

«Защита информации»

Вопросы и ответы из теста по [Защите информации](#) с сайта [oltest.ru](#).

Общее количество вопросов: 247

Тест по предмету «Защита информации».

1. _____ — цель прогресса внедрения и тестирования средств защиты.
 - **Гарантировать правильность реализации средств защиты**
2. _____ — это выделения пользователем и администраторам только тех прав доступа, которые им необходимы.
 - **Принцип минимизации привилегий**
3. _____ — это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные.
 - **Целостность**
4. _____ — это недостаток систем шифрования с открытым ключом.
 - **Относительно низкая производительность**
5. _____ — это политика информационной безопасности.
 - **Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации**
6. _____ — это предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы.
 - **Авторизация**
7. _____ — это присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации.
 - **Идентификация**
8. _____ — это проверка подлинности пользователя по предъявленному им идентификатору.
 - **Аутентификация**
9. _____ — это проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы.
 - **Аутентификация**
10. _____ — это свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов.
 - **Конфиденциальность**
11. _____ — это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования.
 - **Безопасность информации**
12. _____ — это трояские программы.
 - **Часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба**



13. _____ занимается обеспечением скрытности информации в информационных массивах.

- **Стеганография**

14. _____ называется запись определенных событий в журнал безопасности сервера.

- **Аудитом**

15. _____ называется конечное множество используемых для кодирования информации знаков.

- **Алфавитом**

16. _____ называется конфигурация из нескольких компьютеров, выполняющих общее приложение.

- **Кластером**

17. _____ называется метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации.

- **Мандатным**

18. _____ называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий.

- **Профилем защиты**

19. _____ называется оконечное устройство канала связи, через которое процесс может передавать или получать данные.

- **Сокетом**

20. _____ называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля.

- **Мониторингом**

21. _____ называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

- **Электронной подписью**

22. _____ называется процесс имитации хакером дружественного адреса.

- **"Спуфингом"**

23. _____ называется процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска.

- **Управлением риском**

24. _____ называется система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую.

- **Брандмауэром**

25. _____ называется совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением.

- **Качеством информации**

26. _____ называется список объектов, к которым может быть получен доступ, вместе с доменом защиты объекта.

- **Перечнем возможностей**

27. _____ называется удачная криптоатака.

- **Взломом**



28. _____ называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС.
- **Программными закладками**
29. _____ обеспечивается защита исполняемых файлов.
- **Обязательным контролем попытки запуска**
30. _____ обеспечивается защита от программных закладок.
- **Аппаратным модулем, устанавливаемым на системную шину ПК**
31. _____ обеспечивается защита от форматирования жесткого диска со стороны пользователей.
- **Аппаратным модулем, устанавливаемым на системную шину ПК**
32. _____ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.
- **Криптоанализ**
33. _____ определяется как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных.
- **Причастность**
34. _____ режим тиражирования гарантирует полную согласованность баз данных.
- **Синхронный**
35. _____ режим тиражирования данных улучшает рабочие характеристики системы.
- **Асинхронный**
36. _____ создается для реализации технологии RAID.
- **Псевдодрайвер**
37. _____ составляет основу политики безопасности.
- **Способ управления доступом**
38. _____ управляет регистрацией в системе Windows 2000.
- **Процедура winlogon**
39. _____ уровень ОС определяет взаимодействие с глобальными ресурсами других организаций.
- **Внешний**
40. _____ уровень ОС связан с доступом к информационным ресурсам внутри организации.
- **Сетевой**
41. _____ характеризует соответствие средств безопасности решаемым задачам.
- **Эффективность**
42. _____ является администратором базы данных.
- **Любой пользователь, создавший БД**
43. _____ является достоинством дискретных моделей политики безопасности.
- **Простой механизм реализации**
44. _____ является достоинством матричных моделей безопасности.
- **Легкость представления широкого спектра правил обеспечения безопасности**



45. _____ является достоинством модели конечных состояний политики безопасности.
- **Высокая степень надежности**
46. _____ является достоинством модели политики безопасности на основе анализа угроз системе.
- **Числовая вероятностная оценка надежности**
47. _____ является задачей анализа модели политики безопасности на основе анализа угроз системе.
- **Минимизация вероятности преодоления системы защиты**
48. _____ является наиболее надежным механизмом для защиты содержания сообщений.
- **Криптография**
49. _____ является наукой, изучающей математические методы защиты информации путем ее преобразования.
- **Криптология**
50. _____ является недостатком дискретных моделей политики безопасности я.
- **Статичность**
51. _____ является недостатком матричных моделей безопасности.
- **Отсутствие контроля за потоками информации**
52. _____ является недостатком многоуровневых моделей безопасности.
- **Невозможность учета индивидуальных особенностей субъекта**
53. _____ является недостатком модели конечных состояний политики безопасности.
- **Сложность реализации**
54. _____ является недостатком модели политики безопасности на основе анализа угроз системе.
- **Изначальное допущение вскрываемости системы**
55. _____ является первым этапом разработки системы защиты ИС.
- **Анализ потенциально возможных угроз информации**
56. _____ является сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях.
- **Kerberos**
57. _____ является содержанием параметра угрозы безопасности информации "конфиденциальность".
- **Несанкционированное получение**
58. _____ являются достоинствами аппаратной реализации криптографического закрытия данных.
- **Высокая производительность и простота**
59. _____ являются достоинствами программной реализации криптографического закрытия данных.
- **Практичность и гибкость**
60. "Троянский конь" является разновидностью модели воздействия программных закладок
- **искажение**



61. "Уполномоченные серверы" были созданы для решения проблемы

- **имитации IP-адресов**

62. "Уполномоченные серверы" фильтруют пакеты на уровне

- **приложений**

63. ACL-список ассоциируется с каждым

- **объектом**

64. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности

- **Белла-ЛаПадула**

65. Административные действия в СУБД позволяют выполнять привилегии

- **безопасности**

66. Администратор _____ занимается регистрацией пользователей СУБД.

- **сервера баз данных**

67. Администратор сервера баз данных имеет имя

- **ingres**

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

- **физическом**

69. Брандмауэры второго поколения представляли собой ...

- **"уполномоченные серверы"**

70. Брандмауэры первого поколения представляли собой ...

- **маршрутизаторы с фильтрацией пакетов**

71. Брандмауэры третьего поколения используют для фильтрации

- **специальные многоуровневые методы анализа состояния пакетов**

72. В "Европейских критериях" количество классов безопасности равно:

- **10**

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

- **доминировать**

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

- **быть равен**

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

- **доминировать**

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

- **никакие запросы на выполняются**

77. В модели политики безопасности Лендвера многоуровневая информационная структура называется:

- **контейнером**



78. В модели политики безопасности Лендвера одноуровневый блок информации называется:

- **объектом**

79. В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется ...

- **прямой**

80. В модели политики безопасности Лендвера ссылка на сущность, если это последовательность имен сущностей, называется ...

- **косвенной**

81. В СУБД Oracle под ролью понимается:

- **набор привилегий**

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

- **доступность**

83. Восстановление данных является дополнительной функцией услуги защиты

- **целостность**

84. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство

- **доступность**

85. Два ключа используются в криптосистемах

- **с открытым ключом**

86. Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели

- **искажение**

87. Дескриптор защиты в Windows 2000 содержит список

- **пользователей и групп, имеющих доступ к объекту**

88. Длина исходного ключа в ГОСТ 28147-89 (бит):

- **256**

89. Длина исходного ключа у алгоритма шифрования DES (бит):

- **56**

90. Для решения проблемы правильности выбора и надежности функционирования средств защиты в "Европейских критериях" вводится понятие:

- **адекватности средств защиты**

91. Для создания базы данных пользователь должен получить привилегию от:

- **администратора сервера баз данных**

92. Домены безопасности согласно "Оранжевой книге" используются в системах класса

- **B3**

93. Единственный ключ используется в криптосистемах

- **симметричных**

94. Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается:

- **высокой**



95. Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается:

- **средней**

96. Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается:

- **базовой**

97. Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты

- **встроенных в ОС**

98. Защита с применением меток безопасности согласно "Оранжевой книге" используется в системах класса

- **B1**

99. Идентификаторы безопасности в Windows 2000 представляют собой ...

- **двоичное число, состоящее из заголовка и длинного случайного компонента**

100. Из перечисленного ACL-список содержит:

- **домены, которым разрешен доступ к объекту**
- **тип доступа**

101. Из перечисленного аутентификация используется на уровнях:

- **прикладном**
- **сетевом**
- **транспортном**

102. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:

- **аутентификация**
- **контроль доступа**
- **причастность**
- **целостность**

103. Из перечисленного в автоматизированных системах используется аутентификация по:

- **паролю**
- **предмету**
- **физиологическим признакам**

104. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:

- **расследование причин нарушения защиты**
- **управление доступом пользователей к данным**

105. Из перечисленного в ОС UNIX регистрационная запись средств аудита включает поля:

- **дата и время события**
- **идентификатор пользователя**
- **результат действия**
- **тип события**

106. Из перечисленного в ОС UNIX существуют администраторы:

- **аудита**
- **печати**
- **системных утилит**
- **службы аутентификации**



107. Из перечисленного в соответствии с видами объектов привилегии доступа подразделяются на:
- **базы данных**
 - **процедуры**
 - **сервер баз данных**
 - **события**
108. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:
- **владельца**
 - **всех основных пользователей**
 - **членов группы владельца**
109. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:
- **визуальное сканирование**
 - **исследование динамических характеристик движения руки**
110. Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:
- **непосредственное сравнение изображений**
 - **сравнение характерных деталей в цифровом виде**
111. Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются:
- **голос**
 - **личная подпись**
 - **отпечатки пальцев**
 - **форма кисти**
112. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие:
- **выполнение**
 - **запись**
 - **чтение**
113. Из перечисленного для СУБД важны такие аспекты информационной безопасности, как:
- **доступность**
 - **конфиденциальность**
 - **целостность**
114. Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как:
- **изменение**
 - **чтение**
115. Из перечисленного защита процедур и программ осуществляется на уровнях:
- **аппаратуры**
 - **данных**
 - **программного обеспечения**
116. Из перечисленного контроль доступа используется на уровнях:
- **прикладном**
 - **сетевом**
 - **транспортном**
117. Из перечисленного метка безопасности состоит из таких компонентов, как:
- **категория**
 - **области**
 - **уровень секретности**



118. Из перечисленного методами защиты потока сообщений являются:

- **использование случайных чисел**
- **нумерация сообщений**
- **отметка времени**

119. Из перечисленного на сетевом уровне рекомендуется применение услуг:

- **аутентификации**
- **контроля доступа**
- **конфиденциальности**
- **целостности**

120. Из перечисленного на транспортном уровне рекомендуется применение услуг:

- **аутентификации**
- **контроля доступа**
- **конфиденциальности**
- **целостности**

121. Из перечисленного объектами для монитора обращений являются:

- **задания**
- **программы**
- **устройства**
- **файлы**

122. Из перечисленного подсистема управления криптографическими ключами структурно состоит из:

- **программно-аппаратных средств**
- **центра распределения ключей**

123. Из перечисленного пользователи СУБД разбиваются на категории:

- **администратор базы данных**
- **администратор сервера баз данных**
- **конечные пользователи**

124. Из перечисленного привилегии в СУБД могут передаваться:

- **группам**
- **ролям**
- **субъектам**

125. Из перечисленного привилегии СУБД подразделяются на категории:

- **безопасности**
- **доступа**

126. Из перечисленного привилегиями безопасности являются:

- **createdb**
- **operator**
- **security; operator**
- **trace**

127. Из перечисленного система брандмауэра может быть:

- **ПК**
- **маршрутизатором**
- **хостом**

128. Из перечисленного система защиты электронной почты должна:

- **быть кросс-платформенной**
- **обеспечивать все услуги безопасности**
- **поддерживать работу с почтовыми клиентами**



129. Из перечисленного составляющими информационной базы для монитора обращений являются:

- **виды доступа**
- **форма допуска**

130. Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни:

- **внешний**
- **приложений**
- **сетевой**
- **системный**

131. Из перечисленного субъектами для монитора обращений являются:

- **порты**
- **программы**
- **терминалы**

132. Из перечисленного типами услуг аутентификации являются:

- **достоверность объектов коммуникации**
- **достоверность происхождения данных**

133. Из перечисленного тиражирование данных происходит в режимах:

- **асинхронном**
- **синхронном**

134. Из перечисленного управление маршрутизацией используется на уровнях:

- **прикладном**
- **сетевом**

135. Из перечисленного услуга защиты целостности доступна на уровнях:

- **прикладном**
- **сетевом**
- **транспортном**

136. Из перечисленного услуга обеспечения доступности реализуется на уровнях:

- **прикладном**
- **сетевом**

137. Из перечисленного формами причастности являются:

- **к посылке сообщения**
- **подтверждение получения сообщения**

138. Из перечисленного функция подтверждения подлинности сообщения использует следующие факты:

- **доставка по адресу**
- **неизменность сообщения при передаче**
- **санкционированный отправитель**

139. Из перечисленного цифровая подпись используется для обеспечения услуг:

- **аутентификации**
- **целостности**

140. Из перечисленного электронная почта состоит из:

- **краткого содержания письма**
- **прикрепленных файлов**
- **тела письма**

141. Из перечисленного ядро безопасности ОС выделяет типы полномочий:

- **подсистем**
- **ядра**



142. Из перечисленного, аспектами адекватности средств защиты являются:

- **корректность**
- **эффективность**

143. Из перечисленного, в модели политики безопасности Лендвера сущностью могут являться:

- **контейнер**
- **объект**

144. Из перечисленного, видами политики безопасности являются:

- **избирательная**
- **полномочная**

145. Из перечисленного, ГОСТ 28147-89 используется в режимах:

- **выработка имитовставки**
- **гаммирование**
- **гаммирование с обратной связью**
- **простая замена**

146. Из перечисленного, группами требований к документированию системы защиты информации являются:

- **обработка угроз**
- **протоколирование**
- **тестирование программ**

147. Из перечисленного, группами требований к системам защиты информации являются:

- **конкретные**
- **общие**
- **организационные**

148. Из перечисленного, модель политики безопасности Адепт-50 рассматривает следующие группы безопасности:

- **задания**
- **пользователи**
- **терминалы**
- **файлы**

149. Из перечисленного, параметрами классификации угроз безопасности информации являются:

- **источники угроз**
- **предпосылки появления**
- **природа происхождения**

150. Из перечисленного, подсистема регистрации и учета системы защиты информации должна обеспечивать:

- **оповещение о попытках нарушения защиты**
- **учет носителей информации**

151. Из перечисленного, подсистема управления доступом системы защиты информации должна обеспечивать:

- **аутентификация**
- **идентификация**
- **управление потоками информации**

152. Из перечисленного, проблемами модели Белла-ЛаПадула являются:

- **завышение уровня секретности**
- **запись вслепую**
- **привилегированные субъекты**
- **удаленная запись**



153. Из перечисленного, процесс анализа рисков при разработке системы защиты ИС включает:

- **анализ потенциальных угроз**
- **оценка возможных потерь**

154. Из перечисленного, различают модели воздействия программных закладок на компьютеры:

- **искажение**
- **наблюдение и компрометация**
- **перехват**
- **уборка мусора**

155. Из перечисленного, с точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются:

- **ограничения**
- **правила**

156. Из перечисленного, согласно "Оранжевой книге" требованиями в области аудита являются:

- **идентификация и аутентификация**
- **регистрация и учет**

157. Из перечисленного, угрозы безопасности по предпосылкам появления классифицируются как:

- **объективная**
- **субъективная**

158. Из перечисленного, угрозы безопасности по природе происхождения классифицируются как:

- **преднамеренная**
- **случайная**

159. Из перечисленных категорий требований безопасности, в "Оранжевой книге" предложены:

- **аудит**
- **корректность**
- **политика безопасности**

160. Из перечисленных классов, признаки присутствия программной закладки в компьютере можно разделить на:

- **качественные и визуальные**
- **обнаруживаемые средствами тестирования и диагностики**

161. Из перечисленных множеств, модель безопасности Хартстона описывается множествами:

- **операции**
- **пользователи**
- **ресурсы**
- **установленные полномочия**

162. Из перечисленных моделей, моделями политики безопасности на основе анализа угроз системе являются:

- **игровая**
- **с полным перекрытием**

163. Из перечисленных моделей, моделями политики безопасности на основе дискретных компонент являются:

- **Адепт-50**
- **Хартстона**

164. Из перечисленных моделей, моделями политики безопасности на основе конечных состояний являются:

- **LWM**
- **Белла-ЛаПадула**
- **Лендвера**



165. Из перечисленных предположений, при разработке модели нарушителя ИС определяются:

- **о категориях лиц**
- **о квалификации**
- **о мотивах**

166. Из перечисленных программных закладок, по методу внедрения в компьютерную систему различают:

- **драйверные**
- **загрузочные**
- **прикладные**
- **программно-аппаратные**

167. Из перечисленных разделов, криптография включает:

- **криптосистемы с открытым ключом**
- **симметричные криптосистемы**
- **системы электронной подписи**
- **управление ключами**

168. Из перечисленных свойств, безопасная система обладает:

- **доступность**
- **конфиденциальность**
- **целостность**

169. Из перечисленных типов, все клавиатурные шпионы делятся на:

- **заместители**
- **имитаторы**
- **фильтры**

170. Из перечисленных требований, при разработке протоколирования в системе защиты учитываются:

- **накопление статистики**
- **необходимость записи всех движений защищаемых данных**

171. Из перечисленных уровней безопасности, в "Европейских критериях" определены:

- **базовый**
- **высокий**
- **средний**

172. Как предотвращение неавторизованного использования ресурсов определена услуга защиты

- **контроль доступа**

173. Класс F-AV согласно "Европейским критериям" характеризуется повышенными требованиями к:

- **обеспечению работоспособности**

174. Класс F-DC согласно "Европейским критериям" характеризуется повышенными требованиями к:

- **конфиденциальности**

175. Количество уровней адекватности, которое определяют "Европейские критерии":

- **7**

176. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

- **LWM**

177. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

- **адресов отправителя и получателя**



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

- **сетевом**

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

- **за определенное время**

180. На _____ уровне ОС происходит определение допустимых для пользователя ресурсов ОС.

- **системном**

181. На многопользовательские системы с информацией одного уровня конфиденциальности согласно "Оранжевой книге" рассчитан класс

- **C1**

182. Надежность СЗИ определяется:

- **самым слабым звеном**

183. Наименее затратный криптоанализ для криптоалгоритма DES

- **перебор по всему ключевому пространству**

184. Наименее затратный криптоанализ для криптоалгоритма RSA

- **разложение числа на простые множители**

185. Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем.

- **транспортном**

186. Обеспечение целостности информации в условиях случайного воздействия изучается:

- **теорией помехоустойчивого кодирования**

187. Обычно в СУБД применяется управление доступом

- **произвольное**

188. Операционная система Windows 2000 отличает каждого пользователя от других по:

- **идентификатору безопасности**

189. Операционная система Windows NT соответствует уровню Оранжевой книги:

- **C2**

190. Организационные требования к системе защиты

- **административные и процедурные**

191. Основной целью системы брандмауэра является управление доступом

- **к защищаемой сети**

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

- **хотя бы одного средства безопасности**

193. По документам ГТК количество классов защищенности АС от НСД:

- **9**

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

- **6**



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

- **1**

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

- **6**

197. По умолчанию пользователь не имеет никаких прав доступа к:

- **таблицам и представлениям**

198. По умолчанию право на подключение к общей базе данных предоставляется:

- **всем пользователям**

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

- **сеансовом**

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

- **компрометация**

201. Показатель _____ является главным параметром криптосистемы.

- **криптостойкости**

202. Полномочия подсистем ядра безопасности ОС ассоциируются с:

- **пользователями**

203. Полномочия ядра безопасности ОС ассоциируются с:

- **процессами**

204. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем

- **прикладном**

205. Преобразование форматов реализуется на уровне модели взаимодействия открытых систем

- **представления данных**

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

- **тип разрешенного доступа**

207. При избирательной политике безопасности в матрице доступа объекту системы соответствует:

- **строка**

208. При избирательной политике безопасности в матрице доступа субъекту системы соответствует:

- **столбец**

209. При качественном подходе риск измеряется в терминах

- **заданных с помощью шкалы или ранжирования**

210. При количественном подходе риск измеряется в терминах

- **денежных потерь**

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

- **контроля ошибок**

212. При передаче по каналам связи на физическом уровне избыточность вводится для:

- **реализации проверки со стороны получателя**



213. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:

- **уровень безопасности**

214. Привелегия _____ дает право на запуск сервера.

- **operator**

215. Привелегия _____ дает право на изменение состояния флагов отладочной трассировки.

- **trace**

216. Привелегия _____ дает право на удаление баз данных.

- **createdb**

217. Привелегия _____ дает право на управление расположением сервера баз данных.

- **maintain locations**

218. Привелегия _____ дает право управлять безопасностью СУБД и отслеживать действия пользователей.

- **security**

219. Применение услуги причастности рекомендуется на _____ уровне модели OSI.

- **прикладном**

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

- **перехват**

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

- **имитатор**

222. С использованием прикладных ресурсов ИС связан уровень ОС:

- **приложений**

223. С помощью закрытого ключа информация:

- **расшифровывается**

224. С помощью открытого ключа информация:

- **зашифровывается**

225. С точки зрения ГТК основной задачей средств безопасности является обеспечение:

- **защиты от НСД**

226. Система защиты должна гарантировать, что любое движение данных

- **идентифицируется, авторизуется, обнаруживается, документируется**

227. Согласно "Европейским критериям" для систем с высокими потребностями в обеспечении целостности предназначен класс

- **F-IN**

228. Согласно "Европейским критериям" минимальную адекватность обозначает уровень

- **E0**

229. Согласно "Европейским критериям" на распределенные системы обработки информации ориентирован класс

- **F-DI**



230. Согласно "Европейским критериям" предъявляет повышенные требования и к целостности, и к конфиденциальности информации класс

- **F-DX**

231. Согласно "Европейским критериям" только общая архитектура системы анализируется на уровне

- **E1**

232. Согласно "Европейским критериям" формальное описание функций безопасности требуется на уровне

- **E6**

233. Согласно "Оранжевой книге" верифицированную защиту имеет группа критериев

- **A**

234. Согласно "Оранжевой книге" дискреционную защиту имеет группа критериев

- **C**

235. Согласно "Оранжевой книге" мандатную защиту имеет группа критериев

- **B**

236. Согласно "Оранжевой книге" минимальную защиту имеет группа критериев

- **D**

237. Согласно "Оранжевой книге" с объектами должны быть ассоциированы

- **метки безопасности**

238. Согласно "Оранжевой книге" уникальные идентификаторы должны иметь

- **все субъекты**

239. Средствами проверки подлинности пользователей обеспечивается безопасность информации на уровне ОС

- **сетевом**

240. Стандарт DES основан на базовом классе

- **блочные шифры**

241. Структурированная защита согласно "Оранжевой книге" используется в системах класса

- **B2**

242. Требования к техническому обеспечению системы защиты

- **аппаратурные и физические**

243. У всех программных закладок имеется общая черта

- **обязательно выполняют операцию записи в память**

244. Услугами _____ ограничивается применение средств защиты физического уровня.

- **конфиденциальности**

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

- **канальном**

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

- **попала в оперативную память**



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

- **фильтры**
-

Файл скачан с сайта oltest.ru

oltest.ru

