**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОН АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕУЧРЕЖДЕНИЕ 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.

**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)

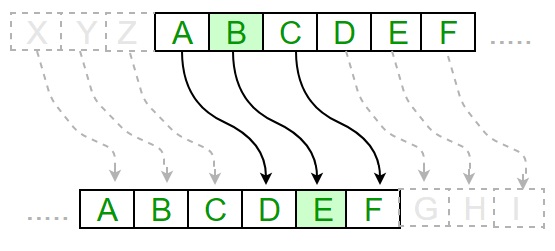
[Алгоритм разработанной программы 4](#__RefHeading___7)

[Код программы 5](#__RefHeading___8)

[Результаты работы программы 8](#__RefHeading___9)

## 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

Ключом моего шифра служит число 8.

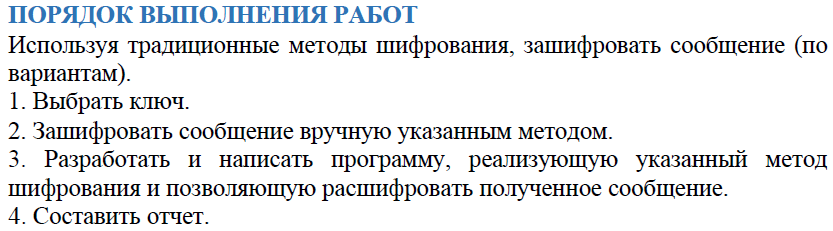
### Криптографическое преобразование

В программе выполняется поиск нужного для шифрования символа в алфавите. 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

### Алгоритм разработанной программы



## Код программы

alphabet = " ():!\_?<>.,-абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"  
izh = input("Введите сообщение: ")  
key = 8  
print("ключ шифрования - ", key)  
encrypto = ""  
decrypto = ""  
  
for message in izh:  
 position = alphabet.find(message)  
 position1 = position + key  
 encrypted = encrypted + alphabet[position1]  
print("Зашифрованное сообщение: ", encrypted)  
  
for message in encrypted:  
 position = alphabet.find(message)  
 position1 = position - key  
 decrypted = decrypted + alphabet[position1]  
print("Расшифрованное сообщение: ", decrypted)

print('выберите тип шифрования (s) - симметричное или (as) - асимметричное')

a = str(input('Напишите s или as'))

if a == 's':

print('Выбранный тип шифрования - симметричное')

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

key = [28]

print('Исходное сообщение: ', IZHODNIK)

print('Ключ - ', key)

text = []

for \_\_ in list(IZHODNIK):

text.append(ord(\_\_)) # ord() - представление слова, как число

print('после перевода текста в цифры: ', text)

etext = []

\_\_key = 0

for \_\_ in range(0,len(text)):

etext.append(text[\_\_]+key[\_\_key])

if \_\_key == len(key)-1:

\_\_key = 0

else:

\_\_key+=1

print('Результат работы шифратора: ', etext)

unetext = []

\_\_key = 0

for \_\_ in range(0,len(etext)):

unetext.append(chr(etext[\_\_]-key[\_\_key]))

if \_\_key == len(key)-1:

\_\_key = 0

else:

\_\_key+=1

print('Результат работы дешифратора: ', unetext)

## Результаты работы программы