1. К выполняемой функции защиты относится:

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

2. Какие компоненты входят в комплекс защиты охраняемых объектов:

- √ Датчики
- админ
- Оружие
- Система
- Вирус

3. Политика информационной безопасности — это

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

4. Защита информации это:

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

5. Защита информации от утечки это деятельность по предотвращению:

- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации
- √ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

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

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

7. Что такое политики безопасности?

- Детализированные документы по обработке инцидентов безопасности
- Правила использования программного и аппаратного обеспечения в компании
- √ Широкие, высокоуровневые заявления руководства

- Пошаговые инструкции по выполнению задач безопасности
- Общие руководящие требования по достижению определенного уровня безопасности

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

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

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

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

10. Кто является основным ответственным за определение уровня классификации информации?

- Пользователь
- Проектировщик
√ Владелец
- Руководитель среднего звена
- Высшее руководство

11. К функциям информационной безопасности не относятся:

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

12. К посторонним лицам нарушителям информационной безопасности относится

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

13. К основным непреднамеренным искусственным угрозам АСОИ относится:

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

14. Икусственные угрозы безопасности информации вызваны:

- корыстными устремлениями злоумышленников
- ошибками при действиях персонала
√ деятельностью человека
- ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения

- воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

15. Естественные угрозы безопасности информации вызваны:

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

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

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

17. Что является определением воздействия (exposure) на безопасность?

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

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

- √ Руководство
- Сотрудники
- Администраторы
- Пользователи
- Владельцы данных

19. Что самое главное должно продумать руководство при классификации данных?

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

20. Какие степени сложности устройства Вам известны

- √ простые
- сложная
- оптические
- встроенные
- упрощенные

21. В соответствии с законом АР «Об информации, информатизации и защите информации» (1995) информация - это:

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

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

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

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

- √ Министерство Информатики АР
- • Росинформресурс
- • все выше перечисленные
- • правильного ответа нет
- • Комитет по Использованию Информации при Госдуме

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

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

25. Какие секретные сведения входят в понятие «коммерческая тайна»?

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

26. Какие сведения на территории РФ могут составлять коммерческую тайну?

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

27. Кто может быть владельцем защищаемой информации?

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

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

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

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

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

30. Что включает в себя ранжирование как метод защиты информации?

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

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

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

32. Что включают в себя технические мероприятия по защите информации?

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

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

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

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

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

35. Какие существуют наиболее общие задачи защиты информации на предприятии?

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

36. Что в себя морально-нравственные методы защиты информации?

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

37. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

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

38. Виды уязвимостей

√ постоянная
- вероятная
- объективная
- случайная
- субъективная

39. Показателями безопасности информации являются:

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

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

√ актуальной
- понятной
- полной
- достоверной
- полезной

41. В соответствии с законом АР «Об информации, информатизации и защите информации» (1995) информация - это:

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

42. Примером числовой информации может служить:

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

43. Информация в семантической теории - это:

√ сведения, полностью снимающие или уменьшающие существующую до их получения неопределеность
- неотъемлемое свойство материи
- сигналы, импульсы, коды, наблюдающиеся в технических и биологических системах

- всякие сведения, сообщения, знания
- сведения, обладающие новизной

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

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

45. 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
- не буду загружать, т.к. на моём компьюторе есть все необходимые мне прогаммы
- загружу и установлю, т.к. давно хотел сменить антивирусник
- я уже загрузил ранее такую программу

√ не буду загружать, т.к. эта программа – фальшивый антивирус, она сама станет источником вирусов

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

√ не реже раз в неделю
- при каждом посещении интернета
- при каждой угрозе заражения
- не реже раза в год
- не реже раз в месяц

47. Программу нужно обязательно проверить на наличие вирусов…

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

48. Что такое файрволл?

√ комплекс аппаратных или прграммных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами
- 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
- вирусная программа
- брандмауэр

49. Это вид мошенничества, называется…Вам звонит не знакомый человек и претставляется инспектором ГИБДД. Он сообщает, что кто-то из ваших родственников попал в автопроишествие,
и требует, что бы вы перевели на его номер телефона некоторую сумму, в качестве штрафа.

√ социльная презумпция
- психологическая презумпция
- социальная инженерия
- юридическая презумпция
- психологическая инженерия

50. Цель применения фишинга?

√ замануть вас на поддельный сайт, что бы украсть данные вашего аккаунта (т. е. логин и пароль)

- почистить ваш компьютер от вирусов на бесплатном сайте
- реклама новых сайтов
- переписка от чужого лица с целью вымогательства денежных средств
- заманить вас на поддельный сайт, что бы вы не смогли размещать в Интернете инфор мацию

51. Что такое фишинг?

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

52. Для чего нужен хакеру пароль от вашего почтового ящика?

√ 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.
- чтобы украсть деньги с электронного кошелька, закреплённого за этим ящиком
- вредоносная программа от вашего имени будет рассылать по имеющимся в вашей адресной книге адресам письма с поздравлениями
- чтобы от вашего имени рассылать спам-сообщения на имеющиеся в вашей адресной книге адреса
- чтобы переписываться с другими хакерами

53. Что нельзя публиковать в Интернете?

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

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

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

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

√ Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
- Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
- Руководство должно одобрить создание группы
- Чтобы убедиться, что проводится справедливая оценка

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

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

57. Что такое процедура?

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

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

√ Банковская тйна
• Коммерческая тайна
• Конфиденциальная информация
• Государственная тайна
• Информационная безопасность

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

√ Информационная вйна
• Информационное оружие
• Информационное вычисление
• Информационная безопасность
• Информационное превосходство

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

• Защита информации
• Информационная защита
√ Защищаемая информация
• Защищенность информации
• Защищенность потребителей информации

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

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

62. Действие субъектов по обеспечению пользователей информационными продуктами:

√ Инфрмационные услуги
• Информационная сфера
• Информационная система
• Информационные ресурсы
• Информационные продукты

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

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

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

- Принцип разумной достаточности
- Принцип гибкости системы
- Принцип системности
- √ Принцп комплексности
- Принцип непрерывной защиты

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

- Доступность
- Контролируемость
- Точность
- Надежность
- √ Устйчивость

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

- √ Аутентчность
- Доступность
- Целостность
- Конфиденциальность
- Аппелируемость

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

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

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

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

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

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

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

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

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

- Защита информации

- Государственная безопасность
- √ Национальная безпасность
- Информационная безопасность
- Безопасность

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

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

73. С доступом к информационным ресурсам внутри организации связан уровень ОС

- приложений
- внешний
- √ сетевой
- канальный
- системный

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

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

75. Почему количественный анализ рисков в чистом виде не достижим?

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

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

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

77. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- √ Улучшить контроль за безопасностью этой информации
- Всегда требовать специального разрешения
- Снизить уровень классификации этой информации
- 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

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

- √ 6.0
- 2.0

- 1.0
- 0.0
- 9.0

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

√ 6.0
- 5.0
- 7.0
- 8.0
- 9.0

80. Первым этапом разработки системы защиты ИС является

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

81. К внутренним нарушителям информационной безопасности относится:клиенты;

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

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

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

83. Эффективная программа безопасности требует сбалансированного применения:

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

84. Тактическое планирование – это:

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

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

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

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

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

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

√ не реже раз в неделю
- при каждом посещении интернета
- при каждой угрозе заражения
- не реже раза в год
- не реже раз в месяц

88. Программу нужно обязательно проверить на наличие вирусов…

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

89. Идентификатор субъекта доступа, который является его секретом:

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

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

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

91. Что не относится к информационной инфекции

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

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

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

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

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

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

√ конфиденциальность
- аутентичность
- целостность
- защита
- доступность

95. Что относится к классу информационных ресурсов:

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

96. Наиболее распространенные угрозы информационной безопасности:

√ угрозы целостности
- угрозы безопасности
- угрозы деятельности
- угрозы вируса
- угрозы защищенности

97. Информационная безопасность это:

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

98. К национальным интересам РФ в информационной сфере относятся:

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

99. Охранное освещение бывает:

√ дежурное
- заключеной
- открытое
- архив
- световое

100. К оборонительным системам защиты относятся:

√ звуковые установки
- электрохимические датчики
- электромеханические датчики

- электрофизические датчики
- датчики

101. К системам оповещения относятся:

√ инфракрасные датчики
- электромеханические датчики
- электрохимические датчики
- электрофизические датчики
- неэлектрические датчики

102. К тщательно контролируемым зонам относятся:

√ архив
- пользователя
- электрохимические датчики
- световые
- администратор

103. К достоинствам технических средств защиты относятся:

- Все варианты верны

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

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

√ сканером
- иммунизатором
- доктора и фаги
- полиморфные
- ревизором

105. Хранение паролей может осуществляться

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

106. К вирусам не изменяющим среду обитания относятся:

√ спутник
- студенческие
- полиморфные
- доступность
- ревизоро

107. К типам угроз безопасности парольных систем относятся

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

108. К функциям информационной безопасности не относятся:

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

109. Особенностями информационного оружия являются:

- √ универсальность
- открытость
- надежность
- доступность
- системность

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

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

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

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

112. Гарантия точного и полного выполнения команд в АС:

- √ точность
- доступность
- устойчивость
- контролируемость
- надежность

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

- √ целостность
- доступность
- аутентичность
- аппелеруемость
- конфиденциальность

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

- √ коммерческая тайна
- банковская тайна
- конфиденциальная информация
- информационное превосходство
- государственная тайна

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

√ информационное оружие
• информационное превосходство
• Информационная защита
• Информационная безопасность
• информационная война

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

• Внутренная защита
• Защита информации
• Защищенность информации
• Безопасность данных
√ Компьютерная безопасность

117. К выполняемой функции защиты относится:

√ все варианты верны
• сложная
• внешняя защита
• внутренняя защита
• исходная

118. Какие компоненты входят в комплекс защиты охраняемых объектов:

√ Датчики
• Система
• Оружие
• admin
• Вирус

119. К механическим системам защиты относятся:

√ сигнализация
• защита
• вы
• вирус
• непроволока

120. Какие степени сложности устройства Вам известны

√ простые
• сложная
• оптические
• встроенные
• упрощенные

121. Какие средства защиты информации в ПК наиболее распространены?

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

122. Какие существуют наиболее общие задачи защиты информации на предприятии?

√ снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной

- документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы
- создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия
- все вышеперечисленные
- предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации

123. Метод скрытие — это...

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

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

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

125. Из каких четырех доменов состоит CobiT?

- √ Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
- Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Приобретение и Внедрение, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

126. Что является наилучшим описанием количественного анализа рисков?

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

127. Что из перечисленного не является целью проведения анализа рисков?

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

128. Как рассчитать остаточный риск?

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

129. Брандмауэры третьего поколения используют для фильтрации

- √ специальные многоуровневые методы анализа состояния пакетов
- методы электронной подписи

- методы анализа контрольной информации
- общий анализ контрольной информации
- общий анализ трафика

130. Брандмауэры второго поколения представляли собой

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

131. Администратором базы данных является

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

132. Административные действия в СУБД позволяют выполнять привилегии

√ безопасности
- чтения
- доступа
- недоступа
- тиражирования

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

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

134. Гарантия точного и полного выполнения команд в АС:

√ точность
- контролируемость
- устойчивость
- доступность
- надежность

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

√ целостность
- доступность
- аутентичность
- аппелеруемость
- конфиденциальность

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

√ нельзя устанавливать одновременно на компьютер два антивируса от разных производителей, они будут конфликтовать друг с другом
- можно одновременно устанавливать на компьютер два антивируса от разных производителей, они будут дополнять функции друг друга
- антивирус и брандмауэр не могут быть от разных производителей, потому что они не смогут обмениваться базой вирусов

- антивирус и брандмауэр могут быть от одинаковых производителей, потому что они выполняют одинаковые задачи
- антивирус и брандмауэр могут быть от разных производителей, потому что они выполняют разные задачи

137. Регистрацией в системе Windows 2000 управляет

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

138. Проверка подлинности пользователя по предъявленному им идентификатору — это

- идентификация
- аудит
- контроля доступа
√ аутентификация
- авторизация

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

√ идентификация
- авторизация
- аутентификация
- контроля доступа
- аудит

140. Применение средств защиты физического уровня ограничивается услугами

√ конфиденциальности
- целостности
- аутентификации
- аудит
- контроля доступа

141. При передаче по каналам связи на канальном уровне избыточность вводится для

√ контроля ошибок
- реализации проверки со стороны отправителя
- реализации проверки со стороны получателя
- мониторингом
- контроля канала связи

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

√ авторизация
- идентификация
- аудит
- администрированием
- аутентификация

143. Право управлять безопасностью СУБД и отслеживать действия пользователей дает привилегия

√ security
- createdb
- operator
- security operator
- trace

144. Право на удаление баз данных дает привилегия

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

145. Право на запуск сервера дает привилегия

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

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

- √ мониторингом
- администрированием
- аудитом
- аутентификация
- управлением ресурсами

147. Полномочия ядра безопасности ОС ассоциируются с

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

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

- √ сеансовом
- транспортном
- сетевом
- Представительный
- канальном

149. По умолчанию пользователь не имеет никаких прав доступа к

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

150. Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

- √ системном
- внешнем
- сетевом
- внутренним
- приложений

151. Операционная система Windows 2000 отличает каждого пользователя от других по

- дескриптору защиты

- идентификатору защиты
- √ идентификатору безопасности
- маркеру безопасности
- маркеру доступа

152. Обычно в СУБД применяется управление доступом

- √ произвольное
- административное
- декларируемое
- древовидное
- иерархическое

153. Недостатком многоуровневых моделей безопасности является

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

154. Наиболее надежным механизмом для защиты содержания сообщений является

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

155. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

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

156. Как предотвращение неавторизованного использования ресурсов определена услуга защиты

- √ контроль доступа
- идентификация
- целостность
- аутентификация
- причастность

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

- √ 2.4
- 3.4
- 1.2
- 1.4
- 1.3

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

- √ 3,4,5
- 1,4,5
- 1,2,3

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

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

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

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

√ 1.5
- 2,4,6
- 3.5
- 2,3,5
- 2.6

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

√ 1.5
- 5.6
- 3.5
- 4.6
- 2,4,6

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

√ 2.3
- 1.2
- 1.4
- 1.3
- 3.4

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

√ 1.6
- 4.5
- 2.3
- 3.4
- 2.4

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

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

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

√ 2, 3
- 3, 4

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

166. Виды уязвимостей

√ постоянная
- случайная
- объективная
- вероятная
- субъективная

167. Показателями безопасности информации являются:

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

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

√ актуальной
- понятной
- полной
- достоверной
- полезной

169. В соответствии с законом АР «Об информации, информатизации и защите информации» (1995) информация - это:

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

170. Примером числовой информации может служить:

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

171. Информация в семантической теории - это:

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

172. Для создания базы данных пользователь должен получить привилегию от

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

173. Дескриптор защиты в Windows 2000 содержит список

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

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

- √ доступность
- • целостность
- • детермированность
- • совокупность
- • восстанавливаемость

175. В СУБД Oracle под ролью понимается

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

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

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

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

- √ доминировать
- • быть меньше
- • специально оговариваться
- • быть больше
- • быть равен

178. Брандмауэры первого поколения представляли собой

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

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

- √ физическом
- • транспортном
- • канальном
- • сеансовым
- • сетевом

180. Администратор сервера баз данных имеет имя

- √ ingres
- • sysadm
- • root
- • system
- • admin

181. ACL-список ассоциируется с каждым

- √ объектом
- • доменом
- • процессом
- • типом
- • типом доступа

182. «Уполномоченные серверы» фильтруют пакеты на уровне

- √ приложений
- • канальном
- • физическом
- • прикладным
- • транспортном

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

- √ фильтры
- • заместители
- • имитаторы
- • нарушители
- • перехватчики

184. Цель прогресса внедрения и тестирования средств защиты —

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

185. У всех программных закладок имеется общая черта

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

186. Требования к техническому обеспечению системы защиты

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

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

√ NIST и OCTAVE ориентирован на ИТ
• AS/NZS ориентирован на ИТ
• NIST и AS/NZS являются корпоративными
• AS/NZS не ориентирован на ИТ
• NIST и OCTAVE являются корпоративными

188. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

√ COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
• COSO учитывает корпоративную культуру и разработку политик
• COSO – это система отказоустойчивости
• COSO – это система управления рисками
• COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

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

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

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

√ информационное оружие
• информационное превосходство
• Информационная защита
• Информационная безопасность
• информационная война

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

√ 2,3
• 3,4
• только 3
• только 4
• 1,2,3

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

√ 1,2,,3
• 1,3
• только 3
• только 1
• 2,3

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

√ сканерром
• иммунизатором
• доктора и фаги
• нет правильного ответа
• ревизором

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

- √ 1,,2,4
- 3,4,5
- 1.0
- 2,3
- 2,3,4

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

- √ 1,4
- 3,4
- 2,3
- 3.0
- 2,4

196. К типам угроз безопасности парольных систем относятся

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

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

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

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

- 1,4
- √ 3,4
- 1,2
- 2,3
- только 4

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

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

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

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

201. Гарантия точного и полного выполнения команд в АС:

- √ точнасть
- • контролируемость
- • устойчивость
- • доступность
- • надежность

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

- √ коммерческаяя тайна
- • банковская тайна
- • конфиденциальная информация
- • неконфиденциальная информация
- • государственная тайна

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

- √ информационное оружиее
- • информационное превосходство
- • информационная сдача
- • информационная среда
- • информационная война

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

- √ Кампьютерная безопасность
- • Защищенность информации
- • Безопасность данных
- • доступность данных
- • Защита информации

205. К выполняемой функции защиты относится:

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

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

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

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

- √ 1,2,4
- • 3,4
- • 2,3
- • 4.0
- • 2,3,4

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

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

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

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

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

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

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

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

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

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

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

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

214. К видам системы обнаружения атак относятся :

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

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

√ 2.0

- 1.7
- 6.7
- 3.4
- 1.3

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

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

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

- 4.5
- 1.6
- √ 3.6
- 1.2
- 2.4

218. Конечное множество используемых для кодирования информации знаков называется

- шифром
- символом
- √ алфавитом
- кодом
- ключом

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

- кодирования
- перестановки
- √ гаммирования
- аналитических преобразований
- подстановки

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

- √ подстановки
- аналитических преобразований
- перестановки
- кодирования
- гаммирования

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

- √ перестановки
- гаммирования
- аналитических преобразований
- кодирования
- подстановки

222. Что представляет собой стандарт ISO/IEC 27799?

- √ Стандарт по защите персональных данных о здоровье
- Новая версия ISO 17799
- Новая версия NIST 800-60

- Определения для новой серии ISO 27000
- Новая версия BS 17799

223. Что лучше всего описывает цель расчета ALE?

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

224. Удачная криптоатака называется

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

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

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

226. Что такое файрволл?

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

227. Это вид мошенничества, называется… Вам звонит не знакомый человек и претставляется инспектором ГИБДД. Он сообщает, что кто-то из ваших родственников попал в автопроишествие, и требует, что бы вы перевели на его номер телефона некоторую сумму, в качестве штрафа.

- социальная инженерия
- юридическая презумпция
- √ социльная презумпция
- психологическая инженерия
- психологическая презумпция

228. Цель применения фишинга?

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

229. Что такое фишинг?

- √ создание бесплатных программ, заржённых вирусами и троянами
- 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.
- переписка от чужого лица с целью вымогательства денежных средств

230. Перехват, который осуществляется путем использования оптической техники называется:

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

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

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

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

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

233. Активный перехват информации это перехват, который:

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

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

- √ сторож
- ревизор
- детектор
- доктор
- сканер

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

- √ ревизор
- детектор
- доктор
- сканер
- сторож

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

- √ доктор
- сторож
- ревизор

- сканер
- детектор

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

√ детектор
- сторож
- ревизор
- сканер
- доктор

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

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

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

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

240. Назначение троянских программ…

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

241. Троянские программы распространяются…

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

242. Какие ошибки допускает пользователь?

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

243. В чем недостатки антивирусов-мониторов?

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

244. Отметьте все правильные утверждения про антивирус-монитор

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

245. Отметьте все правильные утверждения про антивирус-сканер

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

246. Отметьте вредоносные программы, которые распространяются в компьютерных сетях.

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

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

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

248. Какие вредоносные программы могут заражать документы Word и Excel?

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

249. Как могут распространяться вирусы?

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

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

√ загрузка с зарженного DVD-диска
- автозапуск зараженного флэш-диска
- посещение зараженного сайта
- скачивание зараженного файла из Интернета
- копирование зараженного файла на диск

251. Отметьте объекты, которые могут быть заражены компьютерными вирусами

- веб-страницы

- рисунки
- видео
- драйверы устройств

√ исплняемые файлы

252. По каким признакам можно предположить, что компьютер заражен вирусом?

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

253. К чему приводит DoS-атака на сайт в Интернете?

√ сервер физически разршается
- сервер не может справиться с большим потоком запросов
- с сервера удаляются страницы сайта
- страницы сайта подменяются на фальшивые
- взламывается программное обеспечение сервера

254. Какое свойство является главной отличительной чертой компьютерного вируса?

√ он способен причинить вред компьютру
- он может распространяться по сети
- он может находиться в файле или загрузочном секторе диска
- он не может распространяться по сети
- он способен распространяться без участия человека

255. Какие средства защиты информации в ПК наиболее распространены?

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

256. Какие существуют наиболее общие задачи защиты информации на предприятии?

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

257. Метод скрытие — это...

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

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

√ сторож

- доктор
- сканер
- ревизор
- детектор

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

- √ ревизор
- доктор
- сканер
- сторож
- детектор

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

- √ доктор
- сканер
- ревизор
- сторож
- детектор

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

- √ детектор
- сканер
- ревизор
- сторож
- доктор

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

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

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

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

264. Из перечисленного в обязанности сотрудников группы информационной безопасности входят: 1) управление доступом пользователей к данным; 2) расследование причин нарушения защиты;
3) исправление ошибок в программном обеспечении; 4) устранение дефектов аппаратной части

- √ 1, 2
- 3.4
- 1.3
- 1,3,4
- 4.0

265. Кто может быть владельцем защищаемой информации?

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

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

• закрываемая собственником информация
• коммерческая тайна
√ любая информация
• только открытая информация
• запатентованная информация

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

√ политическая разведка
• правильного ответа нет
• конфиденциальная информация
• добросовестная конкуренция
• промышленный шпионаж

268. Что включает в себя ранжирование как метод защиты информации?

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

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

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

270. Что включают в себя технические мероприятия по защите информации?

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

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

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

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

√ использование антивирусных программ
• шифрование

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

273. Какие существуют наиболее общие задачи защиты информации на предприятии?

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

274. Что в себя морально-нравственные методы защиты информации?

√ воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений
- вариант ответа 1, 2 и 3
- вариант ответа 1 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

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

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

276. Сетевым протоколом является...

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

277. Для безопасного использования ресурсов в сети Интернет предназначен протокол…

√ HTTPS
- NNTP
- SMTP
- FTP
- IRC

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

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

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

- Канал
- Описание
- Программа

- Порт
√ Протокол

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

√ Четырех
- Двух
- Пяти
- Трех
- шестерка

281. Домен .ru является _____ доменом.

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

282. Укажите правильно записанный IP-адрес в компьютерной сети

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

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

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

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

√ http
- smpt
- www
- ftp
- POP3

285. Протокол SMTP предназначен для…

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

286. Поток сообщений в сети передачи данных определяется:

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

287. Протокол POP3 работает на _____ уровне

√ Прикладном
• Основным
• Физическом
• Транспортном
• Сетевом

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

√ хотя бы одного средства безопасности
• логина
• всех средств безопасности
• пароля
• аудита

289. Обеспечением скрытности информации в информационных массивах занимается

• криптография
• криптология
√ стеганография
• криптоанализ
• криптология

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

• системой защиты
• системойбезопасности
√ профилем защиты
• профилем безопасности
• стандартом безопасности

291. Надежность СЗИ определяется

• усредненным показателем
• самым сильным звеном
√ самым слабым звеном
• сильным звеном
• количеством отраженных атак

292. Перехват, который осуществляется путем использования оптической техники называется:

√ видеоперехват
• просмотр мусора
• аудиоперехват
• пассивный перехват
• активный перехват

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

√ пассивный перехват
• активный перехват
• просмотр мусора
• видеоперехват
• аудиоперехват

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

√ аудиоперехват
• просмотр мусора
• видеоперехват
• пассивный перехват
• активный перехват

295. Активный перехват информации это перехват, который:

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

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

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

297. Назначение троянских программ…

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

298. Троянские программы распространяются…

√ самстоятельно
• с помощью пользователя
• с помощью неисправного ПО
• с помощью хакера
• с помощью компьютерных вирусов

299. Какие ошибки допускает пользователь?

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

300. В чем недостатки антивирусов-мониторов?

√ не умеют унчтожать вирусы
• замедляют работу компьютера
• не умеют блокировать вирусы, полученные из сети Интернет
• не умеют уничтожать вирусы в файлах
• могут привести к серьезному сбою системы

301. Отметьте все правильные утверждения про антивирус-монитор

√ может обнаруживать и уничтожат все вирусы
• может обнаруживать вирусы в файлах при обращении к ним
• может блокировать вирус в момент заражения

- реагирует на события, похожие на действия вирусов
- может обнаруживать вирусы в памяти

302. Отметьте все правильные утверждения про антивирус-сканер.

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

303. Отметьте вредоносные программы, которые распространяются в компьютерных сетях.

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

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

√ запустить антивирус
- отключить питание компьютера
- отключить компьютер от сети
- отформатировать винчестер
- перегрузить компьютер

305. Какие вредоносные программы могут заражать документы Word и Excel?

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

306. Как могут распространяться вирусы?

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

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

√ загрузка с зарженного DVD-диска
- автозапуск зараженного флэш-диска
- посещение зараженного сайта
- скачивание зараженного файла из Интернета
- копирование зараженного файла на диск

308. Отметьте объекты, которые могут быть заражены компьютерными вирусами.

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

309. По каким признакам можно предположить, что компьютер заражен вирусом?

√ появляются новые файлы и удаляются сущствующие
• возникают сбои при работе программ
• изменяется размер файлов
• по электронной почте приходят непонятные сообщения
• уменьшается объем свободной оперативной памяти

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

• сервер не может справиться с большим потоком запросов
• страницы сайта подменяются на фальшивые
√ сервер физически разршается
• взламывается программное обеспечение сервера
• с сервера удаляются страницы сайта

311. Какое свойство является главной отличительной чертой компьютерного вируса?

√ он способен причинить вред компьютру
• он может распространяться по сети
• он может находиться в файле или загрузочном секторе диска
• он не может распространяться по сети
• он способен распространяться без участия человека

312. Какие средства защиты информации в ПК наиболее распространены?

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

313. Какие существуют наиболее общие задачи защиты информации на предприятии?

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

314. Метод скрытие — это...

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

315. В соответствии с законом АР «Об информации, информатизации и защите информации» (1995) информация - это:

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

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

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

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

√ Министерство Информатики АР
- Росинформресурс
- все выше перечисленные
- правильного ответа нет
- Комитет по Использованию Информации при Госдуме

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

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

319. Какие секретные сведения входят в понятие «коммерческая тайна»?

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

320. Какие сведения на территории АР могут составлять коммерческую тайну?

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

321. Как подразделяются вирусы в зависимости от деструктивных возможностей?

√ Безвредные, неопасные, опасные, очень опасные
- Сетевые, файловые, загрузочные, комбинированные
- Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы
- Безвредные, неопасные, загрузочные, комбинированные
- Сетевые, файловые, загрузочные, комбинированные

322. Что такое компьютерный вирус?

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

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

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

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

√ надеженность
- контролируемость
- устойчивость
- доступность
- точность

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

√ конфинденциальность
- доступность
- аутентичность
- аппелеруемость
- целостность

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

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

327. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….

√ Информационная война
- информационное превосходство
- bнформационная запись
- информационная сдача
- информационное оружие

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

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

329. Преднамеренная угроза безопасности информации

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

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

√ пассивная

- оба варианта
- нет правильного ответа
- нейтральная
- активная

331. Средства защиты объектов файловой системы основаны на…

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

332. Защита информации обеспечивается применением антивирусных средств

√ да
- не всегда
- всегда
- иногда
- нет

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

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

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

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

335. Утечка информации – это …

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

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

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

√ Аранжевая книга

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

√ 1,2,,4,7

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

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

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

339. Наиболее эффективное средство для защиты от сетевых атак

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

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

√ 1.4
- 1.3
- 3.4
- 2.4
- 1.2

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

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

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

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

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

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

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

√ МЭ были разрабатаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

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

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

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

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

√ с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование
- не создает информационных угроз для элементов самой системы и внешней среды
- способна противостоять только информационным угрозам, как внешним так и внутренним
- способна противостоять только внешним информационным угрозам
- Ничего не верно
- 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

347. Основные угрозы доступности информации:1.непреднамеренные ошибки пользователей2.злонамеренное изменение данных3.хакерская атака4.отказ программного и аппаратно обеспечения5.разрушение или повреждение помещений6.перехват данных

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

348. К внутренним нарушителям информационной безопасности относится:клиенты

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

349. Почему количественный анализ рисков в чистом виде не достижим?

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

350. Что является наилучшим описанием количественного анализа рисков?

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

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

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

352. Что из перечисленного не является целью проведения анализа рисков?

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

353. Как рассчитать остаточный риск?

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

354. Эффективная программа безопасности требует сбалансированного применения:

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

355. Что является определением воздействия (exposure) на безопасность?

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

356. Тактическое планирование – это:

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

357. Что лучше всего описывает цель расчета ALE?

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

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

- √ Анализ затрат / выгоды

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

359. Что такое политики безопасности?

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

360. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

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

361. Что такое процедура?

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

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

- √ Руководство
- Пользователи
- Администраторы
- Сотрудники
- Владельцы данных

363. Что самое главное должно продумать руководство при классификации данных?

- √ 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
- Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

364. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

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

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

- Пользователи
- √ Сотрудники
- Хакеры

- Атакующие
- Контрагенты (лица, работающие по договору)

366. Кто является основным ответственным за определение уровня классификации информации?

- Проектировщик
- Пользователь
- Высшее руководство
- Руководитель среднего звена

√ Владелец

367. 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…»

√ Информация с ограниченным дступом

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

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

√ Информационные прдукты

- Информационные услуги
- Информационные ресурсы
- Информационная система
- Информационная сфера

369. 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:

- Атака на автоматизированную систему
- Политика безопасности

√ Комплексное обспечение информационной безопасности

- Безопасность АС
- Угроза безопасности

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

√ Принцип системности

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

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

√ Аппелируемость

- Конфиденциальность
- Целостность
- Доступность
- Аутентичность

372. Организационные требования к системе защиты

- аппаратурные и физические

- физические
- √ административные и процедурные
- управленческие и идентификационные
- административные и аппаратурные

373. Обеспечение целостности информации в условиях случайного воздействия изучается

- криптоанализом
- криптография
- √ теорией помехоустойчивого кодирования
- криптологией
- стеганографией

374. Недостаток систем шифрования с открытым ключом

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

375. Недостатком модели конечных состояний политики безопасности является

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

376. Наукой, изучающей математические методы защиты информации путем ее преобразования, является

- √ криптология
- криптоанализ
- статичность
- криптография
- стеганография

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

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

378. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

- √ криптоанализ
- стеганология
- криптология
- стеганография
- криптография

379. «Уполномоченные серверы» были созданы для решения проблемы

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

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

√ попала в оперативную память
• внедрилась в операционную систему
• не попала в оперативную память
• перехватила прерывания
• попала на жесткий диск

381. К типам угроз безопасности парольных систем относятся

• ревизоро
• доступность
√ спутник
• студенческие
• полиморфные

382. Выделите группы, на которые делятся средства защиты информации:

√ физические, аппаратные, программные, криптографические, комбинированные
• криптографические, комбинированные
• химические, аппаратные, программные, этнографические, комбинированные
• химические, аппаратные, программные, криптографические, комбинированные
• химические, аппаратные, программные, криптографические, комбинированные

383. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

√ операционной системы, сетевого программного обеспечения и системы управления базами данных
• системы управления базами данных
• сетевого программного обеспечения и системы управления базами данных
• операционной системы, сетевого программного обеспечения
• операционной системы, сетевого программного обеспечения

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

• пароль
• код
√ информация
• данные
• данные

385. Что такое криптография?

• защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
• защиту информации от компьютерных вирусов
√ метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
• область доступной информации
• область доступной информации

386. Под ИБ понимают

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

387. Угроза - это

√ возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов

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

388. Уровень секретности - это

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

389. Прочность защиты в АС

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

390. Линейное шифрование -

√ криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
- санкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
- несанкционированное изменение информации, корректное по форме, содержанию и 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

391. 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 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 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

392. Утечка информации

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

393. Кодирование информации -

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

394. Верификация -

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

395. "Маскарад"- это

- √ выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями
- 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
- осуществление специально разработанными программами перехвата имени и пароля

396. Что такое аутентификация?

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

397. Под ИБ понимают

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

398. В чем состоит задача криптографа?

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

399. Кто является знаковой фигурой в сфере информационной безопасности

- Шеннон
- Беббидж
- √ Митник
- Шелдон
- Шеннон

400. Что такое целостность информации?

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

401. Недостатком модели политики безопасности на основе анализа угроз системе является

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

402. Недостатком дискретных моделей политики безопасности является

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

403. Наименее затратный криптоанализ для криптоалгоритма RSA

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

404. Защита от форматирования жесткого диска со стороны пользователей обеспечивается

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

405. Защита исполняемых файлов обеспечивается

√ обязательным контролем попытки запуска
• стандартным запуском
• дополнительным хостом
• специальным режимом запуска
• криптографией

406. Запись определенных событий в журнал безопасности сервера называется

√ аудитом
• контролем
• учетом
• трафиком
• мониторингом

407. Достоинством матричных моделей безопасности является

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

408. Для реализации технологии RAID создается

• специальный процесс
• компилятор

- аппаратные средства
- интерпретатор
- √ псевдодрайвер

409. Восстановление данных является дополнительной функцией услуги защиты

- контроль доступа
- идентификация
- √ целостность
- аутентификация
- причастность

410. Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС

- √ внешний
- внутренний
- сетевой
- приложений
- системный

411. В многоуровневой модели, если уровни безопасности субъекта и объекта доступа не сравнимы, то

- √ никакие запросы на выполняются
- ни один запрос не выполняется
- все запросы выполняются
- выполняются запросы минимального уровня безопасности
- доступ специально оговаривается

412. К достоинствам технических средств защиты относятся:

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

413. Хранение паролей может осуществляться

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

414. Для чего нужен хакеру пароль от вашего почтового ящика?

- √ 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
- чтобы украсть деньги с электронного кошелька, закреплённого за этим ящиком
- чтобы переписываться с другими хакерами
- чтобы от вашего имени рассылать спам-сообщения на имеющиеся в вашей адресной книге адреса

415. К посторонним лицам нарушителям информационной безопасности относится:

- √ представители конкурирующих организаций.
- лица, нарушившие пропускной режим
- технический персонал, обслуживающий здание
- пользователи

- сотрудники службы безопасности

416. К основным непреднамеренным искусственным угрозам АСОИ относится:

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

417. Икусственные угрозы безопасности информации вызваны:

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

418. Естественные угрозы безопасности информации вызваны:

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

419. Защита информации это:

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

420. Защита информации от утечки это деятельность по предотвращению:

- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации
- √ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию
доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

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

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

422. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

- √ COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
- COSO – это система управления рисками
- COSO – это система отказоустойчивости

- COSO учитывает корпоративную культуру и разработку политик
- COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

423. Что представляет собой стандарт ISO/IEC 27799?

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

424. Из каких четырех доменов состоит CobiT?

√ Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Приобретение и Внедрение, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Приобретение 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

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

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

426. Утечка информации – это …

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

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

- «совершенно секретно»
√ «для служебного пользования»
- «секретно»
- правовая
- «особой важности»

428. Наиболее эффективное средство для защиты от сетевых атак

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

429. К формам защиты информации не относится…

√ аналитическая
- Зональным
- страховая
- организационно-техническая
- правовая

430. Причины возникновения ошибки в данных

√ Неверная интерпретация данных
• Ошибки при переносе данных с промежуточного документа в компьютер
• Использование недопустимых методов анализа данных
• Неустранимые причины природного характера
• Преднамеренное искажение данных

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

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

432. Методы повышения достоверности входных данных

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

433. Суть компрометации информации

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

434. Основные угрозы доступности информации:

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

435. Что не относится к информационной инфекции:

√ Фальсификация данных
• Черви
• Вирусы
• Логическая бомба
• Троянский конь

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

√ Информационный саботаж
• Информационные инфекции
• Информационные оружия
• Информационное общество
• Физический инфекции

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

√ конфиденциальность

- аутентичность
- целостность
- защита
- доступность

438. Что относится к классу информационных ресурсов:

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

439. Наиболее распространенные угрозы информационной безопасности:

√ угрозы целостности
- угрозы безопасности
- угрозы деятельности
- угрозы вируса
- угрозы защищенности

440. Информационная безопасность это:

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

√ Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз

441. К национальным интересам АР в информационной сфере относятся:

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

442. Охранное освещение бывает:

√ дежурное
- заключеной
- открытое
- архив
- световое

443. К оборонительным системам защиты относятся:

√ звуковые установки
- электрохимические датчики
- электромеханические датчики
- электрофизические датчики
- датчики

444. К системам оповещения относятся:

√ инфракрасные датчики
- электромеханические датчики
- электрохимические датчики
- электрофизические датчики

- неэлектрические датчики

445. К тщательно контролируемым зонам относятся:

- √ архив
- пользователя
- электрохимические датчики
- световые
- администратор

446. Что такое криптология?

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

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

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

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

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

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

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

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

- √ сокетом
- портом
- терминалом
- кластером
- портом

451. Недостатком матричных моделей безопасности является

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

452. Конфигурация из нескольких компьютеров, выполняющих общее приложение, называется

- √ кластером
- • суперсервером
- • сетью
- • портом
- • суперсервером

453. Троянские программы — это

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

454. Идентификатор субъекта доступа, который является его секретом:

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

455. Структурированная защита согласно «Оранжевой книге» используется в системах класса

- • C2
- • B3
- √ B2
- • C1
- • B1

456. Стандарт DES основан на базовом классе

- • гаммирование
- • шифры
- √ блочные шифры
- • замещения
- • перестановки

457. Содержанием параметра угрозы безопасности информации «конфиденциальность» является

- • несанкционированная модификация
- • искажение
- √ несанкционированное получение
- • модификация
- • уничтожение

458. Согласно «Оранжевой книге» с объектами должны быть ассоциированы

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

459. Согласно «Оранжевой книге» мандатную защиту имеет группа критериев

√ B
• D
• E
• C
• A

460. Согласно «Оранжевой книге» верифицированную защиту имеет группа критериев

√ A
• E
• B
• C
• D

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

√ E1
• E4
• E0
• E2
• E3

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

• F-IN
• F-DX
• F-D
• F-AV
√ F-DI

463. Система защиты должна гарантировать, что любое движение данных

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

464. С помощью открытого ключа информация

√ зашифровывается
• некопируется
• расшифровывается
• транслируется
• копируется

465. При количественном подходе риск измеряется в терминах

√ денежных потерь
• заданных с помощью шкалы
• заданных с помощью информации
• объема информации
• заданных с помощью ранжирования

466. Соответствие средств безопасности решаемым задачам характеризует

√ эффективность
• надежность
• корректность
• унификация

- адекватность

467. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

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

468. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

- A
- C
- B
- A
- √ D

469. Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев

- √ C
- B
- D
- E
- A

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

- √ E6
- E5
- E7
- E1
- E4

471. Согласно «Европейским критериям» минимальную адекватность обозначает уровень

- √ E0
- E6
- E1
- E2
- E7

472. С точки зрения ГТК основной задачей средств безопасности является обеспечение

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

473. С помощью закрытого ключа информация

- √ расшифровывается
- копируется
- зашифровывается
- шифруется
- транслируется

474. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует

√ уровень безопасности
• область равного доступа
• уровень доступности
• уровень равной доступности
• область равной критичности

475. При качественном подходе риск измеряется в терминах

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

476. При избирательной политике безопасности в матрице доступа субъекту системы соответствует

√ столбец
• ячейка
• строка
• поле
• прямоугольная область

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

√ тип разрешенного доступа
• субъект системы
• факт доступа
• наблюдение
• объект системы

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

• 9.0
• 6.0
• 5.0
√ 1.0
• 7.0

479. По документам ГТК количество классов защищенности АС от НСД

√ 9.0
• 8.0
• 7.0
• 5.0
• 6.0

480. Основу политики безопасности составляет

√ способ управления доступом
• управление риском
• выбор каналов связи
• управление объектом
• программное обеспечение

481. Организационные требования к системе защиты

√ административные и процедурные
• административные и аппаратурные
• аппаратурные и физические
• физические

- управленческие и идентификационные

482. Обеспечение целостности информации в условиях случайного воздействия изучается

- √ теорией помехоустойчивого кодирования
- стеганографией
- криптоанализом
- криптография
- криптологией

483. Недостаток систем шифрования с открытым ключом

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

484. Недостатком модели конечных состояний политики безопасности является

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

485. Наукой, изучающей математические методы защиты информации путем ее преобразования, является

- √ криптология
- стеганография
- криптография
- статичность
- криптоанализ

486. Наименее затратный криптоанализ для криптоалгоритма DES

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

487. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

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

488. При избирательной политике безопасности в матрице доступа объекту системы соответствует

- поле
- прямоугольная область
- ячейка
- столбец
- √ строка

489. Политика информационной безопасности — это

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

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

√ 6.0
• 0.0
• 1.0
• 2.0
• 9.0

491. По документам ГТК количество классов защищенности СВТ от НСД к информации

√ 6.0
• 8.0
• 7.0
• 5.0
• 9.0

492. Первым этапом разработки системы защиты ИС является

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

493. Обеспечением скрытности информации в информационных массивах занимается

√ стеганография
• криптология
• криптография
• криптология
• криптоанализ

494. Недостатком модели политики безопасности на основе анализа угроз системе является

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

495. Недостатком дискретных моделей политики безопасности является

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

496. Наименее затратный криптоанализ для криптоалгоритма RSA

√ разложение числа на простые множители
• перебор по выборочному ключевому пространству
• разложение числа на сложные множители
• на сложные множители

- перебор по всему ключевому пространству

497. Надежность СЗИ определяется

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

498. Конечное множество используемых для кодирования информации знаков называется

- √ алфавитом
- ключом
- шифром
- символом
- кодом

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

- √ a,c
- a,b
- a
- b
- b,c

500. К достоинствам технических средств защиты относятся:

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