1613y_Ru_Y2017_Qiyabi_Yekun imtahan testinin sualları

Fənn : 1613y Kompüter sistemlərində informasiya təhlükəsizliyi

1 К выполняемой функции защиты относится:

- исходная
- сложная
- внутренняя защита
- все варианты верны
- внешняя защита

2 Какие компоненты входят в комплекс защиты охраняемых объектов:

- админ
- Датчики
- Вирус
- Система
- Оружие

3 Политика информационной безопасности — это

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

4 Защита информации это:

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

5 Защита информации от утечки это деятельность по предотвращению:

- 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
- 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

6 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 целостности и доступности данных, а военные – о конфиденциальности
  Руководство должно одобрить создание группы
  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

7 Что такое политики безопасности?

  Пошаговые инструкции по выполнению задач безопасности
- Широкие, высокоуровневые заявления руководства
  Правила использования программного и аппаратного обеспечения в компании
  Детализированные документы по обработке инцидентов безопасности
  Общие руководящие требования по достижению определенного уровня безопасности

8 Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

  Когда необходимые защитные меры слишком просты
- Когда стоимость контрмер превышает ценность актива и потенциальные потери
  Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
  Когда риски не могут быть приняты во внимание по политическим соображениям
  Когда необходимые защитные меры слишком сложны

9 Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

  Пользователи
- Сотрудники
  Хакеры
  Атакующие
  Контрагенты (лица, работающие по договору)

10 Кто является основным ответственным за определение уровня классификации информации?

  Руководитель среднего звена
- Владелец
  Проектировщик
  Пользователь
  Высшее руководство

11 К функциям информационной безопасности не относятся:

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

12 К посторонним лицам нарушителям информационной безопасности относится

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

13 К основным непреднамеренным искусственным угрозам АСОИ относится:

  чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы
  физическое разрушение системы путем взрыва, поджога и т.п.
  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.

14 Икусственные угрозы безопасности информации вызваны:

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

15 Естественные угрозы безопасности информации вызваны:

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

16 Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

- Стандарты
- Должная забота (Duecare)
  Повышение обязательств
  Снижение обязательств
  Должный процесс (Dueprocess)

17 Что является определением воздействия (exposure) на безопасность?

- Контрмер и защитные механизмы
- Нечто, приводящее к ущербу от угрозы
  Любая потенциальная опасность для информации или систем
  Любой недостаток или отсутствие информационной безопасности
  Потенциальные потери от угрозы

18 Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- Сотрудники
- Руководство
  Владельцы данных
  Пользователи
  Администраторы

19 Что самое главное должно продумать руководство при классификации данных?

- Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- Необходимый уровень доступности, целостности и конфиденциальности
  Управление доступом, которое должно защищать данные
  Проведение тренингов по безопасности для всех сотрудников
  Оценить уровень риска и отменить контрмеры

20 Какие степени сложности устройства Вам известны

встроенные
сложная
упрощенные
- простые
оптические

21 В соответствии с законом АР «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

22 В каком документе содержаться основные требования к безопасности информационных систем в США?

в красном блокноте
в оранжевой книге
в желтой прессе
- в красной книге
в черном списке

23 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

24 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

25 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

26 Какие сведения на территории РФ могут составлять коммерческую тайну?

любые
документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности
сведенья о численности работающих, их заработной плате и условиях труда
- учредительные документы и устав предприятия
другие

27 Кто может быть владельцем защищаемой информации?

- кто угодно
- общественные организации
- предприятия акционерные общества, фирмы
- ● только государство и его структуры
- только вышеперечисленные

28 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

29 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

30 Что 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

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

- на всех вышеперечисленных
- на тактическом
- на социально политическом
- ● на организационно-правовом
- на инженерно-техническом

32 Что включают в себя технические мероприятия по защите информации?

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

33 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

34 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

35 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

36 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

37 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

38 Виды уязвимостей

вероятная
- постоянная

субъективная
случайная
объективная

39 Показателями безопасности информации являются:

вероятность сбоя системы безопасности
время, в течение которого обеспечивается определённый уровень безопасности
время, необходимое на взлом защиты информации
- вероятност предотвращения угрозы

вероятность возникновения угрозы информационной безопасности

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

достоверной
понятной
полезной
- актуальной

полной

41 В соответствии с законом АР «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

42 Примером числовой информации может служить:

- разговор по телефону
- иллюстрация в книге
- симфония
- ● таблица значений тригоннометрических функций
- поздравительная открытка

43 Информация в семантической теории - это:

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

44 то нельзя делать при установки антивирусного ПО (программного обеспече-ния)?

- 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

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

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

46 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

47 Программу нужно обязательно проверить на наличие вирусов…

- перед вторым запуском

после первого запуска
перед каждым запуском
- перед первым запуском

после каждого запуска

48 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 прграммных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами

межсетевой экран

49 Это вид мошенничества, называется…Вам звонит не знакомый человек и претставляется 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
- социльная презумпция

социальная инженерия

50 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
- замантъ вас на поддельный сайт, что бы украсть данные вашего аккаунта (т. е. логин и пароль)

реклама новых сайтов

51 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

52 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 прграмма 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

53 Что нельзя публиковать в Интернете?

свои заметки
свои фотографии
свою биографию
- сведния о учёбе и работе

паспортные данные

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

- OCTAVE
- ISO\IEC
- Безопасная OECD
- OECD
- CPTED

55 Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- Руководство должно одобрить создание группы
- Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- Чтобы убедиться, что проводится справедливая оценка
- 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

56 Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

- Выявление рисков
- Определение цели и границ
- Поддержка
- Выполнение анализа рисков
- Делегирование полномочий

57 Что такое процедура?

- Обязательные действия
- Правила использования программного и аппаратного обеспечения в компании
- Эффективные защитные меры и методы их внедрения
- Пошаговая инструкция по выполнению задачи
- Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

58 Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

- Информационная безопасность
- Коммерческая тайна
- Государственная тайна
- Конфиденциальная информация
- Банковская тйна

59 Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:

- Информационное вычисление
- Информационная безопасность
- Информационная вйна
- Информационное оружие
- Информационное превосходство

60 Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:

- Защищенность информации

- Защищаемая информация
  Информационная защита
  Защита информации
  Защищенность потребителей информации

61 К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…»

  Объект интеллектуальной собственности
  Информация без ограничения права доступа
- Информация с огрниченным доступом
  Информация, распространение которой наносит вред интересам общества
  Иная общедоступная информация

62 Действие субъектов по обеспечению пользователей информационными продуктами:

  Информационные продукты
  Информационные ресурсы
  Информационная система
  Информационная сфера
- Инфрмационные услуги

63 Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:

  Политика безопасности
  Атака на автоматизированную систему
- Безопсность АС
  Комплексное обеспечение информационной безопасности
  Угроза информационной безопасности

64 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
- Принцп комплексности
  Принцип разумной достаточности
  Принцип гибкости системы
  Принцип непрерывной защиты

65 Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:

- Устйчивость
  Надежность
  Точность
  Контролируемость
  Доступность

66 Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:

  Аппелируемость
  Конфиденциальность
  Целостность
  Доступность
- Аутентчность

67 Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ

- Конфиденциальность
- Конфиденциальная информация
- ● Государствнная тайна
- Коммерческая тайна
- Банковская тайна

68 Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:

- Интересы общества в информационной сфере
- ● Интресы общества
- Интересы личности в информационной сфере
- Интересы государства в информационной сфере
- Интересы государства

69 Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:

- Информационное вычисление
- ● Информационное превсходство
- Информационная война
- Информационное оружие
- Информационная безопасность

70 Защищенность от негативных информационно-психологических и информационно- технических воздействий:

- Безопасность
- ● Защищенность потребителей информации
- Защита информации
- Компьютерная безопасность
- Защищенность информации

71 Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:

- Информационная безопасность
- ● Национальная безпасность
- Государственная безопасность
- Защита информации
- Безопасность

72 К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»

- Информация без ограничения права доступа
- ● Информция, распространение которой наносит вред интересам общества
- Иная общедоступная информация
- Объект интеллектуальной собственности
- Информация с ограниченным доступом

73 С доступом к информационным ресурсам внутри организации связан уровень ОС

- приложений
- системный

канальный
- сетевой
внешний

74 Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

Сотрудники должны одобрить создание группы
- Много информации нужно собрать и ввести в программу
Руководство должно одобрить создание группы
Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
Множество людей должно одобрить данные

75 Почему количественный анализ рисков в чистом виде не достижим?

Множество людей должно одобрить данные
Это связано с точностью количественных элементов
- Количественные измерения должны применяться к качественным элементам
Он достижим и используется
Он присваивает уровни критичности. Их сложно перевести в денежный вид

76 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
- Поддержка высшего руководства
Эффективные защитные меры и методы их внедрения
Актуальные и адекватные политики и процедуры безопасности
Проведение тренингов по безопасности для всех сотрудников

77 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
- Улучшить контроль за безопасностью этой информации
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
Снизить уровень классификации этой информации

78 По документам ГТК самый низкий класс защищенности СВТ от НСД к информации

2.0
- 6.0
9.0
0.0
1.0

79 По документам ГТК количество классов защищенности СВТ от НСД к информации

5.0
- 6.0
9.0
8.0
7.0

80 Первым этапом разработки системы защиты ИС является

оценка потерь

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

81 К внутренним нарушителям информационной безопасности относится:клиенты;

  представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
- технический персонал, обслуживающий здание
  пользователи системы
  посетители
  любые лица, находящиеся внутри контролируемой территории

82 Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

  Внедрение управления механизмами безопасности
- Уровень доверия, обеспечиваемый механизмом безопасности
  Выявление рисков
  Соотношение затрат / выгод
  Классификацию данных после внедрения механизмов безопасности

83 Эффективная программа безопасности требует сбалансированного применения:

  Соотношения затрат / выгод
  Контрмер и защитных механизмов
  Физической безопасности и технических средств защиты
  Процедур безопасности и шифрования
- Технических и нетехнических методов

84 Тактическое планирование – это:

  Планирование на год
  Планирование на 6 месяцев
- Среднесрочное планирование
  Долгосрочное планирование
  Ежедневное планирование

85 Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

  Анализ рисков
- Анализ затрат / выгоды
  Анализ действий
  Выявление уязвимостей и угроз, являющихся причиной риска
  Результаты ALE

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

  Внутренная защита
  Защищенность информации
  Защита информации
- Компьютерная безопасность
  Безопасность данных

87 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

88 Программу нужно обязательно проверить на наличие вирусов…

перед вторым запуском
после первого запуска
перед каждым запуском
- перед первым запуском
после каждого запуска

89 Идентификатор субъекта доступа, который является его секретом:

админом
электронно-цифровая подпись
ключ
- пароль
сертификат ключа подписи

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

защита информации от несанкционированного воздействия
- защита от утечки информации
Без защитная информация от несанкционированного воздействия
защита информации от несанкционированного доступа
защита информации от непреднамеренного воздействия

91 Что не относится к информационной инфекции

Логическая бомба
Черви
Троянский конь
- Фальсификация данных
Вирусы

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

Информационное общество
Информационные инфекции
Физический инфекции
- Информационный саботаж
Информационные оружия

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

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

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

защита
аутентичность
доступность
- конфиденциальность

целостность

95 Что относится к классу информационных ресурсов:

Промышленные образцы, рецептуры и технологии
Персонал
Документы
- все правельные ответы

Организационные единицы

96 Наиболее распространенные угрозы информационной безопасности:

угрозы вируса
угрозы безопасности
угрозы защищенности
- угрозы целостности

угрозы деятельности

97 Информационная безопасность это:

Политическая экономическая и социальная стабильность
Состояние, когда не угрожает опасность информационным системам
Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
- Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз

Политика национальной безопасности России

98 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

99 Охранное освещение бывает:

архив
заключеной
световое
- дежурное

открытое

100 К оборонительным системам защиты относятся:

электрофизические датчики
электрохимические датчики
датчики
- звуковые установки

электромеханические датчики

101 К системам оповещения относятся:

электрофизические датчики
электромеханические датчики

неэлектрические датчики
- инфракрасные датчики

электрохимические датчики

102 К тщательно контролируемым зонам относятся:

световые
пользователя
администратор
- архив

электрохимические датчики

103 К достоинствам технических средств защиты относятся:

регулярный контроль
Все ответы не верны
Все варианты верны
степень сложности устройства
- создание комплексных систем защиты

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

полиморфные
иммунизатором
ревизором
- сканером

доктора и фаги

105 Хранение паролей может осуществляться

все варианты ответа верны
в закрытом виде
в закрытом виде
- в виде сверток

в незашифрованном виде

106 К вирусам не изменяющим среду обитания относятся:

доступность
студенческие
ревизоро
- спутник

полиморфные

107 К типам угроз безопасности парольных систем относятся

разглашение параметров учетной записи
тотальный перебор
словарная атака
- все варианты ответа верны

атака на основе психологии

108 К функциям информационной безопасности не относятся:

подготовка специалистов по обеспечению информационной безопасности
выявление источников внутренних и внешних угроз
совершенствование законодательства РФ в сфере обеспечения информационной безопасности
- Незащита государственных информационных ресурсов

Страхование информационных ресурсов

109 Особенностями информационного оружия являются:

доступность
открытость
системность
- универсальность
надежность

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

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

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

принцип гибкости системы
принцип комплексности
принцип системности
- принцип разумной достаточности
принцип непрерывности

112 Гарантия точного и полного выполнения команд в АС:

доступность
- точность
надежность
контролируемость
устойчивость

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

аппелеруемость
доступность
конфиденциальность
- целостность
аутентичность

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

информационное превосходство
банковская тайна
государственная тайна
- коммерческая тайна
конфиденциальная информация

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

Информационная безопасность
информационное превосходство

информационная война
- информационное оружие

Информационная защита

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

- Компьютерная безопасность

Безопасность данных
Защищенность информации
Защита информации
Внутренная защита

117 К выполняемой функции защиты относится:

внутренняя защита
сложная
исходная
- все варианты верны

внешняя защита

118 Какие компоненты входят в комплекс защиты охраняемых объектов:

админ
Система
Вирус
- Датчики

Оружие

119 К механическим системам защиты относятся:

вирус
защита
непроволока
- сигнализация

вы

120 Какие степени сложности устройства Вам известны

встроенные
сложная
упрощенные
- простые

оптические

121 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

122 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

123 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

124 Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

OCTAVE
AS/NZS
Анализ связующего дерева
- Анализ сбоев и дефектов

NIST

125 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

126 Что является наилучшим описанием количественного анализа рисков?

Анализ, основанный на информации, выявленной при оценке рисков
Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

Метод, основанный на суждениях и интуиции

127 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

128 Как рассчитать остаточный риск?

(Угрозы x Ценность актива) x Риски
(Угрозы x Ценность актива x Уязвимости) x Риски
Угрозы x Риски x Ценность актива
- (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

SLE x Частоту = ALE

129 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

130 Брандмауэры второго поколения представляли собой

хосты пакетов
маршрутизаторы с фильтрацией пакетов
хосты с фильтрацией пакетов
- «уполномоченные серверы»

«неприступные серверы»

131 Администратором базы данных является

пользователь группы
старший пользователь группы
администратор сервера баз данных
- любой пользователь, создавший БД

системный администратор

132 Административные действия в СУБД позволяют выполнять привилегии

недоступа
чтения
тиражирования
- безопасности

доступа

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

5.4
3, 4, 5, 6
2, 3, 5, 6
- 1, 2, 5, 6

5, 2, 3, 4

134 Гарантия точного и полного выполнения команд в АС:

доступность
контролируемость
надежность
- точность

устойчивость

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

аппелеруемость
доступность
конфиденциальность
- целостность

аутентичность

136 Что нельзя делать при установки антивирусного ПО (программного обеспече-ния)?

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

137 Регистрацией в системе Windows 2000 управляет

logon.lld
msgina.dll
logon.dll
- процедура winlogon

процедура lsass

138 Проверка подлинности пользователя по предъявленному им идентификатору — это

аудит
идентификация
- аутентификация

контроля доступа
авторизация

139 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

140 Применение средств защиты физического уровня ограничивается услугами

аудит
целостности
контроля доступа
- конфиденциальности

аутентификации

141 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 получателя

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

администрированием
идентификация
аутентификация
- авторизация

аудит

143 Право управлять безопасностью СУБД и отслеживать действия пользователей дает привилегия

- security operator
- createdb
- trace
- ● security
- operator

144 Право на удаление баз данных дает привилегия

- security operator
- trace
- create trace
- ● createdb
- operator

145 Право на запуск сервера дает привилегия

- create trace
- trace
- security operator
- ● operator
- security

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

- аутентификация
- администрированием
- управлением ресурсами
- ● мониторингом
- аудитом

147 Полномочия ядра безопасности ОС ассоциируются с

- базами данных
- приложениями
- периферийными устройствами
- ● процессами
- пользователями

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

- Представительный
- транспортном
- канальном
- ● сеансовом
- сетевом

149 По умолчанию пользователь не имеет никаких прав доступа к

- таблицам
- событиям
- базам данных
- ● таблицам и представлениям
- Представительный

150 Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

внутренним
внешнем
приложений
- системном
сетевом

151 Операционная система Windows 2000 отличает каждого пользователя от других по

дескриптору защиты
- идентификатору безопасности
идентификатору защиты
маркеру доступа
маркеру безопасности

152 Обычно в СУБД применяется управление доступом

древовидное
административное
иерархическое
- произвольное
декларируемое

153 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

154 Наиболее надежным механизмом для защиты содержания сообщений является

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

155 Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

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

156 Как предотвращение неавторизованного использования ресурсов определена услуга защиты

идентификация
- контроль доступа
причастность
аутентификация
целостность

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

1.4
3.4

1.3
- 2.4
1.2

158 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
1,4,5
2,3,4
- 3,4,5
1,2,3

159 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
3,4,5
1,2,4,5
- 2,4,5
1,2,3

160 Из перечисленного услуга обеспечения доступности реализируется 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

161 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

162 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

163 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

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

- 2,3,4
- 1,2,3
- 3,4,5
- 1,4,5
- 1,3,4

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

- 3, 4
- 3, 4
- 1, 4
- 2, 3
- 1, 2

166 Виды уязвимостей

- вероятная
- случайная
- субъективная
- постоянная
- объективная

167 Показателями безопасности информации являются:

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

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

- достоверной
- понятной
- полезной
- актуальной
- полной

169 В соответствии с законом АР «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

170 Примером числовой информации может служить:

- разговор по телефону
- иллюстрация в книге
- симфония
- таблица значений тригоннометрических функций
- поздравительная открытка

171 Информация в семантической теории - это:

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

172 Для создания базы данных пользователь должен получить привилегию от

- баз данных
- системного администратора
- сетевого администратора
- ● администратора сервера баз данных
- старшего пользователя своей группы

173 Дескриптор защиты в Windows 2000 содержит список

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

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

- совокупность
- целостность
- восстанавливаемость
- ● доступность
- детермированность

175 В СУБД Oracle под ролью понимается

- совокупность
- группа объектов
- совокупность процессов
- ● набор привилегий
- группа субъектов

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

- совокупность
- специально оговариваться
- доминировать
- ● быть равен
- быть меньше

177 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

178 Брандмауэры первого поколения представляли собой

- хосты с фильтрацией
- «уполномоченные серверы»
- неприступные серверы»
- маршрутизаторы с фильтрацией пакетов
- хосты с фильтрацией пакетов

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

- сеансовым
- транспортном
- сетевом
- физическом
- канальном

180 Администратор сервера баз данных имеет имя

- system
- sysadm
- admin
- ingres
- root

181 ACL-список ассоциируется с каждым

- типом
- доменом
- типом доступа
- объектом
- процессом

182 «Уполномоченные серверы» фильтруют пакеты на уровне

- прикладным
- канальном
- транспортном
- приложений
- физическом

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

- нарушители
- заместители
- перехватчики
- фильтры
- имитаторы

184 Цель прогресса внедрения и тестирования средств защиты —

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

185 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

186 Требования к техническому обеспечению системы защиты

документарные и аппаратурные
процедурные и раздельные
правленческие и документарные
- аппаратурные и физические
административные и аппаратурные

187 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 являются корпоративными
- NIST и OCTAVE ориентирован на ИТ
NIST и AS/NZS являются корпоративными

188 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

189 Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

Текущая версия ISO 27000
Текущая версия ISO 17799
Список стандартов, процедур и политик для разработки программы безопасности
- Открытый стандарт, определяющий цели контроля
Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

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

Информационная безопасность
информационное превосходство
информационная война
- информационное оружие
Информационная защита

191 В соответствии с особенностями алгоритма вирусы можно разделить на два класса:1.вирусы изменяющие среду обитания, но не распространяющиеся 2.вирусы изменяющие среду обитания при распространении 3.вирусы не изменяющие среду обитания при распространении4.вирусы не изменяющие среду обитания и не способные к распространению в дальнейшем

только 4
3,4
1,2,3

- 2,3
  только 3

192 Выбрать недостатки имеющиеся у антивирусной программы ревизор:1.неспособность поймать вирус в момент его появления в системе2.небольшая скорость поиска вирусов 3.невозможность определить вирус в новых файлах (в электронной почте, на дискете)

  только 1
  1,3
  2,3
- 1,2„3
  только 3

193 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
  иммунизатором
  ревизором
- сканерром
  доктора и фаги

194 Хранение паролей может осуществляться1.в виде сверток2.в открытом виде3.в закрытом виде4.в зашифрованном виде5.все варианты ответа верны

  2,3
  3,4,5
  2,3,4
- 1„2,4
  1.0

195 К вирусам не изменяющим среду обитания относятся:1.черви2.студенческие3.полиморфные4.спутники

  3.0
  3,4
  2,4
- 1,4
  2,3

196 К типам угроз безопасности парольных систем относятся

  разглашение параметров учетной записи
  тотальный перебор
  словарная атака
- вси варианты ответа верны
  атака на основе психологии

197 К функциям информационной безопасности относятся:1.совершенствование законодательства РФ в сфере обеспечения информационной безопасности2.выявление источников внутренних и внешних угроз 3.Страхование информационных ресурсов 4.защита государственных информационных ресурсов5.подготовка специалистов по обеспечению информационной безопасности

  3,4,5
  1,2,3
  1,4,5
- вси варианты
  2,3,4

198 Особенностями информационного оружия являются:1.системность2.открытость3.универсальность4.скрытность

- 1,2
- только 4
- 1,4
- 2,3
- 3,4 ●

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

- Комплексное обеспечение информационной безопасности
- Угроза информационной безопасности
- атака на автоматизированную систему
- палитика безопасности ●
- Безопасность АС

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

- принцип гибкости системы
- принцип комплексности
- принцип системности
- принцип разумной достаточности ●
- принцип непрерывности

201 Гарантия точного и полного выполнения команд в АС:

- доступность
- контролируемость
- надежность
- точнасть ●
- устойчивость

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

- неконфиденциальная информация
- банковская тайна
- государственная тайна
- коммерческаяя тайна ●
- конфиденциальная информация

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

- информационная среда
- информационное превосходство
- информационная война
- информационное оружиее ●
- информационная сдача

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

- доступность данных
- Защищенность информации
- Защита информации

- Кампьютерная безопасность
- Безопасность данных

205 К выполняемой функции защиты относится:

- внутреняя память
- внутренняя защита
- внешняя защита
- вси варианты верны
- внешняя память

206 Какие компоненты входят в комплекс защиты охраняемых объектов:1.сигнализация2.охрана3.датчики4.телевизионная система

- 2,3
- 3,4
- 1,2
- все вариантыы
- 1,4

207 К механическим системам защиты относятся:1.проволока2.стена3.сигнализация4.вы

- 4.0
- 3,4
- 2,3,4
- 1,2,4
- 2,3

208 Какие степени сложности устройства Вам известны1.упрощенные2.простые3.сложные4.оптические5.встроенные

- только 1
- 1,3
- 3,4
- 2,3
- только 3

209 Система физической безопасности включает в себя следующие подсистемы:1.оценка обстановки2.скрытность3.строительные препятствия4.аварийная и пожарная сигнализация

- только 2
- 1,2,4
- 1,3,4,
- 2,3,4
- только 4

210 Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…

- Доступность данных
- Защищенность информации
- Компьютерная безопасность
- Защщита информации
- Безопасность данных

211 Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….

- пороль пользователя
- идентификатор пользователя
- учетная запись пользователя
- парольная система
- Защщита информации

212 Основными компонентами парольной системы являются 1.интервейс администратора2.хранимая копия пароля3.база данных учетных записей4.все варианты верны

- нет правильного ответа
- 2.3
- 3.4
- 2.4
- 1.3

213 Автоматизированная система должна обеспечивать1.надежность2.даступность3.целосдность4.контролируемость

- нет правильного твета
- 1.3
- 2.3
- 1.2
- 3.4

214 К видам системы обнаружения атак относятся :

- нет правильного ответа
- вси варианты верны
- системы, обнаружения атаки на ОС
- системы, обнаружения атаки на конкретные приложения
- системы, обнаружения атаки на удаленных БД

215 Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:1.компаньон - вирусами2.ччерви3.паразитические4.студенческие5.призраки6.стелс - вирусы7.макровирусы

- 1.7
- 2.0
- 1.3
- 3.4
- 6.7

216 Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

- политика безопасности
- комплегсное обеспечение ИБ
- безопасность АС
- угроза ИБ
- атака на АС

217 В классификацию вирусов по способу заражения входят1.опасные2.файловые3.резидентные4.Загрузочные5.файлово -загрузочные6.нерезидентные

- 1.2
- 3.6
- 1.6
- 4.5
- 2.4

218 Конечное множество используемых для кодирования информации знаков называется

- кодом
- ● алфавитом
- символом
- шифром
- ключом

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

- кодирования
- подстановки
- аналитических преобразований
- ● гаммирования
- перестановки

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

- аналитических преобразований
- ● подстановки
- гаммирования
- кодирования
- перестановки

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

- аналитических преобразований
- кодирования
- ● перестановки
- гаммирования
- подстановки

222 Что представляет собой стандарт ISO/IEC 27799?

- Новая версия ISO 17799
- ● Стандарт по защите персональных данных о здоровье
- Новая версия BS 17799
- Определения для новой серии ISO 27000
- Новая версия NIST 800-60

223 Что лучше всего описывает цель расчета ALE?

- Выявление уязвимостей и угроз, являющихся причиной риска
- ● Оценить потенциальные потери от угрозы в год
- Количественно оценить уровень безопасности среды
- Оценить возможные потери для каждой контрмеры
- Количественно оценить затраты / выгоды

224 Удачная криптоатака называется

- ● взломом
- проникновением
- социальная инженерия
- вскрытием
- раскрытием шифра

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

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

226 Что такое файрволл?

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

227 Это вид мошенничества, называется… Вам звонит не знакомый человек и претставляется 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
- социльная презумпция
- социальная инженерия

228 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
- замант вас на поддельный сайт, что бы украсть данные вашего аккаунта (т. е. логин и пароль)
- реклама новых сайтов

229 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, заражённых вирусами и троянами
- бесплатное антивирусное приложение для разблокировки компьютера

230 Перехват, который осуществляется путем использования оптической техники называется:

- активный перехват
- просмотр мусора
- аудиоперехват
- видеоперехват
- пассивный перехват

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

- просмотр мусора
- аудиоперехват
- активный перехват
- пассивный перехват

видеоперехват

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

просмотр мусора
пассивный перехват
активный перехват
- аудиоперехват
видеоперехват

233 Активный перехват информации это перехват, который:

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

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

детектор
сканер
ревизор
- сторож
доктор

235 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:

детектор
сканер
сторож
- ревизор
доктор

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

сторож
сканер
детектор
- доктор
ревизор

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

сторож
сканер
доктор
- детектор
ревизор

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

пустые письма
нигерийские письма
черный пиар
- фишинг

источник слухов

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

пустые письма
нигерийские письма
фишинг
- черный пиар

источник слухов

240 Назначение троянских программ…

ограничение доступа пользователя в Интернет
уничтожать компьютер пользователя
реклама и промоакции
- краст и уничтожать данные пользователя

засорение ПО

241 Троянские программы распространяются…

с помощью хакера
с помощью пользователя
с помощью компьютерных вирусов
- самстоятельно

с помощью неисправного ПО

242 Какие ошибки допускает пользователь?

пользуется сложными паролями
не пользуется защитными программами
месяцами не меняет пароли, оставляет избыточную информацию о себе в открытом доступе
- Выбрать несклько ответов

просматривает все электронные письма с вложениями

243 В чем недостатки антивирусов-мониторов?

замедляют работу компьютера
не умеют блокировать вирусы, полученные из сети Интернет
не умеют уничтожать вирусы в файлах
- не умеют унчтожать вирусы

могут привести к серьезному сбою системы

244 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

245 Отметьте все правильные утверждения про антивирус-сканер

реагирует на события, похожие на действия вирусов
- может обнруживать и уничтожать все вирусы

может уничтожать известные ему вирусы
может обнаруживать вирусы в файлах
может блокировать вирус в момент заражения

246 Отметьте вредоносные программы, которые распространяются в компьютерных сетях.

вирусы-черви
файловые вирусы
загрузочные вирусы
- троянские прграммы
макровирусы

247 Какое действие нужно выполнить в самом начале, если на компьютере обнаружен вирус?

отформатировать винчестер
отключить питание компьютера
перегрузить компьютер
- запустить антвирус
отключить компьютер от сети

248 Какие вредоносные программы могут заражать документы Word и Excel?

сетевые черви
макровирусы
загрузочные вирусы
- файлвые вирусы
троянские программы

249 Как могут распространяться вирусы?

через документы Word
через рисунки и звуковые файлы
при копировании данных через флэш-диски
- через компьютрные сети
через сообщения электронной почты

250 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 зарженного DVD-диска
посещение зараженного сайта

251 Отметьте объекты, которые могут быть заражены компьютерными вирусами

- исплняемые файлы
драйверы устройств
видео
рисунки
веб-страницы

252 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 сущствующие
изменяется размер файлов

253 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 разршается
- с сервера удаляются страницы сайта

254 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 компьютру
- он может находиться в файле или загрузочном секторе диска

255 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

256 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

257 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

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

- ревизор
- доктор
- детектор
- сторож
- сканер

259 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:

- сторож
- доктор

- детектор
- ● ревизор
- сканер

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

- сторож
- сканер
- детектор
- ● доктор
- ревизор

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

- сторож
- сканер
- доктор
- ● детектор
- ревизор

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

- пустые письма
- нигерийские письма
- черный пиар
- ● фишинг
- источник слухов

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

- пустые письма
- нигерийские письма
- фишинг
- ● черный пиар
- источник слухов

264 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

- 4.0
- 1,3,4
- 1.3
- 3.4
- ● 1, 2

265 Кто может быть владельцем защищаемой информации?

- кто угодно
- только вышеперечисленные
- ● только государство и его структуры
- предприятия акционерные общества, фирмы
- общественные организации

266 Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

- только открытая информация
- любая информация
- коммерческая тайна
- закрываемая собственником информация
- запатентованная информация

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

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

268 Что включает в себя ранжирование как метод защиты информации?

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

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

- на социально политическом
- на организационно-правовом
- на всех вышеперечисленных
- на инженерно-техническом
- на тактическом

270 Что включают в себя технические мероприятия по защите информации?

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

271 Выделите три наиболее важных метода защиты информации от ошибочных действий пользователя

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

272 Выделите три наиболее важных метода защиты информации от нелегального доступа

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

273 Какие существуют наиболее общие задачи защиты информации на предприятии?

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

274 Что в себя морально-нравственные методы защиты информации?

- вариант ответа 1, 2 и 3
- воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений
- контроль работы сотрудников, допущенных к работе с секретной информацией
- обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней
- вариант ответа 1 и 3

275 Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

- изменить, повредить или ее уничтожить
- получить, изменить, а затем передать ее конкурентам
- размножить или уничтожить ее
- получить, изменить или уничтожить
- изменить и уничтожить ее

276 Сетевым протоколом является...

- страховая
- Набор правил
- Инструкция
- Программа
- Набор программ

277 Для безопасного использования ресурсов в сети Интернет предназначен протокол…

- SMTP
- FTP
- HTTPS
- NNTP
- IRC

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

- Десятичные числа от 0 до 999
- Десятичные числа от 0 до 255
- Десятичные числа от 0 до 998
- Буквы латинского алфавита
- Двоичный код

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

- Описание
- Канал
- Протокол

Порт
Программа

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

шестерка
Трех
Пяти
Двух
- Четырех

281 Домен .ru является _____ доменом.

организационно-техническая
Первичным
- Зональным
Основным
Надежным

282 Укажите правильно записанный IP-адрес в компьютерной сети

www.50.50.10
- 10.172.122.26
193.264.255.10
www.alfa193.com.
192.154.144.270

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

- Система URL-адресации
Доменная система имен (DNS)
Интернет-протокол
Протокол передачи гипертекста
общения в чатах

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

POP3
ftp
www
smpt
- http

285 Протокол SMTP предназначен для…

передачи файлов
Приема электронной почты
- Отправки электронной почты
Общения в чате
Просмотра веб-страниц

286 Поток сообщений в сети передачи данных определяется:

Треком
- Трафиком
Сетевом
Скоростью передачи данных

Объемом памяти канала передачи сообщений

287 Протокол POP3 работает на _____ уровне

Основным
- Прикладном
Сетевом
Транспортном
Физическом

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

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

289 Обеспечением скрытности информации в информационных массивах занимается

криптоанализ
- стеганография
криптология
криптография
криптология

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

профилем безопасности
- профилем защиты
системойбезопасности
системой защиты
стандартом безопасности

291 Надежность СЗИ определяется

усредненным показателем
количеством отраженных атак
сильным звеном
- самым слабым звеном
самым сильным звеном

292 Перехват, который осуществляется путем использования оптической техники называется:

просмотр мусора
- видеоперехват
активный перехват
пассивный перехват
аудиоперехват

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

просмотр мусора
видеоперехват
- пассивный перехват
активный перехват

аудиоперехват

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

- просмотр мусора
- аудиоперехват
- активный перехват
- пассивный перехват
- видеоперехват

295 Активный перехват информации это перехват, который:

- коммуникаций
- 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
- неправомерно использует технологические отходы информационного процесса

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

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

297 Назначение троянских программ…

- ограничение доступа пользователя в Интернет
- реклама и промоакции
- краст и уничтожать данные пользователя
- засорение ПО
- уничтожать компьютер пользователя

298 Троянские программы распространяются…

- с помощью хакера
- с помощью пользователя
- с помощью компьютерных вирусов
- самстоятельно
- с помощью неисправного ПО

299 Какие ошибки допускает пользователь?

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

300 В чем недостатки антивирусов-мониторов?

- не умеют уничтожать вирусы в файлах
- замедляют работу компьютера
- могут привести к серьезному сбою системы
- не умеют унчтожать вирусы

не умеют блокировать вирусы, полученные из сети Интернет

301 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

302 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 обнруживать и уничтожать все вирусы
- может блокировать вирус в момент заражения

303 Отметьте вредоносные программы, которые распространяются в компьютерных сетях.

- вирусы-черви
- файловые вирусы
- загрузочные вирусы
- ● троянские прграммы
- макровирусы

304 Какое действие нужно выполнить в самом начале, если на компьютере обнаружен вирус?

- отформатировать винчестер
- отключить питание компьютера
- перегрузить компьютер
- ● запустить антвирус
- отключить компьютер от сети

305 Какие вредоносные программы могут заражать документы Word и Excel?

- сетевые черви
- макровирусы
- загрузочные вирусы
- ● файлвые вирусы
- троянские программы

306 Как могут распространяться вирусы?

- через документы Word
- через рисунки и звуковые файлы
- при копировании данных через флэш-диски
- ● через компьютрные сети
- через сообщения электронной почты

307 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 зарженного DVD-диска
- посещение зараженного сайта

308 Отметьте объекты, которые могут быть заражены компьютерными вирусами.

веб-страницы
видео
рисунки
- исплняемые файлы

драйверы устройств

309 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 сущствующие

изменяется размер файлов

310 К чему приводит DoS-атака на сайт в Интернете?

сервер не может справиться с большим потоком запросов
- сервер физически разршается

страницы сайта подменяются на фальшивые
с сервера удаляются страницы сайта
взламывается программное обеспечение сервера

311 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 компьютру

он может находиться в файле или загрузочном секторе диска

312 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

313 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

314 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

315 В соответствии с законом АР «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

316 В каком документе содержаться основные требования к безопасности информационных систем в США?

- в красном блокноте
- в оранжевой книге
- в желтой прессе
- ● в красной книге
- в черном списке

317 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

318 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

319 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

320 Какие сведения на территории АР могут составлять коммерческую тайну?

- любые
- ● учредительные документы и устав предприятия
- сведенья о численности работающих, их заработной плате и условиях труда
- документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности
- другие

321 Как подразделяются вирусы в зависимости от деструктивных возможностей?

- Безвредные, неопасные, загрузочные, комбинированные
- Сетевые, файловые, загрузочные, комбинированные
- Сетевые, файловые, загрузочные, комбинированные

- Безвредные, неопасные, опасные, очень опасные
  Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

322 Что такое компьютерный вирус?

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

323 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 системности
- принцип комплексности
- принцип непрерывной защиты
- принцип гибгости системы

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

- доступность
- контролируемость
- точность
- надеженность
- устойчивость

325 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

- аппелеруемость
- доступность
- целостность
- конфинденциальность
- аутентичность

326 Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами

- служебная информация
- банковская тайна
- условная информация
- конфинденциальная информация
- коммерческая тайна

327 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
- bнформационная запись

328 Концепция системы защиты от информационного оружия не должна включать…

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

329 Преднамеренная угроза безопасности информации

нет правильного ответа
повреждение кабеля, по которому идет передача, в связи с погодными условиями
наводнение
- кража
ошибка разработчика

330 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

331 Средства защиты объектов файловой системы основаны на…

активная
задании атрибутов файлов и каталогов, зависящих от прав пользователей
задании атрибутов файлов и каталогов, независящих от прав пользователей
- определении прав пользователя на операции с файлами и каталогами
Нет правильного ответа

332 Защита информации обеспечивается применением антивирусных средств

иногда
не всегда
нет
- да
всегда

333 Элементы знака охраны авторского права:1.буквы С в окружности или круглых скобках2.буквы Р в окружности или круглых скобках3.наименования правообладателя4.наименование охраняемого объекта5.года первого выпуска программы

1,5,6
2,3,4
1,2,5
- 1.,3.,5
4,5,6

334 Основные угрозы конфиденциальности информации:1.москарад2.карнавал3.переадресовка4.перихват данных5.блокирование6.злоупатребления полномочиями

1,2,3
2,3,4
1,2,3
- 1.,4,6
4,5,6

335 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

336 Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасностирекомендации X.800

- Аранжевая книга
- нет правильного ответа
- Конституция
- Закону «Об информации, информационных технологиях и о защите информации»
- Система безопасности

337 Разделы современной криптографии:1.Симметричные криптосистемы2.Криптосистемы с открытым ключом3.Криптосистемы с дублированием защиты 4.Системы электронной подписи5.Управление паролями6.Управление передачей данных7.Управление ключами

- 2,4,6,7
- 4,5,6,7
- 1,3,4,7
- 1,2,,4,7
- 1,3,6,7

338 Информация, составляющая государственную тайну не может иметь гриф…

- нет правильного ответа
- «совершенно секретно»
- «секретно»
- «для служебнаго пользования»
- «особой важности»

339 Наиболее эффективное средство для защиты от сетевых атак

- нет правильного ответа
- посещение только «надёжных» Интернет-узлов
- использование антивирусных программ
- использавание сетевых экранов или «firewall»
- использование только сертифицированных программ-броузеров при доступе к сети Интернет

340 К формам защиты информации не относится…1.аналитическая2.правовая3.организационно-техническая4.страховая

- 2.4
- 1.3
- 1.2
- 1.4
- 3.4

341 Причины возникновения ошибки в данных1.Погрешность измерений2.Ошибка при записи результатов измерений в промежуточный документ3.Неверная интерпретация данных4.Ошибки при переносе данных с промежуточного документа в компьютер 5.Использование недопустимых методов анализа данных6.Неустранимые причины природного характера7.Преднамеренное искажение данных8.Ошибки при идентификации объекта или субъекта хозяйственной деятельности

- 1,5,6

3,4,5,6,7
1,2,3,7,8
- 1,,2,4,7,8
4,5,6

342 Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

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

343 Сервисы безопасности:1.идентификация и аутентификация2.шифрование3.инверсия паролей4.контроль целостности5.регулирование конфликтов6.экранирование7.обеспечение безопасного восстановления8.кэширование записей

1,3,4,6,7
3,4,5,6,7
1,2,3,4,5
- 1,2,,4,6,7
1,2,3,4,5

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

вмешательства в личную жизнь
МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
- МЭ были разрабатаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
Ничего не верно

345 Методы повышения достоверности входных данных1.Замена процесса ввода значения процессом выбора значения из предлагаемого множества2.Отказ от использования данных3.Проведение комплекса регламентных работ 4.Использование вместо ввода значения его считывание с машиночитаемого носителя5.Введение избыточности в документ первоисточник6.Многократный ввод данных и сличение введенных значений

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

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

Ничего не верно
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
- 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

347 Основные угрозы доступности информации:1.непреднамеренные ошибки пользователей2.злонамеренное изменение данных3.хакерская атака4.отказ программного и аппаратно

обеспечения5.разрушение или повреждение помещений6.перехват данных

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

348 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

349 Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

Должный процесс (Due process)
- Должная забота (Due care)
Повышение обязательств
Снижение обязательств
Стандарты

350 Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

Множество людей должно одобрить данные
Руководство должно одобрить создание группы
- Много информации нужно собрать и ввести в программу
Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
Сотрудники должны одобрить создание группы

351 Почему количественный анализ рисков в чистом виде не достижим?

Он достижим и используется
- Количественные измерения должны применяться к качественным элементам
Это связано с точностью количественных элементов
Множество людей должно одобрить данные
Он присваивает уровни критичности. Их сложно перевести в денежный вид

352 Что является наилучшим описанием количественного анализа рисков?

- Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
Метод, основанный на суждениях и интуиции
Анализ, основанный на информации, выявленной при оценке рисков

353 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 сами являются одной из причин рисков, они должны быть ответственны за их оценку

- Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

354 Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

- Выявление рисков
- Делегирование полномочий
- Выполнение анализа рисков
- Поддержка
- Определение цели и границ

355 Что из перечисленного не является целью проведения анализа рисков?

- Количественная оценка воздействия потенциальных угроз
- Делегирование полномочий
- Определение цели и границ
- Определение баланса между воздействием риска и стоимостью необходимых контрмер
- Выявление рисков

356 Как рассчитать остаточный риск?

- (Угрозы x Ценность актива) x Риски
- (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля
- Угрозы x Риски x Ценность актива
- (Угрозы x Ценность актива x Уязвимости) x Риски
- SLE x Частоту = ALE

357 Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

- Руководство должно одобрить создание группы
- Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
- Только военные имеют настоящую безопасность
- Военным требуется больший уровень безопасности, т.к. их риски существенно выше
- Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

358 Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

- Внедрение управления механизмами безопасности
- Уровень доверия, обеспечиваемый механизмом безопасности
- Выявление рисков
- Соотношение затрат / выгод
- Классификацию данных после внедрения механизмов безопасности

359 Эффективная программа безопасности требует сбалансированного применения:

- Контрмер и защитных механизмов
- Технических и нетехнических методов
- Соотношения затрат / выгод
- Процедур безопасности и шифрования
- Физической безопасности и технических средств защиты

360 Что является определением воздействия (exposure) на безопасность?

- Любой недостаток или отсутствие информационной безопасности
- Любая потенциальная опасность для информации или систем

Контрмер и защитные механизмы
- Нечто, приводящее к ущербу от угрозы

Потенциальные потери от угрозы

361 Тактическое планирование – это:

Планирование на год
- Среднесрочное планирование

Долгосрочное планирование
Ежедневное планирование
Планирование на 6 месяцев

362 Что лучше всего описывает цель расчета ALE?

Количественно оценить уровень безопасности среды
Оценить возможные потери для каждой контрмеры
- Оценить потенциальные потери от угрозы в год

Выявление уязвимостей и угроз, являющихся причиной риска
Количественно оценить затраты / выгоды

363 Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

Анализ действий
- Анализ затрат / выгоды

Анализ рисков
Результаты ALE
Выявление уязвимостей и угроз, являющихся причиной риска

364 Что такое политики безопасности?

Правила использования программного и аппаратного обеспечения в компании
- Широкие, высокоуровневые заявления руководства

Пошаговые инструкции по выполнению задач безопасности
Общие руководящие требования по достижению определенного уровня безопасности
Детализированные документы по обработке инцидентов безопасности

365 Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Когда необходимые защитные меры слишком просты
- Когда стоимость контрмер превышает ценность актива и потенциальные потери

Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
Когда риски не могут быть приняты во внимание по политическим соображениям
Когда необходимые защитные меры слишком сложны

366 Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Эффективные защитные меры и методы их внедрения
Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
Проведение тренингов по безопасности для всех сотрудников
Актуальные и адекватные политики и процедуры безопасности
- Поддержка высшего руководства

367 Что такое процедура?

Эффективные защитные меры и методы их внедрения
Обязательные действия
- Пошаговая инструкция по выполнению задачи

Правила использования программного и аппаратного обеспечения в компании

Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

368 Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Сотрудники
- Руководство

Владельцы данных
Пользователи
Администраторы

369 Что самое главное должно продумать руководство при классификации данных?

Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- Необходимый уровень доступности, целостности и конфиденциальности

Проведение тренингов по безопасности для всех сотрудников
Управление доступом, которое должно защищать данные
Оценить уровень риска и отменить контрмеры

370 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
- Улучшить контроль за безопасностью этой информации

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
Снизить уровень классификации этой информации

371 Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Пользователи
- Сотрудники

Хакеры
Атакующие
Контрагенты (лица, работающие по договору)

372 Кто является основным ответственным за определение уровня классификации информации?

- Владелец

Руководитель среднего звена
Высшее руководство
Пользователь
Проектировщик

373 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 без ограничения права доступа
Информация, распространение которой наносит вред интересам общества
Объект интеллектуальной собственности
- Информация с ограниченным дступом

374 Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:

Информационные ресурсы
Информационная система
- Информационные прдукты

Информационные услуги
Информационная сфера

375 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:

Безопасность АС
- Комплексное обспечение информационной безопасности

Политика безопасности
Атака на автоматизированную систему
Угроза безопасности

376 Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

Принцип гибкости системы
- Принцип системности

Принцип комплексности
Принцип непрерывной защиты
Принцип разумной достаточности

377 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
- Аппелируемость

Аутентичность
Доступность
Целостность

378 Организационные требования к системе защиты

управленческие и идентификационные
- административные и процедурные

физические
аппаратурные и физические
административные и аппаратурные

379 Обеспечение целостности информации в условиях случайного воздействия изучается

криптологией
- теорией помехоустойчивого кодирования

криптография
криптоанализом
стеганографией

380 Недостаток систем шифрования с открытым ключом

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

на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

381 Недостатком модели конечных состояний политики безопасности является

средняястепень надежности
- сложность реализации
изменение линий связи
статичность
низкая степень надежности

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

статичность
криптография
- криптология
криптоанализ
стеганография

383 Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

Фиксированнымкомпетенцией
- за определенное время
фиксированными затратами
ограниченной компетенцией злоумышленника
фиксированным ресурсом

384 Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

стеганология
- криптоанализ
криптография
стеганография
криптология

385 «Уполномоченные серверы» были созданы для решения проблемы

блокировки трафика
перехвата трафика
НСД
- имитации IP-адресов
подделки электронной подписи

386 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

387 К типам угроз безопасности парольных систем относятся

доступность
полиморфные
студенческие

- спутник
  ревизоро

388 Выделите группы, на которые делятся средства защиты информации:

  криптографические, комбинированные
  химические, аппаратные, программные, криптографические, комбинированные
  химические, аппаратные, программные, криптографические, комбинированные
- физические, аппаратные, программные, криптографические, комбинированные
  химические, аппаратные, программные, этнографические, комбинированные

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

  безопасность информации
  защитой информации
  защитой информации
- политикой безопасности
  организацией безопасности

390 К методам защиты от НСД относятся 1) разделение доступа;2) разграничение доступа;3) увеличение доступа;4) ограничение доступа.5) аутентификация и идентификация

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

391 К видам защиты информации относятся: 1) правовые и законодательные:2) морально-этические;3) юридические;4) административно-организационные

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

392 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 угроз
  системой угроз
- системой защиты
  системой уничтожения

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

  системы управления базами данных
  операционной системы, сетевого программного обеспечения
  операционной системы, сетевого программного обеспечения
- операционной системы, сетевого программного обеспечения и системы управления базами данных
  сетевого программного обеспечения и системы управления базами данных

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

безопасностью
опасностью
опасностью
- угрозой
предостережением

395 Разновидности угроз безопасности 1) техническая разведка ;2) программные ;3) программно-математичекие ;4) организационные ;5) технические ;6) физические .

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

396 Основные группы технических средств ведения разведки 1) радиомикрофоны;2) фотоаппараты ;3) электронные "уши" ;4) дистанционное прослушивание разговоров ;5) системы определения местоположения контролируемого объекта .

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

397 Виды технической разведки (по месту размещения аппаратуры) 1) космическая ;2) оптическая ;3) наземная ;4) фотографическая ;5) морская ;6) воздушная ;7) магнитометрическая .

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

398 Организационные угрозы подразделяются на 1) угрозы воздействия на персонал ;2) физические угрозы ;3) действия персонала ;4) несанкционированный доступ ;5) атаки на уровне СУБД .

2; 4
1; 3
1; 3
- 1; 2; 4
2; 3

399 Какие атаки предпринимают хакеры на программном уровне?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
1; 3; 5
1; 3; 5
- 1; 2; 4
2; 3; 5

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

код
данные
данные

- информация
- пароль

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

- достоверной
- шифруемой
- шифруемой
- защищаемой
- кодируемой

402 Что такое криптография?

- защиту информации от компьютерных вирусов
- область доступной информации
- 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 искуственного характера

403 Под ИБ понимают

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

404 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
- 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
- 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

405 Уровень секретности - это

- несанкционированное изменение информации, корректное по форме, содержанию и смыслу
- ответственность за модификацию и НСД информации
- 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

406 Прочность защиты в АС

- вероятность преодоления защиты нарушителем за установленный промежуток времени
- способность системы защиты информации обеспечить достаточный уровень своей безопасности
- 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

407 Линейное шифрование -

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

408 К аспектам ИБ относятся.Выберите несколько из 5 вариантов ответа:1) дискретность ;2) целостность ;3) конфиденциальность ;4) актуальность ;5) доступность ;

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

1; 3; 4

409 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 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 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)

410 Утечка информации

- ознакомление постороннего лица с содержанием секретной информации

это присвоение имени субъекту или объекту
несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
защищенная информация

411 Кодирование информации -

Определение файлов, из которых удалена служебная информация
метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
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

412 Верификация -

Определение файлов, из которых удалена служебная информация
это проверка принадлежности субъекту доступа предъявленного им идентификатора
это проверка принадлежности субъекту доступа предъявленного им идентификатора
- проверка целостности и подлинности инф, программы, документа

защищенная информация

413 "Маскарад"- это

представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
осуществление специально разработанными программами перехвата имени и пароля
осуществление специально разработанными программами перехвата имени и пароля
- выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями

взломать систему защиты

414 Что такое аутентификация?

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

Определение файлов, из которых удалена служебная информация

415 Под ИБ понимают

защиту информации искуственного характера
защиту от несанкционированного доступа
защиту от несанкционированного доступа
- защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

защиту от санкционированного доступа

416 В чем состоит задача криптографа?

осуществление специально разработанными программами перехвата имени и пароля
взломать систему защиты
взломать систему защиты
- обеспечить конфиденциальность и аутентификацию передаваемых сообщений

взломать систему защиты

417 Кто является знаковой фигурой в сфере информационной безопасности

Шелдон
Шеннон
Шеннон
- Митник

Беббидж

418 Что такое целостность информации?

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

Свойство информации, заключающееся в возможности ее изменения любым субъектом

419 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

420 Недостатком модели политики безопасности на основе анализа угроз системе является

механизм реализации
сложный механизм реализации
необходимость дополнительного обучения персонала
- изначальное допущение вскрываемости системы

статичность

421 Недостатком дискретных моделей политики безопасности является

допущение вскрываемости системы
изначальное допущение вскрываемости системы
необходимость дополнительного обучения персонала
- статичность

сложный механизм реализации

422 Наименее затратный криптоанализ для криптоалгоритма RSA

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

разложение числа на сложные множители

423 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

424 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

425 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

426 Защита исполняемых файлов обеспечивается

стандартным запуском
специальным режимом запуска
криптографией
- обязательным контролем попытки запуска

дополнительным хостом

427 Запись определенных событий в журнал безопасности сервера называется

контролем
трафиком
мониторингом
- аудитом

учетом

428 Достоинством матричных моделей безопасности является

гибкость управления
обеспепечение безопасности
контроль за потоками информации
расширенный аудит
- легкость представления широкого спектра правил обеспечения безопасности

429 Для реализации технологии RAID создается

аппаратные средства
интерпретатор
специальный процесс
- псевдодрайвер

компилятор

430 Восстановление данных является дополнительной функцией услуги защиты

идентификация
причастность
аутентификация
- целостность

контроль доступа

431 Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС

внутренний
приложений
системный
- внешний

сетевой

432 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 на выполняются

все запросы выполняются

433 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

434 К достоинствам технических средств защиты относятся:

Все ответы не верны

степень сложности устройства
регулярный контроль
- создание комплексных систем защиты

Все варианты верны

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

полиморфные
ревизором
иммунизатором
- сканером

доктора и фаги

436 Хранение паролей может осуществляться

все варианты ответа верны
в закрытом виде
в закрытом виде
- в виде сверток

в незашифрованном виде

437 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 прграмма 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

438 К посторонним лицам нарушителям информационной безопасности относится:

технический персонал, обслуживающий здание
- представители конкурирующих организаций.

лица, нарушившие пропускной режим
сотрудники службы безопасности
пользователи

439 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
физическое разрушение системы путем взрыва, поджога и т.п
- 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.

440 Икусственные 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

441 Естественные угрозы безопасности информации вызваны:

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

442 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
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств

443 Защита информации от утечки это деятельность по предотвращению:

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

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

- аналитических преобразований
- кодирования
- подстановки
- гаммирования
- перестановки

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

- аналитических преобразований
- кодирования
- гаммирования
- подстановки
- перестановки

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

- аналитических преобразований
- подстановки
- гаммирования
- перестановки
- кодирования

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

- OCTAVE
- ISO\IEC
- Безопасная OECD
- OECD
- CPTED

448 Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

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

449 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 являются корпоративными
- NIST и OCTAVE ориентирован на ИТ
- NIST и AS/NZS являются корпоративными

450 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

451 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

452 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

453 Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

- Текущая версия ISO 27000
- Текущая версия ISO 17799

Список стандартов, процедур и политик для разработки программы безопасности
- Открытый стандарт, определяющий цели контроля

Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

454 Утечка информации – это …

года первого выпуска программы
процесс уничтожения информации
процесс раскрытия секретной информации
- несанкционированный процесс переноса информации от источника к злоумышленнику

непреднамеренная утрата носителя информации

455 Информация, составляющая государственную тайну не может иметь гриф…

«совершенно секретно»
- «для служебного пользования»

правовая
«особой важности»
«секретно»

456 Наиболее эффективное средство для защиты от сетевых атак

использование сетевых экранов или «firewall» и использование антивирусных программ
использование антивирусных программ
использование сетевых экранов или «firewall»
- использование только сертифицированных программ-броузеров при доступе к сети Интернет

посещение только «надёжных» Интернет-узлов

457 К формам защиты информации не относится…

Зональным
организационно-техническая
правовая
- аналитическая

страховая

458 Причины возникновения ошибки в данных

Преднамеренное искажение данных
Использование недопустимых методов анализа данных
Ошибки при переносе данных с промежуточного документа в компьютер
- Неверная интерпретация данных

Неустранимые причины природного характера

459 Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

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

вмешательства в личную жизнь

460 Методы повышения достоверности входных данных

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

Проведение комплекса регламентных работ

461 Суть компрометации информации

- способна противостоять только информационным угрозам, как внешним так и внутренним
- 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
- внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
- несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
- способна противостоять только внешним информационным угрозам

462 Основные угрозы доступности информации:

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

463 Что не относится к информационной инфекции:

- Логическая бомба
- Черви
- Троянский конь
- Фальсификация данных
- Вирусы

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

- Информационное общество
- Информационные инфекции
- Физический инфекции
- Информационный саботаж
- Информационные оружия

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

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

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

- защита
- аутентичность
- доступность
- конфиденциальность
- целостность

467 Что относится к классу информационных ресурсов:

- Документы
- Организационные единицы
- Персонал
- все правельные ответы
- Промышленные образцы, рецептуры и технологии

468 Наиболее распространенные угрозы информационной безопасности:

- угрозы защищенности
- угрозы вируса
- угрозы деятельности
- угрозы безопасности
- ● угрозы целостности

469 Информационная безопасность это:

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

470 К национальным интересам АР 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

471 Охранное освещение бывает:

- архив
- заключеной
- световое
- ● дежурное
- открытое

472 К оборонительным системам защиты относятся:

- электрофизические датчики
- электрохимические датчики
- датчики
- ● звуковые установки
- электромеханические датчики

473 К системам оповещения относятся:

- электрофизические датчики
- электромеханические датчики
- неэлектрические датчики
- ● инфракрасные датчики
- электрохимические датчики

474 К тщательно контролируемым зонам относятся:

- световые
- пользователя
- администратор
- ● архив
- электрохимические датчики

475 Что такое криптология?

область недоступной информации
- тайная область связи

область доступной информации
область доступной информации
незащищенная информация

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

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

477 Технические средства защиты информации .Выберите один из 4 вариантов ответа:

осуществление специально разработанными программами перехвата имени и пароля
средства, которые реализуются в виде автономных устройств и систем
- средства, которые реализуются в виде электрических, электромеханических и электронных устройств устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

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

с появлением интернета
- с недостаточной образованностью в области безопасности

с достаточной образованностью в области безопасности
средства, которые реализуются в виде автономных устройств и систем
с появлением интернета

479 Физические средства защиты информации . Выберите один из 4 вариантов ответа:

средства, которые реализуются в виде электрических, электромеханических и электронных устройств 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

устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
это программы, предназначенные для выполнения функций, связанных с защитой информации

480 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
2; 3; 5; 6
2; 3; 5; 6
1; 4; 5; 6
- 1; 2; 3; 6

481 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

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

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

портом
- сокетом
терминалом
кластером
портом

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

сеансовом
сеансовом
канальном
прикладном
- транспортном

484 Недостатком матричных моделей безопасности является

отсутствие части аудита
отсутствие полного аудита
отсутствие полного аудита
сложность представления широкого спектра правил обеспечения безопасности
- отсутствие контроля за потоками информации

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

прикладном
транспортном
- сетевом
канальном
канальном

486 Конфигурация из нескольких компьютеров, выполняющих общее приложение, называется

суперсервером
- кластером
портом
сетью
суперсервером

487 Как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных определяется

контроль доступа
аутентификация
- причастность
аутентификация
идентификация

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

- 2.4
- 3, 4
- 3, 4
- 2, 3
- 1, 3

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

- 2.0
- 3, 4
- 1, 2
- 2, 4
- 2, 4

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

- 2 ,4
- 3, 4
- 1, 2
- 1.0
- 2 ,4

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

- 2, 3
- 1, 2, 5
- 2.5
- 3, 5
- 2, 3

492 Из перечисленного тиражирование данных происходит в режимах: 1) синхронном; 2) асинхронном; 3) импульсном; 4) тоновом

- 3, 4
- 2, 4
- 1, 2
- 2, 4
- 3.0

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

- 2, 3, 5
- 1, 2, 5
- 2, 3
- 2.5
- 2, 3, 5

494 Трояские программы — это

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

495 Идентификатор субъекта доступа, который является его секретом:

- ключ
- админом
- сертификат ключа подписи
- электронно-цифровая подпись
- пароль

496 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 от утечки информации
- защита информации от несанкционированного воздействия
- защита информации от несанкционированного доступа
- защита информации от непреднамеренного воздействия

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

- 2, 3, 4
- 1, 2, 3
- 1, 3, 4
- 3, 4, 5
- 1, 4, 5

498 Структурированная защита согласно «Оранжевой книге» используется в системах класса

- B2
- C2
- B3
- B1
- C1

499 Стандарт DES основан на базовом классе

- шифры
- блочные шифры
- замещения
- перестановки
- гаммирование

500 Содержанием параметра угрозы безопасности информации «конфиденциальность» является

- модификация
- искажение
- уничтожение
- несанкционированное получение
- несанкционированная модификация

501 Согласно «Оранжевой книге» с объектами должны быть ассоциированы

- подписи
- типы операций
- электронные подписи
- метки безопасности
- уровни доступа

502 Согласно «Оранжевой книге» мандатную защиту имеет группа критериев

- E
- A
- D
- B
- C

503 Согласно «Оранжевой книге» верифицированную защиту имеет группа критериев

- E
- C
- D
- A
- B

504 Согласно «Европейским критериям» только общая архитектура системы анализируется на уровне

- E4
- E2
- E3
- E1
- E0

505 Согласно «Европейским критериям» на распределенные системы обработки информации ориентирован класс

- F-D
- F-AV
- F-IN
- F-DI
- F-DX

506 Согласно «Европейским критериям» для систем с высокими потребностями в обеспечении целостности предназначен класс

- F-A
- F-DI
- F-DX
- F-IN
- F-AV

507 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

508 С помощью открытого ключа информация

- некопируется
- транслируется
- копируется
- зашифровывается
- расшифровывается

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

- максимизация риска
- оптимизацией средств защиты
- мониторингом средств защиты
- управлением риском
- минимизацией риска

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

- уборка, перехват
- наблюдение
- компрометация
- перехват
- уборка мусора

511 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

512 При количественном подходе риск измеряется в терминах

- заданных с помощью информации
- заданных с помощью ранжирования
- заданных с помощью шкалы
- денежных потерь
- объема информации

513 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

514 Соответствие средств безопасности решаемым задачам характеризует

- надежность
- унификация
- адекватность
- эффективность
- корректность

515 Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

- важные объекты
- наиболее важные субъекты
- наиболее важные объекты
- все субъекты

все объекты

516 Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

A
B
A
● D
C

517 Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев

E
B
A
● C
D

518 Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

E1
E5
E4
● E6
E7

519 Согласно «Европейским критериям» предъявляет повышенные требования и к целостности, и к конфиденциальности информации класс

F-IE
F-AV
F-DI
● F-DX
F-IN

520 Согласно «Европейским критериям» минимальную адекватность обозначает уровень

E2
E6
E7
● E0
E1

521 Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

актуальностью
доступностью
целостностью
● качеством информации
актуальностью информации

522 С точки зрения ГТК основной задачей средств безопасности является обеспечение

простоты
● защиты от НСД
простоты реализации
сохранности информации

надежности функционирования

523 С помощью закрытого ключа информация

- шифруется
- зашифровывается
- транслируется
- копируется
- ● расшифровывается

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

- фильтр
- ● имитатор
- перехватчик
- заместитель
- аудит

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

- фильтр
- ● аутентификация
- идентификация
- аудит
- авторизация

526 При полномочной политике безопасности совокупность меток с одинаковыми значениями образует

- область равной критичности
- ● уровень безопасности
- уровень равной доступности
- уровень доступности
- область равного доступа

527 При качественном подходе риск измеряется в терминах

- денежных потерь
- ● заданных с помощью шкалы или ранжирования
- денежных оценок
- оценок экспертов
- объема информации

528 При избирательной политике безопасности в матрице доступа субъекту системы соответствует

- ячейка
- прямоугольная область
- поле
- ● столбец
- строка

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

- наблюдение
- ● тип разрешенного доступа
- объект системы

субъект системы
факт доступа

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

объект
перехват
- компрометация

уборка мусора
наблюдение

531 По документам ГТК самый высокий класс защищенности СВТ от НСД к информации

5.0
- 1.0

9.0
7.0
6.0

532 По документам ГТК количество классов защищенности АС от НСД

6.0
- 9.0

5.0
7.0
8.0

533 Основу политики безопасности составляет

управление объектом
- способ управления доступом

программное обеспечение
управление риском
выбор каналов связи

534 Организационные требования к системе защиты

физические
административные и аппаратурные
управленческие и идентификационные
- административные и процедурные

аппаратурные и физические

535 Обеспечение целостности информации в условиях случайного воздействия изучается

криптография
стеганографией
криптологией
- теорией помехоустойчивого кодирования

криптоанализом

536 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

537 Недостатком модели конечных состояний политики безопасности является

- изменение линий связи
- средняя степень надежности
- низкая степень надежности
- статичность
- ● сложность реализации

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

- статичность
- стеганография
- криптоанализ
- ● криптология
- криптография

539 Наименее затратный криптоанализ для криптоалгоритма DES

- разложение числа на множители
- разложение числа на простые множители
- разложение числа на сложные множители
- ● перебор по всему ключевому пространству
- перебор по выборочному ключевому пространству

540 На многопользовательские системы с информацией одного уровня конфиденциальности согласно «Оранжевой книге» рассчитан класс

- B3
- C2
- B2
- ● C1
- B1

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

- статичность
- идентифицируемым
- мандатным
- ● мандатным
- избирательным

542 Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

- столбец
- С полным перекрытием
- На основе анализа угроз
- ● LWM
- Лендвера

543 При избирательной политике безопасности в матрице доступа объекту системы соответствует

- поле
- ячейка
- прямоугольная область

- строка
- столбец

544 Политика информационной безопасности — это

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

545 По документам ГТК самый низкий класс защищенности СВТ от НСД к информации

- 2.0
- 0.0
- 9.0
- 6.0
- 1.0

546 По документам ГТК количество классов защищенности СВТ от НСД к информации

- 5.0
- 8.0
- 9.0
- 6.0
- 7.0

547 Первым этапом разработки системы защиты ИС является

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

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

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

549 Обеспечением скрытности информации в информационных массивах занимается

- криптология
- криптология
- криптоанализ
- стеганография
- криптография

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

- профилем защиты
- системой защиты
- стандартом безопасности

профилем безопасности
системой безопасности

551 Недостатком модели политики безопасности на основе анализа угроз системе является

механизм реализации
сложный механизм реализации
необходимость дополнительного обучения персонала
- изначальное допущение вскрываемости системы
статичность

552 Недостатком дискретных моделей политики безопасности является

допущение вскрываемости системы
изначальное допущение вскрываемости системы
необходимость дополнительного обучения персонала
- статичность
сложный механизм реализации

553 Наименее затратный криптоанализ для криптоалгоритма RSA

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

554 Надежность СЗИ определяется

сильным звеном
усредненным показателем
количеством отраженных атак
- самым слабым звеном
самым сильным звеном

555 Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

Фиксированным компетенцией
ограниченной компетенцией злоумышленника
фиксированными затратами
- за определенное время
фиксированным ресурсом

556 Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

стеганология
стеганография
криптография
- криптоанализ
криптология

557 Конечное множество используемых для кодирования информации знаков называется

символом
ключом
кодом
- алфавитом

шифром

558 Охранное освещение бывает:a.дежурноеb.световоес.тревожжное

- b
- a,b
- b,c
- a,c
- a

559 К оборонительным системам защиты относятся:1.проволочные ограждения2.звуковые установки3.датчики4.световые установки

- 3.0
- 1,3,4
- 3,4
- 1,2,4
- 4.0

560 К системам оповещения относятся:1.инфракрасные даттчики2.электрические даттчики3.электромеханические датчики 4.электрохимические датчики

- 2.0
- 1,3
- 3,4
- 1,2
- 1,4

561 К тщательно контролируемым зонам относятся:1.рабочее место администратора2.архив3.рабочее место пользователя

- только 1
- только 3
- 2,3
- 1,2,3
- только 2

562 К достоинствам технических средств защиты относятся:

- нет правильного ответа
- степень сложности устройства
- регулярный контроль
- саздание комплексных систем защиты
- Все варианты верны

563 Протокол FTP предназначен для...

- Транспортном
- просмотра Web-страниц
- общения в чатах
- передачи файлов
- загрузки сообщений из новостных групп

564 Особенностями информационного оружия являются:

- доступность
- системность
- открытость
- универсальность

надежность

565 Виды уязвимостей

вероятная
случайная
субъективная
- постоянная

объективная

566 Показателями безопасности информации являются:

вероятность сбоя системы безопасности
время, в течение которого обеспечивается определённый уровень безопасности
время, необходимое на взлом защиты информации
- вероятност предотвращения угрозы

вероятность возникновения угрозы информационной безопасности

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

достоверной
понятной
полезной
- актуальной

полной

568 В соответствии с законом АР «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

569 Примером числовой информации может служить:

разговор по телефону
иллюстрация в книге
симфония
- таблица значений тригоннометрических функций

поздравительная открытка

570 Информация в семантической теории - это:

всякие сведения, сообщения, знания
неотъемлемое свойство материи
сведения, обладающие новизной
- сведения, полностью снимающие или уменьшающие существующую до их получения неопределеность

сигналы, импульсы, коды, наблюдающиеся в технических и биологических системах

571 Для создания базы данных пользователь должен получить привилегию от

сетевого администратора
баз данных
старшего пользователя своей группы
системного администратора
- администратора сервера баз данных

572 Дескриптор защиты в Windows 2000 содержит список

- объектов
- привилегий, назначенных пользователю
- объектов, не доступных пользователям
- пользова¬телей и групп, имеющих доступ к объекту
- объектов, доступных пользователю и группе

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

- совокупность
- целостность
- восстанавливаемость
- доступность
- детермированность

574 В СУБД Oracle под ролью понимается

- совокупность
- группа объектов
- совокупность процессов
- набор привилегий
- группа субъектов

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

- совокупность
- специально оговариваться
- доминировать
- быть равен
- быть меньше

576 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

577 Брандмауэры первого поколения представляли собой

- хосты с фильтрацией
- уполномоченные серверы
- неприступные серверы
- маршрутизаторы с фильтрацией пакетов
- хосты с фильтрацией пакетов

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

- сеансовым
- транспортном
- сетевом
- физическом
- канальном

579 Администратор сервера баз данных имеет имя

- system
- sysadm
- admin
- ● ingres
- root

580 ACL-список ассоциируется с каждым

- типом
- доменом
- типом доступа
- ● объектом
- процессом

581 «Уполномоченные серверы» фильтруют пакеты на уровне

- прикладным
- канальном
- транспортном
- ● приложений
- физическом

582 Являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от кла¬виатуры, клавиатурные шпионы типа

- нарушители
- заместители
- перехватчики
- ● фильтры
- имитаторы

583 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

584 У всех программных закладок имеется общая черта

- ● обязательно выполняют опера¬цию записи в память
- постоянно находятся в оперативной памяти
- обязательно выполняют опера¬цию чтения из памяти
- перехватывают прерывания
- обязательно выполняют опера¬цию чтения

585 Требования к техническому обеспечению системы защиты

- документарные и аппаратурные
- процедурные и раздельные
- управленческие и документарные
- ● аппаратурные и физические
- административные и аппаратурные

586 В соответствии с федеральным законом АР «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

587 В каком документе содержаться основные требования к безопасности информационных систем в США?

в красном блокноте
в оранжевой книге
в желтой прессе
- в красной книге

в черном списке

588 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

589 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

590 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

591 Какие сведения на территории АР могут составлять коммерческую тайну?

любые
документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности
сведенья о численности работающих, их заработной плате и условиях труда
- учредительные документы и устав предприятия

другие

592 Кто может быть владельцем защищаемой информации?

кто угодно
общественные организации
предприятия акционерные общества, фирмы
- только государство и его структуры

только вышеперечисленные

593 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

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

- правильного ответа нет
- ● политическая разведка
- промышленный шпионаж
- добросовестная конкуренция
- конфиденциальная информация

595 Что включает в себя ранжирование как метод защиты информации?

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

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

- на тактическом
- ● на организационно-правовом
- на социально политическом
- на инженерно-техническом
- на всех вышеперечисленных

597 то включают в себя технические мероприятия по защите информации?

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

598 Выделите три наиболее важных метода защиты информации от ошибочных действий пользователя

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

599 Выделите три наиболее важных метода защиты информации от нелегального доступа

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

600 Какие существуют наиболее общие задачи защиты информации на предприятии?

- 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
- все вышеперечисленные
- предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации
- документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы

601 Что в себя морально-нравственные методы защиты информации?

- вариант ответа 1, 2 и 3
- воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений
- контроль работы сотрудников, допущенных к работе с секретной информацией
- обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней
- вариант ответа 1 и 3

602 Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

- изменить и уничтожить ее
- получить, изменить, а затем передать ее конкурентам
- размножить или уничтожить ее
- получить, изменить или уничтожить
- изменить, повредить или ее уничтожить

603 Какие степени сложности устройства Вам известны

- встроенные
- упрощенные
- сложная
- простые
- оптические

604 Какие компоненты входят в комплекс защиты охраняемых объектов:

- админ
- Система
- Вирус
- Датчики
- Оружие

605 Свойства информации в форме сведений: (укажите правильный вариант)

- материальность
- сложность
- проблемная ориентированность
- накапливаемость
- измеримость

606 К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?

- Научный инструментарий
- Организационные единицы
- Персонал

- Документы
  Промышленные образцы

607 Мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных это:

  скамер
  фишер
  фракер
- кракер
  хакер

608 К антивирусным программам не относятся:

  исполняемые
  ревизоры
  фаги
- интерпретаторы
  мониторы

609 Назначение антивирусных программ, называемых детекторами:

  всегда меняет начало и длину файла
  обнаружение компьютерных вирусов
  обнаружение и уничтожение вирусов
- контроль возможных путей распространения компьютерных вирусов
  уничтожение зараженных файлов

610 Файловый вирус ...

  преступлением
  всегда меняет начало и длину файла
  всегда меняет длину имени файла
- всегда изменяет код заражаемого файла
  поражает загрузочные сектора дисков

611 Перехват, который осуществляется путем использования оптической техники называется:

  просмотр мусора
  пассивный перехват
  активный перехват
- видеоперехват
  аудиоперехват

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

  просмотр мусора
  пассивный перехват
  активный перехват
- аудиоперехват
  видеоперехват

613 Скрытые проявлениям вирусного заражения:

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

614 Стадии жизненного цикла классического трояна

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

615 Типы методов антивирусной защиты

- теоретические
- организационные
- технические
- программные
- практические

616 Использование брандмауэров относят к … методам антивирусной защиты

- троянов
- практическим
- техническим
- организационным
- теоретическим

617 Логические бомбы относятся к классу …

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

618 Цель создания анонимного SMTP-сервера – для …

- не открывать почтовые сообщения, содержащие вложения
- создания ботнета
- размещения на них сайтов с порнографической или другой запрещенной информацией
- рассылки спама
- распределенных вычислений сложных математических задач

619 Антиспамовая программа, установленная на домашнем компьютере, служит для …

- анализе кода на предмет наличия подозрительных команд
- обеспечения регулярной доставки антивирусной программе новых антивирусных баз
- защиты компьютера от хакерских атак
- защиты компьютера от нежелательной и/или незапрошенной корреспонденции
- корректной установки и удаления прикладных программ

620 Косвенное проявление наличия вредоносной программы на компьютере

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

621 Сигнатурный метод антивирусной проверки заключается в …

- выявление уязвимостей в системе защиты

отправке файлов на экспертизу в компанию-производителя антивирусного средства
сравнении файла с известными образцами вирусов
- анализе поведения файла в разных условиях

анализе кода на предмет наличия подозрительных команд

622 Какие мероприятия не являются административными при обеспечении мер безопасности:

порядок хранения документов
контроль журналов работы
пропускной режим
- выявление уязвимостей в системе защиты

контроль смены паролей

623 Отличительными особенностями компьютерного вируса являются:

являются следствием ошибок в операционной системе
помехи корректной работе компьютера
значительный объем программного кода
- маленький объем и способность к самостоятельному запуску и созданию

необходимость запуска со стороны пользователя

624 Под утечкой информации понимается...

Внедрение дезинформации
Непреднамеренная утрата носителя информации
Процесс уничтожения информации
- Несанкционированный процесс переноса информации от источника к злоумышленнику

Процесс раскрытия секретной информации

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

информационное превосходство
банковская тайна
государственная тайна
- коммерческая тайна

конфиденциальная информация

626 Что нельзя публиковать в Интернете?

свои заметки
свои фотографии
свою биографию
- сведния о учёбе и работе

паспортные данные

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

защищенность информации
адекватность
уязвимость информации
надежность информации
- базопасность информации

628 Соответствие средств безопасности решаемым задачам характеризует

надежность

унификация
адекватность
- эффективность
корректность

629 Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

важные объекты
наиболее важные субъекты
наиболее важные объекты
- все субъекты
все объекты

630 Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

C
B
A
- D
E

631 Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев

E
B
A
- C
D

632 Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

E1
E5
E4
- E6
E7

633 Согласно «Европейским критериям» предъявляет повышенные требования и к целостности, и к конфиденциальности информации класс

F-IE
F-AV
F-DI
- F-DX
F-IN

634 актуальностью

E2
E6
E7
- E0
E1

635 Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

актуальностью

доступностью
целостностью
- качеством информации
актуальностью информации

636 С точки зрения ГТК основной задачей средств безопасности является обеспечение

простоты
сохранности информации
простоты реализации
- защиты от НСД
надежности функционирования

637 С помощью закрытого ключа информация

шифруется
копируется
транслируется
- расшифровывается
зашифровывается

638 Программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа

аудит
заместитель
перехватчик
- имитатор
фильтр

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

фильтр
- аутентификация
идентификация
аудит
авторизация

640 При полномочной политике безопасности совокупность меток с одинаковыми значениями образует

- уровень безопасности
уровень доступности
область равного доступа
область равной критичности
уровень равной доступности

641 При качественном подходе риск измеряется в терминах

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

642 При избирательной политике безопасности в матрице доступа субъекту системы соответствует

поле

ячейка
прямоугольная область
- столбец
строка

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

наблюдение
субъект системы
объект системы
- тип разрешенного доступа
факт доступа

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

объект
наблюдение
уборка мусора
- компрометация
перехват

645 По документам ГТК самый высокий класс защищенности СВТ от НСД к информации

5.0
7.0
9.0
- 1.0
6.0

646 По документам ГТК количество классов защищенности АС от НСД

5.0
8.0
6.0
- 9.0
7.0

647 Основу политики безопасности составляет

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

648 Наименее затратный криптоанализ для криптоалгоритма DES

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

649 На многопользовательские системы с информацией одного уровня конфиденциальности согласно «Оранжевой книге» рассчитан класс

B3

C2
B2
- C1
B1

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

статичность
идентифицируемым
привилегированным
- мандатным
избирательным

651 Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

столбец
С полным перекрытием
На основе анализа угроз
- LWM
Лендвера

652 При избирательной политике безопасности в матрице доступа объекту системы соответствует

поле
ячейка
прямоугольная область
- строка
столбец

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

Подлинность
Режиме доступа к
Ценности
- Подлинности
Секретности

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

Червь
Блокировщики
Ревизоры
- Полифаги
Сторожа

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

MS Word, MS Excel
MS Word, MS Excel, Norton Commander
MS-DOS, MS Word, AVP
- AVP, DrWeb, Norton AntiVirus
MS Word, MS Excel, Paint

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

Все перечисленное
На удалении зараженных файлов
На ожидании начала вирусной атаки
- На сравнение программных кодов с известными вирусами

На всех перечисленных

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

База данных
Программные средства
Аппаратные средства
- Аппаратные средства и антивирусные программы

Все перечисленное

658 Элементы знака охраны авторского права:

года первого выпуска программы
наименования (имени) правообладателя
буквы С в окружности или круглых скобках
- буквы Р в окружности или круглых скобках

наименование охраняемого объекта

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

принцип гибкости системы
принцип непрерывности
принцип комплексности
- принцип разумной достаточности

принцип системности

660 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

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

3,4,5
2,3,5
2,4,5
- 1,3,4,5

2.4

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

2,3,5
- 1,2,3

3.4
3,4,5
2,4,5

663 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

664 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

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

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

666 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

667 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

668 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

669 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

4.0
1.4
2.4
- 1.3
1.2

670 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

671 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

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

672 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
- 2,3,4
1,2,5

673 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

674 Идентификаторы безопаснос¬ти в Windows 2000 представляют собой

полную строку симолов
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

675 Защита от программных закладок обеспечивается

системным программным обеспечением
ПО
аппаратным модулем, устанавливаемым на контроллер
специальным программным обеспечением
- аппаратным модулем, устанавливаемым на системную шину ПК

676 Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты

- несетевого уровня
- сетевого уровня
- системного уровня
- встроенных в ОС
- уровня приложений

677 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
- 3.0
- 2.4
- 1.2
- 3.4

678 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

679 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

680 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

681 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

682 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

683 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

684 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

685 Из перечисленного в ОС UNIX существуют администраторы: 1) системных утилит; 2) службы контроля; 3) службы аутентификации; 4) тиражирования; 5) печати; 6) аудита

- 1.2
- 4.5
- 1,2,4
- 1,3,5,6
- 1,2,3

686 Структурированная защита согласно «Оранжевой книге» используется в системах класса

- B3
- B2
- C1
- B1
- C2

687 Стандарт DES основан на базовом классе

- блочные шифры
- замещения
- перестановки
- гаммирование
- шифры

688 Содержанием параметра угрозы безопасности информации «конфиденциальность» является

- несанкционированное получение
- модификация
- несанкционированная модификация
- уничтожение
- искажение

689 Согласно «Оранжевой книге» с объектами должны быть ассоциированы

- электронные подписи
- метки безопасности
- типы операций
- подписи
- уровни доступа

690 Согласно «Оранжевой книге» мандатную защиту имеет группа критериев

- B
- E
- C
- D
- A

691 Согласно «Оранжевой книге» верифицированную защиту имеет группа критериев

- D
- A
- C
- E
- B

692 Согласно «Европейским критериям» только общая архитектура системы анализируется на уровне

- E1
- E4
- E0
- E3
- E2

693 Согласно «Европейским критериям» на распределенные системы обработки информации ориентирован класс

- F-IN
- F-D
- F-DX
- F-AV
- F-DI

694 Согласно «Европейским критериям» для систем с высокими потребностями в обеспечении целостности предназначен класс

- F-A
- F-IN
- F-AV
- F-DX
- F-DI

695 Система защиты должна гарантировать, что любое движение данных

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

696 С помощью открытого ключа информация

- зашифровывается
- некопируется
- расшифровывается
- транслируется
- копируется

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

- управлением риском
- максимизация риска
- минимизацией риска
- оптимизацией средств защиты
- мониторингом средств защиты

698 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, перехват
- уборка мусора
- наблюдение
- компрометация

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

- аудит
- идентификация
- идентификация, аудит
- аутентификация
- авторизация

700 При количественном подходе риск измеряется в терминах

- заданных с помощью шкалы
- заданных с помощью ранжирования
- объема информации
- заданных с помощьюинформации
- денежных потерь