**БЛОЧНЫЕ АЛГОРИТМЫ СИММЕТРИЧНОГО ШИФРОВАНИЯ**

**Вариант №8**

отчет о лабораторной работе №5

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 функции, реализующие базовые циклы зашифрования/расшифрования, аналогичные циклам 32-З и 32-Р шифра «Магма». Разработать программы шифрования/расшифрования одного полного блока данных с использованием созданных функций в соответствии с вариантом задания.

По заданию **размер блока** – 128; **размер ключа** – 512; **число основных шагов** – 32.

**Листинг 1** – Код программы для шифрования и расшифрования

#include <iostream>