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»

Лабораторная работа по дисциплине «Защита информации»

Тема Шифровальная машина «Энигма»

Студент Светличная А.А.

Группа ИУ7-73Б

Преподаватель Чиж И. С.

Москва — 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Криптография — это наука об обеспечении конфиденциальности и безопасности информации с использованием математических методов и алгоритмов. С активным развитием информационных технологий и распространением цифровой коммуникации, роль криптографии в современном мире стала критически важной. Она применяется в различных сферах, начиная от защиты банковских данных и личной переписки до обеспечения национальной безопасности и геополитической разведки.

Одним из самых известных примеров исторической криптографии является машина «Энигма», использовавшаяся немцами во времена Второй мировой войны. Эта машина была спроектирована для шифрования важных сообщений, и вначале казалось, что её код невозможно взломать.

Цель: разработка программной реализации шифровальной машины «Энигма».

Задачи:

- исследование исторических аспектов данной машины;
- анализ алгоритма «Энигмы»;
- программная реализация данного алгоритма.

1 Аналитическая часть

Историческая справка

Машина «Энигма» представляет собой исторически значимый образец криптографического устройства, разработанного и внедренного в начале 20-го века. Её история уходит корнями в Германию, и, несмотря на свою криптографическую сложность и значимость, она также стала символом криптографической гонки и разведывательной деятельности во Второй мировой войне [1].

Концепция машины «Энигма» имела свои корни в работах немецких инженеров Артура Шёнбихлера и Хуго Коха в начале 20-го века. Их исследования в области шифрования и механических устройств для этой цели создали основу для будущего устройства [1].

Первая коммерческая версия машины «Энигма» была выпущена в 1923 году фирмой «Шиффер и Фишер». Позднее, она была приобретена немецкой армией, и впоследствии модифицирована и совершенствована для военных целей [1].

«Энигма» использовала механические роторы и электрические контакты для создания сложных перестановок букв в шифре. Её настройка могла изменяться ежедневно, что делало взлом шифра чрезвычайно сложным заданием [1].

Важным моментом в истории машины «Энигма» был взлом её шифра английским криптоаналитиком Аланом Тьюрингом и его командой во времена Второй мировой войны. Их усилия сыграли решающую роль в разгадывании зашифрованных сообщений нацистской Германии и способствовали успехам союзников [1].

Машина «Энигма» остается важным символом истории криптографии и разведывательной деятельности. Её разработка и взлом дали толчок к развитию современной криптографии и кибербезопасности, а также подчеркивают важность научных и технических исследований в области шифрования [1].

2 Конструкторская часть

Алгоритм работы «Энигма»

Алгоритм работы машины «Энигма» пошагово:

Начальная настройка: В начале каждого дня оператор машины «Энигма» выбирал начальные позиции роторов, исходя из уникального установочного ключа, который изменялся ежедневно. Этот ключ включал в себя информацию о позициях роторов и настройках контактных дисков [2].

Ввод сообщения: Пользователь вводил текст сообщения, который он хотел зашифровать, с помощью клавиатуры машины «Энигма». В качестве усовершенствования на данном этапе использовалась коммутационная панель, которая кодировала каждую букву другой, однако она не вращалась как роторы [2].

Электрические контакты: Каждая нажатая клавиша создавала электрический контакт, который затем передавался через роторы машины «Энигма» [2].

Перемещение роторов: После каждого нажатия клавиши, роторы машины «Энигма» вращались на одну позицию. Это вращение меняло электрические соединения и создавало сложные перестановки символов [2].

Пересылка шифра: Электрический сигнал, проходя через роторы, попадал в контактные диски и затем возвращался обратно через роторы. Этот процесс добавлял дополнительные сложности в шифрование сообщения [2].

Получение зашифрованного текста: Результат шифрования выводился на ламповый дисплей машины «Энигма», представляя собой зашифрованный текст [2].

Расшифровка сообщения: Чтобы расшифровать сообщение, оператору нужно было использовать тот же установочный ключ и повторить весь процесс, начиная с начальной настройки. Таким образом, одни и те же настройки могли использоваться для как зашифровки, так и расшифровки сообщений [2].

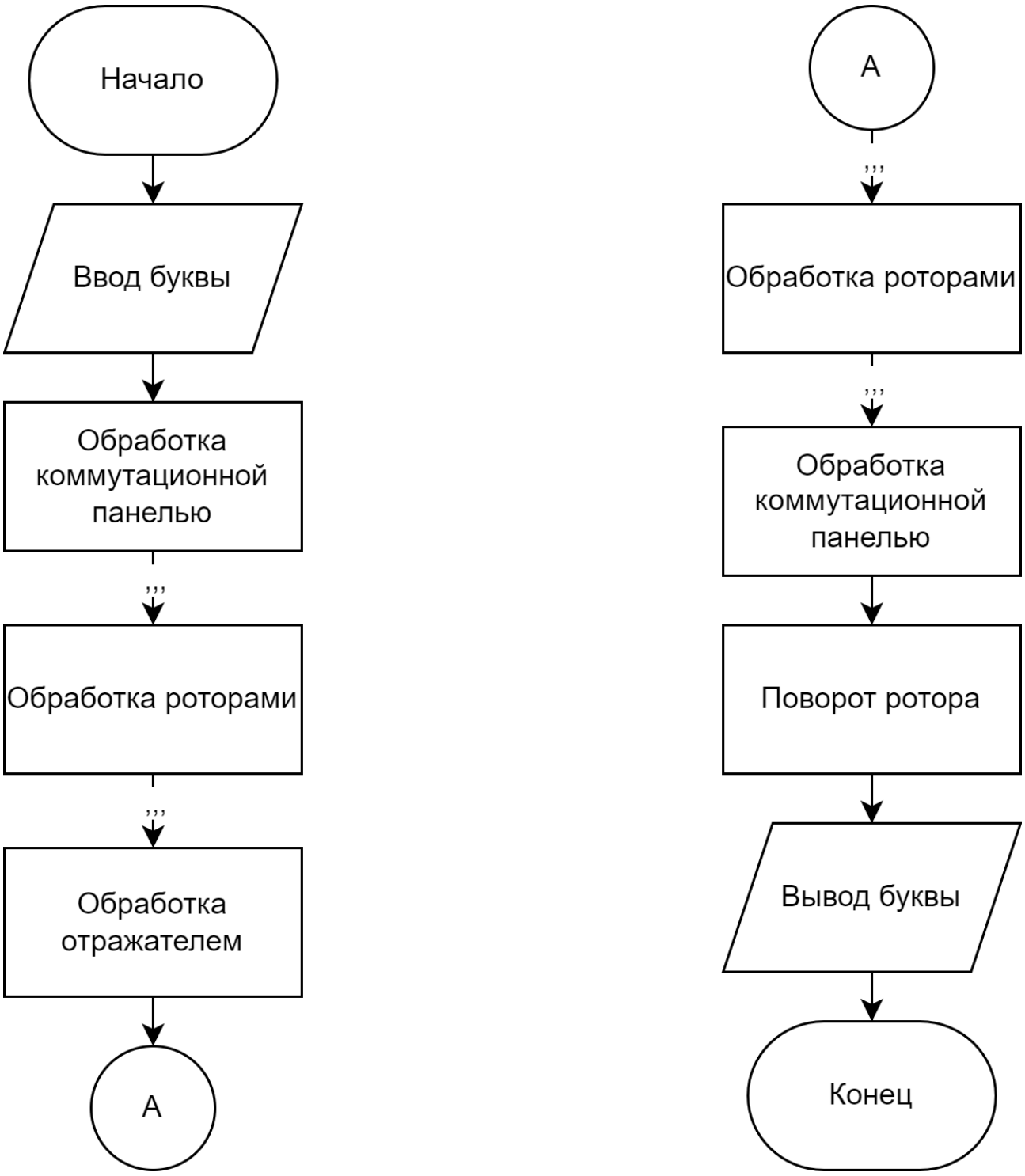

Рисунок 2.1 – Схема алгоритма работы «Энигма»

На рисунке 2.2 представлена наглядная схема обработки буквы данной шифровальной машины.

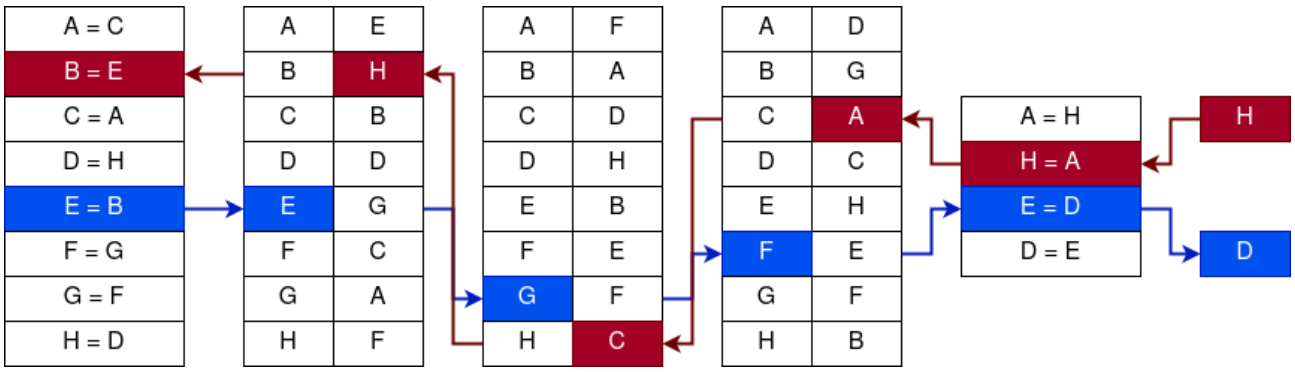

Рисунок 2.2 – Алгоритм обработки одной буквы «Энигмой»

3 Технологическая часть

3.1 Реализация алгоритма

Листинг 3.1 – Реализация алгоритма работы «Энигма»

```
int enigma_encrypt(enigma_t *enigma, int code) {
    uint64_t rotor_queue;
    int new_code = code;

    new_code = enigma->steckbrett[new_code];

    for (int i = 0; i < enigma->num_rotors; ++i)
        new_code = enigma->rotors[i][new_code];

    new_code = enigma->reflector[new_code];

    for (int i = enigma->num_rotors-1; i >= 0; --i)
        new_code = enigma_rotor_find(enigma, i, new_code);

    new_code = enigma->steckbrett[new_code];

    rotor_queue = 1;
    enigma->counter += 1;
    for (int i = 0; i < enigma->num_rotors; ++i) {
        if (enigma->counter % rotor_queue == 0)
            enigma_rotor_shift(enigma, i);

        rotor_queue *= enigma->size_rotor;
    }

    return new_code;
}
```

```
31 void enigma_rotor_shift(enigma_t *enigma, int num) {
32     char temp = enigma->rotors[num][enigma->size_rotor-1];
33     for (int i = enigma->size_rotor-1; i > 0; --i)
34         enigma->rotors[num][i] = enigma->rotors[num][i-1];
35 
36     enigma->rotors[num][0] = temp;
37 }
38 
39 int enigma_rotor_find(enigma_t *enigma, int num, int code) {
40     for (int i = 0; i < enigma->size_rotor; ++i)
41         if (enigma->rotors[num][i] == code)
42             return i;
43 }
```

3.2 Тестирование

Таблица 3.1 – Тестирование реализованного программного обеспечения

Строка запуска	**Входные данные**	**Выходные данные**	**Код возврата**
./app.exe 1.txt			1
./app.exe 1.txt 2.txt где 1.txt - не существует			2
./app.exe 1.txt 2.txt	!	!	3
./app.exe 1.txt 2.txt	H	S	0
./app.exe 1.txt 2.txt	S	H	0

ЗАКЛЮЧЕНИЕ

В ходе лабораторной работы была достигнута поставленная **цель**: разработана программная реализации шифровальной машины «Энигма».

Все **задачи** лабораторной работы выполнены:

- исследованы исторических аспектов данной машины;
- проведен анализ алгоритма «Энигмы»;
- программно реализован данный алгоритм.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. История загадочной и легендарной шифровальной Enigma [Электронный ресурс]. URL: https://un-sci.com/ru/2019/06/22/istoriya-zagadochnoj-i-legendarnoj-enigma/ (дата обращения: 22.09.2023).

2. Как работала шифровальная машина «Энигма» [Электронный ресурс]. URL: https://hi-news.ru/technology/kak-rabotala-shifrovalnaya-mashina-enigma.html (дата обращения: 22.09.2023).