«Методы и средства защиты компьютерной информации»

Вопросы и ответы из теста по Методам и средствам защиты компьютерной информации с сайта oltest.ru.

Общее количество вопросов: *248*

Тест по предмету «Методы и средства защиты компьютерной информации».

---

1. "Троянский конь" является разновидностью модели воздействия программных закладок
• **искажение**

2. "Уполномоченные серверы" были созданы для решения проблемы
• **имитации IP-адресов**

3. "Уполномоченные серверы" фильтруют пакеты на уровне
• **приложений**

4. ACL-список ассоциируется с каждым
• **объектом**

5. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности
• **Белла-ЛаПадула**

6. Административные действия в СУБД позволяют выполнять привилегии
• **безопасности**

7. Администратор сервера баз данных имеет имя
• **ingres**

8. Администратором базы данных является:
• **любой пользователь, создавший БД**

9. Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем.
• **физическом**

10. Брандмауэры второго поколения представляли собой ...
• **"уполномоченные серверы"**

11. Брандмауэры первого поколения представляли собой ...
• **маршрутизаторы с фильтрацией пакетов**

12. Брандмауэры третьего поколения используют для фильтрации
• **специальные многоуровневые методы анализа состояния пакетов**

13. В "Европейских критериях" количество классов безопасности равно:
• **10**

14. В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен:
• **доминировать**

15. В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен:
• **быть равен**

16. В многоуровневой модели, если субъект доступа формирует запрос на чтение, то уровень безопасности субъекта относительно уровня безопасности объекта должен:
• **доминировать**

17. В многоуровневой модели, если уровни безопасности субъекта и объекта доступа не сравнимы, то ...
• **никакие запросы на выполняются**

18. В модели политики безопасности Лендвера многоуровневая информационная структура называется:
• **контейнером**

19. В модели политики безопасности Лендвера одноуровневый блок информации называется:
• **объектом**

20. В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется ...
• **прямой**

21. В модели политики безопасности Лендвера ссылка на сущность, если это последовательность имен сущностей, называется ...
• **косвенной**

22. В СУБД Oracle под ролью понимается:
• **набор привилегий**

23. Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС
• **внешний**

24. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
• **доступность**

25. Восстановление данных является дополнительной функцией услуги защиты
• **целостность**

26. Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это:
• **принцип минимазации привилегий**

27. Гарнтия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это:
• **целостность**

28. Главным параметром криптосистемы является показатель
• **криптостойкости**

29. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство
• **доступность**

30. Два ключа используются в криптосистемах
• **с открытым ключом**

31. Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели
• **искажение**

32. Дескриптор защиты в Windows 2000 содержит список
• **пользователей и групп, имеющих доступ к объекту**

33. Длина исходного ключа в ГОСТ 28147-89 (бит):
• **256**

34. Длина исходного ключа у алгоритма шифрования DES (бит):
• **56**

35. Для реализации технологии RAID создается:
• **псевдодрайвер**

36. Для решения проблемы правильности выбора и надежности функционирования средств защиты в "Европейских критериях" вводится понятие:
• **адекватности средств защиты**

37. Для создания базы данных пользователь должен получить привилегию от:
• **администратора сервера баз данных**

38. Домены безопасности согласно "Оранжевой книге" используются в системах класса
• **B3**

39. Достоинствами аппаратной реализации криптографического закрытия данных являются:
• **высокая производительность и простота**

40. Достоинствами программной реализации криптографического закрытия данных являются:
• **практичность и гибкость**

41. Достоинством дискретных моделей политики безопасности является:
• **простой механизм реализации**

42. Достоинством матричных моделей безопасности является:
• **легкость представления широкого спектра правил обеспечения безопасности**

43. Достоинством модели конечных состояний политики безопасности является:
• **высокая степень надежности**

44. Достоинством модели политики безопасности на основе анализа угроз системе является:
• **числовая вероятностная оценка надежности**

45. Единственный ключ используется в криптосистемах
• **симметричных**

46. Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается:
• **высокой**

47. Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается:
• **средней**

48. Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается:
• **базовой**

49. Задачей анализа модели политики безопасности на основе анализа угроз системе является:
• **минимизация вероятности преодоления системы защиты**

50. Запись определенных событий в журнал безопасности сервера называется:
• **аудитом**

51. Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты
• **встроенных в ОС**

52. Защита исполняемых файлов обеспечивается:
• **обязательным контролем попытки запуска**

53. Защита от программных закладок обеспечивается:
• **аппаратным модулем, устанавливаемым на системную шину ПК**

54. Защита от форматирования жесткого диска со стороны пользователей обеспечивается:
• **аппаратным модулем, устанавливаемым на системную шину ПК**

55. Защита с применением меток безопасности согласно "Оранжевой книге" используется в системах класса
• **B1**

56. Идентификаторы безопасности в Windows 2000 представляют собой ...
• **двоичное число, состоящее из заголовка и длинного случайного компонента**

57. Из перечисленного ACL-список содержит:
• **домены, которым разрешен доступ к объекту**
• **тип доступа**

58. Из перечисленного аутентификация используется на уровнях:
• **прикладном**
• **сетевом**
• **транспортном**

59. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:
• **аутентификация**
• **контроль доступа**
• **причастность**
• **целостность**

60. Из перечисленного в автоматизированных системах используется аутентификация по:
• **паролю**
• **предмету**
• **физиологическим признакам**

61. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:
• **расследование причин нарушения защиты**
• **управление доступом пользователей к данным**

62. Из перечисленного в ОС UNIX регистрационная запись средств аудита включает поля:
• **дата и время события**
• **идентификатор пользователя**
• **результат действия**
• **тип события**

63. Из перечисленного в ОС UNIX существуют администраторы:
• **аудита**
• **печати**
• **системных утилит**
• **службы аутентификации**

64. Из перечисленного в соответствии с видами объектов привилегии доступа подразделяются на:
• **базы данных**
• **процедуры**
• **сервер баз данных**
• **события**

65. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:
• **владельца**
• **всех основных пользователей**
• **членов группы владельца**

66. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:
• **визуальное сканирование**
• **исследование динамических характеристик движения руки**

67. Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:
• **непосредственное сравнение изображений**
• **сравнение характерных деталей в цифровом виде**

68. Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются:
• **голос**
• **личная подпись**
• **отпечатки пальцев**
• **форма кисти**

69. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие:
• **выполнение**
• **запись**
• **чтение**

70. Из перечисленного для СУБД важны такие аспекты информационной безопасности, как:
• **доступность**
• **конфиденциальность**
• **целостность**

71. Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как:
• **изменение**
• **чтение**

72. Из перечисленного защита процедур и программ осуществляется на уровнях:
• **аппаратуры**
• **данных**
• **программного обеспечения**

73. Из перечисленного контроль доступа используется на уровнях:
• **прикладном**
• **сетевом**
• **транспортном**

74. Из перечисленного метка безопасности состоит из таких компонентов, как:
• **категория**
• **области**
• **уровень секретности**

75. Из перечисленного методами защиты потока сообщений являются:
• **использование случайных чисел**
• **нумерация сообщений**
• **отметка времени**

76. Из перечисленного на сетевом уровне рекомендуется применение услуг:
• **аутентификации**
• **контроля доступа**
• **конфиденциальности**
• **целостности**

77. Из перечисленного на транспортном уровне рекомендуется применение услуг:
• **аутентификации**
• **контроля доступа**
• **конфиденциальности**
• **целостности**

78. Из перечисленного объектами для монитора обращений являются:
• **задания**
• **программы**
• **устройства**
• **файлы**

79. Из перечисленного подсистема управления криптографическими ключами структурно состоит из:
• **программно-аппаратных средств**
• **центра распределения ключей**

80. Из перечисленного пользователи СУБД разбиваются на категории:
• **администратор базы данных**
• **администратор сервера баз данных**
• **конечные пользователи**

81. Из перечисленного привилегии в СУБД могут передаваться:
• **группам**
• **ролям**
• **субъектам**

82. Из перечисленного привилегии СУБД подразделяются на категории:
• **безопасности**
• **доступа**

83. Из перечисленного привилегиями безопасности являются:
• **createdb**
• **operator**
• **security; operator**
• **trace**

84. Из перечисленного система брандмауэра может быть:
• **ПК**
• **маршрутизатором**
• **хостом**

85. Из перечисленного система защиты электронной почты должна:
• **быть кросс-платформенной**
• **обеспечивать все услуги безопасности**
• **поддерживать работу с почтовыми клиентами**

86. Из перечисленного составляющими информационной базы для монитора обращений являются:
• **виды доступа**
• **форма допуска**

87. Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни:
• **внешний**
• **приложений**
• **сетевой**
• **системный**

88. Из перечисленного субъектами для монитора обращений являются:
• **порты**
• **программы**
• **терминалы**

89. Из перечисленного типами услуг аутентификации являются:
• **достоверность объектов коммуникации**
• **достоверность происхождения данных**

90. Из перечисленного тиражирование данных происходит в режимах:
• **асинхронном**
• **синхронном**

91. Из перечисленного управление маршрутизацией используется на уровнях:
• **прикладном**
• **сетевом**

92. Из перечисленного услуга защиты целостности доступна на уровнях:
• **прикладном**
• **сетевом**
• **транспортном**

93. Из перечисленного услуга обеспечения доступности реализируется на уровнях:
• **прикладном**
• **сетевом**

94. Из перечисленного формами причастности являются:
• **к посылке сообщения**
• **подтверждение получения сообщения**

95. Из перечисленного функция подтверждения подлинности сообщения использует следующие факты:
• **доставка по адресу**
• **неизменность сообщения при передаче**
• **санкционированный отправитель**

96. Из перечисленного цифровая подпись используется для обеспечения услуг:
• **аутентификации**
• **целостности**

97. Из перечисленного электронная почта состоит из:
• **краткого содержания письма**
• **прикрепленных файлов**
• **тела письма**

98. Из перечисленного ядро безопасности ОС выделяет типы полномочий:
• **подсистем**
• **ядра**

99. Из перечисленного, аспектами адекватности средств защиты являются:
• **корректность**
• **эффективность**

100. Из перечисленного, в модели политики безопасности Лендвера сущностью могут являться:
• **контейнер**
• **объект**

101. Из перечисленного, видами политики безопасности являются:
• **избирательная**
• **полномочная**

102. Из перечисленного, ГОСТ 28147-89 используется в режимах:
• **выработка имитовставки**
• **гаммирование**
• **гаммирование с обратной связью**
• **простая замена**

103. Из перечисленного, группами требований к документированию системы защиты информации являются:
• **обработка угроз**
• **протоколирование**
• **тестирование программ**

104. Из перечисленного, группами требований к системам защиты информации являются:
• **конкретные**
• **общие**
• **организационные**

105. Из перечисленного, модель политики безопасности Адепт-50 рассматривает следующие группы безопасности:
• **задания**
• **пользователи**
• **терминалы**
• **файлы**

106. Из перечисленного, параметрами классификации угроз безопасности информации являются:
• **источники угроз**
• **предпосылки появления**
• **природа происхождения**

107. Из перечисленного, подсистема регистрации и учета системы защиты информации должна обеспечивать:
• **оповещение о попытках нарушения защиты**
• **учет носителей информации**

108. Из перечисленного, подсистема управления доступом системы защиты информации должна обеспечивать:
• **аутентификация**
• **идентификация**
• **управление потоками информации**

109. Из перечисленного, проблемами модели Белла-ЛаПадула являются:
• **завышение уровня секретности**
• **запись вслепую**
• **привилегированные субъекты**
• **удаленная запись**

110. Из перечисленного, процесс анализа рисков при разработке системы защиты ИС включает:
• **анализ потенциальных угроз**
• **оценка возможных потерь**

111. Из перечисленного, различают модели воздействия программных закладок на компьютеры:
• **искажение**
• **наблюдение и компрометация**
• **перехват**
• **уборка мусора**

112. Из перечисленного, с точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются:
• **ограничения**
• **правила**

113. Из перечисленного, согласно "Оранжевой книге" требованиями в области аудита являются:
• **идентификация и аутентификация**
• **регистрация и учет**

114. Из перечисленного, угрозы безопасности по предпосылкам появления классифицируются как:
• **объективная**
• **субъективная**

115. Из перечисленного, угрозы безопасности по природе происхождения классифицируются как:
• **преднамеренная**
• **случайная**

116. Из перечисленных категорий требований безопасности, в "Оранжевой книге" предложены:
• **аудит**
• **корректность**
• **политика безопасности**

117. Из перечисленных классов, признаки присутствия программной закладки в компьютере можно разделить на:
• **качественные и визуальные**
• **обнаруживаемые средствами тестирования и диагностики**

118. Из перечисленных множеств, модель безопасности Хартстона описывается множествами:
• **операции**
• **пользователи**
• **ресурсы**
• **установленные полномочия**

119. Из перечисленных моделей, моделями политики безопасности на основе анализа угроз системе являются:
• **игровая**
• **с полным перекрытием**

120. Из перечисленных моделей, моделями политики безопасности на основе дискретных компонент являются:
• **Адепт-50**
• **Хартстона**

121. Из перечисленных моделей, моделями политики безопасности на основе конечных состояний являются:
• **LWM**
• **Белла-ЛаПадула**
• **Лендвера**

122. Из перечисленных предположений, при разработке модели нарушителя ИС определяются:
• **о категориях лиц**
• **о квалификации**
• **о мотивах**

123. Из перечисленных программных закладок, по методу внедрения в компьютерную систему различают:
• **драйверные**
• **загрузочные**
• **прикладные**
• **программно-аппаратные**

124. Из перечисленных разделов, криптография включает:
• **криптосистемы с открытым ключом**
• **симметричные криптосистемы**
• **системы электронной подписи**
• **управление ключами**

125. Из перечисленных свойств, безопасная система обладает:
• **доступность**
• **конфиденциальность**
• **целостность**

126. Из перечисленных типов, все клавиатурные шпионы делятся на:
• **заместители**
• **имитаторы**
• **фильтры**

127. Из перечисленных требований, при разработке протоколирования в системе защиты учитываются:
• **накопление статистики**
• **необходимость записи всех движений защищаемых данных**

128. Из перечисленных уровней безопасности, в "Европейских критериях" определены:
• **базовый**
• **высокий**
• **средний**

129. Как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных определяется:
• **причастность**

130. Как предотвращение неавторизованного использования ресурсов определена услуга защиты
• **контроль доступа**

131. Класс F-AV согласно "Европейским критериям" характеризуется повышенными требованиями к:
• **обеспечению работоспособности**

132. Класс F-DC согласно "Европейским критериям" характеризуется повышенными требованиями к:
• **конфиденциальности**

133. Количество уровней адекватности, которое определяют "Европейские критерии":
• **7**

134. Конечное множество используемых для кодирования информации знаков называется:
• **алфавитом**

135. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности
• **LWM**

136. Конфигурация из нескольких компьютеров, выполняющих общее приложение, называется:
• **кластером**

137. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки
• **адресов отправителя и получателя**

138. Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем.
• **сетевом**

139. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет:
• **криптоанализ**

140. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
• **мандатным**

141. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты
• **за определенное время**

142. На многопользовательские системы с информацией одного уровня конфиденциальности согласно "Оранжевой книге" рассчитан класс
• **C1**

143. Надежность СЗИ определяется:
• **самым слабым звеном**

144. Наиболее надежным механизмом для защиты содержания сообщений является:
• **криптография**

145. Наименее затратный криптоанализ для криптоалгоритма DES
• **перебор по всему ключевому пространству**

146. Наименее затратный криптоанализ для криптоалгоритма RSA
• **разложение числа на простые множители**

147. Наукой, изучающей математические методы защиты информации путем ее преобразования, является:
• **криптология**

148. Недостатком дискретных моделей политики безопасности является:
• **статичность**

149. Недостатком матричных моделей безопасности является:
• **отсутствие контроля за потоками информации**

150. Недостатком многоуровневых моделей безопасности является:
• **невозможность учета индивидуальных особенностей субъекта**

151. Недостатком модели конечных состояний политики безопасности является:
• **сложность реализации**

152. Недостатком модели политики безопасности на основе анализа угроз системе является:
• **изначальное допущение вскрываемости системы**

153. Недостаток систем шифрования с открытым ключом
• **относительно низкая производительность**

154. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется:
• **профилем защиты**

155. Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем.
• **транспортном**

156. Обеспечение целостности информации в условиях случайного воздействия изучается:
• **теорией помехоустойчивого кодирования**

157. Обеспечением скрытности информации в информационных массивах занимается:
• **стеганография**

158. Обычно в СУБД применяется управление доступом
• **произвольное**

159. Оконечное устройство канала связи, через которое процесс может передавать или получать данные, называется:
• **сокетом**

160. Операционная система Windows 2000 отличает каждого пользователя от других по:
• **идентификатору безопасности**

161. Операционная система Windows NT соответствует уровню Оранжевой книги:
• **C2**

162. Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС
• **системном**

163. Организационные требования к системе защиты
• **административные и процедурные**

164. Основной целью системы брандмауэра является управление доступом
• **к защищаемой сети**

165. Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему
• **хотя бы одного средства безопасности**

166. Основу политики безопасности составляет:
• **способ управления доступом**

167. Первым этапом разработки системы защиты ИС является:
• **анализ потенциально возможных угроз информации**

168. По документам ГТК количество классов защищенности АС от НСД:
• **9**

169. По документам ГТК количество классов защищенности СВТ от НСД к информации:
• **6**

170. По документам ГТК самый высокий класс защищенности СВТ от НСД к информации:
• **1**

171. По документам ГТК самый низкий класс защищенности СВТ от НСД к информации:
• **6**

172. По умолчанию пользователь не имеет никаких прав доступа к:
• **таблицам и представлениям**

173. По умолчанию право на подключение к общей базе данных предоставляется:
• **всем пользователям**

174. Поддержка диалога между удаленными процессами реализуется на _____ уровне модели взаимодействия открытых систем.
• **сеансовом**

175. Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа
• **компрометация**

176. Политика информационной безопасности — это:
• **совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации**

177. Полномочия подсистем ядра безопасности ОС ассоциируются с:
• **пользователями**

178. Полномочия ядра безопасности ОС ассоциируются с:
• **процессами**

179. Полную согласованность баз данных гарантирует режим тиражирования
• **синхронный**

180. Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется:
• **мониторингом**

181. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем
• **прикладном**

182. Право на запуск сервера дает привилегия
• **operator**

183. Право на изменение состояния флагов отладочной трассировки дает привилегия
• **trace**

184. Право на удаление баз данных дает привилегия
• **createdb**

185. Право на управление расположением сервера баз данных дает привилегия
• **maintain locations**

186. Право управлять безопасностью СУБД и отслеживать действия пользователей дает привилегия
• **security**

187. Преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС, называются:
• **программными закладками**

188. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это:
• **авторизация**

189. Преобразование форматов реализуется на уровне модели взаимодействия открытых систем
• **представления данных**

190. При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается:
• **тип разрешенного доступа**

191. При избирательной политике безопасности в матрице доступа объекту системы соответствует:
• **строка**

192. При избирательной политике безопасности в матрице доступа субъекту системы соответствует:
• **столбец**

193. При качественном подходе риск измеряется в терминах
• **заданных с помощью шкалы или ранжирования**

194. При количественном подходе риск измеряется в терминах
• **денежных потерь**

195. При передаче по каналам связи на канальном уровне избыточность вводится для:
• **контроля ошибок**

196. При передаче по каналам связи на физическом уровне избыточность вводится для:
• **реализации проверки со стороны получателя**

197. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:
• **уровень безопасности**

198. Применение средств защиты физического уровня ограничивается услугами
• **конфиденциальности**

199. Применение услуги причастности рекомендуется на _____ уровне модели OSI.
• **прикладном**

200. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это:
• **идентификация**

201. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется:
• **электронной подписью**

202. Проверка подлинности пользователя по предъявленному им идентификатору — это:
• **аутентификация**

203. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это:
• **аутентификация**

204. Программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти в модели воздействия
• **перехват**

205. Программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа
• **имитатор**

206. Процесс имитации хакером дружественного адреса называется:
• **"спуфингом"**

207. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется:
• **управлением риском**

208. Регистрацией в системе Windows 2000 управляет:
• **процедура winlogon**

209. Регистрацией пользователей СУБД занимается администратор
• **сервера баз данных**

210. С доступом к информационным ресурсам внутри организации связан уровень ОС:
• **сетевой**

211. С использованием прикладных ресурсов ИС связан уровень ОС:
• **приложений**

212. С помощью закрытого ключа информация:
• **расшифровывается**

213. С помощью открытого ключа информация:
• **зашифровывается**

214. С точки зрения ГТК основной задачей средств безопасности является обеспечение:
• **защиты от НСД**

215. С управлением доступа к ресурсам ОС связан уровень ОС:
• **системный**

216. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов — это:
• **конфиденциальность**

217. Сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях, является:
• **Kerberos**

218. Система защиты должна гарантировать, что любое движение данных
• **идентифицируется, авторизуется, обнаруживается, документируется**

219. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется:
• **брандмауэром**

220. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:
• **качеством информации**

221. Согласно "Европейским критериям" для систем с высокими потребностями в обеспечении целостности предназначен класс
• **F-IN**

222. Согласно "Европейским критериям" минимальную адекватность обозначает уровень
• **E0**

223. Согласно "Европейским критериям" на распределенные системы обработки информации ориентирован класс
• **F-DI**

224. Согласно "Европейским критериям" предъявляет повышенные требования и к целостности, и к конфиденциальности информации класс
• **F-DX**

225. Согласно "Европейским критериям" только общая архитектура системы анализируется на уровне
• **E1**

226. Согласно "Европейским критериям" формальное описание функций безопасности требуется на уровне
• **E6**

227. Согласно "Оранжевой книге" верифицированную защиту имеет группа критериев
• **A**

228. Согласно "Оранжевой книге" дискреционную защиту имеет группа критериев
• **C**

229. Согласно "Оранжевой книге" мандатную защиту имеет группа критериев
• **B**

230. Согласно "Оранжевой книге" минимальную защиту имеет группа критериев
• **D**

231. Согласно "Оранжевой книге" с объектами должны быть ассоциированы
• **метки безопасности**

232. Согласно "Оранжевой книге" уникальные идентификаторы должны иметь
• **все субъекты**

233. Содержанием параметра угрозы безопасности информации "конфиденциальность" является:
• **несанкционированное получение**

234. Соответствие средств безопасности решаемым задачам характеризует:
• **эффективность**

235. Список объектов, к которым может быть получен доступ, вместе с доменом защиты объекта называется:
• **перечнем возможностей**

236. Средствами проверки подлинности пользователей обеспечивается безопасность информации на уровне ОС
• **сетевом**

237. Стандарт DES основан на базовом классе
• **блочные шифры**

238. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это:
• **базопасность информации**

239. Структурированная защита согласно "Оранжевой книге" используется в системах класса
• **B2**

240. Требования к техническому обеспечению системы защиты
• **аппаратурные и физические**

241. Трояские программы — это:
• **часть программы с известными пользователю функцичми, способная выполнять действия с целью причинения определенного ущерба**

242. У всех программных закладок имеется общая черта
• **обязательно выполняют операцию записи в память**

243. Удачная криптоатака называется:
• **взломом**

244. Улучшает рабочие характеристики системы режим тиражирования данных
• **асинхронный**

245. Формирование пакетов данных реализуется на _____ уровне модели взаимодействия открытых систем.
• **канальном**

246. Цель прогресса внедрения и тестирования средств защиты — ...
• **гарантировать правильностьреализации средств защиты**

247. Чтобы программная закладка могла произвести какие-либо действия, необходимо чтобы она
• **попала в оперативную память**

248. Являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры, клавиатурные шпионы типа
• **фильтры**