Вопросы

по дисциплине «Защита информации и надежность информационных систем», 23/24 уч. год,

летний семестр

1. Сущность проблемы информационной безопасности и надежности систем.
2. Характеристики и параметры ИС и ИВС.
3. Характеристика угроз безопасности современным ИС и ИВС.
4. Характеристика методов и средств защиты информации от несанкционированного доступа.
5. Методология разработки и реализации политики безопасности современных ИС и ИВС
6. Энтропия источника сообщения. Энтропия Шеннона.
7. Энтропия источника сообщения. Энтропия Хартли.
8. Двоичный канал передачи информации.
9. Энтропия двоичного алфавита.
10. Условная энтропия. Энтропийная оценка потерь при передаче информации.
11. Методы и средства структурной, информационной и временной избыточности в ИВС
12. Помехоустойчивое кодирование информации. Основные понятия. Назначение.
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.
17. Код Хемминга с минимальным кодовым расстоянием dmin=3.
18. Код простой четности. Особенности программной реализации
19. Код Хемминга с минимальным кодовым расстоянием dmin=4.
20. Составной код. Итеративные коды.
21. Оценка эффективности использования корректирующего кода в ИВС
22. Особенности использования перемежителей в ИВС
23. Совместное использование перемежителей/деперемежителей и корректирующих кодов в ИВС
24. Математические основы построения и использования циклических кодов
25. Кодирование сообщения циклическим кодом
26. Матрицы циклического кода и кода Хемминга
27. Синдромный метод декодирования циклического кода
28. Характеристика надежности двоичного канала передачи при использовании кодов
29. Общая характеристика и классификация методов сжатия информации.
30. Метод сжатия данных Лемпеля-Зива.
31. Метод сжатия данных Барроуза-Уилера.
32. Метод сжатия данных Хаффмана
33. Метод сжатия данных Шеннона-Фано
34. Арифметический метод сжатия данных
35. Базовые понятия криптографии. Основы теории больших чисел. Проблема дискретного логарифма.
36. Решето Эратосфена.
37. Основная теорема арифметики. Алгоритм Евклида нахождения НОД
38. Основы модулярной арифметики. Вычеты.
39. Обратные вычисления по модулю в криптографии.
40. Функция Эйлера в криптографии.
41. Хеш-функция и ее свойства.
42. Общая классификация криптографических методов защиты информации.
43. Подстановочные шифры. Шифр Цезаря. Криптостойкость.
44. Шифр на основе аффинных преобразований. Криптостойкость.
45. Шифр Виженера. Криптостойкость.
46. Перестановочные шифры. Криптостойкость.