

МАШИНА-СИМУЛЯТОР ЭНИГМА

С помощью языка C++ реализована машина-симулятор Энигма. В ней можно устанавливать начальные позиции роторов, зашифровать и дешифровать сообщение. Машина-симулятор полностью совпадает с алгоритмом оригинальной машины [1, 2]. Программа состоит из двух файлов: в первом файле находится код машины Энигма, во втором – настройки машины. На рисунке 1 показан фрагмент кода реализованного приложения (указаны типы роторов, шаги роторов, сообщение, зашифрованное и дешифрованное сообщения).

```
Enigma Machine Emulator
Type of left Rotor: I
Type of middle Rotor: Beta
Type of right Rotor: Gamma
Type of Reflector: B
Step L-M-R: 3-1-3

Enter message to encrypt: OLEG MELESHKOV

Plain text:      OLEGMELESHKOV
Encrypted:       LIKEIFAOKWPNJ
Decrypted:       OLEGMELESHKOV
```

Рисунок 1– Машина-симулятор Энигма

Ротор *rotorIconf* – с позицией "EKMFLGDQVZNTOWYHXUSPAIBRCJ", ротор *rotorBetaconf* – с позицией "LEYJVCNIXWPBQMDRTAKZGFUHNOS", ротор *rotorGammaconf* – с позицией "VZBRGITYUPSDNHLXAWMJQOFECK". Схема шагов роторов описана в классе *rotateRotors*. В классе *rotorMap* описывается карта сдвига роторов. В классе *rotorValue* описывается выбор буквы. В конструкторе мы можем наблюдать отражение программы визуально, не вникая в подробности алгоритма. В классе *setSettings* через цикл прогоняем все буквы алфавита по роторам. В файле настройки машины мы задаем настройки.

ЛИТЕРАТУРА

1. Энигма [Электронный ресурс]. Режим доступа: <https://ru.wikipedia.org/wiki/Энигма>. Дата доступа: 15.03.2022 г.
2. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 2. Криптографические и стеганографические методы защиты информации: учеб.-метод. пособие для студ. вузов / П. П. Урбанович, Н. П. Шутько. – Минск: БГТУ, 2020. – 226 с.