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 № 1
по дисциплине «Защита информации»

Тема Реализация электронного аналога шифровальной машины «Энигма»

Студент Пермякова Е. Д.

Группа ИУ7-72Б

Преподаватели Руденкова Ю. С.

Москва, 2025

ВВЕДЕНИЕ

Целью данной работы является разработка электронного аналога шифровальной машины, шифрование и расшифровка произвольного файла.

Для достижения поставленной цели требуется решить следующие задачи:

1) провести анализ работы шифровальной машина «Энигма»;

2) описать алгоритм работы электронного аналога шифровальной машины «Энигма»;

3) реализовать виде программы электронный аналог шифровальной машины «Энигма»;

1 Теоретическая часть

Информация – это сведения (сообщения, данные) независимо от формы их представления, воспринимаемые человеком или специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.

Защита информации – это комплекс мероприятий, направленных на обеспечение конфиденциальности (недоступности информации для неавторизованных лиц), целостности (точности и полноты информации) и доступности (возможности получить информацию авторизованным пользователям) информации. Это процесс противодействия угрозам безопасности информации.

Актив – это любой компонент информационной системы (данные, оборудование, программное обеспечение, персонал, услуги, репутация), который имеет ценность для организации и поэтому требует защиты.

Информационная сфера – это совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Это среда, в которой существует и циркулирует информация.

Угроза – это потенциальная возможность того, что определенное лицо, действие, событие или явление (источник угрозы) преднамеренно или случайно нарушит безопасность информации (ее конфиденциальность, целостность, доступность), нанеся ущерб владельцу или пользователю информации.

Шифровальная машина «Энигма» – это портативная электромеханическая шифровальная машина, использовавшаяся в XX веке (в основном нацистской Германией во Второй мировой войне) для защиты служебной переписки. Ее основным принципом работы было многоалфавитное шифрование с изменяющимся алфавитом замены после каждой буквы, реализуемое с помощью системы вращающихся роторов.

Одноалфавитная подстановка – подстановка, при которой каждый символ открытого текста заменяется на один и тот же символ шифрованного текста на протяжении всего сообщения.

Многоалфавитная подстановка – подстановка, при которой каждый символ открытого текста может заменяться на разные символы шифрованного текста в зависимости от своей позиции в тексте и используемого алфавита

замены.

Алгоритм Энигма относится к многоалфавитным подстановочным шифрам.

2 Описание алгоритма работы электронного аналога шифровальной машины «Энигма»

На рисунке 2.1 приведена схема работы шифровальной машины «Энигма»

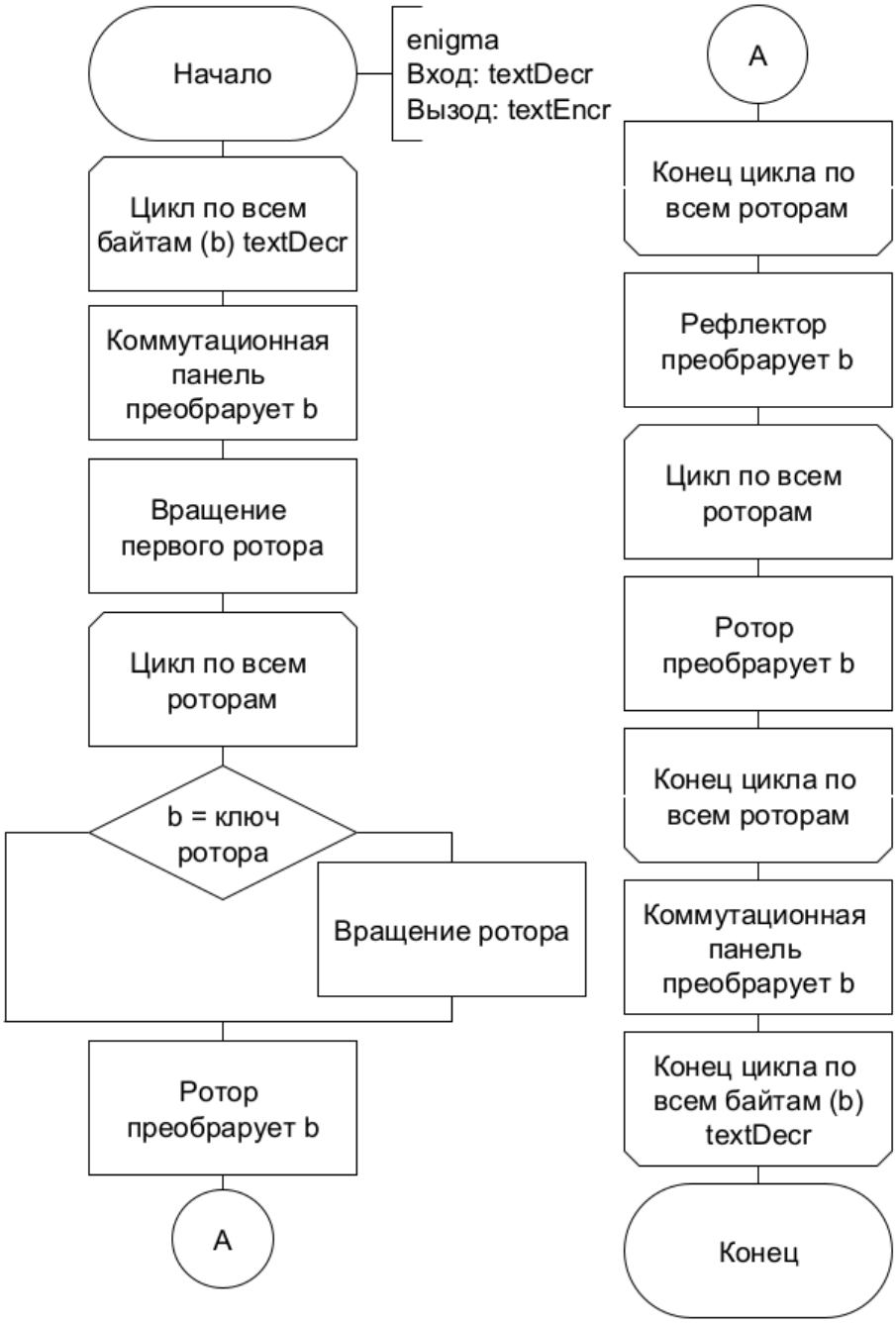

Рисунок 2.1 – Схема работы шифровальной машины «Энигма»

3 Реализация электронного аналога шифровальной машины «Энигма»

```
type Enigma interface {
    EncryptAlpha(alpha byte) byte
    EncryptText(text []byte) []byte
    SetRotorPositions(poses []byte) error
}

type enigma struct {
    switchingPanel Rotor
    rotors         []Rotor
    reflector      Reflector
}

func NewEnigma(switchingPanel Rotor, rotors []Rotor, reflector
   Reflector) Enigma {
    return &enigma{
        switchingPanel: switchingPanel,
        rotors:         rotors,
        reflector:      reflector,
    }
}

func (e *enigma) EncryptText(text []byte) []byte {
    resText := make([]byte, len(text))
    for i, v := range text {
        resText[i] = e.EncryptAlpha(v)
    }
    return resText
}

func (e *enigma) EncryptAlpha(alpha byte) byte {
    alpha = e.switchingPanel.SwitchTo(alpha)
    Nrotors := len(e.rotors)
    e.rotors[0].Rotate()
    nextA := e.rotors[0].Transform(alpha, 0)
    lastRing := e.rotors[0].GetRing()

    for i := 1; i < Nrotors; i++ {
```

```
        if e.rotors[i-1].GetRing() == e.rotors[i-1].
           GetSteppingPos() {
            e.rotors[i].Rotate()
        }
        nextA = e.rotors[i].Transform(nextA, lastRing)
        lastRing = e.rotors[i].GetRing()
    }

    nextA = e.reflector.Transform(nextA, lastRing, -1)

    lastRing = 0
    for i := len(e.rotors) - 1; i >= 0; i-- {
        nextA = e.rotors[i].TransformBack(nextA, lastRing)
        lastRing = e.rotors[i].GetRing()
    }
    nextA = byte((int(nextA) - int(lastRing) + alphabetSize) %
       alphabetSize)
    nextA = e.switchingPanel.SwitchFrom(nextA)

    return nextA
}

func (e *enigma) SetRotorPositions(poses []byte) error {
    if len(poses) != len(e.rotors) {
        return ErrLenPoses
    }
    for i := 0; i < len(e.rotors); i++ {
        e.rotors[i].SetRing(poses[i])
    }
    return nil
}
```

Листинг 3.1 – Реализация электронного аналога шифровальной машины «Энигма»

ЗАКЛЮЧЕНИЕ

В ходе лабораторной работы был реализован электронный аналога шифровальной машина «Энигма».

В процессе выполнения данной работы были выполнены все задачи:

1) провести анализ работы шифровальной машина «Энигма»;

2) описать алгоритм работы электронного аналога шифровальной машины «Энигма»;

3) реализовать виде программы электронный аналог шифровальной машины «Энигма»;