**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

**РУТ (МИИТ)**

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

**Отчёт**

**По лабораторной работе №2**

**по дисциплине**

**«Основы информационной безопасности»**

**Тема: «Многоалфавитная одноконтурная подстановка»**

**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)

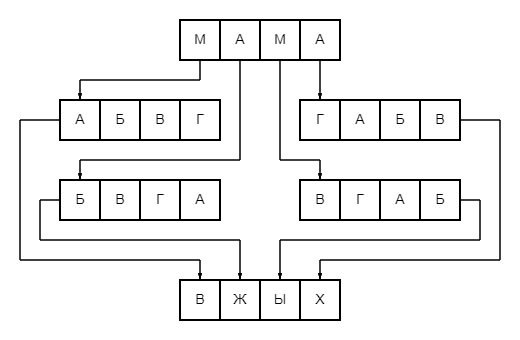
[Алгоритм разработанной программы 5](#__RefHeading___7)

[Код программы 6](#__RefHeading___8)

[Результаты работы программы 7](#__RefHeading___9)

## Теоретическое описание метода шифрования

Много алфавитная одноконтурная подстановка – это когда для замены символов исходного текста используется несколько алфавитов, причем смена алфавита осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующем символом первого алфавита, второй – символом второго алфавита и т.д. до тех пор, пока не будут использованы все выбранные алфавиты.



## Подстановка задачи

### Исходное сообщение

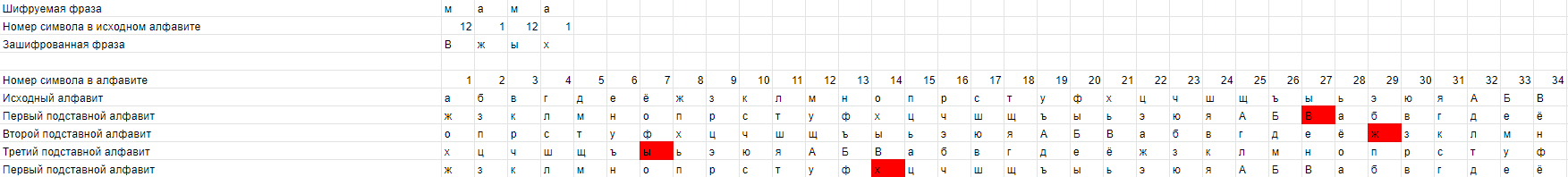
Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования.

### Ключ

Ключ вводится с клавиатуры пользователем.

### Криптографическое преобразование

В программе символ исходного текста, заменяется символом из алфавита циклически повторяющийся алфавит имеет сдвиг на 7 символов. Пользователь с клавиатуры вводит ключ. Ключ это меж символьный интервал внутри алфавита.

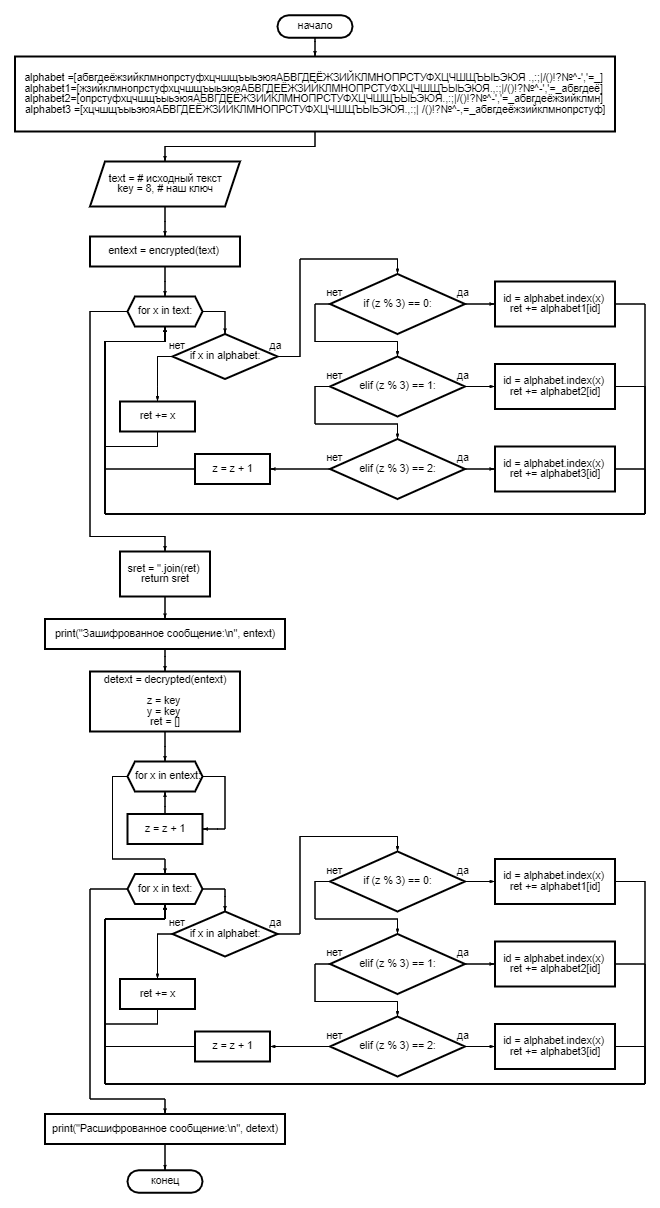


Исходный алфавит В программе представлено 4 алфавита, которые меняются циклически: (alphabet=[абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ .,:;|/()!?№^-','=\_] alphabet1=[жзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,:;|/()!?№^-','=\_абвгдеё] alphabet2=[опрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,:;|/()!?№^-','=\_абв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

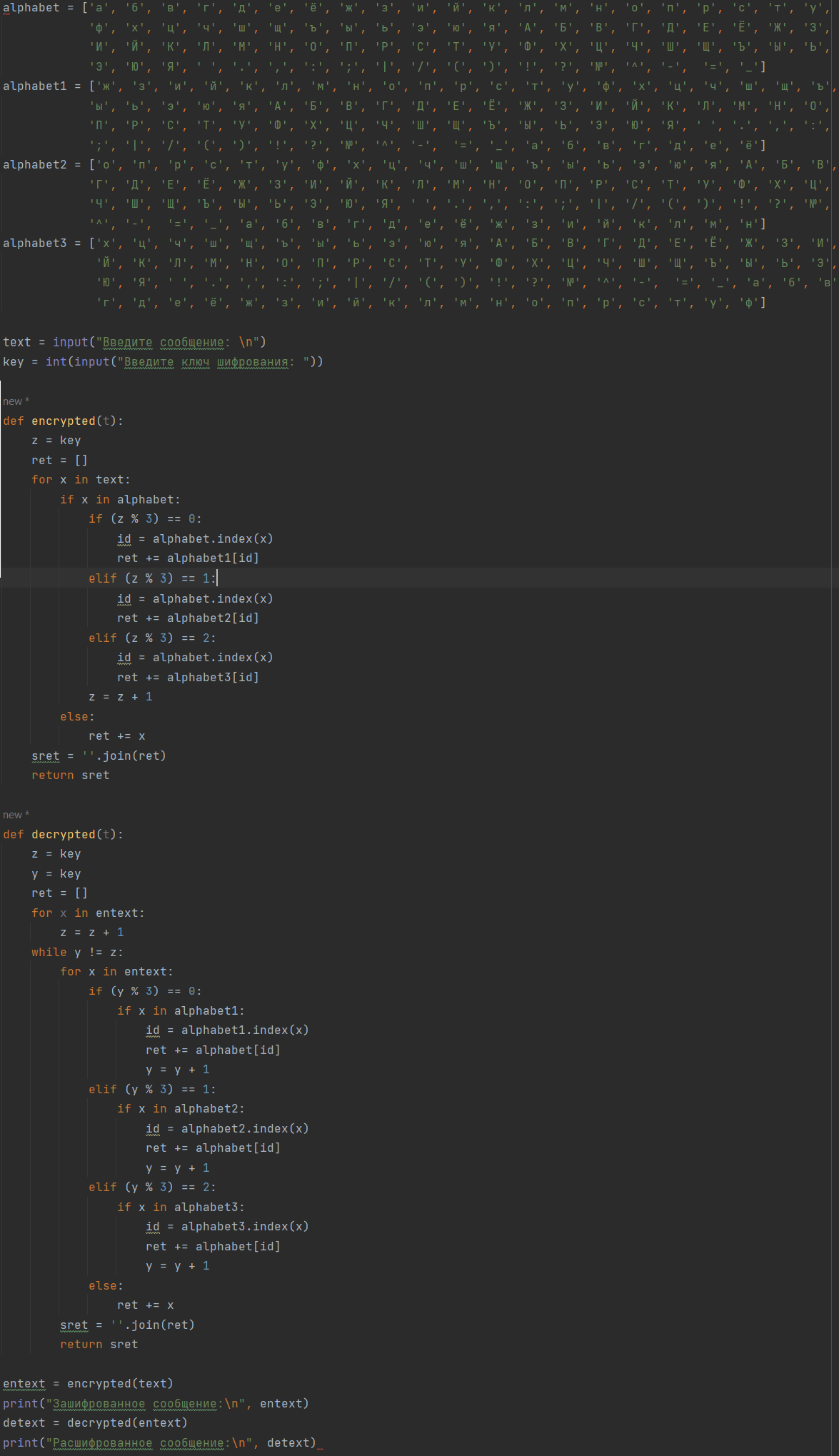
### Криптограмма

|чуДзяхоэчжьюл\_НпГЁхрхфчФ(ыДнуЗ(пРщКёшчВууЗччМфЙВ(чБп\_хшчВууЗччМфЙВ(эЗфэЖпБътКГх\_ЕчуДзяхоэчжьюЁ\_ЁжАНпГЁхрхфчФ)

### Алгоритм разработанной программы



## Код программы



## Результаты работы программы

