**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 ответы:**

1. Криптология.
2. Учит сохранять содержание сообщений в тайне.
3. Шифрование.
4. 1. Правило Керкгоффа: криптостойкость должна обеспечиваться не секретностью алгоритма, а секретностью ключа.  
   2. Алгоритм должен быть вычислительно стойким.
5. Символы шифруемого текста заменяются на символы, взятые из других алфавитов.
6. При полиалфавитной одноконтурной обыкновеннойподстановке для замены символов исходного текста используются несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй – символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.
7. Выбирается размер блока шифрования в n столбцов и m строк и ключевая последовательность, которая формируется из натурального ряда чисел 1,2,…,n случайной перестановкой.Шифрование проводится в следующем порядке:  
   1)Шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером nxm.  
   2) Зашифрованный текст выписывается колонками в порядке возрастания номеров колонок, задаваемых ключевой последовательностью.  
   3)Заполняется новый блок и т.д.
8. Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом (например, используя операцию сложения по модулю 2). Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные.
9. Какова стойкость комбинированные методы шифрования?
10. Стойкость.
11. Трудоемкость метода - определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.
12. Преобразования из шифра маршрутной перестановки состоят в том, что в некоторую фигуру, обычно прямоугольник, исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее.
13. Ключом шифра, называемого "**поворотная решетка**", является трафарет, изготовленный из квадратного листа клетчатой бумаги размера n×n (n - четно). Некоторые из клеток вырезаются.
14. Оцените количество ключей шифра вертикальной перестановки. Во сколько раз это
15. Сложный состоит из нескольких простых шифров.
16. Шифр Виженера