**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

**РУТ (МИИТ)**

**Кафедра «Цифровые технологии управления транспортными процессами»**

**Отчёт**

**По лабораторной работе №5**

**по дисциплине**

**«Основы информационной безопасности»**

**Тема: «Простая перестановка»**

**Вариант №28**

Выполнил: ст. гр. УИС-211

Чаругин А. М.

Проверил: Цыганова Н. А.

Панькина К. Е.

**Москва**

**2022**

Оглавление

[Теоретическое описание метода шифрования - 3](#__RefHeading___1)

[Подстановка задачи 4](#__RefHeading___2)

[Исходное сообщение + 4](#__RefHeading___3)

[Ключ + 4](#__RefHeading___4)

[Криптографическое преобразование - 4](#__RefHeading___5)

[Криптограмма 4](#__RefHeading___6)

[Алгоритм разработанной программы: --- 5](#__RefHeading___7)

[Код программы --- 6](#__RefHeading___8)

[Результаты работы программы --- 7](#__RefHeading___9)

## Теоретическое описание метода шифрования -

Многоконтурная подстановка заключается в том, что для шифрования используются несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения. Частным случаем многоконтурной поли алфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Общая модель шифрования подстановкой может быть представлена в следующем виде:

id = id\_izh + key % (k – 1)

id – номер символа зашифрованного текста ;

id\_izh – номер символа исходного текста;

key – целое число в диапозоне 0 – (k - 1);

k – число символов используемого алфавита;

## Подстановка задачи

### ***Исходное сообщение +***

Механизмы подстановки трафика используются для реализации службы засекречивания потока данных

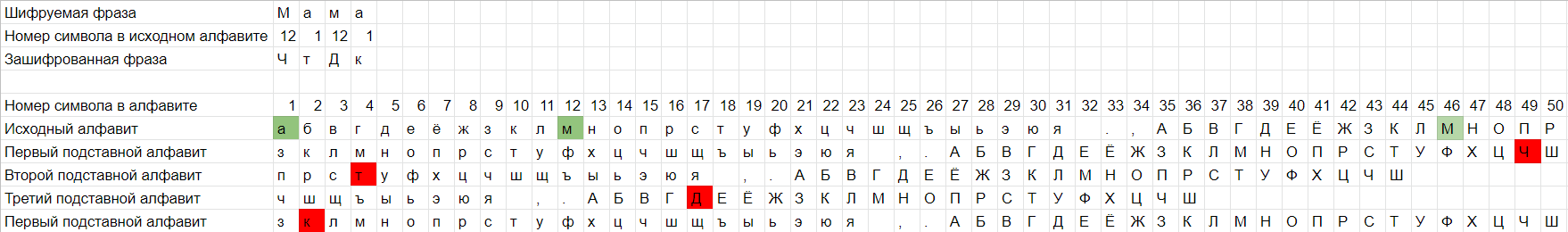
### ***Ключ +***

Ключ вводится с клавиатуры пользователем.

### ***Криптографическое преобразование -***

В программе символ исходного текста, заменяется символом из алфавита циклически повторяющийся алфавит имеет сдвиг на 8 символов. Пользователь с клавиатуры вводит ключ. Ключ применяется по формуле:

id = id\_izh + key mod (k-1).

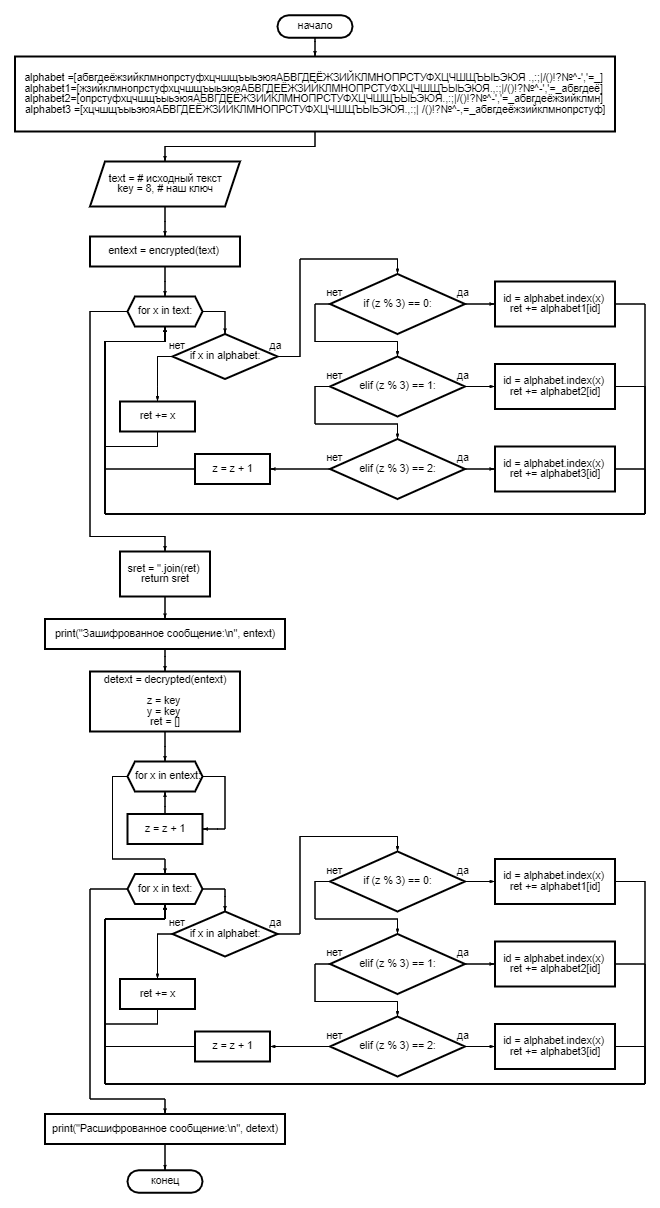


Исходный алфавит В программе представлено 4 алфавита, которые меняются циклически: (alphabet=[абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ .,:;|/()!?№^-','=\_] alphabet1=[жзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,:;|/()!?№^-','=\_абвгдеё] alphabet2=[опрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,:;|/()!?№^-','=\_абвгдеёжзийклмн] alphabet3=[хцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,:;|/()!?№^-','=\_абвгдеёжзийклмнопрстуф])

### ***Криптограмма***

ЪААЗ.ЁьВЗщчЕуыЧьыИэчДГПыпъЁътИш, ИэыЧъААччЕЖНЙьОЧъ, ГуВАхыЧттРуВТЗ, Иш, ьк ЕГчЧштЧэАял, ьк АЖЕЧщ.ЗпцяцОячКМЗ ъъАъмюяшыЦчыЧочЦэчГД ЁьВАЗэЁч.ъшыА

### Алгоритм разработанной программы: ---



## Код программы ---

## Результаты работы программы ---

