Экзаменационные вопросы

по дисциплине «Защита информации и надежность информационных систем» (зимний семестр 24/25 уч. год)

1. Особенности конструкции и принцип функционирования машины ЭНИГМА
2. Оценка криптостойкости шифров машины ЭНИГМА
3. Системы симметричного криптопреобразования
4. Алгоритм криптопреобразования DES
5. Цели и особенности модификации алгоритма DES
6. Криптографические системы с открытым (публичным) ключом. Алгоритм передачи ключа по Диффи-Хеллману
7. Задача об укладке ранца.
8. Алгоритм RSA. Его криптостойкость
9. Алгоритм ЭльГамаля. Его криптостойкость
10. Поточное шифрование. Типы
11. Гаммирование в поточном шифровании. Генераторы ключа
12. Принципы построения генераторов ПСП на основе регистров сдвига
13. Особенности алгоритма RC4.
14. ЭЦП. Назначение и свойства. Основные методы генерирования
15. ЭЦП на основе симметричной криптографии
16. ЭЦП на основе алгоритма RSA
17. ЭЦП на основе симметричной криптосистемы и посредника
18. ЭЦП на основе DSA
19. ЭЦП на основе алгоритма Эль-Гамаля
20. ЭЦП на основе алгоритма Шнорра
21. Хеш-функция в криптографии
22. Хеш-функция на основе MD4
23. Хеш-функция на основе MD5
24. ЭЦП. Назначение и свойства. Основные методы генерирования
25. Особенности использования функций хеширония в криптовалютных технологиях
26. ЭЦП на основе алгоритма RSA и хеш-функции
27. ЭЦП на основе DSA
28. Основы алгебраической геометрии. Операции над точками
29. Эллиптические кривые над действительными числами
30. Эллиптические кривые над конечными полями
31. ЭЦП на основе эллиптических кривых, Особенности стандарта ЭЦП в РБ
32. Стандарт Х.509. SSL/TLS-сертификаты
33. Использование нейросетевых технологий в криптографии
34. Методы текстовой стеганографии
35. Методы графической стеганографии Метод LSB
36. Мандатная модель разграничения доступа
37. Избирательная модель разграничения доступа
38. Парольная защита ПО
39. Безопасное время использования пароля
40. Формула Андерсена
41. Протокол Kerberos
42. Особенности защиты прав интеллектуальной собственности на ПО
43. Методы обфускации в защите ПО
44. Основные характеристики надежности РЭС
45. Функция надежности аппаратных средств ИС
46. Надежность сложных ИС при последовательном соединении элементов
47. Надежность сложных ИС при параллельном соединении элементов
48. Статистические методы исследований надежности. Распределение Пуассона
49. Статистические методы исследований надежности. Распределение Вейбулла
50. Обеспечение отказоустойчивости ИС
51. Способы и средства нейтрализации ошибок и отказов в ИС
52. Способы восстановления отказоустойчивой ИС
53. Характеристика факторов, определяющих надежность ПС
54. Марковские процессы в оценке надежности ИВС
55. Основные параметры надежности ИС
56. Типы ошибок в ПС
57. Надежность ПС
58. Экспоненциальная математическая модель надежности ПО
59. Простая интуитивная модель надежности ПО
60. Деструктивные ПС. Общая классификация и характеристики
61. Меры борьбы с вредоносным ПО
62. Фишинг и спуфинг. Особенности атак и методы противодействия им.
63. Компьютерные вирусы. Классификация и характеристики
64. Основные функциональные блоки компьютерного вируса
65. Методы обнаружения и нейтрализации компьютерных вирусов
66. Использование нейросетевых технологий в криптографии