Вопросы по *Защите информации и надежности информационных систем (20-21)*

1. Сущность проблемы информационной безопасности и надежности систем
2. Характеристика методов и средств защиты информации от несанкционированного доступа
3. Характеристика и параметры ИС
4. Энтропия источника сообщения. Энтропия Шеннона
5. Энтропия источника сообщения. Энтропия Хартли. Количество информации
6. Двоичный канал передачи информации
7. Энтропия двоичного алфавита
8. Условная энтропия источника сообщения
9. Особенности энтропийной оценки информации при ее передаче
10. Абстрактная машина Тьюринга. Роль в развитии ИС
11. Методы и средства информационной и временной избыточности в ИВС
12. Помехоустойчивое кодирование информации. Основные понятия.
13. Помехоустойчивое кодирование информации. Классификация кодов
14. Теоретические основы избыточного кодирования информации
15. Алгоритм использования корректирующего кода
16. Декодирование кодовых слов. Поиск и исправление ошибок. Особенности программной реализации
17. Код простой четности. Особенности программной реализации
18. Код Хемминга с минимальным кодовым расстоянием $d_{min}=3$. Особенности программной реализации
19. Код Хемминга с минимальным кодовым расстоянием $d_{min}=4$. Особенности программной реализации
20. Составной код. Итеративные коды.
21. Назначение и особенности использования перемежителей в ИС
22. Математические основы построения и использования циклических кодов
23. Порождающие полиномы циклических кодов
24. Порождающие и проверочные матрицы циклических кодов
25. Алгоритм и методика вычисления проверочных символов циклических кодов
26. Синдромный метод декодирования циклического кода
27. Характеристика надежности двоичного канала передачи при использовании кодов
28. Сущность криптографических методов преобразования информации
29. Классификация методов криптопреобразования. Базовые методы шифрования данных
30. Основы теории больших чисел и модулярной арифметики. Основная теорема арифметики. Китайская теорема об остатках
31. Алгоритм Евклида. Расширенный алгоритм Евклида.
32. Проблема дискретного логарифма в криптографии
33. Подстановочные и перестановочные шифры. Сущность и особенности
34. Шифр Цезаря. Его криптостойкость
35. Шифр Цезаря с ключевым словом. Его криптостойкость
36. Шифр Цезаря на основе аффинного преобразования.
37. Шифр Виженера
38. Полиграммные и омофонические шифры
39. Полиалфавитные шифры
40. Характеристика и особенности шифров простой и множественной перестановки
41. Системы симметричного криптопреобразования
42. Алгоритм криптопреобразования DES
43. Цели и особенности модификации алгоритма DES
44. Особенности конструкции и принцип функционирования машины ЭНИГМА
45. Оценка криптостойкости шифров машины ЭНИГМА
46. Алгоритм передачи ключа по Диффи-Хеллману
47. Задача об укладке ранца.
48. Криптографические системы с открытым (публичным) ключом. Алгоритм RSA. Его стойкость
49. Криптографические системы с открытым (публичным) ключом. Алгоритм Эль-Гамаля. Его стойкость
50. Поточное шифрование. Типы
51. Гаммирование в поточном шифровании. Генераторы ключа
52. Особенность шифра Вернама
53. Принципы построения генераторов ПСП на основе регистров сдвига
54. Особенности алгоритма RC4.
55. ЭЦП. Назначение и свойства
56. ЭЦП. Основные методы генерирования
57. ЭЦП на основе симметричной криптографии
58. ЭЦП на основе алгоритма RSA
59. ЭЦП на основе симметричной криптосистемы и посредника
60. ЭЦП на основе DSA
61. ЭЦП на основе алгоритма Эль-Гамаля
62. ЭЦП на основе алгоритма Шнорра

63. Хеш-функция в криптографии
64. Хеш-функция на основе MD4

65. Хеш-функция на основе MD5
66. Хеш-функция на основе SHA
67. Особенности использования функций хеширования в криптовалютных технологиях
68. ЭЦП на основе алгоритма RSA и хеш-функции
69. ЭЦП на основе DSA
70. Основы алгебраической геометрии. Операции над точками
71. Эллиптические кривые над действительными числами
72. Эллиптические кривые над конечными полями
73. ЭЦП на основе эллиптических кривых, Особенности стандарта ЭЦП в РБ
74. Стандарт X.509. SSL/TLS-сертификаты
75. Использование нейросетевых технологий в криптографии
76. Методы текстовой стеганографии
77. Методы графической стеганографии Метод LSB
78. Нейрокриптогрфия. Практическое применение
79. Облачные технологии. Их безопасность
80. Сжатие данных. Цели и классификация методов
81. Сжатие данных. Блочно-ориентированные методы
82. Сжатие данных. Метод Барроуза-Уилера
83. Сжатие данных. Метод Лемпеля-Зива
84. Сжатие данных. Арифметические методы
85. Сжатие данных. Метод Шеннона-Фано
86. Сжатие данных. Метод Хаффмана
87. Мандатная модель разграничения доступа
88. Избирательная модель разграничения доступа
89. Парольная защита ПО
90. Безопасное время использования пароля
91. Формула Андерсена
92. Протокол Kerberos
93. Особенности защиты прав интеллектуальной собственности на ПО
94. Методы защиты прав интеллектуальной собственности на ПО. Шифрование ПС и привязка ПС к носителю информации
95. Методы обфускации в защите ПО
96. Методы защиты прав интеллектуальной собственности на ПО. Водяные знаки
97. Методы защиты прав интеллектуальной собственности на ПО. Отпечатки пальцев.
98. Деструктивные ПС. Общая классификация и характеристики
99. Меры борьбы с вредоносным ПО
100. Компьютерные вирусы. Классификация и характеристики
101. Основные функциональные блоки компьютерного вируса
102. Методы обнаружения и нейтрализации компьютерных вирусов
103. Деструктивные ПС. «Троянские кони»
104. Деструктивные ПС. Снифферы
105. Цели и виды сертификационных испытаний ПС
106. Характеристика факторов, определяющих надежность ПС
107. Средства обеспечения надежности ПС
108. Основные параметры и стороны надежности ИС
109. Типы ошибок в ПС
110. Надежность ПС
111. Экспоненциальная математическая модель распределения ошибок в ПО
112. Простая интуитивная модель надежности ПО
113. Основные характеристики надежности РЭС
114. Функция надежности аппаратных средств ИС
115. Средняя наработка РЭС до отказа и ее связь с другими характеристиками надежности
116. Надежность сложных ИС при последовательном соединении элементов
117. Надежность сложных ИС при параллельном соединении элементов
118. Статистические методы исследований надежности. Закон Пуассона
119. Статистические методы исследований надежности. Распределение Вейбулла
120. Обеспечение отказоустойчивости ИС
121. Способы и средства нейтрализации ошибок и отказов в ИС
122. Способы восстановления отказоустойчивой ИС
123. Испытания ИС на надежность
124. Стратегия разработки политики безопасности и защиты информации в организациях
125. Современное состояние проблемы информационной безопасности технических систем.