**Вопросы**

**по дисциплине «Информационная безопасность», 2023-24 уч. год, летний семестр**

1. **Сущность проблемы информационной безопасности систем.** **Характеристики и параметры ИС и ИВС.**

Информационная система – совокупность аппаратно-программных средств, с помощью которых выполняются операции над данными: сбор, передача, обработка, хранение и визуализация информации.

Безопасность ИС/ИВС (информационно-вычислительная система) – способность противодействовать попыткам несанкционированного доступа или нанесения ущерба владельцам и пользователям системы при умышленных и неумышленных воздействиях на нее:

1) конфиденциальность – доступ к

ней осуществляют только субъекты, имеющие на нее право;

2) целостность – избежание несанкционированной модификации

информации;

3) доступность – избежание временного или постоянного сокрытия

информации от пользователей, получивших права доступа.

1. **Характеристика угроз безопасности современным ИС и ИВС.**
2. **Политика безопасности современных ИС и ИВС**
3. **Энтропия источника сообщения. Энтропия Шеннона.**
4. **Энтропия источника сообщения. Энтропия Хартли.**
5. **Двоичный симметричный канал передачи информации.**
6. **Энтропия двоичного алфавита.**
7. **Условная энтропия. Энтропийная оценка потерь при передаче информации.**
8. **Базовые понятия криптографии. Основы теории больших чисел. Проблема дискретного логарифма.**
9. **Основная теорема арифметики. Алгоритм Евклида нахождения НОД**
10. **Основы модулярной арифметики. Вычеты.**
11. **Обратные вычисления по модулю в криптографии. Расширенный алгоритм Евклида.**
12. **Функция Эйлера в криптографии.**
13. **Хеш-функция и ее свойства. Области использования хеш-функций.**
14. **Общая характеристика алгоритмов хеширования классов MD и SHA.**
15. **Алгоритмы хеширования класса MD. Области использования.**
16. **Алгоритмы хеширования класса SHA. Области использования.**
17. **Общая классификация криптографических методов защиты информации.**
18. **Подстановочные шифры. Шифр Цезаря.**
19. **Особенности реализации шифровальной машины Энигма.**
20. **Шифр на основе аффинной системы подстановок Цезаря.**
21. **Система шифрования Цезаря с ключевым словом.**
22. **Шифр Виженера.**
23. **Перестановочные шифры.**
24. **Методы симметричного криптопреобразования. Стандарт DES. Общая характеристика.**
25. **Методы симметричного криптопреобразования. Стандарт DES. Структура одного цикла. Криптостойкость алгоритма.**
26. **Методы симметричного криптопреобразования. Стандарты 3DES. Реализация и криптостойкость.**
27. **Шифровальная машина Энигма. Устройство, функционирование, криптостойкость.**
28. **Сравнительная характеристика алгоритмов Lucifer, IDEA, ГОСТ 28147-89, Blowfish.**
29. **Криптографические системы с открытым (публичным) ключом. Задача об укладке ранца.**
30. **Управление криптографическими ключами. Алгоритм рукопожатия.**
31. **Распределение ключей на основе симметричных систем.**
32. **Алгоритм передачи ключа по Диффи-Хеллману.**
33. **Алгоритм шифрования RSA. Реализация и криптостойкость.**
34. **Алгоритм шифрования Эль-Гамаля. Реализация и криптостойкость.**
35. **Потоковое шифрование. Типы. Гаммирование в потоковом шифровании.**
36. **Генерация ключевой информации для потокового шифрования. Генераторы ПСП на основе регистров сдвига.**
37. **Особенность шифра Вернама.**
38. **Стеганографические методы защиты информации. Классификация и области использования. Метод наименее значащих бит.**
39. **Понятие эллиптической кривой. Принципы построения криптосистемы на эллиптических кривых**
40. **Представление и описание эллиптической кривой на основе алгебраической геометрии**
41. **Арифметические операции в эллиптической криптографии**
42. **ЭЦП. Назначение и свойства.**
43. **ЭЦП. Основные методы генерации. Атаки на ЭЦП**
44. **ЭЦП на основе симметричной криптографии**
45. **ЭЦП на основе алгоритма RSA**
46. **ЭЦП на основе симметричной криптосистемы и посредника**
47. **ЭЦП DSS.**
48. **ЭЦП на основе алгоритма Эль-Гамаля**
49. **ЭЦП на основе эллиптической кривой.**
50. **Алгоритм К. Шнорра. Стандарт ЭЦП в РБ.**
51. **Протокол Kerberos.**
52. **Деструктивные программы. Классификация и методы нейтрализации.**
53. **Оценка безопасности парольной защиты.**