**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

1. **Какие задачи решает криптография?**

Обеспечение конфиденциальности данных,

Обеспечение целостности данных

Обеспечение аутентификации

Обеспечение невозможности отказа от авторства

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

Набор правил, который используется для шифровки информации чтобы ее могли прочитать только авторизованные пользователи

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

зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

знание алгоритма шифрования не должно влиять на надежность защиты;

незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

структурные элементы алгоритма шифрования должны быть неизменными;

дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

длина шифрованного текста должна быть равной длине исходного текста;

не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

любой ключ из множества возможных должен обеспечивать надежную защиту информации;

алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

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

Символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.

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

Шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.

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

элементы исходного открытого текста меняют местами.

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

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. В шифре сложной замены буква открытого текста может быть представлена различными символами, кроме того, один и тот же символ криптограммы может обозначать разные буквы.

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

Шифр Гронсфельда

Шифр Виженера

Система шифрования “Одноразовый блокнот”