b) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;
c) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
d) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
e) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

284. Шифр IDEA это:

a) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;

b) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;
c) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
d) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
e) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

285. Шифр RC2 или RC4 это:

a) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;

b) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;
c) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
d) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
e) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

286. Шифр RSA это:

a) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;

b) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;
c) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
d) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
e) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

287. Шифр ГОСТ 28147-89 это:

a) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;

b) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;
c) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
d) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
e) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

288. Система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки – это шифр:

a) IDEA;

b) RSA;
c) ГОСТ 28147-89;
d) RC2 или RC4;
e) DES.

289. Система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители – это шифр:

a) IDEA;

b) RSA;
c) ГОСТ 28147-89;
d) RC2 или RC4;
e) DES.

290. Блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны – это шифр:

a) IDEA;

b) RSA;
c) ГОСТ 28147-89;
d) RC2 или RC4;
e) DES.

291. Шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами – это шифр:

a) IDEA;

b) RSA;
c) ГОСТ 28147-89;
d) RC2 или RC4;
e) DES.

292. Симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит – это шифр:

a) IDEA;

b) RSA;
c) ГОСТ 28147-89;
d) RC2 или RC4;
e) DES.

293. Сертификации подлежат:

a) средства криптографической защиты информации;

b) средства выявления закладных устройств и программных закладок;
c) защищенные технические средства обработки информации;
d) защищенные информационные системы и комплексы телекоммуникаций;
e) все вышеперечисленные средства.

294. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

a) индивидуальные субъекты должны идентифицироваться;

b) контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
c) необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
d) вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
e) гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

295. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

a) управляющие доступом метки должны быть связаны с объектами;

b) контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
c) индивидуальные субъекты должны идентифицироваться;
d) вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
e) гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

296. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:

a) управляющие доступом метки должны быть связаны с объектами;

b) необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
c) индивидуальные субъекты должны идентифицироваться;
d) вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
e) гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

297. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:

a) управляющие доступом метки должны быть связаны с объектами;

b) необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
c) гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений;
d) вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
e) контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

290. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Гарантии:

a) управляющие доступом метки должны быть связаны с объектами;

b) необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
c) индивидуальные субъекты должны идентифицироваться;
d) вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
e) контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

291. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Гарантии:

a) управляющие доступом метки должны быть связаны с объектами;

b) защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений;
c) индивидуальные субъекты должны идентифицироваться;
d) необходимо иметь явную и хорошо определенную систему обеспечения безопасности;

e) контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

292. В стандарте США «Оранжевой книге» минимальная защита это группа:

a) A;

b) B;
c) C;
d) D;
e) E.

293. В стандарте США «Оранжевой книге» индивидуальная защита это группа:

a) A;

b) B;
c) C;
d) D;
e) E.

294. В стандарте США «Оранжевой книге» мандатная защита это группа:

a) A;

b) B;
c) C;
d) D;
e) E.

295. В стандарте США «Оранжевой книге» верифицированная защита это группа:

a) A;

b) B;
c) C;
d) D;
e) E.

296. В стандарте США «Оранжевой книге» системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов, группа:

a) A;

b) B;
c) C;
d) D;
e) E.

297. В стандарте США «Оранжевой книге» системы, обеспечивающие разделение пользователей и данных, группа:

a) A1;

b) B1;
c) B2;
d) C1;
e) C2.

298. В стандарте США «Оранжевой книге» системы, осуществляющие не только разделение пользователей, но и разделение их по осуществляемым действиям, группа:

a) A1;

b) B1;
c) B2;
d) C1;
e) C2.

299. В стандарте США «Оранжевой книге» системы, дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным и средства мандатного управления доступом ко всем поименованным субъектам и объектам, группа:

a) A1;

b) B1;
c) B2;
d) C1;
e) C2.

300. В стандарте США «Оранжевой книге» системы, дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным и средства мандатного управления доступом ко всем поименованным субъектам и объектам, группа:

a) A1;

b) B1;
c) B2;
d) C1;
e) C2.