Приложение к основной образовательной программе среднего общего образования МАОУ «Школа№58» КГО, утвержденной приказом директора № 156 -о/д от 27.08.2024г

Рассмотрено
на заседании педагогического совета
протокол № 81 от 26.08.2024 года

Утверждены
приказом директора № 157 -о\д
от 27.08.2024 года

Тестовые задания

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….
    1. **информационная война**
    2. информационное оружие
    3. информационное превосходство
2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
    1. служебная информация
    2. коммерческая тайна
    3. банковская тайна
    4. **конфиденциальная информация**
3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
    1. **конфиденциальность**
    2. целостность
    3. доступность
    4. аутентичность
    5. аппелеруемость
4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
    1. **надежность**
    2. точность
    3. контролируемость
    4. устойчивость
    5. доступность
5. 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.
    1. принцип системности
    2. принцип комплексности
    3. принцип непрерывной защиты
    4. принцип разумной достаточности
    5. **принцип гибкости системы**
6. В классификацию вирусов по способу заражения входят
    1. опасные
    2. файловые
    3. **резидентные**
    4. загрузочные
    5. файлово -загрузочные
    6. **нерезидентные**
7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…
    1. **комплексное обеспечение ИБ**

2.безопасность АС
3.угроза ИБ
4. атака на АС
1. политика безопасности

1. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
    1. компаньон - вирусами
    2. **черви**
    3. паразитические
    4. студенческие
    5. призраки
    6. стелс - вирусы
    7. макровирусы
2. К видам системы обнаружения атак относятся :
    1. системы, обнаружения атаки на ОС
    2. системы, обнаружения атаки на конкретные приложения
    3. системы, обнаружения атаки на удаленных БД
    4. **все варианты верны**
3. Автоматизированная система должна обеспечивать
    1. надежность
    2. **доступность**
    3. **целостность**
    4. контролируемость
4. Основными компонентами парольной системы являются
    1. **интерфейс администратора**
    2. хранимая копия пароля
    3. **база данных учетных записей**
    4. все варианты верны
5. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….
    1. идентификатор пользователя
    2. **пароль пользователя**
    3. учетная запись пользователя
    4. парольная система
6. К принципам информационной безопасности относятся
    1. скрытость
    2. масштабность
    3. **системность**
    4. **законность**
    5. **открытости алгоритмов**
7. К вирусам изменяющим среду обитания относятся:
    1. черви
    2. студенческие
    3. **полиморфные**
    4. спутники
8. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…
    1. **Защита информации**
    2. Компьютерная безопасность
    3. Защищенность информации
    4. Безопасность данных
9. Система физической безопасности включает в себя следующие подсистемы:
    1. **оценка обстановки**
    2. скрытность
    3. **строительные препятствия**

4. **аварийная и пожарная сигнализация**

10. Какие степени сложности устройства Вам известны
    1. упрощенные
    2. **простые**
    3. **сложные**
    4. оптические
    5. встроенные
11. К механическим системам защиты относятся:
    1. **проволока**
    2. **стена**
    3. сигнализация
    4. **вы**
12. Какие компоненты входят в комплекс защиты охраняемых объектов:
    1. **сигнализация**
    2. **охрана**
    3. **датчики**
    4. **телевизионная система**
13. К выполняемой функции защиты относится:
    1. внешняя защита
    2. внутренняя защита
    3. **все варианты верны**
14. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
    1. Защита информации
    2. **Компьютерная безопасность**
    3. Защищенность информации
    4. Безопасность данных
15. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
    1. информационная война
    2. **информационное оружие**
    3. информационное превосходство
16. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:
    1. государственная тайна
    2. **коммерческая тайна**
    3. банковская тайна
    4. конфиденциальная информация
17. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
    1. конфиденциальность
    2. **целостность**
    3. доступность
    4. аутентичность
    5. аппелеруемость
18. Гарантия точного и полного выполнения команд в АС:
    1. надежность
    2. **точность**
    3. контролируемость
    4. устойчивость
    5. доступность
19. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:
    1. принцип системности
    2. принцип комплексности
    3. принцип непрерывности

4. **принцип разумной достаточности**
5. принцип гибкости системы

20. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:
    1. Комплексное обеспечение информационной безопасности
    2. Безопасность АС
    3. Угроза информационной безопасности
    4. атака на автоматизированную систему
    5. **политика безопасности**
21. Особенностями информационного оружия являются:
    1. системность
    2. открытость
    3. **универсальность**
    4. **скрытность**
22. К функциям информационной безопасности относятся:
    1. **совершенствование законодательства РФ в сфере обеспечения информационной безопасности**
    2. **выявление источников внутренних и внешних угроз**
    3. **Страхование информационных ресурсов**
    4. **защита государственных информационных ресурсов**
    5. **подготовка специалистов по обеспечению информационной безопасности**
23. К типам угроз безопасности парольных систем относятся
    1. словарная атака
    2. тотальный перебор
    3. атака на основе психологии
    4. разглашение параметров учетной записи
    5. **все варианты ответа верны**
24. К вирусам не изменяющим среду обитания относятся:
    1. **черви**
    2. студенческие
    3. полиморфные
    4. **спутники**
25. Хранение паролей может осуществляться
    1. **в виде сверток**
    2. **в открытом виде**
    3. в закрытом виде
    4. **в зашифрованном виде**
    5. все варианты ответа верны
26. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:
    1. ревизором
    2. иммунизатором
    3. **сканером**
    4. доктора и фаги
27. Выбрать недостатки имеющиеся у антивирусной программы ревизор:
    1. **неспособность поймать вирус в момент его появления в системе**
    2. **небольшая скорость поиска вирусов**
    3. **невозможность определить вирус в новых файлах (в электронной почте, на дискете)**
28. 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 распространении**
    4. вирусы не изменяющие среду обитания и не способные к распространению в дальнейшем
29. К достоинствам технических средств защиты относятся:
    1. регулярный контроль
    2. **создание комплексных систем защиты**

3. степень сложности устройства
4. Все варианты верны

30. К тщательно контролируемым зонам относятся:
    1. **рабочее место администратора**
    2. **архив**
    3. **рабочее место пользователя**
31. К системам оповещения относятся:
    1. **инфракрасные датчики**
    2. **электрические датчики**
    3. электромеханические датчики
    4. электрохимические датчики
32. К оборонительным системам защиты относятся:
    1. **проволочные ограждения**
    2. **звуковые установки**
    3. датчики
    4. **световые установки**
33. Охранное освещение бывает:
    a. **дежурное**
    b. световое
    c. **тревожное**
34. К национальным интересам РФ в информационной сфере относятся:
    1. **Реализация конституционных прав на доступ к информации**
    2. Защита информации, обеспечивающей личную безопасность
    3. Защита независимости, суверенитета, государственной и территориальной целостности
    4. Политическая экономическая и социальная стабильность
    5. Сохранение и оздоровлении окружающей среды
35. Информационная безопасность это:
    1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
    2. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**
    3. Состояние, когда не угрожает опасность информационным системам
    4. Политика национальной безопасности России
36. Наиболее распространенные угрозы информационной безопасности:
    1. **угрозы целостности**
    2. угрозы защищенности
    3. угрозы безопасности
    4. **угрозы доступности**
    5. **угрозы конфиденциальности**
37. Что относится к классу информационных ресурсов:
    1. **Документы**
    2. **Персонал**
    3. **Организационные единицы**
    4. **Промышленные образцы, рецептуры и технологии**
    5. **Научный инструментарий**
38. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:
    1. **конфиденциальность**
    2. доступность
    3. аутентичность
    4. целостность
39. Устройства осуществляющие воздействие на человека путем передачи информации через внечувственное восприятие:
    1. Средства массовой информации
    2. Психотропные препараты
    3. Психотронные генераторы

4. **Средства специального программно-технического воздействия**

40. Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?
    1. **Информационный саботаж**
    2. **Физический саботаж**
    3. Информационные инфекции
41. Что не относится к информационной инфекции:
    1. Троянский конь
    2. **Фальсификация данных**
    3. Черви
    4. Вирусы
    5. Логическая бомба
42. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:
    1. защита информации от непреднамеренного воздействия
    2. защита информации от несанкционированного воздействия
    3. защита информации от несанкционированного доступа
    4. ***защита от утечки информации**
43. Идентификатор субъекта доступа, который является его секретом:
    1. ***пароль**
    2. ключ
    3. электронно-цифровая подпись
    4. сертификат ключа подписи
44. Исследование возможности расшифрования информации без знания ключей:
    1. криптология
    2. **криптоанализ**
    3. взлом
    4. несанкционированный доступ
45. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:
    1. **Информационная безопасность**
    2. Безопасность
    3. Национальная безопасность
    4. Защита информации
46. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:
    1. Защита информации
    2. Компьютерная безопасность
    3. Защищенность информации
    4. Защищенность потребителей информации
    5. **Безопасность данных**
47. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:
    1. Информационная война
    2. **Информационное оружие**
    3. Информационное превосходство
48. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:
    1. Интересы государства
    2. Интересы государства в информационной сфере
    3. **Интересы личности**
    4. Интересы личности в информационной сфере
    5. Интересы общества в информационной сфере
49. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

1. Служебная информация
2. Коммерческая тайна
3. Банковская тайна
4. **Конфиденциальная информация**

50. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.
    1. Комплексное обеспечение информационной безопасности
    2. Безопасность АС
    3. Угроза информационной безопасности
    4. **Атака на автоматизированную систему**
    5. Политика безопасности
51. Вся накопленная информация об окружающей нас дейст вительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производст венных, управленческих и других задач
    1. **Информационные ресурсы**
    2. Информационная система
    3. Информационная сфера
    4. Информационные услуги
    5. Информационные продукты
52. К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»
    1. **Информация без ограничения права доступа**
    2. Информация с ограниченным доступом
    3. Информация, распространение которой наносит вред интересам общества
    4. Объект интеллектуальной собственности
    5. Иная общедоступная информация
53. Состояние защищенности при котором не угрожает опасность это:

1. Информационная безопасность
2. ***Безопасность**
3. Защита информации
4. Национальная безопасность

54. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
    1. **Защита информации**
    2. Компьютерная безопасность
    3. Защищенность информации
    4. Защищенность потребителей информации
55. Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств:
    1. **Информационная война**
    2. Информационное оружие
    3. Информационное превосходство
56. Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя , суверенитета и территориальной целостности это:
    1. Интересы государства
    2. **Интересы государства в информационной сфере**
    3. Интересы личности
    4. Интересы личности в информационной сфере
    5. Интересы общества в информационной сфере
57. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы

1. Информационные ресурсы
2. **Информационная система**
3. Информационная сфера
4. Информационные услуги
5. Информационные продукты

58. К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право…»
    1. Информация без ограничения права доступа
    2. Информация с ограниченным доступом
    3. Информация, распространение которой наносит вред интересам общества
    4. **Объект интеллектуальной собственности**
    5. Иная общедоступная информация
59. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:
    1. Информационная безопасность
    2. Безопасность
    3. Защита информации
    4. **Национальная безопасность**
60. Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:
    1. Защита информации
    2. Компьютерная безопасность
    3. Защищенность информации
    4. **Защищенность потребителей информации**
61. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
    1. Информационная война
    2. **Информационное оружие**
    3. Информационное превосходство
62. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:
    1. **Государственная тайна**
    2. Коммерческая тайна
    3. Банковская тайна
    4. Конфиденциальная информация
63. Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:
    1. Конфиденциальность
    2. Целостность
    3. **Доступность**
    4. Аутентичность
    5. Аппелируемость
64. Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:
    1. Надежность
    2. Точность
    3. **Контролируемость**
    4. Устойчивость
    5. Доступность
65. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:
    1. Принцип системности
    2. Принцип комплексности
    3. **Принцип непрерывной защиты**
    4. Принцип разумной достаточности

5. Принцип гибкости системы

66. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:
    1. Комплексное обеспечение информационной безопасности
    2. Безопасность АС
    3. **Угрозы информационной безопасности**
    4. Атака на автоматизированную систему
    5. Политика безопасности
67. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а так же системы регулирования возникающих при этом общественных отношений
    1. Информационные ресурсы
    2. Информационная система
    3. **Информационная сфера**
    4. Информационные услуги
    5. Информационные продукты
68. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»
    1. Информация без ограничения права доступа
    2. Информация с ограниченным доступом
    3. **Информация, распространение которой наносит вред интересам общества**
    4. Объект интеллектуальной собственности
    5. Иная общедоступная информация
69. Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:
    1. Информационная безопасность
    2. Безопасность
    3. **Национальная безопасность**
    4. Защита информации
70. Защищенность от негативных информационно-психологических и информационно- технических воздействий:
    1. Защита информации
    2. Компьютерная безопасность
    3. Защищенность информации
    4. **Защищенность потребителей информации**
71. Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:
    1. Информационная война
    2. Информационное оружие
    3. **Информационное превосходство**
72. Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:
    1. Интересы государства
    2. Интересы государства в информационной сфере
    3. Интересы личности в информационной сфере
    4. **Интересы общества**
    5. Интересы общества в информационной сфере
73. Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.
    1. **Государственная тайна**
    2. Коммерческая тайна
    3. Банковская тайна
    4. Конфиденциальная информация
74. Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:

1. Конфиденциальность
2. Целостность
3. Доступность
4. **Аутентичность**
5. Аппелируемость

75. Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:
    1. Надежность
    2. Точность
    3. Контролируемость
    4. **Устойчивость**
    5. Доступность
76. Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:
    1. Принцип системности
    2. **Принцип комплексности**
    3. Принцип непрерывной защиты
    4. Принцип разумной достаточности
    5. Принцип гибкости системы
77. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:
    1. Комплексное обеспечение информационной безопасности
    2. **Безопасность АС**
    3. Угроза информационной безопасности
    4. Атака на автоматизированную систему
    5. Политика безопасности
78. Действие субъектов по обеспечению пользователей информационными продуктами:
    1. Информационные ресурсы
    2. Информационная система
    3. Информационная сфера
    4. **Информационные услуги**
    5. Информационные продукты
79. К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…»
    1. Информация без ограничения права доступа
    2. **Информация с ограниченным доступом**
    3. Информация, распространение которой наносит вред интересам общества
    4. Объект интеллектуальной собственности
    5. Иная общедоступная информация
80. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:
    1. Защищенность информации
    2. **Защищаемая информация**
    3. Защищенность потребителей информации
    4. Защита информации
81. Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:
    1. **Информационная война**
    2. Информационное оружие
    3. Информационное превосходство
82. Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:
    1. Государственная тайна
    2. Коммерческая тайна

3. **Банковская тайна**
4. Конфиденциальная информация

83. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:
    1. Конфиденциальность
    2. Целостность
    3. Доступность
    4. Аутентичность
    5. **Аппелируемость**
84. Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:
    1. **Принцип системности**
    2. Принцип комплексности
    3. Принцип непрерывной защиты
    4. Принцип разумной достаточности
    5. Принцип гибкости системы
85. 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:
    1. **Комплексное обеспечение информационной безопасности**
    2. Безопасность АС
    3. Угроза безопасности
    4. Атака на автоматизированную систему
    5. Политика безопасности
86. Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:
    1. Информационные ресурсы
    2. Информационная система
    3. Информационная сфера
    4. Информационные услуги
    5. **Информационные продукты**
87. 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…»
    1. Информация без ограничения права доступа
    2. **Информация с ограниченным доступом**
    3. Информация, распространение которой наносит вред интересам общества
    4. Объект интеллектуальной собственности
    5. Иная общедоступная информация

88. Соотнесите интересы в области информационной безопасности:
    1. Национальные интересы
    2. Интересы личности
    3. Интересы государства
    4. Интересы общества

1. состоят в реализации конституционных прав и свобод [2], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина
2. обеспечиваются институтами государствен ной власти, осуществляющими свои функции, в том

числе во взаимодей ствии с действующими на основе Конституции РФ и законодательства РФ общественными организациями

3. состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политиче ской, экономической и социальной стабильности, в безусловном обеспе чении законности и поддержании правопорядка, в развитии равноправно го и взаимовыгодного международного сотрудничества.
4. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании обще ственного согласия, в духовном обновлении России.

ОТВЕТ: 1-2; 2-1; 3-3; 4-4.

89. Соотнесите основные методы получения паролей:

1. метод тотального перебора
2. словарная атака
3. получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы
4. проверка паролей, устанавливаемых в системах по умолчанию

1. для перебора используется словарь наиболее вероятных ключей
2. двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей
3. опробываются все ключи последовательно, один за другим
4. пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе

ОТВЕТ: 1-3; 2-1; 3-2; 4-4;

90. Соотнесите принципы информационной безопасности, определенные Гостехкомиссией

1. Принцип системности
2. Принцип комплексности
3. Принцип непрерывности защиты
4. Гибкость системы защиты
5. Разумная достаточность

1. правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможно го ущерба были бы приемлемыми
2. непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС
3. предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов
4. освобождает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
5. предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов

ОТВЕТ: 1-5; 2-3; 3-2; 4-4; 5-1;

91. Соотнесите основные понятия в области информационной безопасности:

1. Атака
2. Уязвимость АС
3. Угроза безопасности АС
4. Защищенная система

1. некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы
2. система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности
3. возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности
4. действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

ОТВЕТ: 1-4; 2-1; 3-3; 4-2;

92. Соотнесите функции, выполняемые техническими средствами защиты:
    1. внешняя защита
    2. опознавание
    3. внутренняя защита
1. защита от воздействия дестабилизирую щих факторов, проявляющихся непосредственно в средствах обра ботки информации
2. защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
3. специфическая группа средств, предназначен ных для опознавания людей по различным индивидуальным харак теристикам

ОТВЕТ: 1-2; 2-3; 3-1

93. Соотнесите степени сложности устройств:
    1. простые устройства
    2. системы
    3. сложные устройства
1. комбинированные агрегаты, состоя щие из некоторого количества простых устройств, способные к осу ществлению сложных процедур защиты;
2. несложные приборы и приспособле ния, выполняющие отдельные процедуры защиты;
3. законченные технические комплексы, способные осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение;

ОТВЕТ: 1-2; 2-3; 3-1;

94. Соотнесите основные виды угроз для АС:
    1. Угроза нарушения конфиденциальности
    2. Угроза отказа служб
    3. Угроза нарушения целостности
1. Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую
2. Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС
3. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней

ОТВЕТ: 1-3; 2-2; 3-1

95. Соотнесите классификацию угроз по ряду признаков:

1. по природе возникновения
2. по непосредственному источнику
3. по степени воздействия на АС
4. по способу доступа к ресурсам АС

1. пассивные и активные
2. направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС
3. естественные или искусственные
4. природная среда, человек, санкционированные программные средства и несанкционированные программные средства

ОТВЕТ: 1-3; 2-4; 3-3;4-1

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 763031077282339647893973116338746051518481910 82

Владелец Ремнева Светлана Алексеевна

Действителен С 10.04.2024 по 10.04.2025