**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

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

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

Отчёт

**По лабораторной работе №1 по дисциплине**

**«Основы информационной безопасности» Тема: «Одноалфавитная подстановка» Вариант №28**

Выполнил: ст. гр. УИС-211

Чаругин А. М. Проверил: Цыганова Н. А.

Панькина К. Е.

**МОСКВА2022**

**Оглавление**

[Теоретическое описание метода шифрования 3](#_bookmark0)

[Подстановка задачи 4](#_bookmark1)

[Исходное сообщение 4](#_bookmark2)

[Ключ 4](#_bookmark3)

[Криптографическое преобразование 4](#_bookmark4)

[Криптограмма 4](#_bookmark5)

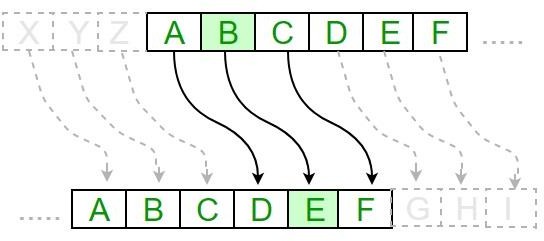
[Алгоритм разработанной программы 4](#_bookmark6)

[Код программы 6](#_bookmark7)

[Результаты работы программы 6](#_bookmark8)

# Теоретическое описание метода шифрования

Одноалфавитная подстановка (Простейшая подстановка) – это шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.



Каждая буква обычного текста заменяется буквой с фиксированным числом позиций вниз по алфавиту.

# Подстановка задачи

## Исходное сообщение

Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).

## Ключ

Ключ вводится с клавиатуры пользователем.

## Криптографическое преобразование

В программе выполняется поиск нужного для шифрования символа в алфавите.

(Наш алфавит: " ():!\_?<>.,-абвгдеёжзийклмнопрстуфхцчшщъыьэ юяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ")).

Берется индекс найденного символа и к нему прибавляется ключ в виде целого числа. Получаем новый зашифрованный символ, который

записывается в переменную, в которой получится новое предложение.

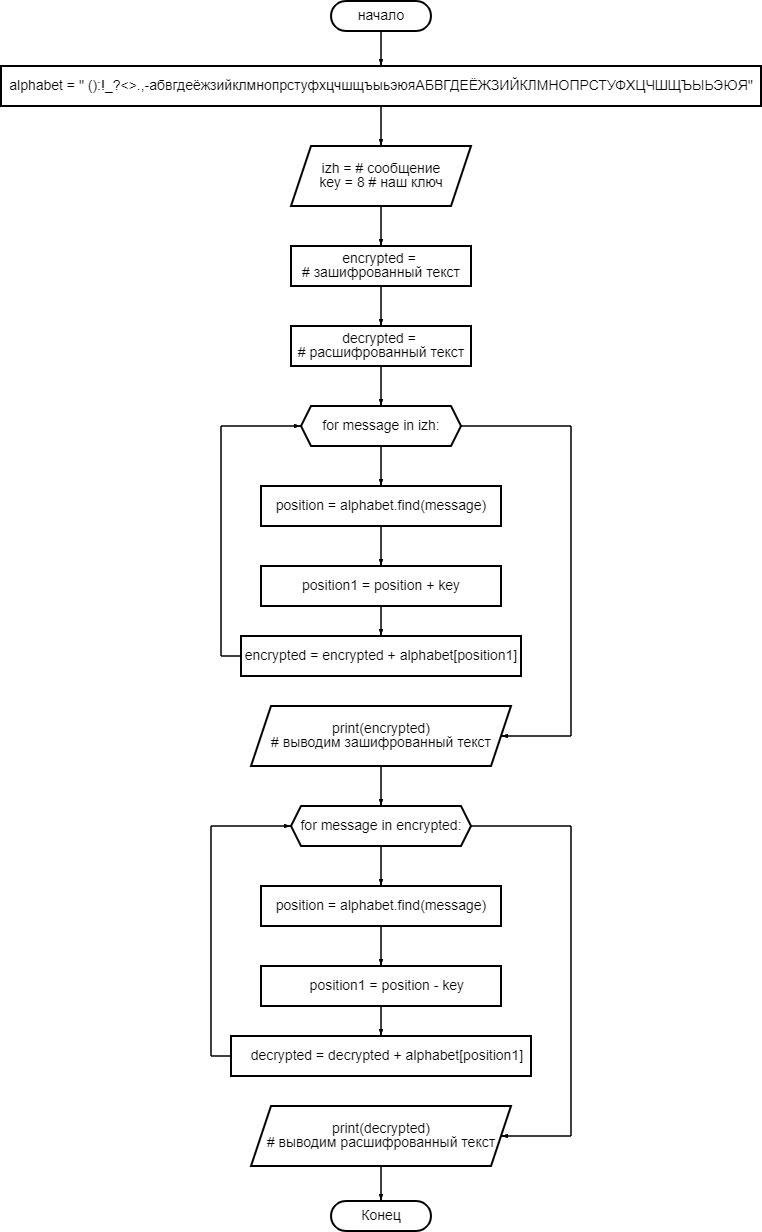
Для расшифровки выполняется точно такая же операция, только теперь ключ не прибавляется, а вычитается.

## Криптограмма

ЩыБмщъйымъ>лйз>тузщщз>тшрчъцщрщъмф-

>щрффмъшряхГм>.цлхцтуЁямйГм,>р>зщрффмъшряхГм>.лйыэтуЁямйГм,е

## Алгоритм разработанной программы:



# Код программы

# Результаты работы программы

