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**»

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

Студент Ковель Александр Денисович

Группа ИУ7-76Б

Предмет Защита информации

Студент		**Ковель А. Д.**
	подпись, дата	*фамилия, и.о.*
Преподаватель		**Чиж И. С.**
	подпись, дата	*фамилия, и.о.*

2023 г.

ВВЕДЕНИЕ

Цель лабораторной работы — разработать программу шифровальной машины «Энигма» [1].

Задачи лабораторной работы:

1) провести анализ работы шифровальной машина «Энигма»;
2) описать алгоритм шифрования;
3) релизовать описанный алгоритм.

1 Аналитическая часть

Шифровальная машина «Энигма» состоит из трех основных частей:

1) роторы — диски обладающие 26 гранями, где каждая грань представляла собой нумерацию английского алфавита;
2) рефлектор — статический механизм, позволящий машине также расшифровать текст;
3) коммутатор — набор парных шифров.

1.1 Алгоритм работы машины

На вход «Энигме» подается строка, которая разбивается на символы. Далее символ проходит через коммутационную панель, который меняет символ в соотвествии с настройкой. После прохождения панели, символ проходит черз три диска и попадает на рефлектор. После работы рефлектора, символ отправляется обратно на диске и оканчательно шифруется через коммутатор. Затем один ротор совершает оборот, если ротор обернулся 26 раз, то поворачивается следующий.

2 Конструкторская часть

2.1 Разработка алгоритма

На рисунке 1 приведена схема работы шифровальной машины Энигма.

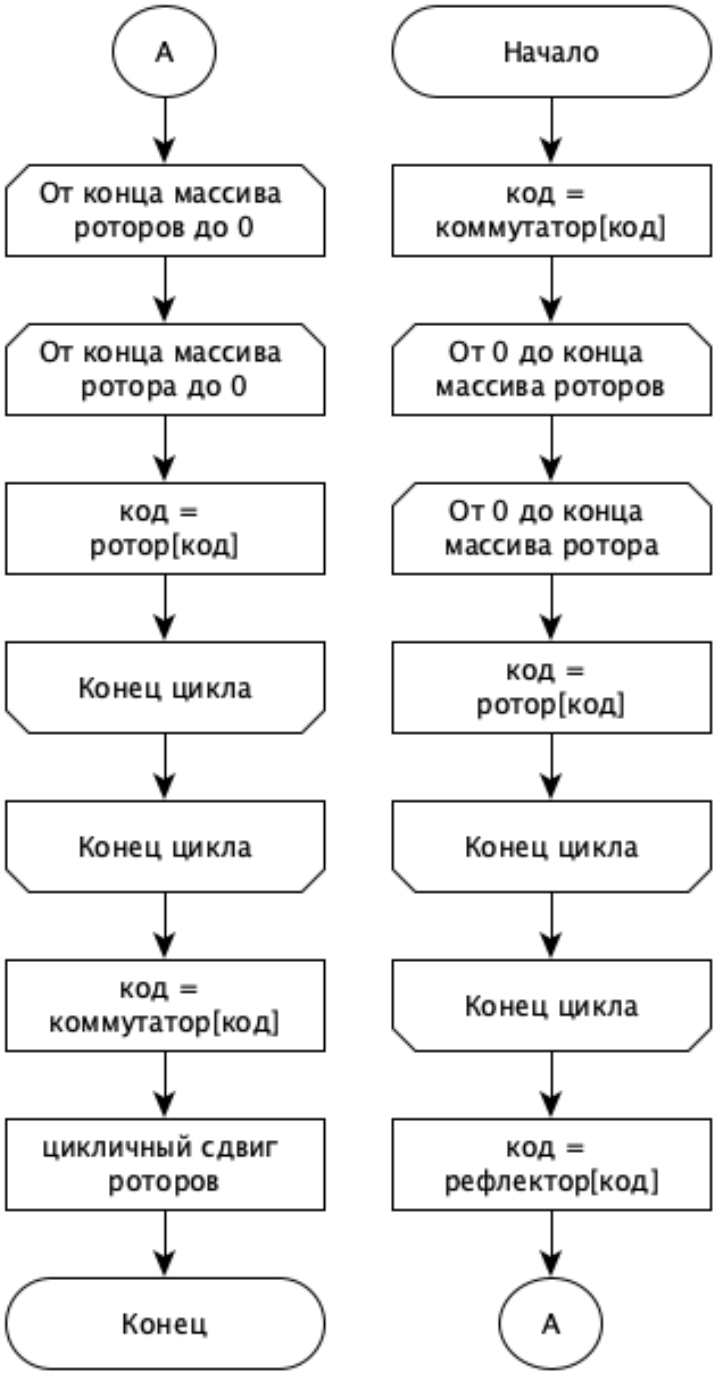

Рисунок 1 – Схема работы шифровальной машина Энигма

3 Технологическая часть

3.1 Средства реализации

Для реализации ПО был выбран язык C++ [2]. В данном языке есть все требующиеся инструменты для данной лабораторной работы. В качестве среды разработки была выбрана среда VS code [3].

3.2 Реализация алгоритма

```
uint8_t Enigma::encrypt(uint8_t code) {
    uint64_t rotor_queue = 1;
    uint8_t new_code = code;

    if (code > size_rotor) {
        throw std::out_of_range("Code␣bigger␣than␣size␣of␣rotor");
    }
    new_code = commutator[new_code];
    for (auto &rotor: rotors) {
        new_code = rotor[new_code];
    }
    new_code = reflector[new_code];
    for (int i = num_rotors - 1; i >= 0; --i) {
        try {
            new_code = find_rotor(i, new_code);
        }
        catch (const std::overflow_error& e) {
            std::cout << e.what() << std::endl;
        }
    }
    counter++;
    for (int i = 0; i < num_rotors; ++i) {
        if (counter % rotor_queue == 0) {
            rotor_shift(i);
        }
        rotor_queue *= size_rotor;
    }
    new_code = commutator[new_code];
    return new_code;
}
```

3.3 Тестовые данные

В таблице 1 приведены тесты для алгоритма шифрования Энигмы. Применена методология черного ящика. Тесты пройдены *успешно*.

Таблица 1 – Функциональные тесты

Входная строка	Выходная строка
$ABOBA$	$BCRGJ$
$BCRGJ$	$ABOBA$
$<<>>$	$<<>>$
A	T
T	A

ЗАКЛЮЧЕНИЕ

В данной лабораторной работе:

1) проведен анализ работы шифровальной машина «Энигма»;
2) описан алгоритм шифрования;
3) реализован описанный алгоритм;

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Список литературы

1. Enigma german code device. https://www.britannica.com/topic/Enigma-German-code-device. дата обращения: 17.09.2023.
2. Язык программирования C++. https://learn.microsoft.com/en-us/cpp/cpp/cpp-language-reference?view=msvc-170. дата обращения: 17.09.2023.
3. Vscode. https://code.visualstudio.com/. дата обращения: 17.09.2023.