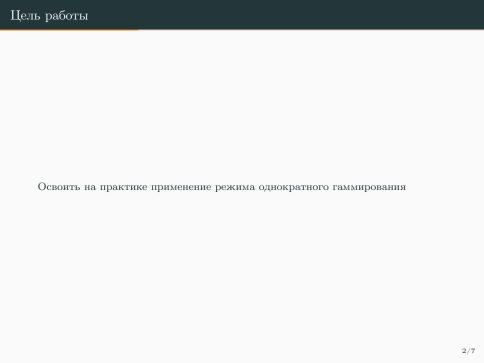
Лабораторная работа  $N_{2}$  7

Элементы криптографии. Однократное гаммирование

Аксёнова Алина Владимировна



Ход работы

## Импорт библиотек и написание функций

```
In [2]: 1 import random 2 import string

In [11]: 1 def generate_key(length, simbols = string.ascii_letters + string.digits): return ''.join(random.choice(simbols) for i in range(length)) def gamming(text, key): text_conv = [ord(i) for i in text] key_conv = [ord(i) for i in key] return ''.join(chr(a ^ b) for a, b in zip(text_conv, key_conv))
```

# Шифрование открытого текста

```
In [14]:

text = 'C Новым Годом, друзья!'
key = generate_key (len(text))
text_shifr = gamming(text, key)
print ('вид шифротекста:', text_shifr)

вид шифротекста: ГЕЮЯФугЅВІЎГЬКЭЗИБЬ
```

# Проверка правильности работы кода

```
In [15]: 1 gamming(gamming(text, key), key)
Out[15]: 'С Новым Годом, друзья!'
```

## Расшифровка зашифрованного текста новым ключом

```
In [16]:

1 key_2 = generate_key (len(text))
2 text_2 = gamming(text_shifr, key_2)
3 print ('Расшифрованный текст:', text_2)
Расшифрованный текст: ы'ѯеОІБ&ЮЇЫфпАШћяжЙЊј>
```

### Вывод

 В результате выполнения данной работы было освоено на практике применение режима однократного гаммирования