Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»
КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

Отчет по лабораторной работе №1
по дисциплине «Защита информации»

Тема Разработка шифровальной машины «Энигма»

Студент Лукьяненко В.А.

Группа ИУ7-71Б

Преподаватель Руденкова Ю.С.

2025 г.

1 Задание

1.1 Цель работы

Цель работы: разработка электронного аналога машины «Энигма».

1.2 Содержание работы

Для выполнения данной лабораторной работы необходимо решить следующие задачи:

1. реализовать в виде программы электронный аналог машины «Энигма»;
2. обеспечить шифрование произвольного файла;
3. обеспечить расшифровку произвольного файла;
4. предусмотреть работу программы с пустым 1-байтовым файлом.

2 Теоретическая часть

1. Определение информации, защиты информации, актив, информационная сфера, угроза, шифровальная машина «Энигма».

— **Информация** — это данные, которые могут быть восприняты, обработаны или использованы человеком или техническими средствами.

— **Защита информации** — это комплекс организационных, технических и программных мер, направленных на предотвращение несанкционированного доступа, искажения, утраты или уничтожения информации.

— **Актив** — это любой объект, обладающий ценностью для владельца (данные, оборудование, программное обеспечение и т.д.).

— **Информационная сфера** — это область деятельности, связанная с формированием, хранением, обработкой и использованием информации, а также воздействием информации на общество и человека.

— **Угроза** — это потенциальное событие или действие, которое может нанести ущерб информационным активам (кража данных, модификация, уничтожение).

— **Шифровальная машина «Энигма»** — электромеханическое устройство для шифрования текста, применявшееся Германией во время Второй мировой войны, основанное на многоалфавитной подстановке с использованием роторов.

2. Дать определение одно- и многоалфавитной подстановки.

— **Однаалфавитная подстановка** — это криптографический метод, при котором каждой букве исходного алфавита соответствует только одна буква шифрованного алфавита на протяжении всего текста (шифр Цезаря).

— **Многоалфавитная подстановка** — это криптографический метод, при котором для разных символов текста могут использоваться разные алфавиты подстановки. Последовательность алфавитов задаётся ключом или механизмом (машина «Энигма»).

3. К какому виду относится алгоритм «Энигма»?

Алгоритм работы шифровальной машины «Энигма» относится к многоалфавитным подстановкам, так как каждый символ может шифроваться с использованием различных алфавитов в зависимости от текущего положения роторов.

4. Приведите схему алгоритма «Энигма».