

Вопросы к тесту для зачета по курсу  
«Защита информации в телекоммуникационных системах»

1. Дайте понятие защищаемой информации
2. Дайте понятие защите информации
3. Дайте понятие эффективности защиты информации
4. Дайте понятие системы защиты информации
5. Дайте понятие средства защиты информации
6. Дайте понятие угрозы безопасности объекта
7. Дайте понятие уязвимости объекта
8. Дайте понятие источника угрозы
9. Дайте понятие атаки
10. Что такое конфиденциальность информации?
11. Что такое целостность информации?
12. Что такое доступность информации?
13. Какая из перечисленных угроз относится к угрозам против конфиденциальности информации?
14. Какая из перечисленных угроз относится к угрозам против доступности информации?
15. Какая из перечисленных угроз относится к угрозам против целостности информации?
16. Какая классификация источников угроз является общепризнанной?
17. Какая классификация уязвимостей объекта защиты является общепризнанной?
18. Какой из приведенных источников угроз относится к антропогенным?
19. Какой из приведенных источников угроз относится к техногенным?
20. Какой из приведенных источников угроз относится к стихийным?
21. Какой из перечисленных источников угроз является антропогенным внешним?
22. Какой из перечисленных источников угроз является антропогенным внутренним?
23. Какой из перечисленных источников угроз является техногенным внешним?
24. Какой из перечисленных источников угроз является техногенным внутренним?
25. Что такое модель нарушителя информационной безопасности?
26. Какой из перечисленных видов нарушителей информационной безопасности относится к внутренним?
27. Какой из перечисленных видов нарушителей информационной безопасности не относится к внутренним?
28. Какой из перечисленных видов нарушителей информационной безопасности относится к внешним?
29. Какой из перечисленных видов нарушителей информационной безопасности не относится к внешним?
30. Определите понятие, скрытое на изображении.
31. Что из перечисленного относится к аппаратным методам защиты информации?
32. Что из перечисленного относится к программным методам защиты информации?
33. Что из перечисленного относится к организационным методам защиты информации?
34. Какие три понятия составляют триаду КДЦ?
35. Какие три понятия дополняют триаду КДЦ до Гексады Паркера?
36. Что из перечисленного представляет собой систему взглядов относительно направлений, средств и способов защиты жизненно важных интересов личности, общества и государства для Республики Беларусь?
37. Какой закон является основополагающим в Республике Беларусь в сфере защиты информации?
38. Какой закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе?
39. Какой закон определяет правовые основы, принципы, основные задачи и направления деятельности органов государственной безопасности Республики Беларусь?

40. Какой закон определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь?

41. Как раскрывается аббревиатура ОАЦ в сфере защиты информации?

42. Какая серия стандартов Республики Беларусь в настоящее время охватывает большую часть вопросов по защите информации?

43. Что такое сертификация?

44. Что такое аттестация объектов информатизации по требованиям безопасности информации?

45. Что из перечисленного является методом криптографического преобразования информации?

46. Что из перечисленного не является методом криптографического преобразования информации?

47. Какой из представленных алгоритмов относится к симметричным криптосистемам?

48. Какой из представленных алгоритмов относится к асимметричным криптосистемам?

49. Какой из представленных алгоритмов используется при создании электронной цифровой подписи?

50. Какой из представленных алгоритмов не относится к классическим симметричным криптосистемам?

51. К какому типу шифров относится шифрование с использованием скитала?

52. К какому типу шифров относится шифрование с использованием шифра Цезаря?

53. К какому типу шифров относится шифрование с использованием диска Альберти?

54. К какому типу шифров относится шифрование с использованием таблицы Виженера?

55. К какому типу шифров относится шифрование с использованием шифровальной машинки Энигма?

56. К какому типу шифров относится шифрование с использованием шифра Triple DES?

57. К какому типу шифров относится шифрование с использованием шифра AES?

58. К какому типу шифров относится шифрование с использованием шифра RSA?

59. Определите по рисунку средство или метод шифрования.

60. К какому классу алгоритмов шифрования относится шифрование Цезаря?

61. К какому классу алгоритмов шифрования относится шифрование таблицами Виженера?

62. К какому классу алгоритмов шифрования относится шифрование алгоритмом DES?

63. К какому классу алгоритмов шифрования относится шифрование алгоритмом RSA?

64. Для чего используется алгоритм Эль Гамала?

65. Для чего используется алгоритм Диффи-Хеллмана?

66. Сколько циклов шифрования содержит алгоритм DES?

67. Какова длина ключа DES?

68. Какова длина информационного блока, шифрующегося алгоритмом DES?

69. Упрощенная схема работы какого метода шифрования изображена на рисунке?

70. Определите класс средств аутентификации по изображению.

71. Какое из перечисленных средств аутентификации относится к средствам, базирующимся на условных, заранее присваиваемых признаках (сведениях), известных субъекту?

72. Какое из перечисленных средств аутентификации относится к средствам, базирующимся на физических средствах, действующих аналогично физическому ключу?

73. Какое из перечисленных средств аутентификации относится к средствам, базирующимся на индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц?

74. Какое из перечисленных средств аутентификации относится к биометрическим?

75. Какое из перечисленных средств аутентификации не относится к биометрическим?

76. Определите принцип организации разграничения доступа по его описанию. Каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому

элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента, которую ему может выдать администратор или владелец элемента.

77. Определите принцип организации разграничения доступа по его описанию. Для каждого элемента защищаемых данных составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу.

78. Определите принцип организации разграничения доступа по его описанию. Используются такие понятия, как «должность» и «круг должностных обязанностей», наборы которых должны соответствовать перечню различных должностей, существующих на предприятии.

79. Определите принцип организации разграничения доступа по его описанию. Строки таблицы содержат идентификаторы зарегистрированных пользователей, а столбцы – идентификаторы защищаемых элементов данных, в ячейках таблицы – полномочия.

80. Дайте понятие фильтрации трафика.

81. Дайте понятие межсетевого экрана.

82. Дайте понятие прокси-сервера.

83. Дайте понятие мониторинга сетевого трафика.

84. Дайте понятие системы обнаружения вторжений.

85. Определите назначение ACL, примененного к указанному интерфейсу маршрутизатора сети.

86. Дайте понятие троянской программы.

87. Дайте понятие сетевого червя.

88. Дайте понятие компьютерному вирусу.

89. Дайте понятие программной закладке.

90. Дайте понятие ботнету.

91. Как раскрывается аббревиатура АСУ ТП?

92. Как раскрывается аббревиатура КВОИ?

93. Что из перечисленного не входит в перечень отраслевых критериев отнесения объектов информатизации к КВОИ?

94. Определите вероятность подбора с первой попытки пароля длиной  $k$  символов алфавита  $A$ .

95. Определите вероятность подбора с  $n$ -й попытки пароля длиной  $k$  символов алфавита  $A$ .

96. Определите вероятность подбора за  $n$  попыток пароля длиной  $k$  символов алфавита  $A$ .

97. Определите вероятность подбора с первой попытки PIN-кода длиной  $k$  символов.

98. Определите вероятность подбора с  $n$ -й попытки PIN-кода длиной  $k$  символов.

99. Определите вероятность подбора за  $n$  попыток PIN-кода длиной  $k$  символов.

100. Определите вероятность подбора пароля длиной  $k$  символов алфавита  $A$  за время  $T$  при времени ввода одной комбинации  $t$ .

101. Определите вероятность подбора пароля длиной  $k$  символов алфавита  $A$  за время  $T$  при интенсивности перебора паролей  $i$ .

102. Определите время полного перебора всех вариантов пароля длиной  $k$  символов алфавита  $A$  при времени ввода одной комбинации  $t$ .

103. Определите время полного перебора всех вариантов пароля длиной  $k$  символов алфавита  $A$  при интенсивности перебора паролей  $i$ .