1613Y_Ru_Æyani_Yekun imtahan testinin sualları

Fənn : 1613Y Kompüter sistemlərində informasiya təhlükəsizliyi

1 Кто является основным ответственным за определение уровня классификации информации?

- ◯ Проектировщик
- ◯ Высшее руководство
- ◯ Руководитель среднего звена
- ◉ Владелец
- ◯ Пользователь

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

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

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

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

4 Что такое политики безопасности?

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

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

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

6 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

7 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

8 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

9 Какие компоненты входят в комплекс защиты охраняемых объектов:

- admin
- Система
- Вирус
- Датчики
- Оружие

10 К выполняемой функции защиты относится:

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

11 Что самое главное должно продумать руководство при классификации данных?

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

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

- Сотрудники

- ○ Пользователи
- ○ Владельцы данных
- ◉ Руководство
- ○ Администраторы

13 Что является определением воздействия (exposure) на безопасность?

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

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

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

15 Естественные угрозы безопасности информации вызваны:

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

16 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

17 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.

18 К посторонним лицам нарушителям информационной безопасности относится

- ○ лица, нарушившие пропускной режим
- ○ пользователи
- ○ технический персонал, обслуживающий здание
- ◉ представители конкурирующих организаций

- ○ сотрудники службы безопасности

19 К функциям информационной безопасности не относятся:

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

20 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

21 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

22 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

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

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

24 Что нельзя публиковать в Интернете?

- ○ свои заметки
- ○ свои фотографии
- ○ свою биографию
- ● сведния о учёбе и работе
- ○ паспортные данные

25 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

26 Что такое фишинг?

- переписка от чужого лица с целью вымогательства денежных средств
- комплекс аппаратных или программных средств, осуществляющий лечение компьютера
- бесплатное антивирусное приложение для разблокировки компьютера
- создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д.
- создание бесплатных программ, заражённых вирусами и троянами

27 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

28 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

29 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

30 Программу нужно обязательно проверить на наличие вирусов…

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

31 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

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

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

33 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

34 Информация в семантической теории - это:

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

35 Примером числовой информации может служить:

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

36 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

- [x] 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

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

- [ ] достоверной
- [ ] понятной
- [ ] полезной
- [x] актуальной
- [ ] полной

38 Показателями безопасности информации являются:

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

39 Виды уязвимостей

- [ ] случайная
- [x] постоянная
- [ ] вероятная
- [ ] объективная
- [ ] субъективная

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

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

41 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
- [x] воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений
- [ ] вариант ответа 1 и 3

42 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
- [x] 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

43 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

44 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

45 Что включают в себя технические мероприятия по защите информации?

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

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

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

47 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

48 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

49 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

50 Кто может быть владельцем защищаемой информации?

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

51 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

52 Какие секретные сведения входят в понятие «коммерческая тайна»?

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

53 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

54 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

55 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

56 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
- [x] 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

57 Какие степени сложности устройства Вам известны

- встроенные
- сложная
- упрощенные
- [x] простые
- оптические

58 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
- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- [x] Улучшить контроль за безопасностью этой информации
- Снизить уровень классификации этой информации

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

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

60 Почему количественный анализ рисков в чистом виде не достижим?

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

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

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

- ○ Множество людей должно одобрить данные

62 С доступом к информационным ресурсам внутри организации связан уровень ОС

- ○ канальный
- ◉ сетевой
- ○ системный
- ○ приложений
- ○ внешний

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

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

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

- ○ Государственная безопасность
- ○ Безопасность
- ○ Информационная безопасность
- ◉ Национальная безпасность
- ○ Защита информации

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

- ○ Безопасность
- ○ Компьютерная безопасность
- ○ Защита информации
- ◉ Защищенность потребителей информации
- ○ Защищенность информации

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

- ○ Информационное вычисление
- ○ Информационное оружие
- ○ Информационная война
- ◉ Информационное превсходство
- ○ Информационная безопасность

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

- ○ Интересы личности в информационной сфере
- ○ Интересы государства
- ○ Интересы общества в информационной сфере
- ◉ Интресы общества
- ○ Интересы государства в информационной сфере

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

- ◯ Конфиденциальность
- ◯ Банковская тайна
- ◯ Коммерческая тайна
- ◉ Государственная тайна
- ◯ Конфиденциальная информация

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

- ◯ Аппелируемость
- ◯ Целостность
- ◯ Конфиденциальность
- ◉ Аутентчность
- ◯ Доступность

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

- ◯ Доступность
- ◯ Точность
- ◯ Надежность
- ◉ Устйчивость
- ◯ Контролируемость

71 Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:

- ◯ Принцип гибкости системы
- ◯ Принцип непрерывной защиты
- ◯ Принцип системности
- ◉ Принцп комплексности
- ◯ Принцип разумной достаточности

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

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

73 Действие субъектов по обеспечению пользователей информационными продуктами:

- ◯ Информационные продукты
- ◯ Информационная система
- ◯ Информационные ресурсы
- ◉ Инфрмационные услуги
- ◯ Информационная сфера

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

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

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

- ● Защищаемая информация
- ○ Защита информации
- ○ Защищенность потребителей информации
- ○ Защищенность информации
- ○ Информационная защита

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

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

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

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

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

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

79 Тактическое планирование – это:

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

80 Эффективная программа безопасности требует сбалансированного применения:

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

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

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

82 К внутренним нарушителям информационной безопасности относится:клиенты;

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

83 Первым этапом разработки системы защиты ИС является

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

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

- 5.0
- 8.0
- 9.0
- 6.0
- 7.0

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

- 2.0
- 0.0
- 9.0
- 6.0
- 1.0

86 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

87 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

88 Что является наилучшим описанием количественного анализа рисков?

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

89 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

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

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

91 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

92 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

93 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

94 Какие степени сложности устройства Вам известны

- встроенные
- сложная
- упрощенные
- простые
- оптические

95 К механическим системам защиты относятся:

- вирус
- защита
- непроволока
- сигнализация
- вы

96 Какие компоненты входят в комплекс защиты охраняемых объектов:

- admin
- Система
- Вирус
- Датчики
- Оружие

97 К выполняемой функции защиты относится:

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

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

- Внутренная защита
- Защищенность информации
- Защита информации
- Компьютерная безопасность
- Безопасность данных

99 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

100 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

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

- доступность
- целостность
- аппелеруемость
- аутентичность
- конфиденциальность

102 Гарантия точного и полного выполнения команд в АС:

- доступность
- точность
- надежность
- контролируемость
- устойчивость

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

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

104 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

105 Особенностями информационного оружия являются:

- доступность
- открытость
- системность
- универсальность

- надежность

106 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

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 вирусам не изменяющим среду обитания относятся:

- доступность
- студенческие
- ревизоро
- спутник
- полиморфные

109 Хранение паролей может осуществляться

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

110 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

111 К достоинствам технических средств защиты относятся:

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

112 К тщательно контролируемым зонам относятся:

- световые
- пользователя
- администратор

- [x] архив
- [ ] электрохимические датчики

113 К системам оповещения относятся:

- [ ] электрофизические датчики
- [ ] электромеханические датчики
- [ ] неэлектрические датчики
- [x] инфракрасные датчики
- [ ] электрохимические датчики

114 К оборонительным системам защиты относятся:

- [ ] электромеханические датчики
- [ ] датчики
- [x] звуковые установки
- [ ] электрофизические датчики
- [ ] электрохимические датчики

115 Охранное освещение бывает:

- [ ] архив
- [ ] заключеной
- [ ] световое
- [x] дежурное
- [ ] открытое

116 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
- [x] Реализация конституционных прав на доступ к информации
- [ ] Политическая экономическая и социальная стабильность

117 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
- [x] Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз
- [ ] Политика национальной безопасности России

118 Наиболее распространенные угрозы информационной безопасности:

- [ ] угрозы вируса
- [ ] угрозы безопасности
- [ ] угрозы защищенности
- [x] угрозы целостности
- [ ] угрозы деятельности

119 Что относится к классу информационных ресурсов:

- [ ] Промышленные образцы, рецептуры и технологии

- Персонал
- Документы
- все правельные ответы
- Организационные единицы

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

- защита
- аутентичность
- доступность
- конфиденциальность
- целостность

121 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

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

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

123 Что не относится к информационной инфекции

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

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

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

125 Идентификатор субъекта доступа, который является его секретом:

- админом
- электронно-цифровая подпись
- ключ

- [x] пароль
- [ ] сертификат ключа подписи

126 Программу нужно обязательно проверить на наличие вирусов…

- [ ] перед вторым запуском
- [ ] после первого запуска
- [ ] перед каждым запуском
- [x] перед первым запуском
- [ ] после каждого запуска

127 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
- [x] не реже раз в неделю
- [ ] при каждой угрозе заражения

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

- [ ] Внутренная защита
- [ ] Защищенность информации
- [ ] Защита информации
- [x] Компьютерная безопасность
- [ ] Безопасность данных

129 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
- [x] Открытый стандарт, определяющий цели контроля
- [ ] Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

130 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
- [x] COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
- [ ] COSO – это система отказоустойчивости

131 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
- [x] NIST и OCTAVE ориентирован на ИТ

- NIST и AS/NZS являются корпоративными

132 Требования к техническому обеспечению системы защиты

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

133 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

134 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

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

- нарушители
- заместители
- перехватчики
- фильтры
- имитаторы

136 «Уполномоченные серверы» фильтруют пакеты на уровне

- прикладным
- канальном
- транспортном
- приложений
- физическом

137 ACL-список ассоциируется с каждым

- типом
- доменом
- типом доступа
- объектом
- процессом

138 Администратор сервера баз данных имеет имя

- system
- sysadm

- admin
- ingres
- root

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

- физическом
- канальном
- транспортном
- сетевом
- сеансовым

140 Брандмауэры первого поколения представляли собой

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

141 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

142 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

143 В СУБД Oracle под ролью понимается

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

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

- совокупность
- целостность
- восстанавливаемость
- доступность
- детермированность

145 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

146 Для создания базы данных пользователь должен получить привилегию от

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

147 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

148 Примером числовой информации может служить:

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

149 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

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

- достоверной
- понятной
- полезной
- актуальной
- полной

151 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

152 Виды уязвимостей

- субъективная
- вероятная
- объективная
- случайная
- постоянная

153 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

154 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

155 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

156 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

157 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

- [x] 1.5
- [ ] 3.5

158 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
- [x] 1.5
- [ ] 3.5

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
- [x] 2,4,5
- [ ] 1,2,3

160 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
- [x] 3,4,5
- [ ] 1,2,3

161 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
- [x] 2.4
- [ ] 1.2

162 Как предотвращение неавторизованного использования ресурсов определена услуга защиты

- [ ] идентификация
- [x] контроль доступа
- [ ] причастность
- [ ] аутентификация
- [ ] целостность

163 Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

- [ ] адрес приложения
- [ ] электронной подписи

- структуры данных
- [x] адресов отправителя и получателя
- содержания сообщений

164 Наиболее надежным механизмом для защиты содержания сообщений является

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

165 Недостатком многоуровневых моделей безопасности является

- недоступность специального режима передачи сообщений
- сложность представления широкого спектра правил обеспечения безопасности
- отсутствие полного аудита
- [x] невозможность учета индивидуальных особенностей субъекта
- отсутствие контроля за потоками информации

166 Обычно в СУБД применяется управление доступом

- древовидное
- административное
- иерархическое
- [x] произвольное
- декларируемое

167 Операционная система Windows 2000 отличает каждого пользователя от других по

- идентификатору защиты
- дескриптору защиты
- маркеру безопасности
- [x] идентификатору безопасности
- маркеру доступа

168 Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

- внутренним
- внешнем
- приложений
- [x] системном
- сетевом

169 По умолчанию пользователь не имеет никаких прав доступа к

- таблицам
- событиям
- базам данных
- [x] таблицам и представлениям
- Представительный

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

- Представительный

- транспортном
- канальном
- сеансовом
- сетевом

171 Полномочия ядра безопасности ОС ассоциируются с

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

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

- аутентификация
- администрированием
- управлением ресурсами
- мониторингом
- аудитом

173 Право на запуск сервера дает привилегия

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

174 Право на удаление баз данных дает привилегия

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

175 Право управлять безопасностью СУБД и отслеживать действия пользователей дает привилегия

- security
- operator
- createdb
- trace
- security operator

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

- администрированием
- идентификация
- аутентификация
- авторизация
- аудит

177 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

178 Применение средств защиты физического уровня ограничивается услугами

- аудит
- целостности
- контроля доступа
- конфиденциальности
- аутентификации

179 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

180 Проверка подлинности пользователя по предъявленному им идентификатору — это

- контроля доступа
- авторизация
- идентификация
- аутентификация
- аудит

181 Регистрацией в системе Windows 2000 управляет

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

182 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

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

- аппелеруемость
- доступность
- конфиденциальность
- [x] целостность
- аутентичность

184 Гарантия точного и полного выполнения команд в АС:

- доступность
- контролируемость
- надежность
- [x] точность
- устойчивость

185 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
- [x] 1, 2, 5, 6
- 5, 2, 3, 4

186 Административные действия в СУБД позволяют выполнять привилегии

- недоступа
- чтения
- тиражирования
- [x] безопасности
- доступа

187 Администратором базы данных является

- пользователь группы
- старший пользователь группы
- администратор сервера баз данных
- [x] любой пользователь, создавший БД
- системный администратор

188 Брандмауэры второго поколения представляли собой

- хосты с фильтрацией пакетов
- хосты пакетов
- «неприступные серверы»
- маршрутизаторы с фильтрацией пакетов
- [x] «уполномоченные серверы»

189 Брандмауэры третьего поколения используют для фильтрации

- общий анализ контрольной информации
- методы электронной подписи
- общий анализ трафика
- [x] специальные многоуровневые методы анализа состояния пакетов
- методы анализа контрольной информации

190 Что лучше всего описывает цель расчета ALE?

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

191 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

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

- аналитических преобразований
- подстановки
- гаммирования
- перестановки
- кодирования

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

- аналитических преобразований
- кодирования
- гаммирования
- подстановки
- перестановки

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

- аналитических преобразований
- кодирования
- подстановки
- гаммирования
- перестановки

195 Конечное множество используемых для кодирования информации знаков называется

- символом
- ключом
- кодом
- алфавитом
- шифром

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

- 1.6
- 2.4
- 1.2
- 3.6
- 4.5

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

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

198 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
- 3.4
- 1.3
- 2.0
- 6.7

199 К видам системы обнаружения атак относятся :

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

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

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

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

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

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

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

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

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

204 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

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

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

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

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

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

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

208 К выполняемой функции защиты относится:

- внутреняя память
- внутренняя защита
- внешняя защита

- [x] вси варианты верны
- [ ] внешняя память

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

- [ ] доступность данных
- [ ] Защищенность информации
- [ ] Защита информации
- [x] Кампьютерная безопасность
- [ ] Безопасность данных

210 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
- [x] информационное оружиее
- [ ] информационная сдача

211 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
- [x] коммерческаяя тайна
- [ ] конфиденциальная информация

212 Гарантия точного и полного выполнения команд в АС:

- [ ] доступность
- [ ] контролируемость
- [ ] надежность
- [x] точнасть
- [ ] устойчивость

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

- [ ] принцип гибкости системы
- [ ] принцип комплексности
- [ ] принцип системности
- [x] принцип разумной достаточности
- [ ] принцип непрерывности

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

- [ ] Безопасность АС
- [ ] атака на автоматизированную систему
- [x] палитика безопасности

- Комплексное обеспечение информационной безопасности
- Угроза информационной безопасности

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

- только 4
- 2,3
- 1,2
- 3,4
- 1,4

216 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

217 К типам угроз безопасности парольных систем относятся

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

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

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

219 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

220 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

221 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

222 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

223 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

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

- ○ пустые письма
- ○ нигерийские письма
- ○ фишинг
- ◉ черный пиар
- ○ источник слухов

225 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

226 Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях

путем подсчета и сравнения с эталоном контрольной суммы:

- сторож
- сканер
- доктор
- (●) детектор
- ревизор

227 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

228 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

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

- ревизор
- доктор
- детектор
- (●) сторож
- сканер

230 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

231 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

232 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

233 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

234 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

235 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

236 Отметьте объекты, которые могут быть заражены компьютерными вирусами

- веб-страницы
- видео
- рисунки
- исплняемые файлы
- драйверы устройств

237 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

238 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

239 Какие вредоносные программы могут заражать документы Word и Excel?

- [x] файлвые вирусы
- [ ] троянские программы
- [ ] макровирусы
- [ ] загрузочные вирусы
- [ ] сетевые черви

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

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

241 Отметьте вредоносные программы, которые распространяются в компьютерных сетях.

- [ ] вирусы-черви
- [ ] файловые вирусы
- [ ] загрузочные вирусы
- [x] троянские прграммы
- [ ] макровирусы

242 Отметьте все правильные утверждения про антивирус-сканер

- [ ] реагирует на события, похожие на действия вирусов
- [ ] может обнаруживать вирусы в файлах
- [ ] может уничтожать известные ему вирусы
- [x] может обнруживать и уничтожать все вирусы
- [ ] может блокировать вирус в момент заражения

243 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
- [x] может обнаруживать и уничтожат все вирусы
- [ ] может блокировать вирус в момент заражения

244 В чем недостатки антивирусов-мониторов?

- [ ] не умеют уничтожать вирусы в файлах
- [ ] замедляют работу компьютера
- [ ] могут привести к серьезному сбою системы
- [x] не умеют унчтожать вирусы
- [ ] не умеют блокировать вирусы, полученные из сети Интернет

245 Какие ошибки допускает пользователь?

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

246 Троянские программы распространяются…

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

247 Назначение троянских программ…

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

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

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

249 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

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

- сторож
- сканер
- доктор
- детектор
- ревизор

251 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

252 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
- ○ детектор
- ○ доктор
- ○ сканер
- ● ревизор

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

- ○ детектор
- ○ сканер
- ○ ревизор
- ● сторож
- ○ доктор

254 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

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

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

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

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

257 Перехват, который осуществляется путем использования оптической техники называется:

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

258 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

259 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

260 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

261 Что такое файрволл?

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

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

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

263 Удачная криптоатака называется

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

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

- изменить, повредить или ее уничтожить
- получить, изменить или уничтожить
- размножить или уничтожить ее

- [x] получить, изменить, а затем передать ее конкурентам
- [ ] изменить и уничтожить ее

265 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
- [x] воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений
- [ ] вариант ответа 1 и 3

266 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
- [x] 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

267 Выделите три наиболее важных метода защиты информации от нелегального доступа

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

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

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

269 Что включают в себя технические мероприятия по защите информации?

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

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

- [ ] на всех вышеперечисленных
- [ ] на тактическом
- [ ] на социально политическом
- [x] на организационно-правовом

- ○ на инженерно-техническом

271 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

272 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

273 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

274 Кто может быть владельцем защищаемой информации?

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

275 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
- ○ 1,3,4
- ◉ 1, 2
- ○ 3.4

276 Активный перехват информации это перехват, который:

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

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

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

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

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

279 Перехват, который осуществляется путем использования оптической техники называется:

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

280 Надежность СЗИ определяется

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

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

- ○ системойбезопасности
- ○ стандартом безопасности
- ○ профилем безопасности
- ● профилем защиты
- ○ системой защиты

282 Обеспечением скрытности информации в информационных массивах занимается

- ○ криптология
- ○ криптология
- ○ криптоанализ
- ● стеганография
- ○ криптография

283 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

284 Протокол POP3 работает на _____ уровне

- Основным
- Транспортном
- Сетевом
- Прикладном
- Физическом

285 Поток сообщений в сети передачи данных определяется:

- Сетевом
- Объемом памяти канала передачи сообщений
- Треком
- Трафиком
- Скоростью передачи данных

286 Протокол SMTP предназначен для…

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

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

- ftp
- POP3
- smpt
- www
- http

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

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

289 Укажите правильно записанный IP-адрес в компьютерной сети

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

290 Домен .ru является _____ доменом.

- организационно-техническая
- Надежным
- Основным
- Зональным
- Первичным

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

- шестерка
- Пяти
- Трех
- Четырех
- Двух

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

- Программа
- Порт
- Канал
- Протокол
- Описание

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

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

294 Для безопасного использования ресурсов в сети Интернет предназначен протокол…

- SMTP
- IRC
- NNTP
- HTTPS
- FTP

295 Сетевым протоколом является...

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

296 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

297 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

298 .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

299 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

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

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

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

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

302 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

303 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

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

- 2.4
- 1.3
- 1.2
- 1.4
- 3.4

305 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

306 Информация, составляющая государственную тайну не может иметь гриф…

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

307 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

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

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

309 Утечка информации – это …

- ○ нет правильного ответа
- ○ процесс уничтожения информации
- ○ процесс раскрытия секретной информации
- ◉ несанкцианированный процесс переноса информации от источника к злоумышленнику
- ○ непреднамеренная утрата носителя информации

310 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

311 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

312 Защита информации обеспечивается применением антивирусных средств

- ○ иногда
- ○ не всегда
- ○ нет
- ◉ да
- ○ всегда

313 Средства защиты объектов файловой системы основаны на…

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

314 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

315 Преднамеренная угроза безопасности информации

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

316 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

317 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

318 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

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

- аппелеруемость
- доступность
- целостность
- конфинденциальность
- аутентичность

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

- доступность
- контролируемость
- точность
- надеженность
- устойчивость

321 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 системности
- принцип непрерывной защиты
- принцип разумной достаточности
- принцип гибгости системы
- принцип комплексности

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 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

324 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

325 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

326 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

327 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

328 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

329 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

330 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

331 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

332 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

333 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

334 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

335 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

336 Отметьте объекты, которые могут быть заражены компьютерными вирусами.

- веб-страницы
- видео
- рисунки
- исплняемые файлы
- драйверы устройств

337 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

338 Как могут распространяться вирусы?

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

339 Какие вредоносные программы могут заражать документы Word и Excel?

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

340 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

341 Отметьте вредоносные программы, которые распространяются в компьютерных сетях.

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

342 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

343 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

344 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

345 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

346 Троянские программы распространяются…

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

347 Назначение троянских программ…

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

348 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

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

- стеганология
- стеганография
- криптография
- криптоанализ
- криптология

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

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

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

- криптоанализ
- статичность
- криптография
- стеганография
- криптология

352 Недостатком модели конечных состояний политики безопасности является

- средняястепень надежности
- статичность
- изменение линий связи

- [x] сложность реализации
- [ ] низкая степень надежности

353 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
- [x] относительно низкая производительность
- [ ] на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

354 Обеспечение целостности информации в условиях случайного воздействия изучается

- [ ] криптография
- [ ] стеганографией
- [ ] криптологией
- [x] теорией помехоустойчивого кодирования
- [ ] криптоанализом

355 Организационные требования к системе защиты

- [ ] физические
- [ ] административные и аппаратурные
- [ ] управленческие и идентификационные
- [x] административные и процедурные
- [ ] аппаратурные и физические

356 Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:

- [ ] Конфиденциальность
- [ ] Доступность
- [ ] Аутентичность
- [x] Аппелируемость
- [ ] Целостность

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

- [ ] Принцип гибкости системы
- [ ] Принцип непрерывной защиты
- [ ] Принцип комплексности
- [x] Принцип системности
- [ ] Принцип разумной достаточности

358 Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:

- [ ] Политика безопасности
- [ ] Угроза безопасности
- [ ] Безопасность АС

- [x] Комплексное обспечение информационной безопасности
- [ ] Атака на автоматизированную систему

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

- [ ] Информационные ресурсы
- [ ] Информационная сфера
- [ ] Информационные услуги
- [x] Информационные прдукты
- [ ] Информационная система

360 К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия…»

- [ ] Иная общедоступная информация
- [ ] Информация, распространение которой наносит вред интересам общества
- [ ] Информация без ограничения права доступа
- [x] Информация с ограниченным дступом
- [ ] Объект интеллектуальной собственности

361 Кто является основным ответственным за определение уровня классификации информации?

- [ ] Проектировщик
- [x] Владелец
- [ ] Руководитель среднего звена
- [ ] Высшее руководство
- [ ] Пользователь

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

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

363 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
- [x] 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

364 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

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

- Администраторы
- Руководство
- Владельцы данных
- Пользователи
- Сотрудники

366 Что такое процедура?

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

367 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
- Актуальные и адекватные политики и процедуры безопасности
- Эффективные защитные меры и методы их внедрения
- Проведение тренингов по безопасности для всех сотрудников

368 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

369 Что такое политики безопасности?

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

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

- Анализ действий
- Результаты ALE
- Анализ рисков

- [x] Анализ затрат / выгоды
- [ ] Выявление уязвимостей и угроз, являющихся причиной риска

371 Что лучше всего описывает цель расчета ALE?

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

372 Тактическое планирование – это:

- [ ] Планирование на год
- [ ] Ежедневное планирование
- [ ] Долгосрочное планирование
- [x] Среднесрочное планирование
- [ ] Планирование на 6 месяцев

373 Что является определением воздействия (exposure) на безопасность?

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

374 Эффективная программа безопасности требует сбалансированного применения:

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

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

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

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

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

377 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

378 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

379 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

380 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

381 Что является наилучшим описанием количественного анализа рисков?

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

382 Почему количественный анализ рисков в чистом виде не достижим?

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

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

- Сотрудники должны одобрить создание группы

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

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

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

385 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

386 Недостатком дискретных моделей политики безопасности является

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

387 Недостатком модели политики безопасности на основе анализа угроз системе является

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

388 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

389 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

- [x] 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

390 Кто является знаковой фигурой в сфере информационной безопасности

- [ ] Шелдон
- [ ] Шеннон
- [ ] Шеннон
- [x] Митник
- [ ] Беббидж

391 В чем состоит задача криптографа?

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

392 Под ИБ понимают

- [ ] защиту информации искуственного характера
- [ ] защиту от несанкционированного доступа
- [ ] защиту от несанкционированного доступа
- [x] защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
- [ ] защиту от санкционированного доступа

393 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
- [x] Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
- [ ] Определение файлов, из которых удалена служебная информация

394 "Маскарад"- это

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

395 Верификация -

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

396 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

397 Утечка информации

- защищенная информация
- несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- ознакомление постороннего лица с содержанием секретной информации
- это присвоение имени субъекту или объекту

398 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)

399 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

400 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

401 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

402 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

403 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

404 Под ИБ понимают

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

405 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

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

- достоверной
- шифруемой
- шифруемой
- защищаемой
- кодируемой

407 Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо

известие - это

- данные
- информация
- код
- пароль
- данные

408 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

409 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

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

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

411 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

412 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

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

- безопасностью
- опасностью
- опасностью
- угрозой
- предостережением

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

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

415 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

416 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

417 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

418 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

419 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

420 К типам угроз безопасности парольных систем относятся

- ◯ ревизоро
- ◯ студенческие
- ◉ спутник
- ◯ доступность
- ◯ полиморфные

421 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

422 «Уполномоченные серверы» были созданы для решения проблемы

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

423 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

424 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

425 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

426 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

427 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

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

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

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

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

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

- аналитических преобразований
- подстановки
- гаммирования
- перестановки
- кодирования

431 Символы шифруемого текста заменяются другими символами, взятыми из одного или

нескольких алфавитов, это метод:

- аналитических преобразований
- кодирования
- гаммирования
- подстановки
- перестановки

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

- аналитических преобразований
- кодирования
- подстановки
- гаммирования
- перестановки

433 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

434 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

435 Естественные угрозы безопасности информации вызваны:

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

436 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

437 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.

438 К посторонним лицам нарушителям информационной безопасности относится:

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

439 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

440 Хранение паролей может осуществляться

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

441 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

442 К достоинствам технических средств защиты относятся:

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

443 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

444 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

445 Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС

- ◉ внешний
- ◯ сетевой
- ◯ приложений
- ◯ системный
- ◯ внутренний

446 Восстановление данных является дополнительной функцией услуги защиты

- ◯ идентификация
- ◯ причастность
- ◯ аутентификация
- ◉ целостность
- ◯ контроль доступа

447 Для реализации технологии RAID создается

- ◯ аппаратные средства
- ◯ интерпретатор
- ◯ специальный процесс
- ◉ псевдодрайвер
- ◯ компилятор

448 Достоинством матричных моделей безопасности является

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

449 Запись определенных событий в журнал безопасности сервера называется

- ◯ контролем
- ◯ трафиком
- ◯ мониторингом

- [x] аудитом
- [ ] учетом

450 Защита исполняемых файлов обеспечивается

- [ ] стандартным запуском
- [ ] специальным режимом запуска
- [ ] криптографией
- [x] обязательным контролем попытки запуска
- [ ] дополнительным хостом

451 Защита от форматирования жесткого диска со стороны пользователей обеспечивается

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

452 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
- [x] 2, 4
- [ ] 1, 2

453 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
- [x] 1, 3, 4, 6
- [ ] 2, 3, 4

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

- [ ] 2.5
- [ ] 2, 3, 5
- [ ] 2, 3, 5
- [x] 1, 2, 5
- [ ] 2, 3

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

- [ ] 3.0
- [ ] 2, 4
- [ ] 2, 4
- [x] 1, 2

- 3, 4

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

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

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

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

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

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

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

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

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

- идентификация
- аутентификация
- аутентификация
- причастность
- контроль доступа

461 Конфигурация из нескольких компьютеров, выполняющих общее приложение, называется

- портом
- суперсервером
- суперсервером
- кластером
- сетью

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

- прикладном
- канальном
- канальном
- сетевом
- транспортном

463 Недостатком матричных моделей безопасности является

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

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

- прикладном
- сеансовом
- сеансовом
- транспортном
- канальном

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

- кластером
- портом
- портом
- сокетом
- терминалом

466 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
- 2; 3; 4; 6
- 2; 3; 4; 6
- 1; 2; 4; 6
- 1; 3; 5; 6

467 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; 2; 3; 6
- 1; 4; 5; 6

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

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

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

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

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

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

471 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

472 Что такое криптология?

- область недоступной информации
- область доступной информации
- область доступной информации
- тайная область связи
- незащищенная информация

473 К тщательно контролируемым зонам относятся:

- световые
- пользователя
- администратор
- архив
- электрохимические датчики

474 К системам оповещения относятся:

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

475 К оборонительным системам защиты относятся:

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

476 Охранное освещение бывает:

- ○ архив
- ○ заключеной
- ○ световое
- ● дежурное
- ○ открытое

477 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

478 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

479 Наиболее распространенные угрозы информационной безопасности:

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

480 Что относится к классу информационных ресурсов:

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

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

- ◯ защита
- ◯ аутентичность
- ◯ доступность
- ◉ конфиденциальность
- ◯ целостность

482 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

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

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

484 Что не относится к информационной инфекции:

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

485 Основные угрозы доступности информации:

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

486 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

487 Методы повышения достоверности входных данных

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

488 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
- [x] несанкционированного управления удаленным компьютером
- вмешательства в личную жизнь

489 Причины возникновения ошибки в данных

- Преднамеренное искажение данных
- Использование недопустимых методов анализа данных
- Ошибки при переносе данных с промежуточного документа в компьютер
- [x] Неверная интерпретация данных
- Неустранимые причины природного характера

490 К формам защиты информации не относится…

- Зональным
- организационно-техническая
- правовая
- [x] аналитическая
- страховая

491 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»
- [x] использование только сертифицированных программ-броузеров при доступе к сети Интернет
- посещение только «надёжных» Интернет-узлов

492 Информация, составляющая государственную тайну не может иметь гриф…

- правовая
- «совершенно секретно»
- «секретно»
- [x] «для служебного пользования»
- «особой важности»

493 Утечка информации – это …

- года первого выпуска программы
- процесс уничтожения информации
- процесс раскрытия секретной информации
- [x] несанкционированный процесс переноса информации от источника к злоумышленнику
- непреднамеренная утрата носителя информации

494 К достоинствам технических средств защиты относятся:

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

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

- только 1
- только 3
- 2,3
- [x] 1,2,3
- только 2

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

- 1,3
- [x] 1,2
- 2.0
- 1,4
- 3,4

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

- 3.0
- [x] 1,2,4
- 3,4
- 1,3,4
- 4.0

498 Охранное освещение бывает:a.дежуррноеb.световоес.тревожжное

- b
- a,b
- b,c
- [x] a,c
- a

499 Конечное множество используемых для кодирования информации знаков называется

- символом
- ключом
- кодом
- [x] алфавитом
- шифром

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

- стеганология
- стеганография
- криптография

- [x] криптоанализ
- [ ] криптология

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

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

502 Надежность СЗИ определяется

- [ ] сильным звеном
- [ ] усредненным показателем
- [ ] количеством отраженных атак
- [x] самым слабым звеном
- [ ] самым сильным звеном

503 Наименее затратный криптоанализ для криптоалгоритма RSA

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

504 Недостатком дискретных моделей политики безопасности является

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

505 Недостатком модели политики безопасности на основе анализа угроз системе является

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

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

- [ ] системой безопасности
- [ ] стандартом безопасности
- [ ] профилем безопасности
- [x] профилем защиты
- [ ] системой защиты

507 Обеспечением скрытности информации в информационных массивах занимается

- [ ] криптология

- криптология
- криптоанализ
- [x] стеганография
- криптография

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

- логина
- пароля
- аудита
- [x] хотя бы одного средства безопасности
- всех средств безопасности

509 Первым этапом разработки системы защиты ИС является

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

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

- 5.0
- 8.0
- 9.0
- [x] 6.0
- 7.0

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

- 2.0
- 0.0
- 9.0
- [x] 6.0
- 1.0

512 Политика информационной безопасности — это

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

513 При избирательной политике безопасности в матрице доступа объекту системы соответствует

- поле
- ячейка
- прямоугольная область
- [x] строка
- столбец

514 Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

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

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

- статичность
- идентифицируемым
- мандатным
- мандатным
- избирательным

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

- B3
- C2
- B2
- C1
- B1

517 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

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

- статичность
- стеганография
- криптоанализ
- криптология
- криптография

519 Недостатком модели конечных состояний политики безопасности является

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

520 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

521 Обеспечение целостности информации в условиях случайного воздействия изучается

- ○ криптография
- ○ стеганографией
- ○ криптологией
- ◉ теорией помехоустойчивого кодирования
- ○ криптоанализом

522 Организационные требования к системе защиты

- ○ физические
- ○ административные и аппаратурные
- ○ управленческие и идентификационные
- ◉ административные и процедурные
- ○ аппаратурные и физические

523 Основу политики безопасности составляет

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

524 По документам ГТК количество классов защищенности АС от НСД

- ○ 5.0
- ○ 8.0
- ○ 6.0
- ◉ 9.0
- ○ 7.0

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

- ○ 5.0
- ○ 7.0
- ○ 9.0
- ◉ 1.0
- ○ 6.0

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

- ○ объект
- ○ наблюдение
- ○ уборка мусора
- ◉ компрометация
- ○ перехват

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

- наблюдение
- субъект системы
- объект системы
- тип разрешенного доступа
- факт доступа

528 При избирательной политике безопасности в матрице доступа субъекту системы соответствует

- поле
- ячейка
- прямоугольная область
- столбец
- строка

529 При качественном подходе риск измеряется в терминах

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

530 При полномочной политике безопасности совокупность меток с одинаковыми значениями образует

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

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

- фильтр
- аудит
- идентификация
- аутентификация
- авторизация

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

- аудит
- заместитель
- перехватчик
- имитатор
- фильтр

533 С помощью закрытого ключа информация

- шифруется
- копируется
- транслируется

- [x] расшифровывается
- [ ] зашифровывается

534 С точки зрения ГТК основной задачей средств безопасности является обеспечение

- [x] защиты от НСД
- [ ] надежности функционирования
- [ ] сохранности информации
- [ ] простоты реализации
- [ ] простоты

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

- [ ] актуальностью
- [ ] доступностью
- [ ] целостностью
- [x] качеством информации
- [ ] актуальностью информации

536 Согласно «Европейским критериям» минимальную адекватность обозначает уровень

- [ ] E2
- [ ] E6
- [ ] E7
- [x] E0
- [ ] E1

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

- [ ] F-IE
- [ ] F-AV
- [ ] F-DI
- [x] F-DX
- [ ] F-IN

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

- [ ] E1
- [ ] E5
- [ ] E4
- [x] E6
- [ ] E7

539 Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев

- [ ] E
- [ ] B
- [ ] A
- [x] C
- [ ] D

540 Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

- A
- B
- A
- D
- C

541 Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

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

542 Соответствие средств безопасности решаемым задачам характеризует

- надежность
- унификация
- адекватность
- эффективность
- корректность

543 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

544 При количественном подходе риск измеряется в терминах

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

545 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

546 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
- [x] перехват
- уборка мусора

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

- мониторингом средств защиты
- максимизация риска
- минимизацией риска
- оптимизацией средств защиты
- [x] управлением риском

548 С помощью открытого ключа информация

- некопируется
- транслируется
- копируется
- [x] зашифровывается
- расшифровывается

549 Система защиты должна гарантировать, что любое движение данных

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

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

- F-A
- F-DI
- F-DX
- [x] F-IN
- F-AV

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

- F-D
- F-AV
- F-IN
- [x] F-DI
- F-DX

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

- E4
- E2
- E3
- [x] E1
- E0

553 Согласно «Оранжевой книге» верифицированную защиту имеет группа критериев

- E
- C
- D
- A
- B

554 Согласно «Оранжевой книге» мандатную защиту имеет группа критериев

- E
- A
- D
- B
- C

555 Согласно «Оранжевой книге» с объектами должны быть ассоциированы

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

556 Содержанием параметра угрозы безопасности информации «конфиденциальность» является

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

557 Стандарт DES основан на базовом классе

- шифры
- перестановки
- замещения
- блочные шифры
- гаммирование

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

- B3
- B1
- C1
- B2
- C2

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

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

- [x] 2, 3, 4
- [ ] 1, 3, 4

560 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
- [ ] Без защитная информация от несанкционированного воздействия
- [ ] защита информации от непреднамеренного воздействия
- [ ] защита информации от несанкционированного доступа
- [x] защита от утечки информации

561 Идентификатор субъекта доступа, который является его секретом:

- [ ] админом
- [ ] электронно-цифровая подпись
- [ ] ключ
- [x] пароль
- [ ] сертификат ключа подписи

562 Троянские программы — это

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

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

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

564 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
- [x] воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений
- [ ] вариант ответа 1 и 3

565 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

- [x] 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

566 Выделите три наиболее важных метода защиты информации от нелегального доступа

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

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

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

568 то включают в себя технические мероприятия по защите информации?

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

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

- [ ] на всех вышеперечисленных
- [ ] на тактическом
- [ ] на социально политическом
- [x] на организационно-правовом
- [ ] на инженерно-техническом

570 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
- [x] регламентацию допуска и разграничение доступа к защищаемой информации
- [ ] вариант ответа 1 и 2

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

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

572 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

573 Кто может быть владельцем защищаемой информации?

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

574 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

575 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

576 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

577 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

578 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

579 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

580 Требования к техническому обеспечению системы защиты

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

581 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

582 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

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

- нарушители
- заместители
- перехватчики
- фильтры
- имитаторы

584 «Уполномоченные серверы» фильтруют пакеты на уровне

- прикладным
- канальном
- транспортном
- приложений

- ○ физическом

585 ACL-список ассоциируется с каждым

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

586 Администратор сервера баз данных имеет имя

- ○ system
- ○ sysadm
- ○ admin
- ● ingres
- ○ root

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

- ○ сеансовым
- ○ транспортном
- ○ сетевом
- ● физическом
- ○ канальном

588 Брандмауэры первого поколения представляли собой

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

589 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

590 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

591 В СУБД Oracle под ролью понимается

- ○ совокупность

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

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

- совокупность
- целостность
- восстанавливаемость
- доступность
- детермированность

593 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

594 Для создания базы данных пользователь должен получить привилегию от

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

595 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

596 Примером числовой информации может служить:

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

597 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

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

- ○ достоверной
- ○ понятной
- ○ полезной
- ◉ актуальной
- ○ полной

599 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

600 Виды уязвимостей

- ○ вероятная
- ○ случайная
- ○ субъективная
- ◉ постоянная
- ○ объективная

601 Особенностями информационного оружия являются:

- ○ доступность
- ○ системность
- ○ открытость
- ◉ универсальность
- ○ надежность

602 Протокол FTP предназначен для...

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

603 При избирательной политике безопасности в матрице доступа объекту системы соответствует

- ○ поле
- ○ ячейка
- ○ прямоугольная область
- ◉ строка
- ○ столбец

604 Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

- ○ столбец
- ○ С полным перекрытием
- ○ На основе анализа угроз

- [x] LWM
- [ ] Лендвера

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

- [ ] статичность
- [ ] идентифицируемым
- [ ] привилегированным
- [x] мандатным
- [ ] избирательным

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

- [ ] B3
- [ ] C2
- [ ] B2
- [x] C1
- [ ] B1

607 Наименее затратный криптоанализ для криптоалгоритма DES

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

608 Основу политики безопасности составляет

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

609 По документам ГТК количество классов защищенности АС от НСД

- [ ] 5.0
- [ ] 8.0
- [ ] 6.0
- [x] 9.0
- [ ] 7.0

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

- [ ] 5.0
- [ ] 7.0
- [ ] 9.0
- [x] 1.0
- [ ] 6.0

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

- объект
- наблюдение
- уборка мусора
- компрометация
- перехват

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

- наблюдение
- субъект системы
- объект системы
- тип разрешенного доступа
- факт доступа

613 При избирательной политике безопасности в матрице доступа субъекту системы соответствует

- поле
- ячейка
- прямоугольная область
- столбец
- строка

614 При качественном подходе риск измеряется в терминах

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

615 При полномочной политике безопасности совокупность меток с одинаковыми значениями образует

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

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

- фильтр
- аудит
- идентификация
- аутентификация
- авторизация

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

- аудит
- заместитель

- перехватчик
- имитатор
- фильтр

618 С помощью закрытого ключа информация

- шифруется
- копируется
- транслируется
- расшифровывается
- зашифровывается

619 С точки зрения ГТК основной задачей средств безопасности является обеспечение

- простоты
- сохранности информации
- простоты реализации
- защиты от НСД
- надежности функционирования

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

- актуальностью информации
- целостностью
- качеством информации
- актуальностью
- доступностью

621 актуальностью

- E2
- E6
- E7
- E0
- E1

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

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

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

- E1
- E5
- E4
- E6
- E7

624 Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев

- E
- B
- A
- C
- D

625 Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

- C
- B
- A
- D
- E

626 Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

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

627 Соответствие средств безопасности решаемым задачам характеризует

- надежность
- унификация
- адекватность
- эффективность
- корректность

628 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

629 Что нельзя публиковать в Интернете?

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

630 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

631 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

632 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

633 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

634 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

635 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

636 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

637 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

638 Логические бомбы относятся к классу …

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

639 Использование брандмауэров относят к … методам антивирусной защиты

- троянов
- практическим
- техническим
- организационным
- теоретическим

640 Типы методов антивирусной защиты

- теоретические
- организационные
- технические
- программные
- практические

641 Стадии жизненного цикла классического трояна

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

642 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

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

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

644 Перехват, который осуществляется путем использования оптической техники называется:

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

645 Файловый вирус ...

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

646 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

647 К антивирусным программам не относятся:

- ○ исполняемые
- ○ ревизоры
- ○ фаги
- ◉ интерпретаторы
- ○ мониторы

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

- ○ скамер
- ○ фишер
- ○ фракер
- ◉ кракер
- ○ хакер

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

- ○ Научный инструментарий
- ○ Организационные единицы
- ○ Персонал
- ◉ Документы
- ○ Промышленные образцы

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

- ○ материальность
- ○ сложность
- ○ проблемная ориентированность
- ◉ накапливаемость
- ○ измеримость

651 Какие компоненты входят в комплекс защиты охраняемых объектов:

- ○ admin
- ○ Система
- ○ Вирус
- ◉ Датчики
- ○ Оружие

652 Какие степени сложности устройства Вам известны

- ○ встроенные
- ○ упрощенные
- ○ сложная
- ◉ простые
- ○ оптические

653 При количественном подходе риск измеряется в терминах

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

654 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

655 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
- ◉ перехват
- ○ компрометация
- ○ наблюдение
- ○ уборка мусора

656 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

657 С помощью открытого ключа информация

- ○ некопируется

- транслируется
- копируется
- зашифровывается
- расшифровывается

658 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

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

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

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

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

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

- E4
- E2
- E3
- E1
- E0

662 Согласно «Оранжевой книге» верифицированную защиту имеет группа критериев

- E
- C
- D
- A
- B

663 Согласно «Оранжевой книге» мандатную защиту имеет группа критериев

- E
- A
- D
- B
- C

664 Согласно «Оранжевой книге» с объектами должны быть ассоциированы

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

665 Содержанием параметра угрозы безопасности информации «конфиденциальность» является

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

666 Стандарт DES основан на базовом классе

- шифры
- перестановки
- замещения
- блочные шифры
- гаммирование

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

- B3
- B1
- C1
- B2
- C2

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

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

669 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

670 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

671 Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие: 1) копирование; 2) чтение; 3) запись; 4) выполнение; 5) удаление

- 4.5
- 2,3,4
- 1,3,5
- 3,4,5
- 1.3

672 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

673 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

674 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

675 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

676 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

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

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

678 Защита от программных закладок обеспечивается

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

679 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

680 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

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

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

682 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

683 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

684 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

685 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

686 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

687 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

688 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

689 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

690 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

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

- 3.4
- 2,3,5
- 2,4,5
- 1,2,3
- 3,4,5

692 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

693 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

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

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

695 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

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

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

697 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

698 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

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

- Червь
- Блокировщики

- Ревизоры
- Полифаги
- Сторожа

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

- Подлинность
- Секретности
- Подлинности
- Ценности
- Режиме доступа к