

1602_Rus_Q2017_Yekun imtahan testinin sualları**Fənn : 1602 İnformasiya sistemlərində təhlükəsizliyin təminatı**

1 Под ИБ понимают

- ☐ защиту информации искусственного характера
- ☐ защиту информации от компьютерных вирусов
- ☐ защиту от несанкционированного доступа
- ☒ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера,
- ☐ защиту от санкционированного доступа

2 В чем состоит задача криптографа?

- ☐ осуществление специально разработанными программами перехвата имени и пароля
- ☐ Определение файлов, из которых удалена служебная информация
- ☐ взломать систему защиты
- ☒ обеспечить конфиденциальность и аутентификацию передаваемых сообщений,
- ☐ взломать систему защиты

3 Согласно Оранжевой книге минимальную защиту имеет группа критериев

- ☐ A
- ☐ B
- ☐ A
- ☒ D;
- ☐ C

4 Согласно Оранжевой книге дискреционную защиту имеет группа критериев

- ☐ E
- ☐ B
- ☐ A
- ☒ C;
- ☐ D

5 Согласно Европейским критериям формальное описание функций безопасности требуется на уровне

- ☐ E1
- ☐ E5
- ☐ E4
- ☒ E;6
- ☐ E7

6 Согласно Европейским критериям предъявляет повышенные требования и к целостности, и к конфиденциальности информации класс

- ☐ F-IE
- ☐ F-AV
- ☐ F-DI
- ☒ F-DX
- ☐ F-IN

7 Что такое целостность информации?

- ☐ Свойство информации, заключающееся в ее несуществовании в виде единого набора файлов
- ☐ Свойство информации, заключающееся в ее существовании в виде единого набора файлов

- ☐ Свойство информации, заключающееся в возможности изменения только единственным пользователем
- ☐ Свойство информации, заключающееся в возможности ее изменения любым субъектом
- ☒ Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию.)

8 Согласно Европейским критериям минимальную адекватность обозначает уровень

- ☐ E2
- ☐ E6
- ☐ E7
- ☒ E;0
- ☐ E1

9 Совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

- ☐ актуальностью
- ☐ [yeni savab]
- ☐ целостностью
- ☐ доступностью
- ☒ ;качеством информации
- ☐ актуальностью информации

10 С точки зрения ГТк основной задачей средств безопасности является обеспечение

- ☐ простоты
- ☐ сохранности информации
- ☐ простоты реализации
- ☒ защиты от НСД;
- ☐ надежности функционирования

11 Программный модуль, кото–рый имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа

- ☐ аудит
- ☐ заместитель
- ☐ перехватчик
- ☒ имита;тор
- ☐ фильтр

12 С помощью закрытого ключа информация

- ☐ зашифровывается
- ☐ транслируется
- ☒ расшифровывае;тся
- ☐ шифруется
- ☐ копируется

13 Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

- ☐ фильтр
- ☐ аудит
- ☐ идентификация
- ☒ аутенти;фикация
- ☐ авторизация

14 При полномочной политике безопасности совокупность меток с одинаковыми значениями образует

- ☐ уровень равной доступности
- ☐ область равного доступа
- ☐ область равной критичности
- ☒ уровень безопасности;
- ☐ уровень доступности

15 При качественном подходе риск измеряется в терминах

- ☐ денежных оценок
- ☐ объема информации
- ☐ денежных потерь
- ☒ заданных с; помощью шкалы или ранжирования
- ☐ оценок экспертов

16 При избирательной политике безопасности в матрице доступа субъекту системы соответствует

- ☐ [yeni savab]
- ☐ строка
- ☐ прямоугольная область
- ☐ ячейка
- ☒ столбец;
- ☐ поле

17 При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается

- ☐ наблюдение;
- ☐ субъект системы;
- ☐ объект системы;
- ☒ тип разрешенного доступа.
- ☐ факт доступа;

18 Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа

- ☐ объект;
- ☐ наблюдение;
- ☐ уборка мусора;
- ☒ компрометация.
- ☐ перехват;

19 По документам ГТк самый высокий класс защищенности СВТ от НСД к информации

- ☐ 5
- ☐ 7
- ☐ 9
- ☒ 1.
- ☐ 6

20 По документам ГТк самый высокий класс защищенности СВТ от НСД к информации

- ☐ 5
- ☐ 7
- ☐ 9
- ☒ 1
- ☐ 6

21 Основу политики безопасности составляет

- ☐ управление объектом
- ☐ управление риском
- ☐ программное обеспечение
- ☒ способ управления доступом.
- ☐ выбор каналов связи

22 Обеспечение целостности информации в условиях случайного воздействия изучается

- ☐ криптография
- ☐ стеганографией
- ☐ криптологией
- ☒ теорией помехоустойчивого кодирования.
- ☐ криптоанализом

23 Организационные требования к системе защиты

- ☐ физические
- ☐ административные и аппаратурные
- ☐ управленческие и идентификационные
- ☒ административные и процедурные.
- ☐ аппаратурные и физические

24 По документам ГТк количество классов защищенности АС от НСД

- ☐ 5
- ☐ 8
- ☐ 6
- ☒ 9.
- ☐ 7

25 Недостатком модели конечных состояний политики безопасности является

- ☐ изменение линий связи
- ☐ средняя степень надежности
- ☐ низкая степень надежности
- ☐ статичность
- ☒ сложность реализации.

26 Наукой, изучающей математические методы защиты информации путем ее преобразования, является

- ☐ статичность
- ☐ стеганография
- ☐ криптоанализ
- ☒ криптология.
- ☐ криптография

27 Недостаток систем шифрования с открытым ключом

- ☐ на одном и том же ключе одинаковые 32-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста
- ☐ при использовании простой замены легко произвести подмену одного шифрованного текста другим
- ☐ необходимость распространения секретных ключей
- ☒ относительно низкая производительность.
- ☐ на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

28 На многопользовательские системы с информацией одного уровня конфиденциальности согласно Оранжевой книге рассчитан класс

- ☐ В3
- ☐ С2
- ☐ В2
- ☒ С1.
- ☐ В1

29 Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется

- ☐ статичность
- ☐ идентифицируемым
- ☐ привилегированным
- ☒ мандатным.
- ☐ избирательным

30 конкретизацией модели Белла-ЛаПадула является модель политики безопасности

- ☐ Лендвера
- ☐ С полным перекрытием
- ☐ На основе анализа угроз
- ☒ LWM.
- ☐ Лендвера

31 При избирательной политике безопасности в матрице доступа объекту системы соответствует

- ☐ поле
- ☐ ячейка
- ☐ прямоугольная область
- ☒ строка.
- ☐ столбец

32 По документам ГТк самый низкий класс защищенности СВТ от НСД к информации

- ☐ 2
- ☐ 0
- ☐ 9
- ☒ 6.
- ☐ 1

33 Наименее затратный криптоанализ для криптоалгоритма DES

- ☐ разложение числа на множители
- ☐ перебор по выборочному ключевому пространству
- ☐ разложение числа на сложные множители
- ☐ разложение числа на простые множители
- ☒ перебор по всему ключевому пространству.
- ☐ перебор по выборочному ключевому пространству

34 По документам ГТк количество классов защищенности СВТ от НСД к информации

- ☐ 5
- ☐ 8
- ☐ 9
- ☒ 6
- ☐ 7

35 Обеспечением скрытности информации в информационных массивах занимается

- ☐ криптология

- ☐ криптология
- ☐ криптоанализ
- ☒ стеганография.
- ☐ криптография

36 Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется

- ☐ [yeni cavab]
- ☐ системой защиты
- ☐ профилем безопасности
- ☐ стандартом безопасности
- ☒ профилем защиты
- ☐ системой безопасности

37 Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему

- ☐ всех средств безопасности
- ☐ аудита
- ☒ хотя бы одного средства безопасности
- ☐ логина
- ☐ пароля

38 Политика информационной безопасности — это

- ☐ анализ рисков
- ☐ профиль защиты
- ☐ стандарт безопасности
- ☒ совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации.
- ☐ итоговый документ анализа рисков

39 Что такое криптография?

- ☐ защиту информации от компьютерных вирусов
- ☐ область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом
- ☐ область доступной информации
- ☒ метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом,
- ☐ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера

40 Под ИБ понимают

- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ☐ защиту информации от компьютерных вирусов
- ☐ защиту от несанкционированного доступа
- ☒ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера,
- ☐ ответственность за модификацию и НСД информации

41 Угроза - это

- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ☐ административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов
- ☐ ответственность за модификацию и НСД информации
- ☒ возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов,
- ☐ событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

42 Уровень секретности - это

- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ☐ возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
- ☐ ответственность за модификацию и НСД информации
- ☒ административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов,
- ☐ событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

43 Защита от программных закладок обеспечивается

- ☐ аппаратным модулем, устанавливаемым на контроллер
- ☐ специальным программным обеспечением
- ☐ системным программным обеспечением
- ☒ аппаратным; модулем; устанавливаемым на системную шину ПК

44 Идентификаторы безопасности в Windows 2000 представляют собой

- ☐ ; полную строку символов
- ☐ ; число, вычисляемое с помощью хэш-функции
- ☐ ; константу, определенную администратором для каждого пользователя
- ☒ двоичное число, состоящее из заголовка и длинного случайного компонента
- ☐ ; строку символов, содержащую имя пользователя и пароль

45 . Из перечисленного для СУБД важны такие аспекты информационной безопасности, как 1) своевременность; 2) целостность; 3) доступность; 4) конфиденциальность; 5) многоплатформенность

- ☐ 1,2,5
- ☐ 1,3, 5
- ☐ 2, 3, 5
- ☒ 2, 3, 4;
- ☐ 1, 2, 3

46 к аспектам ИБ относятся Выберите несколько из 5 вариантов ответа: 1) дискретность 2) целостность 3) конфиденциальность 4) актуальность 5) доступность

- ☐ 2,4,5
- ☐ 3,4,5
- ☐ 1,3,5
- ☒ 2,3,5,
- ☐ 1,3,4

47 Технические средства защиты информации Выберите один из 4 вариантов ответа:

- ☐ осуществление специально разработанными программами перехвата имени и пароля
- ☐ устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- ☐ средства, которые реализуются в виде автономных устройств и систем
- ☒ .. средства, которые реализуются в виде электрических, электромеханических и электронных устройств
- ☐ это программы, предназначенные для выполнения функций, связанных с защитой информации

48 В чем заключается основная причина потерь информации, связанной с Пк? Выберите один из 3 вариантов ответа:

- ☐ с достаточной образованностью в области безопасности
- ☐ с появлением интернета
- ☐ с глобальным хищением информации
- ☒ с недостаточной образова,,нностью в области безопасности
- ☐ средства, которые реализуются в виде автономных устройств и систем

49 Физические средства защиты информации Выберите один из 4 вариантов ответа:

- ☐ это программы, предназначенные для выполнения функций, связанных с защитой информации
- ☐ это программы, предназначенные для выполнения функций, связанных с защитой информации
- ☐ устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- ☒ , средства, которые реализуются в виде автономных устройств и систем
- ☐ средства, которые реализуются в виде электрических, электромеханических и электронных устройств

50 Выделите группы, на которые делятся средства защиты информации:

- ☐ химические, аппаратные, программные, этнографические, комбинированные;
- ☐ химические, аппаратные, программные, криптографические, комбинированные;
- ☒ физические, аппаратные, программные, криптографические, комбинированные;
- ☐ криптографические, комбинированные;
- ☐ физические, аппаратные, программные, этнографические, комбинированные;

51 Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется

- ☐ безопасность информации
- ☐ защитой информации
- ☐ политикой информации
- ☒ политикой безопасности,
- ☐ организацией безопасности

52 как подразделяются вирусы в зависимости от деструктивных возможностей?

- ☐ Безвредные, неопасные, загрузочные, комбинированные
- ☐ Резидентные, нерезидентные
- ☐ Сетевые, файловые, загрузочные, комбинированные
- ☒ Безвредные, неопасные, опасные, очень опасные,
- ☐ Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

53 комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

- ☐ системы управления базами данных
- ☐ системой безопасности;
- ☐ системой угроз;
- ☒ системой защиты;
- ☐ системой уничтожения

54 Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

- ☐ системы управления базами данных
- ☐ операционной системы, системы управления базами данных;
- ☐ операционной системы, сетевого программного обеспечения
- ☒ операционной системы, сетевого программного обеспечения и системы управления базами данных;.
- ☐ сетевого программного обеспечения и системы управления базами данных

55 какие существуют основные уровни обеспечения защиты информации? Выберите несколько из 7 вариантов ответа: 1) законодательный 2) административный 3) программно-технический 4) физический 5) вероятностный 6) процедурный 7) распределительный

- ☐ [yeni cavab]
- ☐ 1; 4; 5; 6;

- ☐ 2; 3; 5; 6;
- ☐ 5; 4; 6;
- ☒ „1; 2; 3; 6;
- ☐ 3; 5; 6;

56 Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

- ☐ безопасностью;
- ☐ намерением;
- ☐ опасностью;
- ☒ угрозой;
- ☐ предостережением.

57 какие законы существуют в России в области компьютерного права? Выберите несколько из 6 вариантов ответа: 1) О государственной тайне 2) об авторском праве и смежных правах 3) о гражданском долге 4) о правовой охране программ для ЭВМ и БД 5) о правовой ответственности 6) об информации, информатизации, защищенности информации

- ☐ 2; 4; 5; 6;
- ☐ 5; 4; 6;
- ☐ 2; 3; 4; 6;
- ☒ ..1; 2; 4; 6;
- ☐ 1; 3; 5; 6;

58 Оконечное устройство канала связи, через которое процесс может передавать или получать данные, называется

- ☐ кластером.
- ☐ хостом.
- ☐ портом.
- ☒ сокетом
- ☐ терминалом.

59 Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

- ☐ код
- ☐ данные
- ☐ текст
- ☒ информация,
- ☐ пароль

60 Что такое компьютерный вирус?

- ☐ Разновидность программ, которые не самоуничтожаются
- ☐ Разновидность программ, которые не работают
- ☐ Разновидность программ, которые самоуничтожаются
- ☒ Разновидность программ, которые способны к размножению,
- ☐ Разновидность программ, которые плохо работают

61 к методам защиты от НСД относятся

- ☐ 3; 4; 5;
- ☐ 3; 4; 5;
- ☐ 2; 3; 4; 5;
- ☒ 1; 2; 4; 5,;
- ☐ 1; 3; 4; 5;

62 к видам защиты информации относятся:

- ☐ 2; 4; 5;
- ☐ 1; 3; 5;
- ☐ 2; 3; 5;
- ☒ 1; 2; 4,;
- ☐ 3; 4; 5;

63 как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных определяется

- ☐ аутентификация
- ☐ идентификация
- ☐ контроль доступа
- ☐ целостность
- ☒ ;причастность

64 Из перечисленного ядро безопасности ОС выделяет типы полномочий: 1) ядра; 2) периферийных устройств; 3) подсистем; 4) пользователей

- ☐ 2,4
- ☐ 2
- ☐ 3,4
- ☒ 1,3,
- ☐ 2,3

65 Из перечисленного формами причастности являются: 1) контроль доступа; 2) аутентификация; 3) к посылке сообщения; 4) подтверждение получения сообщения

- ☐ 1
- ☐ 1,4
- ☐ 2,4
- ☒ 3,4,
- ☐ 1,2

66 Из перечисленного цифровая подпись используется для обеспечения услуг: 1) аутентификации; 2) целостности; 3) контроля доступа; 4) контроля трафика

- ☐ 2
- ☐ 2,3
- ☐ 2,4
- ☒ 1,2,
- ☐ 3,4

67 Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- ☐ 2,5
- ☐ 4,5,6
- ☐ 2,3
- ☒ 1,2,5,
- ☐ 3,5

68 Из перечисленного субъектами для монитора обращений являются: 1) терминалы; 2) программы; 3) файлы; 4) задания; 5) порты; 6) устройства

- ☐ 2,5
- ☐ 4,5,6
- ☐ 2,3,5

- ☒ 1,2,5,
☐ 2,3

69 Из перечисленного система защиты электронной почты должна: 1) обеспечивать все услуги безопасности; 2) обеспечивать аудит; 3) поддерживать работу только с лицензионным ПО; 4) поддерживать работу с почтовыми клиентами; 5) быть кросс-платформенной

- ☐ 4,5
☐ 2, 3
☐ 2, 3, 5
☒ 1, 4, 5,
☐ 2, 3, 4

70 Под изоляцией и разделением (требование к обеспечению ИБ) понимают

- ☐ разделение объектов защиты на группы так, чтобы нарушение защиты одной группы влияло на безопасность всех групп
☐ разделение объектов защиты на группы так, чтобы нарушение защиты одной группы влияло на безопасность других групп
☐ разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
☒ разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп,
☐ разделение информации на группы так, чтобы нарушение одной группы информации влияло на безопасность других групп информации (документов)

71 Основные группы технических средств ведения разведки

- ☐ 2; 4; 5;
☐ 3; 4; 5;
☐ 2; 3; 5;
☒ 1; 3; 5,;
☐ 1; 2; 4

72 Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем

- ☐ прикладном
☐ сетевом
☐ сеансовом
☒ ,транспортном
☐ канальном

73 Виды технической разведки (по месту размещения аппаратуры)

- ☐ 2; 4; 5;
☐ 1; 2; 3; 5;
☐ 2; 3; 4; 5;
☒ 1; 3; 5; 6,;
☐ 3; 4; 5;

74 . Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем

- ☐ прикладном
☐ физическом
☐ канальном
☒ сетевом,
☐ транспортном

75 конфигурация из нескольких компьютеров, выполняющих общее приложение, называется

- ☐ портом
- ☐ сервером
- ☐ суперсервером
- ☒ кластеро,м
- ☐ сетью

76 Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

- ☐ достоверной
- ☒ защищаемой,
- ☐ кодируемой
- ☐ шифруемой
- ☐ недостоверной

77 . Из перечисленного привилегиями безопасности являются: 1) security; operator; 2) create trace; 3) createdb; 4) operator; 5) trace

- ☐ 3,4,5
- ☐ 2,3
- ☐ 2,4,5
- ☐ 2,3,5
- ☒ 1, 3, 4, 5,
- ☐ 2,4

78 Утечка информации

- ☐ защищенная информация
- ☐ потеря, хищение, разрушение или неполучение переданных данных
- ☐ несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- ☒ ознакомление постороннего лица с содержанием секретной информации,
- ☐ это присвоение имени субъекту или объекту

79 . Из перечисленного привилегии в СУБД могут передаваться: 1) субъектам; 2) группам; 3) ролям; 4) объектам; 5) процессам

- ☐ 3,4,5
- ☐ 2,3,5
- ☐ 2, 4, 5
- ☒ 1, 2, 3,
- ☐ 2,4

80 кодирование информации -

- ☐ Определение файлов, из которых удалена служебная информация
- ☐ это присвоение имени субъекту или объекту
- ☐ метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
- ☒ представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.,
- ☐ защищенная информация

81 Верификация -

- ☐ Определение файлов, из которых удалена служебная информация
- ☐ это присвоение имени субъекту или объекту
- ☐ это проверка принадлежности субъекту доступа предъявленного им идентификатора.

- ☒ проверка целостности и подлинности инф, программы, документа,
☐ защищенная информация

82 . Из перечисленного пользователи СУБД разбиваются на категории: 1) системный администратор; 2) сетевой администратор; 3) администратор сервера баз данных; 4) администратор базы данных; 5) конечные пользователи; 6) групповые пользователи

- ☐ 2,3,5,
☐ 1, 2, 5,
☐ 4, 5, 6,
☒ 3, 4, 5
☐ 1, 4, 6,

83 . Из перечисленного объектами для монитора обращений являются: 1) терминалы; 2) программы; 3) файлы; 4) задания; 5) порты; 6) устройства

- ☐ 2,5,6
☐ 1, 2, 5
☐ 2, 4, 6
☒ 2, 3, 4, 6;
☐ 1, 2, 4

84 . Из перечисленного метка безопасности состоит из таких компонентов, как 1) уровень секретности; 2) категория; 3) множество ролей; 4) ключ шифра; 5) области

85 Маскарад - это

- ☐ представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
☐ обеспечить конфиденциальность и аутентификацию передаваемых сообщений
☐ осуществление специально разработанными программами перехвата имени и пароля
☒ выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.,
☐ взломать систему защиты

86 Из перечисленного защита процедур и программ осуществляется на уровнях: 1) аппаратуры; 2) программного обеспечения; 3) данных; 4) канальном; 5) сеансовом; 6) прикладном

- ☐ 1,2,6
☐ 1, 2, 5
☐ 2, 4, 6
☒ 1, 2, 3;
☐ 4, 5, 6

87 Что такое аутентификация?

- ☐ Определение файлов, из которых удалена служебная информация
☐ Нахождение файлов, которые изменены в информационной системе несанкционированно
☐ Проверка количества переданной и принятой информации
☒ Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
☐ Определение файлов, из которых удалена служебная информация

88 кто является знаковой фигурой в сфере информационной безопасности

- ☐ Шелдон
☐ Паскаль
☐ Шеннон
☒ Митник
☐ Беббидж

89 . Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы: 1) визуальное сканирование; 2) фрагментарное сканирование; 3) исследование динамических характеристик движения руки; 4) исследование траектории движения руки

- ☐ 4
- ☐ 1, 4
- ☐ 2, 4
- ☒)) 1, 3
- ☐ 1, 2

90 . Из перечисленного в автоматизированных системах используется аутентификация по: 1) терминалу; 2) паролю; 3) предмету; 4) физиологическим признакам; 5) периферийным устройствам

- ☐ 2, 4, 5
- ☐ 1, 4, 5
- ☐ 1, 2, 4
- ☐ 1, 4, 5
- ☒ 2, 3, 4;
- ☐ 1, 2, 5

91 Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются: 1) отпечатки пальцев; 2) форма кисти; 3) форма губ; 4) форма ушной раковины; 5) голос; 6) личная подпись

- ☐ 1,4,6
- ☐ 4, 5, 6
- ☐ 1, 4, 5
- ☒ 1, 2, 5, 6;
- ☐ 1,3,4

92 Оконечное устройство канала связи, через которое процесс может передавать или получать данные, называется

- ☐ кластером
- ☐ хостом
- ☐ портом
- ☒ сокетом;
- ☐ терминалом

93 Информационная безопасность это:

- ☐ Состояние, когда угрожает опасность информационным системам
- ☐ Состояние, когда не угрожает опасность информационным системам
- ☒ Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз;
- ☐ Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
- ☐ Политика национальной безопасности России

94 к национальным интересам РФ в информационной сфере относятся:

- ☐ Сохранение и оздоровлении окружающей среды
- ☐ Защита независимости, суверенитета, государственной и территориальной целостности
- ☐ Защита информации, обеспечивающей личную безопасность
- ☒ Реализация конституционных прав на доступ к информации.
- ☐ Политическая экономическая и социальная стабильность

95 Вопрос: как подразделяются вирусы в зависимости от деструктивных возможностей?

- ☐ Безвредные, неопасные, загрузочные, комбинированные

- ☐ Резидентные, нерезидентные
- ☒ Безвредные, неопасные, опасные, очень опасные;
- ☐ Сетевые, файловые, загрузочные, комбинированные
- ☐ Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

96 Прочность защиты в АС

- ☐ вероятность преодоления защиты нарушителем за установленный промежуток времени
- ☒ вероятность не преодоления защиты нарушителем за установленный промежуток времени,
- ☐ способность системы защиты информации обеспечить достаточный уровень своей безопасности
- ☐ группа показателей защиты, соответствующая определенному классу защиты
- ☐ группа показателей защиты, несоответствующая определенному классу защиты

97 Линейное шифрование -

- ☐ санкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
- ☐ криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
- ☐ несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
- ☒ криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому,,
- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу

98 Охранное освещение бывает:

- ☐ архив
- ☐ заключенной
- ☐ световое
- ☒ дежурное;
- ☐ открытое

99 Вопрос: Виды технической разведки (по месту размещения аппаратуры) Выберите несколько из 7 вариантов ответа: 1) космическая 2) оптическая 3) наземная 4) фотографическая 5) морская 6) воздушная 7) магнитометрическая

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 2; 3; 5;
- ☐ 2; 3; 4; 5;
- ☒ 1; 3; 5; 6

100 Из перечисленного подсистема управления криптографическими ключами структурно состоит из: 1) центра распределения ключей; 2) программно-аппаратных средств; 3) подсистемы генерации ключей; 4) подсистемы защиты ключей

- ☐ 2,3,4
- ☐ 3
- ☐ 2, 4
- ☒ 1,2;
- ☐ 3,4

101 Вопрос: Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

- ☐ код
- ☒ информация.
- ☐ данные
- ☐ текст
- ☐ пароль

102 Вопрос: Что такое криптография?

- ☐ защиту информации от компьютерных вирусов
- ☐ область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом
- ☐ область доступной информации
- ☒ метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом;
- ☐ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера

103 Вопрос: Уровень секретности - это

- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ☐ возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
- ☒ административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов;
- ☐ ответственность за модификацию и НСД информации
- ☐ событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

104 Из перечисленного на транспортном уровне рекомендуется применение услуг: 1) идентификации; 2) конфиденциальности; 3) контроля трафика; 4) контроля доступа; 5) целостности; 6) аутентификации

- ☐ 1,4,6
- ☐ 1, 3
- ☐ 4, 5, 6
- ☒ 2, 4, 5, 6;;
- ☐ 4, 6

105 к аспектам ИБ относятся

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☒ 2; 3; 5;;
- ☐ 1; 3; 4;

106 .Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты

- ☐ системного уровня
- ☐ сетевого
- ☐ уровня приложений
- ☐ сетевого уровня
- ☒ встроенных в ОС

107 Из перечисленного аутентификация используется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- ☐ 4,5,6
- ☐ 1, 3, 5
- ☐ 4, 5, 6
- ☒ 1, 2, 5;
- ☐ 1, 3

108 Из перечисленного в соответствии с видами объектов привилегии доступа подразделяются на: 1) терминалы; 2) процедуры; 3) модули; 4) базы данных; 5) сервер баз данных; 6) события

- ☐ 2,3,5,6
- ☐ 2, 3, 5

- ☐ 1, 3, 5, 6
☒ ; 2, 4, 5, 6
☐ 1, 2, 3

109 . Из перечисленного в ОС UNIX регистрационная запись средств аудита включает поля: 1) дата и время события; 2) команда, введенная пользователем; 3) результат действия; 4) пароль пользователя; 5) тип события; 6) идентификатор пользователя

- ☐ 1, 2, 4, 6
☐ 1, 2, 3, 4
☐ 2, 3, 4, 6
☒ 1, 3, 5, 6;

110 Вопрос: Утечка информации

- ☐ защищенная информация
☐ потеря, хищение, разрушение или неполучение переданных данных
☒ ознакомление постороннего лица с содержанием секретной информации.
☐ несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
☐ это присвоение имени субъекту или объекту

111 Вопрос: Верификация -

- ☐ Определение файлов, из которых удалена служебная информация
☐ это присвоение имени субъекту или объекту
☒ проверка целостности и подлинности инф, программы, документа.
☐ это проверка принадлежности субъекту доступа предъявленного им идентификатора
☐ защищенная информация

112 . Недостатком матричных моделей безопасности является

- ☐ отсутствие части аудита
☐ невозможность учета индивидуальных особенностей субъекта
☐ отсутствие полного аудита
☒ отсутствие контроля з.а потоками информации
☐ сложность представления широкого спектра правил обеспечения безопасности

113 Организационные угрозы подразделяются на

- ☐ 2; 4;
☐ 1; 3;
☐ 2; 3;
☒ 1; 2; 4;,
☐ 4; 5;

114 Вопрос: Маскарад - это

- ☐ представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
☐ обеспечить конфиденциальность и аутентификацию передаваемых сообщений
☒ выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями;
☐ осуществление специально разработанными программами перехвата имени и пароля
☐ взломать систему защиты

115 Вопрос: Под ИБ понимают

- ☐ защиту информации искусственного характера
☐ защиту информации от компьютерных вирусов

- ☒ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера;
- ☐ защиту от несанкционированного доступа
- ☐ защиту от санкционированного доступа

116 Вопрос: В чем состоит задача криптографа?

- ☐ осуществление специально разработанными программами перехвата имени и пароля
- ☐ Определение файлов, из которых удалена служебная информация
- ☒ обеспечить конфиденциальность и аутентификацию передаваемых сообщений;
- ☐ взломать систему защиты
- ☐ взломать систему защиты

117 Вопрос: Что такое целостность информации?

- ☐ Свойство информации, заключающееся в ее несуществовании в виде единого набора файлов
- ☐ Свойство информации, заключающееся в ее существовании в виде единого набора файлов
- ☐ Свойство информации, заключающееся в возможности изменения только единственным пользователем
- ☐ Свойство информации, заключающееся в возможности ее изменения любым субъектом
- ☒ Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

118 Разновидности угроз безопасности

- ☐ 2; 4; 5;
- ☐ 1; 3; 5;
- ☐ 2; 3; 5;
- ☒ 1; 3; 4,;
- ☐ 3; 4; 5;

119 какие атаки предпринимают хакеры на программном уровне?

- ☒ 1; 2; 4,;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☐ 2; 3; 5;
- ☐ 2; 4; 5;

120 Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни: 1) внешний; 2) сетевой; 3) клиентский; 4) серверный; 5) системный; 6) приложений

- ☐ 2, 3, 4, 6
- ☐ 3, 4, 5, 6
- ☐ 2, 3, 5, 6
- ☒ 1, 2, 5, 6;
- ☐ 5, 2, 3, 4

121 Брандмауэры третьего поколения используют для фильтрации

- ☐ общий анализ контрольной информации
- ☐ методы электронной подписи
- ☐ общий анализ трафика
- ☒ специальные многоуровневые методы анализа состояния пакетов;
- ☐ методы анализа контрольной информации

122 Вопрос: Что такое компьютерный вирус?

- ☐ Разновидность программ, которые не самоуничтожаются
- ☐ Разновидность программ, которые не работают
- ☐ Разновидность программ, которые самоуничтожаются

- ☒ Разновидность программ, которые способны к размножению.
- ☐ Разновидность программ, которые плохо работают

123 Вопрос: к аспектам ИБ относятся Выберите несколько из 5 вариантов ответа: 1) дискретность 2) целостность 3) конфиденциальность 4) актуальность 5) доступность

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☒ 2; 3; 5
- ☐ 1; 3; 4;

124 Вопрос: Технические средства защиты информации

- ☐ осуществление специально разработанными программами перехвата имени и пароля
- ☐ это программы, предназначенные для выполнения функций, связанных с защитой информации
- ☐ устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- ☐ средства, которые реализуются в виде автономных устройств и систем
- ☒ средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

125 Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?

- ☐ Информационное общество
- ☐ Информационные инфекции
- ☐ Физический инфекции
- ☒ Информационный саботаж;
- ☐ Информационные оружия

126 Вопрос: Что такое криптология?

- ☐ область недоступной информации
- ☒ тайная область связи;
- ☐ область доступной информации
- ☐ защищенная информация
- ☐ незащищенная информация

127 Устройства осуществляющие воздействие на человека путем передачи информации через внечувственное восприятие:

- ☐ Психотропные программы
- ☐ Психотронные генераторы
- ☐ Психотропные препараты
- ☐ Средства массовой информации
- ☒ Средства специального программно-технического воздействия;

128 Вопрос: Выделите группы, на которые делятся средства защиты информации:

- ☐ криптографические, комбинированные;
- ☐ физические, аппаратные, программные, этнографические, комбинированные;
- ☐ химические, аппаратные, программные, криптографические, комбинированные;
- ☒ физические, аппаратные, программные, криптографические, комбинированные
- ☐ химические, аппаратные, программные, этнографические, комбинированные;

129 Вопрос: Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется

- ☐ безопасность информации

- ☒ политикой безопасности;
- ☐ защитой информации
- ☐ политикой информации
- ☐ организацией безопасности

130 Вопрос: Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

- ☐ безопасностью;
- ☐ намерением;
- ☐ опасностью;
- ☒ угрозой
- ☐ предостережением;

131 Вопрос: Разновидности угроз безопасности Выберите несколько из 6 вариантов ответа: 1) техническая разведка 2) программные 3) программно-математические 4) организационные 5) технические 6) физические

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☐ 2; 3; 5;
- ☒ 1; 3; 4

132 Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:

- ☐ защита
- ☐ аутентичность
- ☐ доступность
- ☒ конфиденциальность.
- ☐ целостность

133 Брандмауэры второго поколения представляли собой

- ☐ хосты пакетов
- ☐ маршрутизаторы с фильтрацией пакетов
- ☐ хосты с фильтрацией пакетов
- ☒ «уполномоченные серверы»;
- ☐ «неприступные серверы»

134 Вопрос: к методам защиты от НСД относятся Выберите несколько из 5 вариантов ответа: 1) разделение доступа; 2) разграничение доступа; 3) увеличение доступа; 4) ограничение доступа. 5) аутентификация и идентификация

- ☐ 3; 4; 5;
- ☐ 3; 4; 5;
- ☒ 1; 2; 4; 5
- ☐ 2; 3; 4; 5;
- ☐ 1; 3; 4; 5;

135 Вопрос: к видам защиты информации относятся: Выберите несколько из 4 вариантов ответа: 1) правовые и законодательные; 2) морально-этические; 3) юридические; 4) административно-организационные;

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☐ 2; 3; 5;

136 Вопрос: Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

- ☐ системы управления базами данных
- ☐ операционной системы, системы управления базами данных
- ☒ операционной системы, сетевого программного обеспечения и системы управления базами данных;
- ☐ операционной системы, сетевого программного обеспечения
- ☐ сетевого программного обеспечения и системы управления базами данных

137 Трояские программы — это

- ☐ часть программы с известными пользователю функциями
- ☒ часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба.
- ☐ все программы, содержащие ошибки
- ☐ текстовые файлы, распространяемые по сети
- ☐ программы-вирусы, которые распространяются самостоятельно

138 Что не относится к информационной инфекции:

- ☐ Логическая бомба
- ☐ Черви
- ☒ Фальсификация данных.
- ☐ Троянский конь
- ☐ Вирусы

139 Уполномоченные серверы были созданы для решения проблемы

- ☐ блокировки трафика
- ☐ перехвата трафика
- ☐ НСД
- ☒ имитации IP-адресов;
- ☐ подделки электронной подписи

140 Чтобы программная закладка могла произвести какие-либо действия, необходимо чтобы она

- ☐ не попала в оперативную память
- ☐ попала на жесткий диск
- ☐ внедрилась в операционную систему
- ☒ попала в оперативную память;
- ☐ перехватила прерывания

141 Удачная криптоатака называется

- ☐ социальная инженерия
- ☐ вскрытием
- ☐ раскрытием шифра
- ☒ взломом;
- ☐ проникновением

142 Идентификатор субъекта доступа, который является его секретом:

- ☐ админом
- ☐ электронно-цифровая подпись
- ☐ ключ
- ☒ пароль;
- ☐ сертификат ключа подписи

143 Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

- ☐ без защитная информация от несанкционированного воздействия
- ☐ защита информации от несанкционированного доступа
- ☐ защита информации от несанкционированного воздействия
- ☐ защита информации от непреднамеренного воздействия
- ☒ защита от утечки информации;

144 Вопрос: комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

- ☐ системой уничтожения;
- ☒ системой защиты
- ☐ системой угроз;
- ☐ системы управления базами данных;
- ☐ системой безопасности;

145 Вопрос: Основные группы технических средств ведения разведки Выберите несколько из 5 вариантов ответа: 1) радиомикрофоны 2) фотоаппараты 3) электронные уши 4) дистанционное прослушивание разговоров 5) системы определения местоположения контролируемого объекта

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☒ 1; 3; 5
- ☐ 2; 3; 5;
- ☐ 2; 4; 5;

146 Администратором базы данных является

- ☐ пользователь группы
- ☐ старший пользователь группы
- ☐ администратор сервера баз данных
- ☒ любой пользователь, создавший БД.
- ☐ системный администратор

147 Административные действия в СУБД позволяют выполнять привилегии

- ☐ недоступа
- ☐ чтения
- ☐ тиражирования
- ☒ безопасности.
- ☐ доступа

148 Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- ☐ 2,5
- ☐ 4, 5, 6
- ☐ 2, 3
- ☒ 1, 2, 5;
- ☐ 3, 5

149 Вопрос: Организационные угрозы подразделяются на Выберите несколько из 4 вариантов ответа: 1) угрозы воздействия на персонал 2) физические угрозы 3) действия персонала 4) несанкционированный доступ 5) атаки на уровне СУБД

- ☐ 2; 4;

- ☐ 4; 5;
- ☐ 1; 3;
- ☐ 2; 3;
- ☒ 1; 2; 4

150 Вопрос: какие атаки предпринимают хакеры на программном уровне? Выберите несколько из 5 вариантов ответа: 1) атаки на уровне ОС 2) атаки на уровне сетевого ПО 3) атаки на уровне пакетов прикладных программ 4) атаки на уровне СУБД 5) атаки на уровне персонала

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☐ 2; 3; 5;
- ☒ 1; 2; 4

151 Вопрос: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

- ☐ достоверной
- ☐ недостоверной
- ☐ шифруемой
- ☐ кодируемой
- ☒ защищаемой;

152 Вопрос: Под изоляцией и разделением (требование к обеспечению ИБ) понимают

- ☐ разделение объектов защиты на группы так, чтобы нарушение защиты одной группы влияло на безопасность всех групп
- ☐ разделение объектов защиты на группы так, чтобы нарушение защиты одной группы влияло на безопасность других групп
- ☒ разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп;
- ☐ разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
- ☐ разделение информации на группы так, чтобы нарушение одной группы информации влияло на безопасность других групп информации (документов)

153 Вопрос: Под ИБ понимают

- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ☐ защиту информации от компьютерных вирусов
- ☒ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера.
- ☐ защиту от несанкционированного доступа
- ☐ ответственность за модификацию и НСД информации

154 Вопрос: Угроза - это

- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ☒ возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов;
- ☐ административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов
- ☐ ответственность за модификацию и НСД информации
- ☐ событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

155 Вопрос: Прочность защиты в АС

- ☐ вероятность преодоления защиты нарушителем за установленный промежуток времени
- ☐ группа показателей защиты, соответствующая определенному классу защиты

- ☐ способность системы защиты информации обеспечить достаточный уровень своей безопасности
- ☒ вероятность не преодоления защиты нарушителем за установленный промежуток времени.
- ☐ группа показателей защиты, несоответствующая определенному классу защиты

156 Вопрос: к аспектам ИБ относятся Выберите несколько из 5 вариантов ответа: 1) дискретность 2) целостность 3) конфиденциальность 4) актуальность 5) доступность

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☒ 2; 3; 5
- ☐ 1; 3; 4;

157 Вопрос: кодирование информации -

- ☐ это присвоение имени субъекту или объекту
- ☒ представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д;
- ☐ Определение файлов, из которых удалена служебная информация
- ☐ защищенная информация
- ☐ метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

158 Из перечисленного формами причастности являются: 1) контроль доступа; 2) аутентификация; 3) к посылке сообщения; 4) подтверждение получения сообщения

- ☐ 1
- ☐ 1, 4
- ☐ 2, 4
- ☒ 3, 4;
- ☐ 1, 2

159 конфигурация из нескольких компьютеров, выполняющих общее приложение, называется

- ☐ портом
- ☐ сервером
- ☐ суперсервером
- ☒ кластером;
- ☐ сетью

160 как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных определяется

- ☐ идентификация
- ☐ целостность
- ☐ аутентификация
- ☒ причастность.
- ☐ контроль доступа

161 Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем

- ☐ прикладном
- ☐ сетевом
- ☐ сеансовом
- ☒ транспортном.
- ☐ канальном

162 Недостатком матричных моделей безопасности является

- ☐ отсутствие части аудита
- ☐ невозможность учета индивидуальных особенностей субъекта
- ☐ отсутствие полного аудита
- ☒ отсутствие контроля за потоками информации;
- ☐ сложность представления широкого спектра правил обеспечения безопасности

163 Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем

- ☐ прикладном
- ☐ физическом
- ☐ канальном
- ☒ сетевом.
- ☐ транспортном

164 Вопрос: В чем заключается основная причина потерь информации, связанной с ПК?

- ☐ с достаточной образованностью в области безопасности
- ☒ с недостаточной образованностью в области безопасности;
- ☐ с появлением интернета
- ☐ с глобальным хищением информации
- ☐ средства, которые реализуются в виде автономных устройств и систем

165 Вопрос: Что такое аутентификация?

- ☐ Определение файлов, из которых удалена служебная информация
- ☒ Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
- ☐ Нахождение файлов, которые изменены в информационной системе несанкционированно
- ☐ Проверка количества переданной и принятой информации
- ☐ Определение файлов, из которых удалена служебная информация

166 Вопрос: кто является знаковой фигурой в сфере информационной безопасности

- ☐ Шелдон
- ☐ Паскаль
- ☐ Шеннон
- ☒ Митник.
- ☐ Беббидж

167 Вопрос: Физические средства защиты информации

- ☐ это программы, предназначенные для выполнения функций, связанных с защитой информации
- ☐ это программы, предназначенные для выполнения функций, связанных с защитой информации
- ☐ устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- ☒ средства, которые реализуются в виде автономных устройств и систем;
- ☐ средства, которые реализуются в виде электрических, электромеханических и электронных устройств

168 Из перечисленного цифровая подпись используется для обеспечения услуг: 1) аутентификации; 2) целостности; 3) контроля доступа; 4) контроля трафика

- ☐ 2
- ☐ 2, 3
- ☐ 2, 4
- ☒ 1, 2;
- ☐ 3, 4

169 Что относится к классу информационных ресурсов:

- ☒ все правильные ответы;
- ☐ Организационные единицы
- ☐ Персонал
- ☐ Документы
- ☐ Промышленные образцы, рецептуры и технологии

170 Наиболее распространенные угрозы информационной безопасности:

- ☐ угрозы защищенности
- ☐ угрозы вируса
- ☐ угрозы деятельности
- ☐ угрозы безопасности
- ☒ угрозы целостности;

171 Из перечисленного ядро безопасности ОС выделяет типы полномочий: 1) ядра; 2) периферийных устройств; 3) подсистем; 4) пользователей

- ☐ 2,4
- ☐ 2
- ☐ 3,4
- ☒ 1,3.
- ☐ 2,3

172 Вопрос: какие существуют основные уровни обеспечения защиты информации? Выберите несколько из 7 вариантов ответа: 1) законодательный 2) административный 3) программно-технический 4) физический 5) вероятностный 6) процедурный 7) распределительный

- ☐ 3; 5; 6;
- ☐ 5; 4; 6;
- ☐ 2; 3; 5; 6;
- ☒ 1; 2; 3; 6
- ☐ 1; 4; 5; 6;

173 Вопрос: какие законы существуют в России в области компьютерного права? Выберите несколько из 6 вариантов ответа: 1) О государственной тайне 2) об авторском праве и смежных правах 3) о гражданском долге 4) о правовой охране программ для ЭВМ и БД 5) о правовой ответственности 6) об информации, информатизации, защищенности информации

- ☐ 2; 4; 5; 6;
- ☐ 5; 4; 6;
- ☐ 2; 3; 4; 6;
- ☒ 1; 2; 4; 6
- ☐ 1; 3; 5; 6;

174 Первым этапом разработки системы защиты ИС является

- ☐ оценка потерь
- ☐ стандартизация программного обеспечения
- ☐ оценка возможных потерь
- ☒ анализ потенциально возможных угроз информации.
- ☐ изучение информационных потоков

175 Вопрос: Линейное шифрование -

- ☐ санкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
- ☐ криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
- ☒ криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому;

- ☐ несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
- ☐ несанкционированное изменение информации, корректное по форме, содержанию и смыслу

176 к оборонительным системам защиты относятся:

- ☐ электрофизические датчики
- ☐ электрохимические датчики
- ☐ датчики
- ☒ звуковые установки.
- ☐ электромеханические датчики

177 к аспектам ИБ относятся

- ☐ 2; 4; 5;
- ☐ 3; 4; 5;
- ☐ 1; 3; 5;
- ☒ 2; 3; 5,;
- ☐ 1; 3; 4;

178 Что такое криптология?

- ☐ область недоступной информации
- ☒ таинная область связи
- ☐ защищенная информация
- ☐ область доступной информации
- ☐ незащищенная информация

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

- ☐ аналитических преобразований
- ☐ кодирования
- ☐ подстановки
- ☒ гаммирования;
- ☐ перестановки

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

- ☐ аналитических преобразований
- ☐ кодирования
- ☒ подстановки;
- ☐ гаммирования
- ☐ перестановки

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

- ☐ аналитических преобразований
- ☐ кодирования
- ☐ подстановки
- ☐ гаммирования
- ☒ перестановки;

182 к основным непреднамеренным искусственным угрозам АСОИ относится:

- ☒ неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы
- ☐ изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

- ☐ перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
- ☐ физическое разрушение системы путем взрыва, поджога и т.п.;
- ☐ чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

183 Искусственные угрозы безопасности информации вызваны

- ☐ ошибками при действиях персонала;
- ☐ воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
- ☐ ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- ☒ деятельностью человека
- ☐ корыстными устремлениями злоумышленников;

184 Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем

- ☐ сеансовым
- ☐ транспортном
- ☐ сетевом
- ☒ физическом.
- ☐ канальном

185 какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

- ☐ изменить, повредить или ее уничтожить;
- ☐ получить, изменить или уничтожить;
- ☐ размножить или уничтожить ее;
- ☒ получить, изменить, а затем передать ее конкурентам.
- ☐ изменить и уничтожить ее;

186 Примером числовой информации может служить:

- ☐ разговор по телефону;
- ☐ иллюстрация в книге;
- ☐ симфония;
- ☒ таблица значений тригонометрических функций.
- ☐ поздравительная открытка;

187 Информация в семантической теории - это:

- ☐ всякие сведения, сообщения, знания;
- ☐ сведения, обладающие новизной;
- ☐ неотъемлемое свойство материи;
- ☒ сведения, полностью снимающие или уменьшающие существующую до их получения неопределенность.
- ☐ сигналы, импульсы, коды, наблюдающиеся в технических и биологических системах;

188 Для создания базы данных пользователь должен получить привилегию от

- ☐ баз данных
- ☐ системного администратора
- ☐ сетевого администратора
- ☒ администратора сервера баз данных.
- ☐ старшего пользователя своей группы

189 Что такое фишинг?

- ☐ комплекс аппаратных или программных средств, осуществляющий лечение компьютера
- ☐ создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д

- ☐ переписка от чужого лица с целью вымогательства денежных средств
- ☒ создание бесплатных программ, заржённых вирусами и троянами;
- ☐ бесплатное антивирусное приложение для разблокировки компьютера

190 Троянские программы распространяются...

- ☐ с помощью хакера
- ☐ с помощью пользователя
- ☐ с помощью компьютерных вирусов
- ☒ самостоятельно.
- ☐ с помощью неисправного ПО

191 Виды уязвимостей.

- ☐ вероятная;
- ☐ случайная;
- ☐ субъективная;
- ☒ постоянная.
- ☐ объективная;

192 В соответствии с законом АР Об информации, информатизации и защите информации (1995) информация - это:

- ☒ та часть знаний, которая используется для ориентирования, активного действия, управления, то есть в целях сохранения, совершенствования, развития системы.
- ☐ все то, что так или иначе может быть представлено в знаковой форме;
- ☐ сведения, обладающие новизной для их получателя;
- ☐ сведения, фиксируемые в виде документов;
- ☐ сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

193 как могут распространяться вирусы?

- ☐ через документы Word
- ☐ через рисунки и звуковые файлы
- ☐ при копировании данных через флэш-диски
- ☒ через компьютерные сети.
- ☐ через сообщения электронной почты

194 к чему приводит DoS-атака на сайт в Интернете?

- ☐ страницы сайта подменяются на фальшивые
- ☐ сервер не может справиться с большим потоком запросов
- ☐ взламывается программное обеспечение сервера
- ☒ сервер физически разрывается;
- ☐ с сервера удаляются страницы сайта

195 какое свойство является главной отличительной чертой компьютерного вируса?

- ☐ он не может распространяться по сети
- ☐ он может распространяться по сети
- ☐ он способен распространяться без участия человека
- ☒ он способен причинить вред компьютеру;
- ☐ он может находиться в файле или загрузочном секторе диска

196 Отметьте все правильные утверждения про антивирус-сканер.

- ☐ реагирует на события, похожие на действия вирусов
- ☐ может обнаруживать вирусы в файлах
- ☐ может уничтожать известные ему вирусы

- ☒ может обнаруживать и уничтожать все вирусы.
- ☐ может блокировать вирус в момент заражения

197 Отметьте вредоносные программы, которые распространяются в компьютерных сетях

- ☐ вирусы-черви
- ☐ файловые вирусы
- ☐ загрузочные вирусы
- ☒ троянские программы.
- ☐ макровирусы

198 какие ошибки допускает пользователь?

- ☐ пользуется сложными паролями
- ☐ не пользуется защитными программами
- ☐ месяцами не меняет пароли, оставляет избыточную информацию о себе в открытом доступе
- ☒ Выбрать несколько ответов.
- ☐ просматривает все электронные письма с вложениями

199 В чем недостатки антивирусов-мониторов?

- ☐ не умеют уничтожать вирусы в файлах
- ☐ замедляют работу компьютера
- ☐ могут привести к серьезному сбою системы
- ☒ не умеют уничтожать вирусы.
- ☐ не умеют блокировать вирусы, полученные из сети Интернет

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

- ☐ сторож;
- ☐ сканер;
- ☐ доктор;
- ☒ детектор
- ☐ ревизор;

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

- ☐ пустые письма;
- ☐ нигерийские письма;
- ☐ фишинг;
- ☒ черный пиар
- ☐ источник слухов;

202 Защита информации это:

- ☒ деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё
- ☐ получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- ☐ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- ☐ процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- ☐ совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

203 какие сведения на территории РФ могут составлять коммерческую тайну?

- ☐ любые;

- ☐ документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
- ☐ сведения о численности работающих, их заработной плате и условиях труда;
- ☒ учредительные документы и устав предприятия
- ☐ другие;

204 какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

- ☐ коммерческая тайна;
- ☐ запатентованная информация;
- ☐ только открытая информация;
- ☒ любая информация
- ☐ закрываемая собственником информация;

205 к посторонним лицам нарушителям информационной безопасности относится:

- ☐ лица, нарушившие пропускной режим;
- ☐ сотрудники службы безопасности;
- ☐ пользователи;
- ☐ технический персонал, обслуживающий здание;
- ☒ представители конкурирующих организаций

206 Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

- ☐ OCTAVE
- ☒ OECD.
- ☐ ISO/IEC
- ☐ Безопасная OECD
- ☐ CPTED

207 какие вредоносные программы могут заражать документы Word и Excel?

- ☐ сетевые черви
- ☐ макровирусы
- ☐ загрузочные вирусы
- ☒ файловые вирусы.
- ☐ троянские программы

208 Метод скрытие — это...

- ☐ поиск максимального числа лиц, допущенных к секретам;
- ☐ уменьшение числа секретов неизвестных большинству сотрудников;
- ☐ максимального ограничения числа лиц, допускаемых к секретам;
- ☒ максимальное ограничение числа секретов, из-за допускаемых к ним лиц
- ☐ выбор правильного места, для утаивания секретов от конкурентов;

209 какое действие нужно выполнить в самом начале, если на компьютере обнаружен вирус?

- ☐ отформатировать винчестер
- ☐ отключить питание компьютера
- ☐ перегрузить компьютер
- ☒ запустить антивирус.
- ☐ отключить компьютер от сети

210 Отметьте все ситуации, в которых компьютер может быть заражен вирусом.

- ☐ скачивание зараженного файла из Интернета
- ☐ автозапуск зараженного флэш-диска

- ☐ копирование зараженного файла на диск
- ☒ загрузка с зараженного DVD-диска.
- ☐ посещение зараженного сайта

211 Отметьте объекты, которые могут быть заражены компьютерными вирусами

- ☐ веб-страницы
- ☐ видео
- ☐ рисунки
- ☒ исполняемые файлы;
- ☐ драйверы устройств

212 По каким признакам можно предположить, что компьютер заражен вирусом?

- ☐ по электронной почте приходят непонятные сообщения
- ☐ возникают сбои при работе программ
- ☐ уменьшается объем свободной оперативной памяти
- ☒ появляются новые файлы и удаляются существующие;
- ☐ изменяется размер файлов

213 какие существуют наиболее общие задачи защиты информации на предприятии?

- ☐ все вышеперечисленные;
- ☐ документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
- ☐ предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
- ☒ снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной
- ☐ создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;

214 Показателями безопасности информации являются:

- ☐ вероятность сбоя системы безопасности;
- ☐ время, в течение которого обеспечивается определённый уровень безопасности;
- ☐ время, необходимое на взлом защиты информации;
- ☒ вероятность предотвращения угрозы.
- ☐ вероятность возникновения угрозы информационной безопасности;

215 Информацию, существенную и важную в настоящий момент времени, называют:

- ☐ достоверной;
- ☐ понятной;
- ☐ полезной;
- ☒ актуальной.
- ☐ полной;

216 Структурированная защита согласно Оранжевой книге используется в системах класса

- ☐ B3
- ☒ B2.
- ☐ C1
- ☐ B1
- ☐ C2

217 ACL-список ассоциируется с каждым

- ☐ процессом
- ☐ типом доступа

- ☒ объектом.
- ☐ типом
- ☐ доменом

218 резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры, клавиатурные шпионы типа

- ☐ нарушители
- ☐ заместители
- ☐ перехватчики
- ☒ фильтры.
- ☐ имитаторы

219 Требования к техническому обеспечению системы защиты

- ☐ документарные и аппаратурные
- ☐ процедурные и отдельные
- ☐ управленческие и документарные
- ☒ аппаратурные и физические.
- ☐ административные и аппаратурные

220 Стандарт DES основан на базовом классе

- ☐ шифры
- ☐ перестановки
- ☐ замещения
- ☒ блочные шифры.
- ☐ гаммирование

221 Естественные угрозы безопасности информации вызваны:

- ☐ ошибками при действиях персонала;
- ☒ воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека
- ☐ ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- ☐ деятельностью человека;
- ☐ корыстными устремлениями злоумышленников;

222 Защита информации от утечки это деятельность по предотвращению:

- ☐ несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации;
- ☐ воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
- ☐ 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;
- ☐ получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- ☒ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа

223 В соответствии с федеральным законом РФ Об информации, информатизации и защите информации (1995) информация - это

- ☐ сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- ☐ сведения, обладающие новизной для их получателя;
- ☐ сведения, фиксируемые в виде документов;

- ☒ та часть знаний, которая используется для ориентирования, активного действия, управления, то есть в целях сохранения, совершенствования, развития системы
- ☐ все то, что так или иначе может быть представлено в знаковой форме;

224 В каком документе содержатся основные требования к безопасности информационных систем в США?

- ☐ в красном блокноте;
- ☐ в оранжевой книге;
- ☐ в желтой прессе;
- ☒ в красной книге
- ☐ в черном списке;

225 какие секретные сведения входят в понятие коммерческая тайна ?

- ☐ три первых варианта ответа;
- ☐ технические и технологические решения предприятия;
- ☐ связанные с планированием производства и сбытом продукции;
- ☒ связанные с производством
- ☐ только 1 и 2 вариант ответа;

226 Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

- ☐ правильного ответа нет;
- ☐ добросовестная конкуренция;
- ☐ промышленный шпионаж;
- ☒ политическая разведка
- ☐ конфиденциальная информация;

227 какие существуют наиболее общие задачи защиты информации на предприятии?

- ☐ все вышеперечисленные;
- ☐ документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
- ☐ предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
- ☒ снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной.
- ☐ создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;

228 С доступом к информационным ресурсам внутри организации связан уровень ОС

- ☐ канальный
- ☐ приложений
- ☐ системный
- ☒ сетевой.
- ☐ внешний

229 OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

- ☐ AS/NZS не ориентирован на ИТ
- ☐ AS/NZS ориентирован на ИТ
- ☒ NIST и OCTAVE ориентирован на ИТ.
- ☐ NIST и OCTAVE являются корпоративными
- ☐ NIST и AS/NZS являются корпоративными

230 Регистрацией в системе Windows 2000 управляет

- ☐ msgina.dll
- ☒ процедура winlogon.
- ☐ logon.lld
- ☐ процедура lsass
- ☐ logon.dll

231 При передаче по каналам связи на канальном уровне избыточность вводится для

- ☐ мониторингом
- ☐ реализации проверки со стороны отправителя
- ☐ контроля канала связи
- ☒ контроля ошибок.
- ☐ реализации проверки со стороны отправителя

232 Согласно Оранжевой книге мандатную защиту имеет группа критериев

- ☐ E
- ☐ C
- ☐ A
- ☒ B.
- ☐ D

233 Согласно Европейским критериям только общая архитектура системы анализируется на уровне

- ☐ E4
- ☐ E2
- ☐ E3
- ☒ E1.
- ☐ E0

234 Согласно Оранжевой книге с объектами должны быть ассоциированы

- ☐ подписи
- ☐ типы операций
- ☐ электронные подписи
- ☒ метки безопасности.
- ☐ уровни доступа

235 Что включают в себя технические мероприятия по защите информации?

- ☐ все вышеперечисленное;
- ☐ подавление технических средств постановкой помехи;
- ☐ кодирование информации или передаваемого сигнала;
- ☒ поиск и уничтожение технических средств разведки
- ☐ применение детекторов лжи;

236 Соответствие средств безопасности решаемым задачам характеризует

- ☐ надежность
- ☐ унификация
- ☐ адекватность
- ☒ эффективность.
- ☐ корректность

237 На какую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны

- ☐ правильного ответа нет;
- ☐ Росинформресурс;

- ☐ Комитет по Использованию Информации при Госдуме;
- ☒ Министерство Информатики АР
- ☐ все выше перечисленные;

238 В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?

- ☐ в Указе Президента АР № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации»;
- ☐ в Законе об частной охране и детективной деятельности;
- ☐ в Законе об оперативно розыскной деятельности;
- ☒ в Конституции АР
- ☐ в Законе об информации, информатизации и защите информации;

239 какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

- ☐ OCTAVE
- ☐ NIST
- ☐ AS/NZS
- ☐ Анализ связующего дерева
- ☒ Анализ сбоев и дефектов.

240 Проверка подлинности пользователя по предъявленному им идентификатору — это

- ☐ контроль доступа.
- ☐ авторизация.
- ☐ идентификация.
- ☒ аутентификации
- ☐ аудит.

241 Присвоение субъектам и объектам доступа уникального номера, шифра, клда и т.п. с целью получения доступа к информации — это

- ☐ контроля доступа
- ☐ авторизация
- ☐ аудит
- ☒ идентификация.
- ☐ аутентификация

242 Применение средств защиты физического уровня ограничивается услугами

- ☐ аудит
- ☐ целостности
- ☐ контроля доступа
- ☒ конфиденциальности.
- ☐ аутентификации

243 Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это

- ☐ администрированием
- ☐ идентификация
- ☐ аутентификация
- ☒ авторизация.
- ☐ аудит

244 Право управлять безопасностью СУБД и отслеживать действия пользователей дает привилегия

- ☐ security operator.
- ☐ createdb.
- ☐ trace.
- ☒ security
- ☐ operator.

245 Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется

- ☐ аутентификация.
- ☐ администрированием.
- ☐ управлением ресурсами.
- ☒ мониторингом
- ☐ аудитом.

246 Право на удаление баз данных дает привилегия

- ☐ security operator.
- ☐ trace.
- ☐ create trace.
- ☒ createdb
- ☐ operator.

247 Поддержка диалога между удаленными процессами реализуется на _____ уровне модели взаимодействия открытых систем

- ☐ Представительный
- ☐ транспортном
- ☐ канальном
- ☒ сеансовом.
- ☐ сетевом

248 Право на запуск сервера дает привилегия

- ☐ create trace.
- ☐ trace.
- ☐ security operator.
- ☒ operator
- ☐ security.

249 По умолчанию пользователь не имеет никаких прав доступа к

- ☐ таблицам
- ☐ процедурам
- ☐ базам данных
- ☒ таблицам и представлениям.
- ☐ событиям

250 Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

- ☐ внутренним
- ☐ внешнем
- ☐ приложений
- ☒ системном.
- ☐ сетевом

251 Недостатком многоуровневых моделей безопасности является

- ☐ недоступность специального режима передачи сообщений

- ☐ сложность представления широкого спектра правил обеспечения безопасности
- ☐ отсутствие полного аудита
- ☒ невозможность учета индивидуальных особенностей субъекта.
- ☐ отсутствие контроля за потоками информации

252 Наиболее надежным механизмом для защиты содержания сообщений является

- ☐ специальный контроль доступа
- ☐ специальный режим передачи сообщения
- ☐ дополнительный хост
- ☒ криптография.
- ☐ специальный аппаратный модуль

253 Согласно Оранжевой книге верифицированную защиту имеет группа критериев

- ☐ E
- ☐ C
- ☐ B
- ☒ A.
- ☐ D

254 Отметьте все правильные утверждения про антивирус-монитор.

- ☐ реагирует на события, похожие на действия вирусов
- ☐ может обнаруживать вирусы в файлах при обращении к ним
- ☐ может обнаруживать вирусы в памяти
- ☒ может обнаруживать и уничтожат все вирусы.
- ☐ может блокировать вирус в момент заражения

255 Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство

- ☐ совокупность
- ☐ целостность
- ☐ восстанавливаемость
- ☒ доступность.
- ☐ детерминированность

256 В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен

- ☐ быть больше
- ☐ быть меньше
- ☐ быть равен
- ☒ доминировать.
- ☐ специально оговариваться

257 В СУБД Oracle под ролью понимается

- ☐ совокупность
- ☐ группа объектов
- ☐ совокупность процессов
- ☒ набор привилегий.
- ☐ группа субъектов

258 Уполномоченные серверы фильтруют пакеты на уровне

- ☐ прикладным
- ☐ канальном

- ☐ транспортном
- ☒ приложений.
- ☐ физическом

259 У всех программных закладок имеется общая черта

- ☐ обязательно выполняют операцию чтения
- ☐ обязательно выполняют операцию чтения из памяти
- ☐ перехватывают прерывания
- ☒ обязательно выполняют операцию записи в память.
- ☐ постоянно находятся в оперативной памяти

260 Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

- ☒ адресов отправителя и получателя.
- ☐ структуры данных
- ☐ электронной подписи
- ☐ содержания сообщений
- ☐ адрес приложения

261 как предотвращение неавторизованного использования ресурсов определена услуга защиты

- ☐ идентификация
- ☐ причастность
- ☐ аутентификация
- ☐ целостность
- ☒ контроль доступа.

262 Из перечисленного функция подтверждения подлинности сообщения использует следующие факты: 1) санкционированный канал связи; 2) санкционированный отправитель; 3) лицензионное программное обеспечение; 4) неизменность сообщения при передаче; 5) доставка по адресу

- ☐ 1, 3, 5;
- ☐ 1, 2, 3;
- ☒ 2, 4, 5;
- ☐ 1, 2, 4, 5;
- ☐ 3, 4, 5;

263 Из перечисленного, с точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются: 1) нормативы; 2) ограничения; 3) стандарты; 4) правила

- ☐ 1, 3;
- ☒ 2, 4;
- ☐ 1, 4;
- ☐ 1, 2;
- ☐ 3, 4;

264 Из перечисленного электронная почта состоит из: 1) электронного ключа; 2) расширенного содержания письма; 3) краткого содержания письма; 4) тела письма; 5) прикрепленных файлов

- ☐ 2, 3, 5;
- ☐ 1, 2, 3;
- ☐ 1, 4, 5;
- ☐ 2, 3, 4;
- ☒ 3, 4, 5;

265 Полномочия ядра безопасности ОС ассоциируются с

- ☐ базами данных

- ☐ пользователями
- ☐ приложениями
- ☐ периферийными устройствами
- ☒ процессами.

266 к системам оповещения относятся:

- ☐ электрохимические датчики;
- ☐ электрофизические датчики;
- ☐ электромеханические датчики ;
- ☐ неэлектрические датчики
- ☒ инфракрасные датчики.

267 к оборонительным системам защиты относятся:

- ☐ электрофизические датчики;
- ☒ звуковые установки.
- ☐ датчики;
- ☐ электромеханические датчики ;
- ☐ электрохимические датчики;

268 Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:

- ☐ полиморфные
- ☐ иммунизатором;
- ☒ сканером.
- ☐ доктора и фаги;
- ☐ ревизором

269 к тщательно контролируемым зонам относятся:

- ☐ световые;
- ☐ администратор;
- ☐ электрохимические датчики;
- ☒ архив.
- ☐ пользователя;

270 Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:

- ☐ Угроза информационной безопасности
- ☒ политика безопасности.
- ☐ Комплексное обеспечение информационной безопасности
- ☐ атака на автоматизированную систему
- ☐ Безопасность АС

271 Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

- ☐ принцип системности;
- ☐ принцип комплексности;
- ☐ принцип непрерывности;
- ☒ принцип разумной достаточности.
- ☐ принцип гибкости системы ;

272 Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

- ☐ конфиденциальность;

- ☐ аутентичность;
- ☐ апеллируемость;
- ☐ доступность;
- ☒ целостность.

273 Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

- ☐ информационное превосходство
- ☐ государственная тайна
- ☒ коммерческая тайна;
- ☐ банковская тайна
- ☐ конфиденциальная информация

274 Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:

- ☐ Информационная безопасность
- ☐ информационное превосходство;
- ☒ информационное оружие.
- ☐ информационная война;
- ☐ Информационная защита

275 Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

- ☐ Внутренняя защита;
- ☐ Защищенность информации;
- ☐ Защита информации;
- ☒ Компьютерная безопасность.
- ☐ Безопасность данных;

276 к выполняемой функции защиты относится:

- ☐ внутренняя защита
- ☐ сложная
- ☐ исходная
- ☒ все варианты верны.
- ☐ внешняя защита

277 какие компоненты входят в комплекс защиты охраняемых объектов:

- ☐ админ;
- ☐ Система;
- ☒ Датчики.
- ☐ Вирус
- ☐ Оружие;

278 к вирусам не изменяющим среду обитания относятся:

- ☐ доступность
- ☐ полиморфные
- ☐ студенческие;
- ☐ ревизоро;
- ☒ спутник.

279 Согласно Европейским критериям для систем с высокими потребностями в обеспечении целостности предназначен класс

- ☐ F-A
- ☐ F-DI
- ☐ F-DX
- ☒ F-IN.
- ☐ F-AV

280 к типам угроз безопасности парольных систем относятся

- ☒ все варианты ответа верны.
- ☐ атака на основе психологии;
- ☐ тотальный перебор
- ☐ словарная атака;
- ☐ разглашение параметров учетной записи;

281 Что нельзя делать при установке антивирусного ПО (программного обеспечения)?

- ☐ антивирус и брандмауэр могут быть от одинаковых производителей, потому что они выполняют одинаковые задачи
- ☐ можно одновременно устанавливать на компьютер два антивируса от разных производителей, они будут дополнять функции друг друга
- ☐ антивирус и брандмауэр могут быть от разных производителей, потому что они выполняют разные задачи
- ☒ нельзя устанавливать одновременно на компьютер два антивируса от разных производителей, они будут конфликтовать друг с другом.
- ☐ антивирус и брандмауэр не могут быть от разных производителей, потому что они не смогут обмениваться базой вирусов

282 В Интернете всплывает объявление, в котором написано, что ваш компьютер заражён. Вам предлагают загрузить программу для лечения вашего компьютера. какими будут ваши действия?

- ☐ у меня уже имеется похожая программа
- ☐ загружу и установлю, т.к. давно хотел сменить антивирусник
- ☐ не буду загружать, т.к. на моём компьютере есть все необходимые мне программы
- ☒ не буду загружать, т.к. эта программа – фальшивый антивирус, она сама станет источником вирусов;
- ☐ я уже загрузил ранее такую программу

283 когда необходимо проводить полную проверку компьютера и всех дисков (если у вас есть, например, внешние жесткие диски) антивирусом?

- ☐ не реже раза в год;
- ☐ при каждом посещении интернета;
- ☐ не реже раз в месяц;
- ☒ не реже раз в неделю.
- ☐ при каждой угрозе заражения;

284 Программу нужно обязательно проверить на наличие вирусов...

- ☐ перед вторым запуском;
- ☐ после первого запуска;
- ☐ перед каждым запуском
- ☒ перед первым запуском.
- ☐ после каждого запуска;

285 Что такое файрволл?

- ☐ вирусная программа;
- ☐ комплекс аппаратных или программных средств, осуществляющий лечение компьютера и восстановление повреждённых программ и файлов с помощью сетевых пакетов в соответствии с заданными правилами;
- ☐ брандмауэр;
- ☒ комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

- ☐ межсетевой экран;

286 Вам звонит не знакомый человек и претворяется инспектором ГИБДД. Он сообщает, что кто-то из ваших родственников попал в автопроишествие, и требует, что бы вы перевели на его номер телефона некоторую сумму, в качестве штрафа

- ☐ юридическая презумпция
☐ психологическая презумпция
☐ психологическая инженерия
☒ социальная презумпция.
☐ социальная инженерия

287 Цель применения фишинга?

- ☐ переписка от чужого лица с целью вымогательства денежных средств
☐ почистить ваш компьютер от вирусов на бесплатном сайте
☐ заманить вас на поддельный сайт, что бы вы не смогли размещать в Интернете инфор мацию
☒ заманть вас на поддельный сайт, что бы украсть данные вашего аккаунта (т. е. логин и пароль).
☐ реклама новых сайтов

288 Система защиты должна гарантировать, что любое движение данных

- ☐ копируется, шифруется, проектируется
☐ контролируется, кодируется, фиксируется, шифруется
☐ анализируется, идентифицируется, шифруется, учитывается
☒ аидентифицируется, авторизуется, обнаруживается, документируется.
☐ копируется, шифруется, проектируется, авторизуется

289 Программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти в модели воздействия

- ☒ перехват.
☐ уборка мусора
☐ наблюдение
☐ компрометация
☐ уборка, перехват

290 Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

- ☐ адекватность
☐ надежность информации
☐ защищенность информации
☒ базопасность информации.
☐ уязвимость информации

291 При количественном подходе риск измеряется в терминах

- ☐ заданных с помощью информации
☐ заданных с помощью ранжирования
☐ заданных с помощью шкалы
☒ денежных потерь.
☐ объема информации

292 Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется

- ☐ помощью открытого ключа информация

- ☐ минимизацией риска
- ☐ мониторингом средств защиты
- ☐ оптимизацией средств защиты
- ☒ управлением риском.
- ☐ максимизация риска

293 С помощью открытого ключа информация

- ☐ не копируется
- ☐ транслируется
- ☐ копируется
- ☒ зашифровывается.
- ☐ расшифровывается

294 Согласно Европейским критериям на распределенные системы обработки информации ориентирован класс

- ☐ F-D
- ☐ F-AV
- ☐ F-IN
- ☒ F-DI.
- ☐ F-DX

295 Содержанием параметра угрозы безопасности информации конфиденциальность является

- ☐ модификация
- ☐ искажение
- ☐ уничтожение
- ☒ несанкционированное получение.
- ☐ несанкционированная модификация

296 Администратор сервера баз данных имеет имя

- ☐ system
- ☐ sysadm
- ☐ admin
- ☒ ingres.
- ☐ root

297 Брандмауэры первого поколения представляли собой

- ☐ хосты с фильтрацией
- ☐ «уполномоченные серверы»
- ☐ «неприступные серверы»
- ☒ маршрутизаторы с фильтрацией пакетов.
- ☐ хосты с фильтрацией пакетов

298 какие степени сложности устройства Вам известны

- ☐ встроенные;
- ☐ сложная;
- ☒ простые.
- ☐ упрощенные;
- ☐ оптические;

299 хранение паролей может осуществляться

- ☐ все варианты ответа верны
- ☐ в закрытом виде;

- ☐ в закрытом виде;
- ☒ в виде сверток.
- ☐ в незашифрованном виде

300 Гарантия точного и полного выполнения команд в АС:

- ☐ доступность;
- ☐ контролируемость;
- ☒ точность.
- ☐ надежность;
- ☐ устойчивость ;

301 В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен

- ☐ быть меньше
- ☐ доминировать
- ☒ быть равен.
- ☐ совокупность
- ☐ специально оговариваться

302 Дескриптор защиты в Windows 2000 содержит список

- ☐ объектов
- ☒ пользователей и групп, имеющих доступ к объекту.
- ☐ объектов, не доступных пользователям
- ☐ привилегий, назначенных пользователю
- ☐ объектов, доступных пользователю и группе

303 Назначение троянских программ...

- ☐ засорение ПО
- ☐ уничтожить компьютер пользователя
- ☐ реклама и промоакции
- ☒ красть и уничтожать данные пользователя.
- ☐ ограничение доступа пользователя в Интернет

304 Из перечисленного управление маршрутизацией используется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- ☐ 4, 6;
- ☐ 5, 6;
- ☐ 2, 4, 6;
- ☒ 1, 5
- ☐ 3, 5;

305 Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это

- ☐ идентификация, аудит
- ☐ авторизация
- ☐ аудит
- ☒ идентификация.
- ☐ аутентификация

306 Обычно в СУБД применяется управление доступом

- ☐ древовидное
- ☐ административное

- ☐ иерархическое
☒ произвольное.
☐ декларируемое

307 Из перечисленного услуга обеспечения доступности реализуется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- ☐ 2, 3, 5;
☐ 2, 4, 6;
☐ 2, 6;
☒ 1, 5
☐ 3, 5;

308 Из перечисленного типами услуг аутентификации являются: 1) идентификация; 2) достоверность происхождения данных; 3) достоверность объектов коммуникации; 4) причастность;

- ☐ 1, 3
☐ 1, 2
☐ 3, 4
☒ 2, 3;
☐ 1, 4

309 Из перечисленного составляющими информационной базы для монитора обращений являются: 1) виды доступа; 2) программы; 3) файлы; 4) задания; 5) порты; 6) форма допуска

- ☐ 3, 4
☐ 4, 5
☐ 2, 4
☒ 1, 6;
☐ 2, 3

310 Для чего нужен хакеру пароль от вашего почтового ящика?

- ☐ чтобы от вашего имени рассылать спам-сообщения на имеющиеся в вашей адресной книге адреса
☐ чтобы украсть деньги с электронного кошелька, закреплённого за этим ящиком
☐ чтобы переписываться с другими хакерами
☒ вредоносная программа от вашего имени будет рассылать по имеющимся в вашей адресной книге адресам письма с вложенными в них троянами или вирусами и т. д.;
☐ вредоносная программа от вашего имени будет рассылать по имеющимся в вашей адресной книге адресам письма с поздравлениями

311 Выделите три наиболее важных метода защиты информации от ошибочных действий пользователя.

- ☐ шифрование файлов;
☐ дублирование носителей информации;
☐ автоматический запрос на подтверждение выполнения команды или операции;
☒ установление специальных атрибутов файлов.
☐ предоставление возможности отмены последнего действия;

312 Выделите три наиболее важных метода защиты информации от нелегального доступа.

- ☐ шифрование;
☐ использование специальных «электронных ключей»;
☐ архивирование (создание резервных копий);
☒ использование антивирусных программ.
☐ установление паролей на доступ к информации;

313 Операционная система Windows 2000 отличает каждого пользователя от других по

- ☐ идентификатору защиты
- ☐ дескриптору защиты
- ☐ маркеру безопасности
- ☒ идентификатору безопасности.
- ☐ маркеру доступа

314 Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером

- ☐ 3, 4, 5
- ☒ 2, 3, 4;
- ☐ 1, 3, 4
- ☐ 1, 2, 3
- ☐ 1, 4, 5

315 Из перечисленных привилегии СУБД подразделяются на категории: 1) чтения; 2) безопасности; 3) доступа; 4) тиражирования

- ☐ 3, 4
- ☐ 3, 4
- ☐ 1, 4
- ☒ 2, 3;
- ☐ 1, 2

316 На каком уровне защиты информации создаются комплексные системы защиты информации?

- ☐ на всех вышеперечисленных;
- ☐ на тактическом;
- ☐ на социально политическом;
- ☒ на организационно-правовом
- ☐ на инженерно-техническом;

317 включает в себя ранжирование как метод защиты информации?

- ☐ вариант ответа 1, 2 и 3;
- ☐ наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;
- ☐ деление засекречиваемой информации по степени секретности;
- ☒ регламентацию допуска и разграничение доступа к защищаемой информации
- ☐ вариант ответа 1 и 2;

318 Что нельзя публиковать в Интернете?

- ☐ свои заметки
- ☐ свои фотографии
- ☐ свою биографию
- ☒ сведения о учёбе и работе.
- ☐ паспортные данные

319 Согласно Оранжевой книге уникальные идентификаторы должны иметь

- ☐ важные объекты
- ☐ наиболее важные субъекты
- ☐ наиболее важные объекты
- ☒ все субъекты.
- ☐ все объекты

320 Что в себя морально-нравственные методы защиты информации?

- ☐ вариант ответа 1, 2 и 3;

- ☐ обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
- ☐ контроль работы сотрудников, допущенных к работе с секретной информацией;
- ☒ воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений.
- ☐ вариант ответа 1 и 3;

321 какие средства защиты информации в ПК наиболее распространены?

- ☐ все вышеперечисленные;
- ☐ средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
- ☐ средства защиты от копирования коммерческих программных продуктов;
- ☒ применение различных методов шифрования, не зависящих от контекста информации
- ☐ защита от компьютерных вирусов и создание архивов;

322 Цель прогресса внедрения и тестирования средств защиты —

- ☐ выбор мер
- ☐ определить уровень расходов на систему защиты
- ☐ выбор мер и средств защиты
- ☒ гарантировать правильность реализации средств защиты.
- ☐ выявить нарушителя

323 к функциям информационной безопасности не относятся:

- ☐ подготовка специалистов по обеспечению информационной безопасности
- ☐ Страхование информационных ресурсов
- ☐ выявление источников внутренних и внешних угроз
- ☐ совершенствование законодательства РФ в сфере обеспечения информационной безопасности
- ☒ Не защита государственных информационных ресурсов.

324 Особенности информационного оружия являются:

- ☐ доступность
- ☒ универсальность
- ☐ открытость
- ☐ системность
- ☐ надежность

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

- ☐ пустые письма;
- ☐ нигерийские письма;
- ☒ фишинг
- ☐ черный пиар;
- ☐ источник слухов;

326 к достоинствам технических средств защиты относятся:

- ☐ Все ответы не верны;
- ☐ степень сложности устройства;
- ☒ создание комплексных систем защиты.
- ☐ регулярный контроль
- ☐ Все варианты верны

327 Подключение компьютера к локальной сети выполняется при помощи:

- ☐ кабеля
- ☐ сервера

- ☒ сетевого адаптера
- ☐ топологии сети
- ☐ сетевого фильтра

328 Сети, узлы которой расположены на небольшом расстоянии друг от друга, не использующие средства связи общего назначения называют:

- ☐ сетевыми
- ☐ сервисными
- ☐ функциональными
- ☒ локальными
- ☐ глобальными

329 Что представляет таблица в базе данных Access:

- ☐ таблица – это объект, который мы определяем и используем для передачи данных
- ☐ таблица – это объект, который мы определяем и используем для удаления данных
- ☐ таблица – это объект, который мы определяем и используем для манипулирования данных
- ☒ таблица – это объект, который мы определяем и используем для хранения данных
- ☐ таблица – это объект, который мы определяем и используем для обмена данными

330 Объектом обработки MS Access является файл с расширением:

- ☐ .xls
- ☒ .mdb
- ☐ .doc
- ☐ .txt
- ☐ .ppt

331 Что из перечисленного относится к СУБД:

- ☐ Adobe Illustrator
- ☐ MS Outlook
- ☐ MS Powerpoint
- ☒ MS Access
- ☐ Corel Draw

332 MS Access. Что является отчетом:

- ☐ объект, предназначенный для презентаций
- ☐ объект, предназначенный для сохранения документа
- ☐ объект, предназначенный для создания документа
- ☐ объект, предназначенный для удаления документа
- ☒ объект, предназначенный для печати документа

333 Перечислить основные объекты базы данных Access:

- ☒ в базе данных Access основными объектами являются таблицы, запросы, формы, отчеты, макросы и модули
- ☐ в базе данных Access основными объектами являются таблицы, запросы, макросы и формы
- ☐ в базе данных Access основными объектами являются таблицы, запросы, макросы и модули
- ☐ в базе данных Access основными объектами являются таблицы, запросы, формы, отчеты
- ☐ в базе данных Access основными объектами являются таблицы, отчеты, макросы и модули

334 СУБД Access не работает с:

- ☒ презентациями
- ☐ отчетами
- ☐ таблицами
- ☐ формами

- ☐ запросами

335 какие топологии сети бывают:

- ☐ сервисная
☐ кольцо, асимметрия, звезда
☐ шина, асимметрия
☒ шина, кольцо, звезда
☐ в виде овала

336 Что может включать глобальная сеть:

- ☐ произвольная глобальная сеть может включать функциональные сети
☒ произвольная глобальная сеть может включать другие глобальные сети
☐ произвольная глобальная сеть может включать отдельно подключаемые к ней компьютеры (удаленные компьютеры) или отдельно подключаемые устройства ввода-вывода
☐ произвольная глобальная сеть может включать локальные сети
☐ произвольная глобальная сеть может включать другие глобальные сети, локальные сети, а также отдельно подключаемые к ней компьютеры (удаленные компьютеры) или отдельно подключаемые устройства ввода-вывода

337 Самая простая топология сети:

- ☐ звезда
☐ кольцо
☒ шина
☐ асимметрия
☐ в виде овала

338 Что содержит таблица ACCESS:

- ☐ строки
☐ поля (столбцы) и записи
☐ поля (столбцы)
☐ записи
☒ строки и столбцы

339 к логическим функциям в редакторе MS Excel не относятся:

- ☐ или
☐ если
☒ да
☐ не
☐ и

340 какие файлы на практике имеют наибольший коэффициент сжатия:

- ☐ графические файлы
☐ видео-файлы
☒ аудио-файлы
☐ текстовые файлы
☐ программные файлы

341 Локальная сеть. как называется конфигурация локальной сети (схема соединения):

- ☐ ресурс
☐ форма
☒ топология
☐ объединение
☐ система

342 как представляется изображение при кодировании рисунка средствами растровой графики:

- ☒ представляется в виде мозаики из квадратных элементов, каждый из которых имеет свой цвет
- ☐ представляется совокупностью координат точек, имеющих одинаковый цвет
- ☐ преобразуется в черно-белый вариант изображения
- ☐ преобразуется в двумерный массив координат
- ☐ разбивается на ряд областей с одинаковой площадью

343 Сколько ячеек электронной таблицы в диапазоне A2:B4:

- ☐ 12
- ☒ 6
- ☐ 8
- ☐ 4
- ☐ 2

344 команде Открыть в Excel соответствует комбинация клавиш:

- ☐ Ctrl+F10
- ☐ Alt+F12
- ☐ F11+Shift
- ☒ Ctrl+O
- ☐ F6+Ctrl

345 команде Вырезать соответствует комбинация клавиш:

- ☐ Ctrl+B
- ☐ Ctrl+C
- ☐ Ctrl+P
- ☐ Ctrl+V
- ☒ Ctrl+X

346 СУБД Access не работает с:

- ☐ отчетами
- ☐ таблицами
- ☐ формами
- ☐ запросами
- ☒ презентациями

347 Укажите антивирусные программы:

- ☐ Aidtest, UNIX
- ☒ Aidtest, Doctor Web
- ☐ WinZip, MS DOS
- ☐ UNIX, MS DOS
- ☐ WinRar, WinZip

348 В каком окне Access можно увидеть межтабличные связи?

- ☐ панель подстановок
- ☐ конструктор формы
- ☐ конструктор отчета
- ☐ конструктор таблицы
- ☒ схема данных

349 Укажите верное написание адреса Internet страницы:

- ☐ http://www.mail.ru

- ☐ http://www.mail-ru
- ☒ http://www.mail.ru
- ☐ http://www.mail
- ☐ http://www.mail.ru

350 Access. Для отображения результатов вычисления необходимо:

- ☐ создать таблицу с вычисляемыми полями
- ☒ создать запрос с вычисляемыми полями
- ☐ ввести формулу с свободную таблицу
- ☐ создать макрос
- ☐ запустить калькулятор

351 Причины возникновения ошибки в данных

- ☐ Использование недопустимых методов анализа данных
- ☒ Неверная интерпретация данных
- ☐ Ошибка при записи результатов измерений в промежуточный документ
- ☐ Погрешность измерений
- ☐ Ошибки при переносе данных с промежуточного документа в компьютер

352 к формам защиты информации не относится...

- ☐ все ответы не верны
- ☒ аналитическая
- ☐ правовая
- ☐ организационно-техническая
- ☐ страховая

353 Наиболее эффективное средство для защиты от сетевых атак

- ☐ все ответы не верны
- ☐ использование только сертифицированных программ-броузеров при доступе к сети Интернет
- ☐ посещение только «надёжных» Интернет-узлов
- ☒ использование сетевых экранов или «firewall»
- ☐ использование антивирусных программ

354 Информация, составляющая государственную тайну не может иметь гриф...

- ☒ «для служебного пользования»
- ☐ все ответы не верны
- ☐ «совершенно секретно»
- ☐ «особой важности»
- ☐ «секретно»

355 Разделы современной криптографии:

- ☒ Симметричные криптосистемы
- ☐ Криптосистемы с открытым ключом
- ☐ Управление паролями
- ☐ Системы электронной подписи
- ☐ Криптосистемы с дублированием защиты

356 Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности

- ☐ рекомендации X.800
- ☐ все ответы верны.
- ☐ все ответы не верны

- ☒ Закону «Об информации, информационных технологиях и о защите информации»
☐ Оранжевая книга

357 Утечка информации – это ...

- ☒ несанкционированный процесс переноса информации от источника к злоумышленнику
☐ все ответы не верны
☐ непреднамеренная утрата носителя информации
☐ процесс уничтожения информации
☐ процесс раскрытия секретной информации

358 Основные угрозы конфиденциальности информации:

- ☐ карнавал
☒ злоупотребления полномочиями
☐ перехват данных
☐ блокирование
☐ переадресовка

359 Элементы знака охраны авторского права:

- ☐ буквы С в окружности или круглых скобках
☐ года первого выпуска программы
☒ буквы Р в окружности или круглых скобках
☐ наименования (имени) правообладателя
☐ наименование охраняемого объекта

360 Защита информации обеспечивается применением антивирусных средств

- ☐ да
☐ все ответы не верны
☐ обеспечивается
☒ не всегда
☐ нет

361 Средства защиты объектов файловой системы основаны на...

- ☒ определении прав пользователя на операции с файлами и каталогами
☐ все ответы не верны.
☐ антивирусной программе
☐ средства нанесения контратаки с помощью информационного оружия
☐ задании атрибутов файлов и каталогов, независящих от прав пользователей

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

- ☐ Медленная
☐ Быстрая
☐ все ответы не верны
☒ пассивная
☐ активная

363 Найдите отличительные особенности компьютерного вируса:

- ☐ компьютерный вирус легко распознать и просто удалить
☐ он обладает значительным объемом программного кода и ловкостью действий
☐ вирус имеет способности к повышению помехоустойчивости операционной системы и к расширению объема оперативной памяти компьютера
☐ все ответы не верны

- ☒ он обладает маленьким объемом, способностью к самостоятельному запуску и многократному копированию кода, к созданию помех корректной работе компьютера

364 как происходит заражение почтовым вирусом?

- ☒ при открытии зараженного файла, присланного с письмом по e-mail
☐ все не верны.
☐ при получении с письмом, присланном по e-mail, зараженного файла
☐ при подключении к почтовому серверу
☐ при подключении к web-серверу, зараженному «почтовым» вирусом

365 как вирус может появиться в компьютере?

- ☐ при решении математической задачи
☒ при работе компьютера в сети
☐ при работе с макросами
☐ все не верны.
☐ самопроизвольно

366 какие программы не относятся к антивирусным?

- ☐ программы-фаги
☐ все не верны.
☐ программы-детекторы
☒ программы сканирования
☐ программы-ревизоры

367 какая программа не является антивирусной?

- ☐ Norton Antivirus
☒ Defrag
☐ AVP
☐ все не верны.
☐ Dr Web

368 Загрузочные вирусы характеризуются тем, что ...

- ☐ запускаются при загрузке компьютера
☒ поражают загрузочные секторы дисков
☐ поражают программы в начале их работы
☐ изменяют весь код заражаемого файла
☐ все ответы не верны

369 Создание компьютерных вирусов является

- ☐ последствием сбоев операционной системы
☐ все ответы не верны
☒ преступлением
☐ побочным эффектом при разработке программного обеспечения
☐ необходимым компонентом подготовки программистов

370 Что необходимо иметь для проверки на вирус жесткого диска?

- ☐ защищенную программу
☐ все ответы не верны
☒ антивирусную программу, установленную на компьютер
☐ файл с антивирусной программой
☐ загрузочную программу

371 Найдите правильные слова: компьютерные вирусы ...

- ☐ возникают в связи со сбоями в аппаратных средствах компьютера
- ☐ все ответы не верны
- ☐ являются следствием ошибок в операционной системе компьютера
- ☐ зарождаются при работе неверно написанных программных продуктов
- ☒ пишутся людьми специально для нанесения ущерба пользователям персональных компьютеров

372 категории компьютерных вирусов НЕ относятся

- ☐ загрузочные вирусы
- ☐ все ответы не верны
- ☐ сетевые вирусы
- ☐ файловые вирусы
- ☒ туре-вирусы

373 компьютерным вирусом является ...

- ☐ программа проверки и лечения дисков
- ☐ все ответы не верны
- ☒ специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться"
- ☐ программа, скопированная с плохо отформатированной дискеты
- ☐ любая программа, созданная на языках низкого уровня

374 как обнаруживает вирус программа-ревизор?

- ☐ контролирует важные функции компьютера и пути возможного заражения
- ☐ отслеживает изменения загрузочных секторов дисков
- ☒ при открытии файла подсчитывает контрольные суммы и сравнивает их с данными, хранящимися в базе данных
- ☐ периодически проверяет все имеющиеся на дисках файлы
- ☐ все ответы не верны

375 Положения, которые целесообразно вынести в инструкцию по работе за компьютером, разрабатываемую для компьютерного класса средней школы

- ☐ при работе в Интернет не соглашаться на предложения загрузить и/или установить неизвестную программу
- ☐ не открывать почтовые сообщения от неизвестных отправителей
- ☐ перед работой с любым объектом, загруженным из Интернета, его следует проверить на вирусы
- ☐ не открывать почтовые сообщения, содержащие вложения
- ☒ перед работой (копированием, открытием, запуском) с файлами, размещенными на внешнем носителе (компакт-диск, дискета, флеш-накопитель) нужно проверить их на отсутствие вирусов

376 Антиспамовая программа, установленная на домашнем компьютере, служит для ...

- ☐ все ответы не верны
- ☐ корректной установки и удаления прикладных программ
- ☐ обеспечения регулярной доставки антивирусной программе новых антивирусных баз
- ☐ защиты компьютера от хакерских атак
- ☒ защиты компьютера от нежелательной и/или незапрошенной корреспонденции

377 косвенное проявление наличия вредоносной программы на компьютере

- ☐ неожиданное самопроизвольное завершение работы почтового агента
- ☒ неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
- ☐ неожиданно появляющееся всплывающее окно с текстом порнографического содержания
- ☐ неожиданное отключение электроэнергии
- ☐ неожиданное уведомление антивирусной программы об обнаружении вируса

378 Сигнатурный метод антивирусной проверки заключается в ...

- ☐ сравнении файла с известными образцами вирусов
- ☒ анализе поведения файла в разных условиях
- ☐ все ответы не верны
- ☐ анализе кода на предмет наличия подозрительных команд
- ☐ отправке файлов на экспертизу в компанию-производителя антивирусного средства

379 какие мероприятия не являются административными при обеспечении мер безопасности:

- ☒ выявление уязвимостей в системе защиты
- ☐ контроль журналов работы
- ☐ пропускной режим
- ☐ контроль смены паролей
- ☐ порядок хранения документов

380 Чему равен коэффициент сжатия, если начальный объем составлял 250 кбайт, после сжатия 50 кбайт

- ☒ 20%
- ☐ 50%
- ☐ 15 %
- ☐ 10%
- ☐ 25%

381 какого типа файлы лучше всего сжимаются:

- ☐ все ответы не верны
- ☐ текстовые
- ☒ графические
- ☐ исполняемые
- ☐ скрытые

382 Файловые вирусы:

- ☐ все ответы не верны
- ☐ запускаются при запуске компьютера
- ☐ поражают программы в начале их работы
- ☐ поражают загрузочные сектора дисков
- ☒ изменяют весь код заражаемого файла

383 Загрузочные вирусы:

- ☒ поражают загрузочные сектора дисков
- ☐ изменяют весь код заражаемого файла
- ☐ запускаются при открытии файла
- ☐ все ответы не верны
- ☐ запускаются при запуске компьютера

384 Отличительными особенностями компьютерного вируса являются:

- ☐ все ответы верны
- ☐ значительный объем программного кода
- ☒ маленький объем и способность к самостоятельному запуску и созданию
- ☐ помехи корректной работе компьютера
- ☐ необходимость запуска со стороны пользователя

385 компьютерные вирусы:

- ☒ создаются людьми специально для нанесения ущерба ПК
- ☐ зарождаются при работе неверно написанных программных продуктов

- ☐ все ответы верны
- ☐ все ответы не верны
- ☐ являются следствием ошибок в операционной системе

386 какое из названных действий можно произвести со сжатым файлом:

- ☒ распаковать
- ☐ запустить на выполнение
- ☐ все ответы верны
- ☐ все ответы не верны
- ☐ просмотреть

387 Искусственные угрозы безопасности информации вызваны:

- ☐ деятельностью человека;
- ☐ ошибками при действиях персонала.
- ☐ ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- ☐ воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
- ☒ корыстными устремлениями злоумышленников;

388 Естественные угрозы безопасности информации вызваны:

- ☐ деятельностью человека;
- ☐ корыстными устремлениями злоумышленников;
- ☐ ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- ☒ воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
- ☐ ошибками при действиях персонала.

389 Пользователь (потребитель) информации это:

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

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

- ☐ отказ в обслуживании;
- ☐ удаленный контроль над станцией в сети.
- ☒ анализ сетевого трафика;
- ☐ ложный объект распределенной вычислительной сети;
- ☐ подмена доверенного объекта или субъекта распределенной вычислительной сети;

391 к внутренним нарушителям информационной безопасности относится:

- ☐ клиенты.
- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☐ технический персонал, обслуживающий здание;
- ☒ посетители;
- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

392 к внутренним нарушителям информационной безопасности относится:

- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☒ сотрудники отделов разработки и сопровождения ПО;
- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- ☐ посетители;
- ☐ клиенты.

393 к основным непреднамеренным искусственным угрозам АСОИ относится:

- ☐ нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
- ☐ чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- ☐ изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- ☐ перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.
- ☒ физическое разрушение системы путем взрыва, поджога и т.п.;

394 к основным непреднамеренным искусственным угрозам АСОИ относится:

- ☐ физическое разрушение системы путем взрыва, поджога и т.п.;
- ☒ перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.
- ☐ чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- ☐ изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- ☐ неумышленная порча носителей информации;

395 к основным непреднамеренным искусственным угрозам АСОИ относится:

- ☐ чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- ☐ перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.
- ☒ изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- ☐ неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- ☐ физическое разрушение системы путем взрыва, поджога и т.п.;

396 к основным непреднамеренным искусственным угрозам АСОИ относится:

- ☒ неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
- ☐ изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- ☐ перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
- ☐ физическое разрушение системы путем взрыва, поджога и т.п.;
- ☐ чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

397 Выберите вариант, в котором единицы измерения информации расположены в порядке возрастания.

- ☐ гигабайт, мегабайт, терабайт
- ☐ все ответы неверны
- ☐ мегабайт, терабайт, гигабайт
- ☐ терабайт, мегабайт, гигабайт
- ☒ мегабайт, гигабайт, терабайт

398 количество информации содержащееся в одном разряде двоичного числа равно...

- ☐ все ответы неверны
- ☐ 2 байта
- ☐ 1 байт
- ☐ 2 бита
- ☒ 1 бит

399 В вычислительной технике в качестве основной используется _____ система счисления

- ☐ все ответы неверны
- ☐ восьмеричная
- ☐ шестнадцатеричная
- ☒ двоичная
- ☐ десятичная

400 Наибольшее натуральное число, кодируемое 7 битами, равно...

- ☐ все ответы неверны
- ☐ 255
- ☐ 127
- ☐ 256
- ☒ 128

401 В ЭВМ для записи целых положительных чисел используется ...

- ☐ обратный код
- ☒ мантисса и порядок
- ☐ дополнительный код
- ☐ все ответы неверны
- ☐ прямой код

402 Свойство алгоритма _____ означает, что при корректно заданных исходных данных алгоритм выдает результат за фиксированное число шагов

- ☒ конечность
- ☐ детерминированность
- ☐ все ответы неверны
- ☐ понятность
- ☐ массовость

403 Свойство алгоритма _____ означает, что применение алгоритма к одним и тем же данным должно давать одинаковый результат

- ☐ все ответы неверны
- ☐ результативность
- ☐ конечность
- ☐ детерминированность (определенность)
- ☒ массовость

404 к внутренним нарушителям информационной безопасности относится:

- ☒ персонал, обслуживающий технические средства.
- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☐ клиенты;
- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- ☐ посетители;

405 к внутренним нарушителям информационной безопасности относится:

- ☒ пользователи системы;
- ☐ клиенты;
- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
- ☐ посетители;

406 к основным преднамеренным искусственным угрозам АСОИ относится:

- ☐ пересылка данных по ошибочному адресу абонента;
- ☐ неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- ☐ игнорирование организационных ограничений (установленных правил) при работе в системе;
- ☐ разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).
- ☒ незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему;

407 к основным преднамеренным искусственным угрозам АСОИ относится:

- ☐ игнорирование организационных ограничений (установленных правил) при работе в системе;
- ☐ разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).
- ☐ пересылка данных по ошибочному адресу абонента;
- ☐ неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- ☒ незаконное подключение к линиям связи с целью работы "между строк";

408 Энтропия в информатике – это свойство ...

- ☒ знаний
- ☐ все ответы неверны
- ☐ информации
- ☐ условий поиска
- ☐ данных

409 хранение информации это -

- ☐ способ распространения информации во времени
- ☐ процесс создание распределенных компьютерных баз и банков данных;
- ☐ распространение новой информации полученной в процессе научного познания
- ☐ предотвращение доступа к информации лицам, не имеющим на это права
- ☒ предотвращение непредумышленного или несанкционированного использования изменения информации

410 каково максимальное количество символов, в которых может измеряться ширина столбца в Excel:

- ☐ от 0 до 409
- ☐ от 0 до 8
- ☐ от 1 до 898
- ☐ от 0 до 76
- ☒ от 0 до 255

411 какой вид расширения имеют файлы, создаваемые в Excel:

- ☒ .xls
- ☐ .exe
- ☐ .com
- ☐ .pas
- ☐ .txt

412 как называются координаты ячейки в таблицах Excel:

- ☐ номер
- ☐ буква
- ☐ [yeni cavab]
- ☒ адрес
- ☐ цифра

413 какой элемент таблицы Excel является основным:

- ☒ ячейка
- ☐ строка
- ☐ столбец
- ☐ информация
- ☐ адрес

414 как называется информация, которая является результатом различных операций в таблицах Excel:

- ☐ рабочая
- ☒ производная
- ☐ исходная
- ☐ табличная
- ☐ первичная

415 С помощью, какой команды в редакторе Word осуществляется набор текста в несколько колонок:

- ☐ Таблица – Скрыть сетку
- ☐ Файл – Параметры страниц
- ☐ Вид – Схема документа
- ☒ Формат – Колонки
- ☐ Сервис – Параметры

416 В каком пункте горизонтального меню редактора Word находится команда Предварительный просмотр :

- ☐ Окно
- ☐ Правка
- ☒ Файл
- ☐ Сервис
- ☐ Вид

417 В каком пункте горизонтального меню редактора Word находится команда Разрыв, которая позволяет установить принудительный переход на другую страницу:

- ☐ Вид
- ☐ Файл
- ☒ Вставка
- ☐ Правка
- ☐ Сервис

418 Используя, какой пункт горизонтального меню редактора Word, можно вставить сноску:

- ☐ Формат
- ☐ Правка
- ☐ Вставка
- ☐ Файл
- ☒ Вид

419 В каком пункте горизонтального меню редактора Word устанавливаются номера страниц:

- ☐ Правка
- ☐ Файл
- ☐ Вид
- ☒ Вставка
- ☐ Формат

420 . В каком пункте горизонтального меню редактора Word устанавливаются параметры страницы:

- ☐ Сервис

- ☐ Справка
- ☐ Правка
- ☒ Файл
- ☐ Вид

421 При вводе больших текстов в редакторе Word для занесения элемента в список авто коррекции (автозамены), выбирают команду:

- ☒ Сервис – Параметры автозамены
- ☐ Файл – Отправить
- ☐ Правка – Найти
- ☐ Вставка – Автотекст
- ☐ Окно – Новое

422 компьютерный вирус - это

- ☐ файл который при запуске <<заражаем>> другие
- ☒ специальная программа способная размножаться
- ☐ средство для проверке дисков
- ☐ программы для отслеживания вирусов
- ☐ программа

423 Excel. Ячейки, которые находятся слева, справа, сверху и внизу от текущей, называются:

- ☐ специальными
- ☐ соседними
- ☐ встроенными
- ☐ несмежными
- ☒ смежными

424 Excel. Данные в ячейке, которая должна содержать результат вычислений, начинаются с символа:

- ☒ & =
- ☐ \
- ☐ /
- ☐ *
- ☐ +

425 Word. Чтобы вывести на экран изображение координатной линейки, надо воспользоваться пунктом меню:

- ☒ вид
- ☐ правка
- ☐ таблица
- ☐ формат
- ☐ сервис

426 какие из перечисленных элементов не присутствуют в окне приложения Word:

- ☐ строка заголовка
- ☐ линейки
- ☐ строка состояния
- ☒ кнопки диалога
- ☐ горизонтальное меню

427 В каком пункте меню Word находится опция установки междустрочного интервала:

- ☐ вид
- ☐ правка

- ☐ сервис
- ☒ формат
- ☐ вставка

428 каково максимальное количество пунктов, в которых измеряется высота строки в Excel:

- ☐ от 0 до 255
- ☒ от 0 до 409
- ☐ от 1 до 765
- ☐ от 0 до 4
- ☐ от 0 до 567
- ☐ [yeni cavab]

429 Word. Чтобы выделить предложение, надо:

- ☐ подвести курсор на предложение и, удерживая в нажатом положении клавишу ALT, щелкните левой кнопкой мыши
- ☐ подвести курсор на предложение и, удерживая в нажатом положении клавишу ALT, щелкните правой кнопкой мыши
- ☐ подвести курсор на предложение и, удерживая в нажатом положении клавишу CTRL, щелкните правой кнопкой мыши
- ☒ подвести курсор на предложение и, удерживая в нажатом положении клавишу CTRL, щелкните левой кнопкой мыши
- ☐ подвести курсор на предложение и, удерживая в нажатом положении клавишу SHIFT, щелкните левой кнопкой мыши

430 Word. Чтобы выделить слово, надо:

- ☐ удерживая клавишу ALT, один раз щелкнуть по нему
- ☐ один раз щелкнуть по нему
- ☒ дважды щелкнуть по нему
- ☐ удерживая клавишу CTRL, один раз щелкнуть по нему
- ☐ удерживая клавишу SHIFT, два раза щелкнуть по нему

431 Текст в Word нельзя выровнять:

- ☐ по левому краю
- ☐ по центру
- ☐ по ширине
- ☒ по длине
- ☐ по правому краю

432 Что такое тип документа:

- ☒ расширение имени файла-документа
- ☐ месторасположение документа на жестком диске
- ☐ картинка, которая представляет собой какой-либо файл в Windows
- ☐ объем документа
- ☐ название документа

433 Excel. Абсолютный адрес ячейки это:

- ☐ обозначение ячейки, составленное из номера строки
- ☐ обозначение ячейки, составленное из номера столбца
- ☐ обозначение ячейки, составленное буквами латинского алфавита
- ☒ обозначение ячейки, составленное с помощью знака \$ и номера столбца и (или) номера строки
- ☐ обозначение ячейки, составленное из номера столбца и номера строки

434 Excel. какая из формул записана правильно:

- ☐ $A1+A2+A3$
- ☐ $A1+A2+A3=$
- ☒ $=1A+2A$
- ☐ $=A1+A2+3B$
- ☐ $=1+A2+A3$

435 какое расширение имеют графические файлы растрового формата:

- ☐ .txt
- ☒ .bmp или .pcx
- ☐ .doc
- ☐ .arj или .rar
- ☐ .bat

436 Наиболее популярная служба Интернет:

- ☐ Archie
- ☐ FTP
- ☒ E-mail
- ☐ Wais
- ☐ Gopher

437 Электронная почта - это:

- ☐ письмо, в котором можно переслать текстовую информацию
- ☐ письмо, в котором можно переслать анимационные объекты, рисунки, звуки
- ☒ сетевая служба, позволяющая обмениваться текстовыми электронными сообщениями через Интернет
- ☐ обыкновенное письмо, посылаемое не через почтам, а с помощью некоторого электронного оборудования
- ☐ сообщение, посылаемое только с помощью локальной сети

438 В какой программе имеются достаточно эффективные средства, позволяющие создавать высококачественные презентации:

- ☒ Microsoft Power Point
- ☐ Microsoft Excel
- ☐ Adobe PhotoShop
- ☐ Microsoft Word
- ☐ Microsoft Access

439 В электронной таблице выделена группа ячеек A1:C2. Сколько ячеек входит в эту группу:

- ☐ 7
- ☐ 4
- ☐ 3
- ☒ 6
- ☐ 5

440 Укажите элемент, характерный для окна табличного процессора Excel:

- ☐ пункт горизонтального меню «Таблица»
- ☐ кнопка «Пуск»
- ☐ панель задач
- ☐ ярлыки и значки объектов
- ☒ строка формул

441 Рабочий лист книги Excel представляет собой:

- ☐ стандартное окно, содержащее панель Таблица и границы
- ☐ произвольный шаблон таблицы

- ☒ готовую таблицу со столбцами, поименованными заглавными латинскими буквами и пронумерованными строками
- ☐ рабочую область папки
- ☐ чистый лист, на котором с помощью специальных инструментов создается таблица

442 как называется документ табличного процессора Excel:

- ☒ книгой
- ☐ пакетом
- ☐ листом
- ☐ страницей
- ☐ презентацией

443 Электронный табличный процессор Excel позволяет:

- ☐ применить анимации к данным
- ☐ форматировать данные по ширине
- ☐ строить рисованные объекты различного типа
- ☐ форматировать рисунки
- ☒ обрабатывать табличные данные

444 Если набранная последовательность символов начинается со знака = , то Excel считает , что это:

- ☐ текст
- ☐ диаграмма
- ☐ функция
- ☒ формула
- ☐ числа

445 Относительный адрес ячейки это:

- ☐ обозначение ячейки, написанное буквами латинского алфавита
- ☒ обозначение ячейки, составленное из номера столбца и номера строки
- ☐ обозначение ячейки, составленное из номера строки
- ☐ обозначение ячейки, составленное из номера столбца
- ☐ обозначение ячейки, составленное с помощью \$ и номера столбца и (или) номера строки

446 Домен – это:

- ☐ совокупность Web-страниц, принадлежащая частному лицу или организации и размещенная на каком-либо Web-сервере
- ☐ специальное имя пользователя, которое он использует в чатах
- ☐ компьютер, который предоставляет по сети данные, необходимые для работы программ
- ☐ документ, который наряду с обычной текстовой и графической информацией, содержит ссылки на другие документы, причем эти ссылки встроены в текстовые фрагменты или в графические объекты данного документа
- ☒ общая часть имени у группы компьютеров в Интернет, она определяет место нахождения компьютера и категорию организации - владельца

447 По умолчанию числа выравниваются в электронной таблице MS EXCEL:

- ☐ по длине
- ☐ по левому краю
- ☒ по правому краю
- ☐ по ширине
- ☐ по центру

448 По умолчанию текст выравнивается в электронной таблице MS EXCEL:

- ☐ по длине

- ☐ по ширине
- ☐ по центру
- ☒ по левому краю
- ☐ по правому краю

449 Для создания маркированного или нумерованного списков нужно:

- ☐ выполнить команду Вставка – Номера
- ☐ использовать инструмент панели Рисование “Список”
- ☒ выполнить команду Формат – Список – выбрать нужный тип
- ☐ использовать панель Рисование
- ☐ использовать инструмент панели Форматирование “Кисть”

450 Текстовый редактор Word позволяет создать таблицу следующим способом:

- ☒ команда Таблица - Вставить -Таблица
- ☐ команда Вставка – Нарисовать таблицу
- ☐ с помощью инструментов панели «Рисование»
- ☐ использовать карандаш панели Рисование
- ☐ инструмент “Добавить таблицу” панели Рисование

451 какой специальный символ используется при написании адреса электронной почты?

- ☐ *
- ☒ @
- ☐ \$
- ☐ 5
- ☐ #

452 Для создания баз данных, а также выполнения операции поиска и сортировки данных предназначены специальные программы:

- ☐ библиотечные модули
- ☒ автоматические системы управления (АСУ)
- ☐ системы управления базами данных (СУБД)
- ☐ системы автоматического проектирования (САПР)
- ☐ компьютерные сети

453 Access. Что является запросом:

- ☐ запрос – это объект, предназначенный для ввода данных
- ☒ запрос – это объект, предназначенный для отбора, фильтрации, сортировки данных
- ☐ запрос – это объект, предназначенный для отображения данных на бумаге
- ☐ запрос – это объект, предназначенный для форматирования данных
- ☐ запрос – это объект, предназначенный для ввода данных и отображения их на экране

454 Word. Виды списков:

- ☐ линейный
- ☐ разветвляющийся
- ☐ нумерованный
- ☐ немаркированный
- ☒ маркированный, нумерованный, многоуровневый

455 какая программа предназначена для работы в сети Internet?

- ☐ MS Excel
- ☐ Paint
- ☐ MS Access

- ☒ Internet Explorer
- ☐ MS Word

456 MS EXCEL. Чтобы подтвердить ввод формулы в ячейку, надо:

- ☐ нажать клавишу CTRL
- ☐ нажать клавишу ESC
- ☐ щелкнуть мышью на другой ячейке
- ☒ нажать Enter
- ☐ задать команду Файл - Сохранить

457 MS EXCEL . Создать новую рабочую книгу можно:

- ☐ запуском программы MS Word
- ☐ выбором команды Файл – Открыть
- ☐ использованием кнопки Открыть на Стандартной панели инструментов
- ☐ использованием комбинации клавиш Alt + N
- ☒ выбором команды Файл – Создать

458 Access. Что такое база данных:

- ☒ база данных – это набор данных, которые организованы специальным образом
- ☐ база данных – это набор записей, которые организованы специальным образом
- ☐ база данных – это набор файлов, которые организованы специальным образом
- ☐ база данных – это набор символов, которые организованы специальным образом
- ☐ база данных – это набор записей и файлов, которые организованы специальным образом

459 Под угрозой удаленного администрирования в компьютерной сети понимается угроза

- ☒ несанкционированного управления удаленным компьютером
- ☐ поставки неприемлемого содержания
- ☐ вмешательства в личную жизнь
- ☐ внедрения агрессивного программного кода в рамках активных объектов Web-страниц
- ☐ перехвата или подмены данных на путях транспортировки

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

- ☐ МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
- ☐ Многократный ввод данных и сличение введенных значений
- ☐ все ответы не верны
- ☐ МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
- ☒ МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

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

- ☐ все ответы не верны
- ☐ способна противостоять только внешним информационным угрозам
- ☒ 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
- ☐ 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
- ☐ способна противостоять только информационным угрозам, как внешним так и внутренним

462 Сервисы безопасности:

- ☐ шифрование
- ☒ идентификация и аутентификация
- ☐ регулирование конфликтов
- ☐ контроль целостности
- ☐ инверсия паролей

463 Методы повышения достоверности входных данных

- ☐ Введение избыточности в документ первоисточник
- ☒ Использование вместо ввода значения его считывание с машиночитаемого носителя
- ☐ Проведение комплекса регламентных работ
- ☐ Отказ от использования данных
- ☐ Замена процесса ввода значения процессом выбора значения из предлагаемого множества

464 Суть компрометации информации

- ☐ все ответы не верны
- ☐ внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
- ☐ 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;
- ☒ несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

465 Для безопасного использования ресурсов в сети Интернет предназначен протокол...

- ☐ все ответы не верны
- ☐ FTP.
- ☒ HTTPS;
- ☐ NNTP;
- ☐ IRC;

466 Формой написания IP - адреса является запись вида: xxx.xxx.xxx.xxx , где xxx - это...

- ☐ Двоичный код;
- ☒ Десятичные числа от 0 до 255;
- ☐ все ответы не верны
- ☐ Буквы латинского алфавита.
- ☐ Десятичные числа от 0 до 999;

467 Для правильной, полной и безошибочной передачи данных необходимо придерживаться согласованных и установленных правил, которые оговорены в _____ передачи данных.

- ☐ Описание.
- ☒ Протокол;
- ☐ Канал;
- ☐ все ответы не верны
- ☐ Порт;

468 Любой узел сети Интернет имеет свой уникальный IP-адрес, который состоит из _____ чисел в диапазоне от 0 до 255.

- ☒ Четырех;
- ☐ все ответы не верны
- ☐ Двух.
- ☐ Пяти;
- ☐ Трех;

469 Основные угрозы доступности информации:

- ☐ отказ программного и аппаратно обеспечения
- ☐ злонамеренное изменение данных
- ☐ разрушение или повреждение помещений
- ☒ хакерская атака
- ☐ непреднамеренные ошибки пользователей

470 Сетевым протоколом является...

- ☐ все ответы не верны
- ☐ Инструкция;
- ☒ Набор программ;
- ☐ Набор правил;
- ☐ Программа.

471 концепция системы защиты от информационного оружия не должна включать...

- ☐ средства нанесения контратаки с помощью информационного оружия
- ☐ все ответы не верны.
- ☒ процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей
- ☐ механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
- ☐ признаки, сигнализирующие о возможном нападении

472 Преднамеренная угроза безопасности информации

- ☒ кража
- ☐ все ответы не верны
- ☐ ошибка разработчика
- ☐ наводнение
- ☐ повреждение кабеля, по которому идет передача, в связи с погодными условиями

473 к внутренним нарушителям информационной безопасности относится:

- ☐ клиенты.
- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☒ посетители;
- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- ☐ технический персонал, обслуживающий здание;

474 к внутренним нарушителям информационной безопасности относится:

- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- ☒ сотрудники отделов разработки и сопровождения ПО;
- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☐ клиенты.
- ☐ посетители;

475 Заражение компьютерными вирусами может произойти в процессе ...

- ☒ работы с файлами
- ☐ выключения компьютера
- ☐ все ответы не верны
- ☐ печати на принтере
- ☐ форматирования диска

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

- ☐ все ответы не верны

- ☐ Бутовый
- ☐ Червь
- ☐ Троян
- ☒ Макровирус

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

- ☐ Сторожа
- ☒ Полифаги
- ☐ Ревизоры.
- ☐ Блокировщики.
- ☐ все ответы не верны

478 Выберите правильный ответ из предложенных вариантов. какие программы относятся к антивирусным?

- ☐ MS Word, MS Excel, Paint
- ☒ AVP, DrWeb, Norton AntiVirus.
- ☐ MS-DOS, MS Word, AVP.
- ☐ все ответы не верны
- ☐ MS Word, MS Excel, Norton Commander.

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

- ☐ На удалении зараженных файлов.
- ☐ все ответы не верны
- ☐ На всех перечисленных
- ☐ На ожидании начала вирусной атаки.
- ☒ На сравнение программных кодов с известными вирусами.

480 Выберите правильный ответ из предложенных вариантов. какие существуют вспомогательные средства защиты?

- ☐ Все перечисленное
- ☒ Аппаратные средства и антивирусные программы.
- ☐ Аппаратные средства.
- ☐ Программные средства
- ☐ все ответы не верны

481 Выберите правильный ответ из предложенных вариантов. какие существуют основные средства защиты?

- ☒ Резервное копирование наиболее ценных данных.
- ☐ Программные средства
- ☐ Все перечисленное
- ☐ все ответы не верны
- ☐ Аппаратные средства.

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

- ☐ База данных.
- ☐ Прикладная программа.
- ☐ Системная программа.
- ☐ все ответы не верны
- ☒ Программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.

483 Программа для архивации файлов - это:

- ☐ программа для создания резервных копий файлов
- ☐ все ответы верны
- ☒ программа для уменьшения (сжатия) исходного объема файлов
- ☐ программа для просмотра архивных файлов
- ☐ все ответы не верны

484 Троянской программой является...

- ☒ Программа, вредоносное действие которой выражается в удалении и/или модификации системных файлов компьютера;
- ☐ 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.
- ☐ Программа, заражающая компьютер независимо от действий пользователя;
- ☐ Программа, проникающая на компьютер пользователя через Интернет.
- ☐ все ответы не верны

485 Вирусы могут быть: а) загрузочными, б) мутантами, в) невидимками, г) дефектными, д) логическими.

- ☐ все ответы не верны
- ☐ а, в, г;
- ☐ б, г, д;
- ☐ в, г, д;
- ☒ а, б, в;

486 Под утечкой информации понимается...

- ☐ Непреднамеренная утрата носителя информации;
- ☐ все ответы не верны
- ☐ Процесс раскрытия секретной информации.
- ☒ Несанкционированный процесс переноса информации от источника к злоумышленнику;
- ☐ Процесс уничтожения информации;

487 Программными средствами для защиты информации в компьютерной сети являются: 1) Firewall, 2) Brandmauer, 3) Sniffer, 4) Backup.

- ☐ 2 и 3;
- ☒ 1 и 4;
- ☐ все ответы не верны
- ☐ 1 и 2.
- ☐ 3 и 4;

488 Результатом реализации угроз информационной безопасности может быть...

- ☐ Уничтожение устройств ввода/вывода;
- ☒ Внедрение дезинформации.
- ☐ Уничтожение каналов связи;
- ☐ все ответы не верны
- ☐ Изменение конфигурации периферийных устройств;

489 Электронная цифровая подпись документа позволяет решить вопрос о ____ документа(у).

- ☐ Секретности.
- ☐ все ответы не верны
- ☒ Подлинности;
- ☐ Ценности;
- ☐ Режиме доступа к;

490 Из перечисленного: 1) пароли доступа, 2) дескрипторы, 3) шифрование, 4) хеширование, 5) установление прав доступа, 6) запрет печати, к средствам компьютерной защиты информации относятся:

- ☐ 4, 5, 6.
- ☐ 1, 4, 6;
- ☐ 2, 4, 6;
- ☐ все ответы не верны
- ☒ 1, 3, 5;

491 к антивирусным программам не относятся:

- ☐ фаги
- ☐ все ответы не верны
- ☐ ревизоры
- ☒ интерпретаторы
- ☐ мониторы

492 Назначение антивирусных программ, называемых детекторами:

- ☐ все ответы не верны
- ☐ уничтожение зараженных файлов
- ☐ обнаружение и уничтожение вирусов
- ☒ контроль возможных путей распространения компьютерных вирусов
- ☐ обнаружение компьютерных вирусов

493 Файловый вирус ...

- ☐ поражает загрузочные сектора дисков
- ☐ всегда меняет начало и длину файла
- ☐ все ответы не верны
- ☐ всегда меняет длину имени файла
- ☒ всегда изменяет код заражаемого файла

494 Заражение компьютерным вирусом не может произойти...

- ☐ При запуске на выполнение программного файла.
- ☒ При включении и выключении компьютера;
- ☐ При копировании файлов;
- ☐ все ответы не верны
- ☐ При открытии файла, прикрепленного к почте;

495 Типы методов антивирусной защиты

- ☐ практические
- ☒ программные
- ☐ технические
- ☐ теоретические
- ☐ организационные

496 к классу условно опасных относятся программы ...

- ☒ 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
- ☐ которые можно выполнять только при наличии установленного антивирусного программного обеспечения
- ☐ последствия выполнения которых нельзя предугадать
- ☐ о которых нельзя однозначно сказать, что они вредоносны
- ☐ все ответы не верны

497 Логические бомбы относятся к классу ...

- ☒ условно опасных программ
- ☐ файловых вирусов
- ☐ макровирусов
- ☐ сетевых червей
- ☐ троянов

498 Деятельность клавиатурных шпионов

- ☐ все ответы не верны
- ☐ находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают своему хозяину
- ☒ находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором
- ☐ находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими
- ☐ передают хозяину марку и тип используемой пользователем клавиатуры

499 Метаморфизм – это ...

- ☐ метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки
- ☒ метод маскировки от антивирусов с помощью шифрования
- ☐ все ответы не верны
- ☐ создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд
- ☐ создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд

500 Цель создания анонимного SMTP-сервера – для ...

- ☐ все ответы не верны
- ☐ распределенных вычислений сложных математических задач
- ☐ создания ботнета
- ☒ рассылки спама
- ☐ размещения на них сайтов с порнографической или другой запрещенной информацией

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

- ☒ более ясный и интуитивно понятный интерфейс
- ☐ отсутствие необходимости отдельно покупать его и устанавливать
- ☐ все ответы не верны
- ☐ возможность более точно задавать исключения
- ☐ наличие более полного функционала

502 Свойство вируса, позволяющее называться ему загрузочным – способность ...

- ☐ все ответы не верны
- ☒ заражать загрузочные сектора жестких дисков
- ☐ заражать загрузочные дискеты и компакт-диски
- ☐ вызывать перезагрузку компьютера-жертвы
- ☐ подсвечивать кнопку Пуск на системном блоке

503 Использование брандмауэров относят к ... методам антивирусной защиты.

- ☐ все ответы не верны
- ☐ теоретическим
- ☐ практическим
- ☒ организационным

☐ Техническим

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

- ☐ организационным
- ☐ теоретическим
- ☐ все ответы не верны
- ☐ техническим
- ☒ практическим

505 Задача, выполняющая модуль планирования, входящий в антивирусный комплекс

- ☐ настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса
- ☒ настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)
- ☐ определения параметров взаимодействия различных компонентов антивирусного комплекса
- ☐ все ответы не верны
- ☐ определения областей работы различных задач поиска вирусов

506 Обязательные свойства любого современного антивирусного комплекса

- ☒ быть кроссплатформенным (работать под управлением любой операционной системы)
- ☐ не мешать выполнению основных функций компьютера
- ☐ не занимать много системных ресурсов
- ☐ не занимать канал Интернет
- ☐ надежно защищать от вирусов

507 Трояны классифицируются по ...

- ☒ методу распространения
- ☐ методу размножения
- ☐ методу маскировки
- ☐ все ответы не верны
- ☐ типу вредоносной нагрузки

508 Стадии жизненного цикла классического трояна

- ☒ проникновение на чужой компьютер
- ☐ внедрение копий
- ☐ подготовка копий
- ☐ активация
- ☐ поиск объектов для заражения

509 Вирус – это программа, способная...

- ☐ нанести какой-либо вред компьютеру, на котором она запускается, или другим компьютерам в сети
- ☒ 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
- ☐ нанести какой-либо вред компьютеру, на котором она запускается, или другим компьютерам в сети: прямо или посредством других программ и/или приложения
- ☐ все ответы верны
- ☐ все ответы не верны

510 Типы троянов:

- ☐ клавиатурные шпионы
- ☐ логические бомбы
- ☒ утилиты скрытого удаленного управления
- ☐ похитители паролей

- ☐ дефрагментаторы дисков

511 Брандмауэр (firewall) – это программа, ...

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

512 Скрытые проявления вирусного заражения:

- ☐ неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
- ☐ наличие на рабочем столе подозрительных ярлыков
- ☐ подозрительная сетевая активность
- ☒ наличие в оперативной памяти подозрительных процессов
- ☐ наличие на компьютере подозрительных файлов

513 Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает ...

- ☒ явные проявления
- ☐ все ответы не верны
- ☐ скрытые проявления
- ☐ материальные проявления
- ☐ косвенные проявления

514 Преимущества эвристического метода антивирусной проверки над сигнатурным

- ☐ более надежный
- ☐ все ответы не верны
- ☐ позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
- ☒ не требует регулярного обновления антивирусных баз
- ☐ существенно менее требователен к ресурсам

515 Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности

- ☒ уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer
- ☐ все ответы не верны
- ☐ возможность одновременно работать в нескольких окнах
- ☐ возможность установить отличную от www.msn.com стартовую страницу
- ☐ уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer

516 Преимущества сигнатурного метода антивирусной проверки над эвристическим

- ☐ более надежный
- ☐ существенно менее требователен к ресурсам
- ☐ все ответы не верны
- ☒ позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
- ☐ не требует регулярного обновления антивирусных баз

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

- ☒ невозможность запуска антивирусной проверки в режиме реального времени
- ☐ все ответы не верны
- ☐ ложные срабатывания в работе персонального брандмауэра
- ☐ невозможность использовать антиспамовую программу в режиме реального времени
- ☐ трудности с регулярным автоматическим получением новых антивирусных баз

518 Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.

- ☐ да
- ☒ 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
- ☐ все ответы неверны
- ☐ 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
- ☐ нет

519 Активный перехват информации это перехват, который:

- ☐ осуществляется путем использования оптической техники;
- ☐ осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- ☐ основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- ☒ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- ☐ неправомерно использует технологические отходы информационного процесса;

520 Сколько процентов электронных писем являются Спамом?

- ☐ 90.
- ☒ 10;
- ☐ 30;
- ☐ 50;
- ☐ 70;

521 Подозрительная сетевая активность может быть вызвана ...

- ☐ все ответы неверны
- ☐ логической бомбой
- ☐ сетевым червем
- ☒ P2P-червем
- ☐ трояном

522 Перехват, который неправомерно использует технологические отходы информационного процесса называется:

- ☒ просмотр мусора.
- ☐ активный перехват;
- ☐ пассивный перехват;
- ☐ аудиоперехват;
- ☐ видеоперехват;

523 Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:

- ☐ пассивный перехват;
- ☐ активный перехват;
- ☐ просмотр мусора.
- ☒ видеоперехват;
- ☐ аудиоперехват;

524 Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

- ☒ пассивный перехват;
- ☐ активный перехват;
- ☐ просмотр мусора.
- ☐ видеоперехват;
- ☐ аудиоперехват;

525 Перехват, который осуществляется путем использования оптической техники называется:

- ☐ пассивный перехват;
- ☐ активный перехват;
- ☐ просмотр мусора.
- ☒ видеоперехват;
- ☐ аудиоперехват;

526 Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

- ☐ просмотр мусора.
- ☐ активный перехват;
- ☐ пассивный перехват;
- ☒ аудиоперехват;
- ☐ видеоперехват;

527 Аудиоперехват перехват информации это перехват, который:

- ☐ осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- ☒ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- ☐ основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- ☐ неправомерно использует технологические отходы информационного процесса;
- ☐ осуществляется путем использования оптической техники;

528 Пассивный перехват информации это перехват, который:

- ☐ основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- ☐ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- ☐ осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- ☒ осуществляется путем использования оптической техники;
- ☐ неправомерно использует технологические отходы информационного процесса;

529 Необходимость модуля обновления для любого современного антивирусного средства – для ...

- ☐ доставки сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу
- ☐ взаимодействия антивирусной программы с сайтом компании-производителя
- ☒ подключения антивирусных баз к антивирусной программе
- ☐ обеспечения взаимодействия операционной системы с антивирусным комплексом
- ☐ все ответы неверны

530 Основная задача, которую решает антивирусная проверка в режиме реального времени

- ☐ обеспечение невмешательства в процесс деятельности других программ
- ☒ обеспечение непрерывности антивирусной проверки
- ☐ все ответы неверны
- ☐ предоставление возможности глубокой проверки заданных объектов
- ☐ обеспечение взаимодействия между пользователем и антивирусной программой

531 Просмотр мусора это перехват информации, который:

- ☐ основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- ☐ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- ☐ осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- ☐ осуществляется путем использования оптической техники;
- ☒ неправомерно использует технологические отходы информационного процесса;

532 Защита информации от несанкционированного доступа это деятельность по предотвращению

- ☒ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
- ☐ несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- ☐ 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;
- ☐ получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- ☐ воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

533 Защита информации от непреднамеренного воздействия это деятельность по предотвращению:

- ☐ несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- ☒ получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- ☐ 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;
- ☐ воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
- ☐ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

534 Защита информации от несанкционированного воздействия это деятельность по предотвращению:

- ☐ несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- ☐ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
- ☐ получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- ☒ 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;
- ☐ воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

535 Защита информации от утечки это деятельность по предотвращению:

- ☐ несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- ☐ получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

- ☐ 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;
- ☐ воздействия на защищаемую информацию ошибок пользователя информацией, сбоем технических и программных средств информационных систем, а также природных явлений;
- ☒ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

536 Лицо, которое взламывает интрасеть в познавательных целях это:

- ☐ хакер;
- ☐ скамер;
- ☐ кракер.
- ☐ фракер;
- ☒ фишер;

537 Владелец информации это:

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

538 Собственник информации это:

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

539 Носитель информации это:

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

540 Субъект доступа к информации это:

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

541 Доступ к информации это:

- ☐ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- ☐ процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- ☐ деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
- ☒ совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- ☐ получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

542 Шифрование информации это:

- ☐ получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- ☐ процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- ☒ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- ☐ совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- ☐ деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

543 Информационные процессы это:

- ☐ получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- ☒ процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- ☐ деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
- ☐ совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- ☐ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

544 Защита информации это:

- ☐ совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- ☒ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- ☐ процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- ☐ получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- ☐ деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

545 хакер?

- ☐ Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
- ☐ Это лицо, которое взламывает интрасеть в познавательных целях;
- ☐ Так в XIX веке называли плохого игрока в гольф, дилетанта;
- ☐ Это мошенники, которые обманым путем выманивают у доверчивых пользователей сети конфиденциальную информацию.
- ☒ Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

546 как можно выделить весь рабочий лист в Excel:

- ☐ дважды щелкнув в ярлыке самого первого листа
- ☐ нажав Ctrl, нужно с помощью мыши выделить рабочий лист
- ☐ дважды щелкнув в ярлыке последнего листа

- ☒ щелкнув в ячейке стоящей на пересечении заголовка столбцов и строк
- ☐ нажав Shift нужно щелкнуть в ярлыке листа

547 как можно удалить лист рабочей книги в Excel:

- ☐ щелкнуть в ярлыке листа и нажать Delete
- ☐ на ярлыке листа нажать Backspace
- ☐ нельзя удалить лист
- ☐ дважды щелкнуть в ярлычке листа и нажать Delete
- ☒ с помощью вызова контекстного меню в ярлычке листа и выбрать команду Удалить

548 Excel. Чтобы отобразить/убрать строку формул и строку состояния на экране нужно:

- ☐ выполнить последовательность Сервис – Вид и включить соответствующие флажки
- ☐ выполнить последовательность Правка – Параметры – Вид и включить соответствующие флажки
- ☐ выполнить последовательность Сервис – Параметры – Вид и включить соответствующие флажки
- ☐ выполнить последовательность Сервис – Настройка – Вид и включить соответствующие флажки
- ☒ выполнить последовательность Вид – Строка формул и Вид – Строка состояния и включить соответствующие флажки

549 Excel. какие параметры устанавливаются в мастере диаграмм в первую очередь:

- ☒ тип диаграммы
- ☐ дополнительные элементы диаграммы
- ☐ размещение диаграммы
- ☐ размещение легенды
- ☐ диапазон данных

550 Если в меню текстового процессора Word некоторые команды сопровождаются многоточием, то это означает что:

- ☐ они требуют для своего выполнения дополнительной информации
- ☐ они используются наименее часто
- ☒ они при своем выполнении вызывают подменю
- ☐ они в данной ситуации - невыполнимы
- ☐ они используются наиболее часто

551 какая команда в редакторе Word позволяет подобрать синонимы к словам:

- ☐ Правка - Копировать
- ☒ Сервис – Язык - Тезаурус
- ☐ Формат - Шрифт
- ☐ Вставка-Символ
- ☐ Файл - Параметры страницы

552 Перед выводом документа Word на печать документ можно просмотреть с помощью команды:

- ☒ Файл → Предварительный просмотр
- ☐ Правка → Просмотр документа
- ☐ Вид → Просмотр документа
- ☐ Файл → Печать → Предварительный просмотр
- ☐ Вид → Предварительный просмотр

553 Для переименования рабочего листа Excel нужно:

- ☒ дважды щелкнуть на ярлычке листа и ввести новое имя
- ☐ в меню Вид выбрать пункт Переименовать и ввести новое имя
- ☐ в меню Сервис выбрать пункт Лист и ввести новое имя
- ☐ в меню Правка выбрать пункт Переименовать и ввести новое имя

- ☐ в меню Файл выбрать пункт Переименовать и ввести новое имя

554 Excel. Чтобы выделить весь столбец, надо:

- ☐ удерживая кнопку мыши, протянуть выделение вниз
☐ щелкнуть по номеру строки
☐ щелкнуть правой кнопкой мыши
☐ задать команду Правка-Выделить
☒ щелкнуть на ярлычке-заголовке

555 Объединить ячейки таблицы, вставленной в Word можно, если:

- ☒ выделить смежные ячейки и воспользоваться командой Таблица - Объединить ячейки
☐ объединение ячеек возможно только в Excel
☐ удалить одну из смежных ячеек с помощью клавиши Delete
☐ выделить смежные ячейки и воспользоваться командой Формат – Ячейки - Объединение
☐ выделить смежные ячейки и дважды щелкнуть правой кнопкой мыши

556 какая из операций не входит в форматирование текста:

- ☒ создание таблицы
☐ устанавливать межсимвольные интервалы
☐ определять эффекты в шрифтах
☐ устанавливать шрифт
☐ устанавливать межстрочные интервалы

557 Документы Word сохраняются в виде файлов с расширением:

- ☒ .doc
☐ .xls
☐ .dot
☐ .dbf
☐ .txt

558 Access. Что является формой:

- ☐ форма – это объект, предназначенный для отображения данных на экране
☐ форма – это объект, предназначенный для отображения данных на бумаге
☐ форма – это объект, предназначенный для ввода данных
☒ форма – это объект, предназначенный для ввода данных и отображения их на экране
☐ форма – это объект, предназначенный для редактирования данных

559 Домен .ru является _____ доменом.

- ☒ Зональным;
☐ все ответы не верны
☐ Первичным.
☐ Надежным;
☐ Основным;

560 Укажите правильно записанный IP-адрес в компьютерной сети

- ☐ www.50.50.10;
☐ www.alfa193.com.
☐ 192.154.144.270;
☐ 193.264.255.10;
☒ 10.172.122.26;

561 Системой, автоматически устанавливающей связь между IP-адресами в сети Интернет и текстовыми именами, является ...

- ☐ Доменная система имен (DNS);
- ☐ все ответы не верны
- ☐ Протокол передачи гипертекста.
- ☐ Интернет-протокол;
- ☒ Система URL-адресации;

562 Адрес веб-страницы для просмотра в браузере начинается с...

- ☐ ftp;
- ☐ все ответы не верны
- ☒ http;
- ☐ www;
- ☐ smtp

563 Протокол SMTP предназначен для...

- ☐ Общения в чате
- ☐ все ответы не верны
- ☐ Приема электронной почты.
- ☐ Просмотра веб-страниц;
- ☒ Отправки электронной почты;

564 Поток сообщений в сети передачи данных определяется:

- ☐ Треком;
- ☐ все ответы не верны
- ☐ Объемом памяти канала передачи сообщений;
- ☐ Скоростью передачи данных
- ☒ Трафиком;

565 Протокол POP3 работает на _____ уровне.

- ☐ Сетевом;
- ☒ Прикладном.
- ☐ все ответы не верны
- ☐ Транспортном;
- ☐ Физическом;

566 Протокол FTP предназначен для...

- ☐ загрузки сообщений из новостных групп
- ☐ все ответы не верны
- ☐ общения в чатах
- ☒ передачи файлов
- ☐ просмотра Web-страниц

567 Программы, которые позволяют обнаруживать файлы, зараженные одним из нескольких компьютерных вирусов, называют:

- ☐ завирусованные файлы
- ☐ программы-вирусы
- ☐ программы-вакцины
- ☒ программы-детекторы
- ☐ программы-архиваторы

568 Виды адресации в электронной таблице Excel:

- ☐ абсолютная, простая, смешанная
- ☐ абсолютная, смешанная, простая
- ☒ абсолютная, относительная, смешанная
- ☐ относительная, абсолютная, простая
- ☐ относительная, смешанная, простая

569 Что такое активная ячейка в Excel:

- ☐ промежуток ячеек
- ☐ смежные ячейки
- ☒ ячейка, выделенная табличным курсором
- ☐ соседняя ячейка
- ☐ последовательность ячеек

570 концепция системы защиты от информационного оружия не должна включать...

- ☐ инфраструктуры в целом и отдельных пользователей
- ☐ признаки, сигнализирующие о возможном нападении
- ☐ механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
- ☒ средства нанесения контратаки с помощью информационного оружия.
- ☐ процедуры оценки уровня и особенностей атаки против национальной

571 комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...

- ☐ политика безопасности
- ☐ угроза ИБ
- ☐ безопасность АС
- ☒ комплексное обеспечение ИБ
- ☐ атака на АС

572 Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

- ☐ принцип разумной достаточности
- ☐ принцип комплексности
- ☐ принцип системности
- ☒ принцип гибкости системы
- ☐ принцип непрерывной защиты

573 Основными компонентами парольной системы являются 1. интерфейс администратора 2. хранимая копия пароля 3. база данных учетных записей 4. все варианты верны

- ☐ нет правильного ответа
- ☐ 3,4
- ☐ 2,3
- ☒ 1,3,
- ☐ 2,4

574 хранение паролей может осуществляться 1. в виде сверток 2. в открытом виде 3. в закрытом виде 4. в зашифрованном виде 5. все варианты ответа верны

- ☐ 2,3
- ☐ 3,4,5
- ☐ 2,3,4
- ☒ 1,,2,4
- ☐ 2,4

575 Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано

- ☐ доступность
- ☐ контролируемость
- ☐ точность
- ☒ Надежность
- ☐ устойчивость

576 к оборонительным системам защиты относятся: 1. проволочные ограждения 2. звуковые установки 3. датчики 4. световые установки

- ☐ 4
- ☐ 3,4
- ☐ 3
- ☒ 1,2,,4
- ☐ 1,3,4

577 Автоматизированная система должна обеспечивать 1. надежность 2. даступность 3. целостность 4. контролируемость

- ☐ нет правильного ответа
- ☐ 3,4
- ☐ 1,2
- ☒ 2,3.
- ☐ 1,3

578 к видам системы обнаружения атак относятся :

- ☐ нет правильного ответа
- ☐ системы, обнаружения атаки на конкретные приложения
- ☐ системы, обнаружения атаки на ОС
- ☒ все варианты верны.
- ☐ системы, обнаружения атаки на удаленных БД

579 Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это

- ☐ парольная система
- ☐ идентификатор пользователя
- ☒ пороль пользователя.
- ☐ нет правильного ответа
- ☐ учетная запись пользователя

580 Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:

- ☐ нет правильного ответа
- ☐ ревизором
- ☐ иммунизатором
- ☒ сканером.
- ☐ доктора и фаги

581 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

- ☐ аппелеруемость
- ☐ доступность
- ☐ целостность

- ☒ Конфиденциальность
☐ аутентичность

582 Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

- ☐ условная информация
☐ банковская тайна
☐ коммерческая тайна
☒ Конфиденциальная информация
☐ служебная информация

583 к системам оповещения относятся: 1. инфракрасные датчики 2. электрические датчики 3. электромеханические датчики 4. электрохимические датчики

- ☐ 2
☐ 1,3
☐ 3,4
☒ 1,2
☐ 1,4

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

- ☐ нейтральная
☐ оба варианта
☐ активная
☒ пассивная
☐ нет правильного ответа

585 Защита информации обеспечивается применением антивирусных средств

- ☐ иногда
☐ не всегда
☐ нет
☒ да
☐ всегда

586 Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности рекомендации X.800

- ☐ Система безопасности
☐ Конституция
☐ Закону «Об информации, информационных технологиях и о защите информации»
☒ Аранжевая книга
☐ нет правильного ответа

587 Информация, составляющая государственную тайну не может иметь гриф...

- ☐ нет правильного ответа
☐ «совершенно секретно»
☐ «секретно»
☒ «для служебного пользования».
☐ «особой важности»

588 Наиболее эффективное средство для защиты от сетевых атак

- ☐ нет правильного ответа
☐ посещение только «надёжных» Интернет-узлов

- ☐ использование антивирусных программ
- ☒ использование сетевых экранов или «firewall».
- ☐ использование только сертифицированных программ-браузеров при доступе к сети Интернет

589 Утечка информации – это ...

- ☐ нет правильного ответа
- ☐ процесс уничтожения информации
- ☐ процесс раскрытия секретной информации
- ☒ несанкционированный процесс переноса информации от источника к злоумышленнику.
- ☐ непреднамеренная утрата носителя информации

590 к формам защиты информации не относится... 1.аналитическая 2.правовая 3.организационно-техническая 4.страховая

- ☐ 2,4
- ☐ 1,3
- ☐ 1,2
- ☒ 1,4.
- ☐ 3,4

591 Гарантия точного и полного выполнения команд в АС:

- ☐ доступность
- ☐ контролируемость
- ☐ надежность
- ☒ точность
- ☐ устойчивость

592 какие компоненты входят в комплекс защиты охраняемых объектов: 1. сигнализация 2. охрана 3. датчики 4. телевизионная система

- ☐ 3,4
- ☒ все варианты.
- ☐ 2,3
- ☐ 1,4
- ☐ 1,2

593 . Из перечисленного на транспортном уровне рекомендуется применение услуг: 1) идентификации; 2) конфиденциальности; 3) контроля трафика; 4) контроля доступа; 5) целостности; 6) аутентификации

- ☐ 1,4,6;
- ☐ 1, 3;
- ☐ 4, 5, 6;
- ☒ 2, 4, 5, 6
- ☐ 4, 6;

594 Из перечисленного методами защиты потока сообщений являются: 1) нумерация сообщений; 2) отметка времени; 3) использование случайных чисел; 4) нумерация блоков сообщений; 5) копирование потока сообщений

- ☐ 2,4,5
- ☐ 3, 5
- ☐ 2, 4
- ☒ 1, 2, 3;
- ☐ 3, 4, 5

595 Из перечисленного контроль доступа используется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- ☐ 2,5,6
- ☐ 4, 5, 6
- ☐ 3, 5;
- ☒ 1, 2, 5.
- ☐ 2, 3;

596 Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как: 1) чтение; 2) удаление; 3) копирование; 4) изменение

- ☐ 1,3,4
- ☐ 2, 3
- ☐ 2, 4
- ☒ 1, 4;
- ☐ 3, 4

597 Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие: 1) копирование; 2) чтение; 3) запись; 4) выполнение; 5) удаление

- ☐ 4, 5
- ☐ 3, 4, 5
- ☐ 1, 3, 5
- ☒ 2, 3, 4;
- ☐ 1, 3

598 Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы: 1) сравнение отдельных случайно выбранных фрагментов; 2) сравнение характерных деталей в графическом представлении; 3) непосредственное сравнение изображений; 4) сравнение характерных деталей в цифровом виде

- ☐ 1,2,3;
- ☐ 1, 3;
- ☐ 2, 3;
- ☒ 3, 4
- ☐ 1, 2;

599 Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для: 1) владельца; 2) членов группы владельца; 3) конкретных заданных пользователей; 4) конкретных заданных групп пользователей; 5) всех основных пользователей

- ☐ 2,3
- ☐ 1, 2, 3
- ☐ 1, 3, 4
- ☒ 1, 2, 5;
- ☐ 2, 3, 4

600 Из перечисленного в ОС UNIX существуют администраторы: 1) системных утилит; 2) службы контроля; 3) службы аутентификации; 4) тиражирования; 5) печати; 6) аудита

- ☐ 1, 2, 3
- ☐ 4, 5
- ☐ 1, 2, 4
- ☒ 1, 3, 5, 6.

601 Из перечисленного в обязанности сотрудников группы информационной безопасности входят: 1) управление доступом пользователей к данным; 2) расследование причин нарушения защиты; 3) исправление ошибок в программном обеспечении; 4) устранение дефектов аппаратной части

- ☐ 4
- ☐ 1, 3
- ☐ 1, 3, 4
- ☒ 1, 2;
- ☐ 3, 4

602 Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются: 1) аутентификация; 2) идентификация; 3) целостность; 4) контроль доступа; 5) контроль трафика; 6) причастность

- ☐ 3, 4, 5;
- ☐ 1, 2, 5;
- ☐ 1, 3, 5;
- ☒ 1, 3, 4, 6.
- ☐ 2, 3, 4;

603 Из перечисленного ACL-список содержит: 1) срок действия маркера доступа; 2) домены, которым разрешен доступ к объекту; 3) операции, которые разрешены с каждым объектом; 4) тип доступа

- ☐ 2,3;
- ☐ 1, 3;
- ☐ 1, 4;
- ☒ 2, 4.
- ☐ 1, 2;

604 Защита от форматирования жесткого диска со стороны пользователей обеспечивается

- ☐ ПО
- ☐ специальным программным обеспечением
- ☐ системным программным обеспечением
- ☒ аппаратным модулем, устанавливаемым на системную шину ПК.
- ☐ аппаратным модулем, устанавливаемым на контроллер

605 Защита исполняемых файлов обеспечивается

- ☐ специальным режимом запуска
- ☒ обязательным контролем попытки запуска.
- ☐ стандартным запуском
- ☐ дополнительным хостом
- ☐ криптографией

606 Запись определенных событий в журнал безопасности сервера называется

- ☐ контролем;
- ☐ мониторингом;
- ☐ трафиком;
- ☒ аудитом.
- ☐ учетом;

607 Восстановление данных является дополнительной функцией услуги защиты

- ☐ идентификация;
- ☐ причастность;
- ☐ аутентификация;
- ☒ целостность.
- ☐ контроль доступа;

608 Достоинством матричных моделей безопасности является

- ☐ обеспечение безопасности
- ☐ расширенный аудит
- ☐ гибкость управления
- ☒ легкость представления широкого спектра правил обеспечения безопасности.
- ☐ контроль за потоками информации

609 Для реализации технологии RAID создается

- ☐ аппаратные средства
- ☐ интерпретатор
- ☐ специальный процесс
- ☒ псевдодрайвер;
- ☐ компилятор

610 Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС

- ☐ внутренний
- ☐ приложений;
- ☐ системный;
- ☒ внешний.
- ☐ сетевой;

611 В многоуровневой модели, если уровни безопасности субъекта и объекта доступа не сравнимы, то

- ☐ ни один запрос не выполняется
- ☐ выполняются запросы минимального уровня безопасности
- ☐ доступ специально оговаривается
- ☒ никакие запросы не выполняются.
- ☐ все запросы выполняются

612 В многоуровневой модели, если субъект доступа формирует запрос на чтение, то уровень безопасности субъекта относительно уровня безопасности объекта должен

- ☐ быть больше;
- ☐ быть меньше
- ☐ специально оговариваться;
- ☒ доминировать.
- ☐ быть равен

613 Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....

- ☐ информационная сдача
- ☐ информационное превосходство
- ☐ информационное оружие
- ☒ Информационная война
- ☐ информационная запись

614 Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

- ☐ аппелеруемость
- ☐ доступность
- ☐ целостность
- ☒ конфиденциальность.
- ☐ аутентичность

615 Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:

- ☐ информационная среда
- ☐ информационное превосходство
- ☐ информационная война
- ☒ Информационное оружие
- ☐ информационная сдача

616 Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

- ☐ доступность данных
- ☐ защищенность информации
- ☐ защита информации
- ☒ Компьютерная безопасность
- ☐ безопасность данных

617 к выполняемой функции защиты относится:

- ☐ внутренняя память
- ☒ все варианты верны.
- ☐ внутренняя защита
- ☐ внешняя защита
- ☐ внешняя память

618 Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...

- ☐ Защищенность информации
- ☐ Безопасность данных
- ☐ Доступность данных
- ☒ Защита информации
- ☐ Компьютерная безопасность

619 к вирусам изменяющим среду обитания относятся:

- ☐ стелс
- ☐ студенческие
- ☐ полиморфные
- ☐ спутники
- ☒ черви,

620 Выбрать недостатки имеющиеся у антивирусной программы ревизор: 1. неспособность поймать вирус в момент его появления в системе 2. небольшая скорость поиска вирусов 3. невозможность определить вирус в новых файлах (в электронной почте, на дискете)

- ☐ только 1
- ☐ только 3
- ☒ 1,2,,3,
- ☐ 2,3
- ☐ 1,3

621 к тщательно контролируемым зонам относятся: 1. рабочее место администратора 2. архив 3. рабочее место пользователя

- ☐ 2,3
- ☒ 1,,2,3

- ☐ только 1
- ☐ только 2
- ☐ только 3

622 к достоинствам технических средств защиты относятся:

- ☐ регулярный контроль
- ☒ создание комплексных систем защиты.
- ☐ степень сложности устройства
- ☐ все варианты верны
- ☐ нет правильного ответа

623 Преднамеренная угроза безопасности информации

- ☐ нет правильного ответа
- ☒ кража.
- ☐ наводнение
- ☐ повреждение кабеля, по которому идет передача, в связи с погодными условиями
- ☐ ошибка разработчика

624 какие степени сложности устройства Вам известны 1. упрощенные 2. простые 3. сложные 4. оптические 5. встроенные

- ☐ 3,4
- ☒ 2,3,
- ☐ только 1
- ☐ только 3
- ☐ 1,3

625 Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...

- ☐ внедрения агрессивного программного кода в рамках активных объектов Web-страниц
- ☒ несанкционированного управления удаленным компьютером.
- ☐ поставки неприемлемого содержания
- ☐ вмешательства в личную жизнь
- ☐ перехвата или подмены данных на путях транспортировки

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

- ☐ способна противостоять только информационным угрозам, как внешним так и внутренним
- ☐ 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
- ☐ Ничего не верно
- ☒ 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.
- ☐ способна противостоять только внешним информационным угрозам

627 Система физической безопасности включает в себя следующие подсистемы: 1. оценка обстановки 2. скрытность 3. строительные препятствия 4. аварийная и пожарная сигнализация

- ☐ только 2
- ☒ 2,3,4.
- ☐ 1,3,4
- ☐ 1,2,4
- ☐ только 4

628 к принципам информационной безопасности относятся 1. скрытость 2. масштабность 3. системность 4. законность 5. открытости алгоритмов

- ☐ 2,3
☐ 2,3,4
☒ 1,2,3
☐ 3,4,5
☐ 4,5,6

629 к вирусам не изменяющим среду обитания относятся: 1. черви 2. студенческие 3. полиморфные 4. спутники

- ☐ 3
☒ 1,4
☐ 2,4
☐ 3,4
☐ 2,3

630 Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

- ☐ неконфиденциальная информация
☒ коммерческая тайна
☐ государственная тайна
☐ банковская тайна
☐ конфиденциальная информация

631 Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:

- ☐ атака на автоматизированную систему
☐ Угроза информационной безопасности
☐ Безопасность АС
☐ Комплексное обеспечение информационной безопасности
☒ политика безопасности.

632 Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

- ☐ принцип гибкости системы
☐ принцип системности
☐ принцип комплексности
☐ принцип непрерывности
☒ Принцип разумной достаточности

633 Недостатком модели политики безопасности на основе анализа угроз системе является

- ☐ механизм реализации
☐ статичность
☒ изначальное допущение вскрываемости системы.
☐ необходимость дополнительного обучения персонала
☐ сложный механизм реализации

634 к типам угроз безопасности парольных систем относятся

- ☐ разглашение параметров учетной записи
☒ все варианты ответа верны.
☐ словарная атака
☐ тотальный перебор
☐ атака на основе психологии

635 Наименее затратный криптоанализ для криптоалгоритма RSA

- ☐ на сложные множители
- ☒ разложение числа на простые множители.
- ☐ перебор по всему ключевому пространству
- ☐ перебор по выборочному ключевому пространству
- ☐ разложение числа на сложные множители

636 Надежность СЗИ определяется

- ☐ сильным звеном
- ☒ Самым слабым звеном
- ☐ количеством отраженных атак
- ☐ усредненным показателем
- ☐ самым сильным звеном

637 конечное множество используемых для кодирования информации знаков называется

- ☐ кодом
- ☒ алфавитом.
- ☐ символом
- ☐ шифром
- ☐ ключом

638 Недостатком дискретных моделей политики безопасности является

- ☐ необходимость дополнительного обучения персонала,
- ☒ статичность.
- ☐ допущение вскрываемости системы,
- ☐ сложный механизм реализации,
- ☐ изначальное допущение вскрываемости системы,

639 Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

- ☐ ограниченной компетенцией злоумышленника
- ☐ фиксированными затратами
- ☐ фиксированным компетенцией
- ☒ за определенное время.
- ☐ фиксированным ресурсом

640 Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

- ☐ стеганология
- ☒ криптоанализ.
- ☐ криптография
- ☐ стеганография
- ☐ криптология

641 Охранное освещение бывает: а. дежурное б. световое с. тревожное

- ☐ б
- ☐ а
- ☒ а,с.
- ☐ б,с
- ☐ а,б

642 Особенности информационного оружия являются: 1. системность 2. открытость 3. универсальность 4. скрытность

- ☐ только 4
- ☒ 3,4,
- ☐ 1,2
- ☐ 2,3
- ☐ 1,4

643 к механическим системам защиты относятся: 1. проволока 2. стена 3. сигнализация 4. вы

- ☐ 4
- ☒ 1,2,4
- ☐ 2,3,4
- ☐ 3,4
- ☐ 2,3

644 Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:

- ☐ Конфиденциальность
- ☐ Доступность
- ☐ Аутентичность
- ☒ Аппелируемость.
- ☐ Целостность

645 Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

- ☐ Коммерческая тайна
- ☐ Информационная безопасность
- ☐ Конфиденциальная информация
- ☒ Банковская тайна
- ☐ Государственная тайна

646 Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:

- ☐ Информационное вычисление
- ☐ Информационное превосходство
- ☐ Информационное оружие
- ☒ Информационная война
- ☐ Информационная безопасность

647 Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:

- ☐ Принцип системности
- ☐ Принцип разумной достаточности
- ☐ Принцип непрерывной защиты
- ☒ Принцип комплексности
- ☐ Принцип гибкости системы

648 Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:

- ☐ Конфиденциальность
- ☐ Доступность

- ☐ Апеллируемость
- ☒ Аутентичность
- ☐ Целостность

649 Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:

- ☐ Интересы общества в информационной сфере
- ☐ Интересы государства в информационной сфере
- ☐ Интересы личности в информационной сфере
- ☒ Интересы общества
- ☐ Интересы государства

650 Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий

- ☐ Политика безопасности
- ☐ Угроза безопасности
- ☐ Безопасность АС
- ☒ Комплексное обеспечение информационной безопасности
- ☐ Атака на автоматизированную систему

651 Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- ☐ Принцип гибкости системы
- ☐ Принцип непрерывной защиты
- ☐ Принцип комплексности
- ☒ Принцип системности
- ☐ Принцип разумной достаточности

652 к какому уровню доступа информации относится следующая информация: Библиографические и опознавательные данные, личные характеристики, сведения о семейном положении, сведения об имущественном или финансовом состоянии...

- ☐ Информация без ограничения права доступа
- ☐ Объект интеллектуальной собственности
- ☐ Информация, распространение которой наносит вред интересам общества
- ☒ Информация с ограниченным доступом
- ☐ Иная общедоступная информация

653 Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:

- ☐ Информационная защита
- ☐ Защищенность потребителей информации
- ☐ Защищенность информации
- ☒ Защищаемая информация
- ☐ Защита информации

654 Действие субъектов по обеспечению пользователей информационными продуктами:

- ☐ Информационные продукты
- ☐ Информационная система
- ☐ Информационная сфера
- ☒ Информационные услуги
- ☐ Информационные ресурсы

655 Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.

- ☐ Конфиденциальность
- ☐ Банковская тайна
- ☐ Коммерческая тайна
- ☒ Государственная тайна
- ☐ Конфиденциальная информация

656 Возможность сбора, обработки и распространения непрерывного потока информации при восприятии использования информации противником это:

- ☐ Информационная безопасность
- ☐ Информационная война
- ☐ Информационное оружие
- ☒ Информационное превосходство
- ☐ Информационное вычисление

657 Защищенность от негативных информационно-психологических и информационно-технических воздействий:

- ☐ Безопасность
- ☐ Компьютерная безопасность
- ☐ Защищенность информации
- ☒ Защищенность потребителей информации
- ☐ Защита информации

658 Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:

- ☐ Государственная безопасность
- ☐ Безопасность
- ☐ Национальная безопасность
- ☐ Национальная безопасность
- ☒ Информационная безопасность

659 к какому уровню доступа информации относится следующая информация: Ложная реклама, реклама со скрытыми вставками...

- ☐ Иная общедоступная информация
- ☐ Информация с ограниченным доступом
- ☐ Информация без ограничения права доступа
- ☒ Информация, распространение которой наносит вред интересам общества
- ☐ Объект интеллектуальной собственности

660 Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:

- ☐ Доступность
- ☐ точность
- ☐ Контролируемость
- ☒ Устойчивость
- ☐ Надежность

661 Из каких четырех доменов состоит CobIT?

- ☐ Приобретение и Внедрение, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

- ☐ Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
- ☐ Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- ☒ Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка.
- ☐ Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

662 Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

- ☐ Список стандартов, процедур и политик для разработки программы безопасности
- ☐ Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- ☒ Открытый стандарт, определяющий цели контроля
- ☐ Текущая версия ISO 27000
- ☐ Текущая версия ISO 17799

663 Что представляет собой стандарт ISO/IEC 27799?

- ☐ Новая версия ISO 17799
- ☐ Определения для новой серии ISO 27000
- ☐ Новая версия BS 17799
- ☒ Стандарт по защите персональных данных о здоровье.
- ☐ Новая версия NIST 800-60

664 какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

- ☐ Повышение обязательств
- ☐ Стандарты
- ☐ Должный процесс (Due process)
- ☒ Должная забота (Due care.)
- ☐ Снижение обязательств

665 Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

- ☐ Сотрудники должны одобрить создание группы
- ☐ Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
- ☐ Руководство должно одобрить создание группы
- ☒ Много информации нужно собрать и ввести в программу.
- ☐ Множество людей должно одобрить данные

666 Что является наилучшим описанием количественного анализа рисков?

- ☐ Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- ☐ Анализ, основанный на информации, выявленной при оценке рисков
- ☐ Метод, основанный на суждениях и интуиции
- ☒ Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков.
- ☐ Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

667 Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:

- ☐ Политика безопасности
- ☐ Угроза информационной безопасности
- ☐ Комплексное обеспечение информационной безопасности
- ☒ Безопасность АС
- ☐ Атака на автоматизированную систему

668 Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- ☐ Руководство должно одобрить создание группы
- ☐ Чтобы убедиться, что проводится справедливая оценка
- ☐ Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- ☒ Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа.
- ☐ Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

669 CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

- ☐ COSO – это система управления рисками
- ☐ COSO учитывает корпоративную культуру и разработку политик
- ☐ COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
- ☒ COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень.
- ☐ COSO – это система отказоустойчивости

670 Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

- ☐ пассивный перехват;
- ☐ просмотр мусора;
- ☐ видеоперехват;
- ☒ аудиоперехват.
- ☐ активный перехват;

671 Перехват, который осуществляется путем использования оптической техники называется:

- ☐ просмотр мусора;
- ☐ пассивный перехват;
- ☐ активный перехват;
- ☒ видеоперехват.
- ☐ аудиоперехват;

672 Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

- ☐ просмотр мусора;
- ☐ аудиоперехват;
- ☐ активный перехват;
- ☒ пассивный перехват.
- ☐ видеоперехват;

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

- ☐ детектор;
- ☐ ревизор;
- ☐ сканер;
- ☒ доктор.
- ☐ сторож;

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

- ☐ детектор;

- ☐ сканер;
- ☐ ревизор;
- ☒ сторож.
- ☐ доктор;

675 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:

- ☐ сканер;
- ☐ доктор;
- ☐ детектор;
- ☐ сторож;
- ☒ ревизор.

676 Основные угрозы доступности информации: 1.непреднамеренные ошибки пользователей
2.злонамеренное изменение данных 3.хакерская атака 4.отказ программного и аппаратно обеспечения
5.разрушение или повреждение помещений 6.перехват данных

- ☐ 3,5,6
- ☐ 3,4,5
- ☐ 2,3,6
- ☐ 2,3,4
- ☒ 1,4,,5
- ☐ 3,4,5

677 к внутренним нарушителям информационной безопасности относится: клиенты;

- ☐ пользователи системы;
- ☐ любые лица, находящиеся внутри контролируемой территории;
- ☐ представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
- ☒ технический персонал, обслуживающий здание.
- ☐ посетители;

678 Что является наилучшим описанием количественного анализа рисков? ему

- ☐ Множество людей должно одобрить данные
- ☐ Он присваивает уровни критичности. Их сложно перевести в денежный вид
- ☐ Это связано с точностью количественных элементов
- ☒ Количественные измерения должны применяться к качественным элементам.
- ☐ Он достижим и используется

679 как рассчитать остаточный риск?

- ☐ (Угрозы x Ценность актива) x Риски
- ☐ (Угрозы x Ценность актива x Уязвимости) x Риски
- ☐ SLE x Частоту = ALE
- ☒ (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля.
- ☐ Угрозы x Риски x Ценность актива

680 Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

- ☐ Соотношение затрат / выгод
- ☐ Внедрение управления механизмами безопасности
- ☐ Классификацию данных после внедрения механизмов безопасности
- ☒ Уровень доверия, обеспечиваемый механизмом безопасности.
- ☐ Выявление рисков

681 какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

- ☐ Только военные имеют настоящую безопасность
- ☐ Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности
- ☐ Военным требуется больший уровень безопасности, т.к. их риски существенно выше
- ☒ Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности.
- ☐ Руководство должно одобрить создание группы

682 Эффективная программа безопасности требует сбалансированного применения:

- ☐ Соотношения затрат / выгод
- ☐ Физической безопасности и технических средств защиты
- ☐ Контрмер и защитных механизмов
- ☒ Технических и нетехнических методов
- ☐ Процедур безопасности и шифрования

683 Что является определением воздействия (exposure) на безопасность?

- ☐ Контрмер и защитные механизмы
- ☐ Любой недостаток или отсутствие информационной безопасности
- ☐ Любая потенциальная опасность для информации или систем
- ☒ Нечто, приводящее к ущербу от угрозы.
- ☐ Потенциальные потери от угрозы

684 Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

- ☐ Выявление рисков
- ☐ Делегирование полномочий
- ☐ Определение цели и границ
- ☒ Выполнение анализа рисков.
- ☐ Поддержка

685 Что из перечисленного не является целью проведения анализа рисков?

- ☐ Определение цели и границ
- ☐ Выявление рисков
- ☐ Количественная оценка воздействия потенциальных угроз
- ☒ Делегирование полномочий.
- ☐ Определение баланса между воздействием риска и стоимостью необходимых контрмер

686 какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- ☐ Анализ действий
- ☐ Результаты ALE
- ☐ Анализ рисков
- ☒ Анализ затрат./ выгоды
- ☐ Выявление уязвимостей и угроз, являющихся причиной риска

687 когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- ☐ Когда необходимые защитные меры слишком просты
- ☐ Когда риски не могут быть приняты во внимание по политическим соображениям
- ☐ Когда необходимые защитные меры слишком сложны
- ☒ Когда стоимость контрмер превышает ценность актива и потенциальные потери.
- ☐ Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

688 Что лучше всего описывает цель расчета ALE?

- ☒ Оценить потенциальные потери от угрозы в год.
- ☐ Количественно оценить уровень безопасности среды
- ☐ Оценить возможные потери для каждой контрмеры
- ☐ Количественно оценить затраты / выгоды
- ☐ Выявление уязвимостей и угроз, являющихся причиной риска

689 какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

- ☐ Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- ☐ Актуальные и адекватные политики и процедуры безопасности
- ☐ Эффективные защитные меры и методы их внедрения
- ☒ Поддержка высшего руководства
- ☐ Проведение тренингов по безопасности для всех сотрудников

690 Что такое политики безопасности?

- ☐ Правила использования программного и аппаратного обеспечения в компании
- ☐ Общие руководящие требования по достижению определенного уровня безопасности
- ☐ Пошаговые инструкции по выполнению задач безопасности
- ☒ Широкие, высокоуровневые заявления руководства.
- ☐ Детализированные документы по обработке инцидентов безопасности

691 Что такое процедура?

- ☐ Эффективные защитные меры и методы их внедрения
- ☐ Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- ☐ Правила использования программного и аппаратного обеспечения в компании
- ☒ Пошаговая инструкция по выполнению задачи.
- ☐ Обязательные действия

692 Что самое главное должно продумать руководство при классификации данных?

- ☐ Проведение тренингов по безопасности для всех сотрудников
- ☐ Оценить уровень риска и отменить контрмеры
- ☐ Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- ☒ Необходимый уровень доступности, целостности и конфиденциальности.
- ☐ Управление доступом, которое должно защищать данные

693 кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- ☐ Сотрудники
- ☐ Пользователи
- ☐ Администраторы
- ☒ Руководство
- ☐ Владельцы данных

694 Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- ☐ Всегда требовать специального разрешения
- ☐ Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- ☐ Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- ☒ Улучшить контроль за безопасностью этой информации.
- ☐ Снизить уровень классификации этой информации

695 Активный перехват информации это перехват, который:

- ☐ коммуникаций;
- ☐ основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники
- ☐ неправомерно использует технологические отходы информационного процесса;
- ☒ осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- ☐ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

696 Тактическое планирование – это:

- ☐ Планирование на год
- ☐ Ежедневное планирование
- ☐ Долгосрочное планирование
- ☒ Среднесрочное планирование
- ☐ Планирование на 6 месяцев

697 какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- ☐ Пользователи
- ☐ Атакующие
- ☐ Хакеры
- ☒ Сотрудники.
- ☐ Контрагенты (лица, работающие по договору)

698 кто является основным ответственным за определение уровня классификации информации?

- ☐ Пользователь
- ☐ Руководитель среднего звена
- ☐ Высшее руководство
- ☒ Владелец.
- ☐ Проектировщик

699 к какому уровню доступа информации относится следующая информация: Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия...

- ☐ Иная общедоступная информация
- ☐ Информация, распространение которой наносит вред интересам общества
- ☐ Информация без ограничения права доступа
- ☒ Информация с ограниченным доступом
- ☐ Объект интеллектуальной собственности

700 Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:

- ☐ Информационные ресурсы
- ☐ Информационная система
- ☒ Информационные продукты
- ☐ Информационные услуги
- ☐ Информационная сфера