**БЛОЧНЫЕ АЛГОРИТМЫ СИММЕТРИЧНОГО ШИФРОВАНИЯ. РЕЖИМЫ РАБОТЫ**

**Вариант №8**

отчет о лабораторной работе №6

по дисциплине

*МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ*

Выполнила \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ст. гр. №230711, Павлова В.С.

Проверила \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

доцент каф. ИБ, Басалова Г.В.

**ХОД РАБОТЫ**

**Задание.** Разработать 2 программы (для двух режимов) шифрования/расшифрования файлов произвольного размера и типа с использованием функции, реализующей базовый цикл блочного шифра, разработанной в лабораторной работе №4. Используемые режим: **режим простой замены с зацеплением** **и режим гаммирования с обратной связью по выходу**. Размер блока – 128; размер ключа – 512; число основных шагов – 32.

**Листинг 1** – Код программы для шифрования и расшифрования в режиме простой замены с зацеплением

#include <iostream>

**Листинг 2** – Код программы для шифрования и расшифрования в режиме гаммирования с обратной связью по выходу

#include <iostream>