**Тема Симметричные криптосистемы**

**Цель:** Изучить симметричные блочные криптоалгоритмы

**Вопросы практического занятия:**

*Основные понятия и термины современной криптографии. Классификация современных криптосистем. Классическая сеть Фейстеля. Потоковые шифры. Блочные шифры. Методы криптоанализа. Способы реализации стеганографических системе их достоинства и недостатки.*

**Задания практического занятия:**

1 Подготовьте конспект по вопросам практического занятия

2 Ответьте на контрольные вопросы.

**Контрольные вопросы:**

1. **Как называется раздел науки, объединяющий криптографию и криптоанализ?**Криптология – раздел науки, которая занимается шифрованием и расшифрованием.
2. **Какие задачи решает криптография?**

Судя по 1 вопросу, криптография занимается обеспечением конфиденциальности данных, тоисть оно шифрует данные для защиты от чужого любопыства.

1. **Что представляет собой криптографический алгоритм?**

Криптографический алгоритм – алгоритм видоизменение данных, который использует набор тайных параметров.

1. **Какие требования предъявляются для современных криптографических систем защиты?**

Требования: зашифровка должна читаться только с помощью ключа который знаем только мы и число операций.

1. **В чем суть криптографического метода замены и перестановки?**

Суть в том что шифруемый текст заменяют другими буквами, цифрами, знаками, которые взяты из одного или нескольких алфавитов.

1. **Объясните метод шифрования одноконтурной обыкновенной подстановки?**

Это шифр Виженера – шифрование через таблицу виженера, где сдвиг на 1 букву позволяет зашифровать текст.

1. **Объясните метод шифрования простой перестановки?**

Обычная перестановка – есть блок шифрования, в виде таблицы нескольких столбцов и строк (выбираем сами) и создаем последовательность их чисел рандомной установки.

1. **Объясните шифрование методом гаммирования?**

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст.

1. **Какова стойкость комбинированные методы шифрования?**

Комбинированные методы шифрования обладают высокой секретностью, и высокой стокостью

**10 Что является важнейшим показателем надежности криптографического закрытия?**

Стойкость - стойкость шифра рассматривает определенную информацию, при использовании одного ключа.

**11 Как определяется трудоемкость метода шифрования?**

определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

**12 Что такое маршрутная перестановка?**

Маршрутная перестановка- отрезок открытого текста, который записывается в такую фигуру по некоторой траектории

**13 Что называется «поворотной решеткой»?\**

Это шифр, использующий трафарет из прямоугольного листа клетчатой бумаги размера 2\*2 клеток(или более)

**14 Оцените количество ключей шифра вертикальной перестановки. Во сколько раз это**

Количество ключей независимо от способа задания не больше числа столбцов таблицы шифрования

**15 В чем отличие шифров простой и сложной замены?**

В простой замене соответствие между нормативным алфавитом и шифр-алфавитом задается один раз до начала шифрования и не меняется на всем протяжении шифрования сообщения.

**16 Какие шифры сложной замены вам известны?**

Шифр Гронсфельда

Шифр Виженера

Одноразовый блокнот