

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

## ПРЕЗЕНТАЦИЯ

### ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Пиняева Анна Андреевна

Группа: НПИМд-01-24

МОСКВА

2025

---

## Цель работы

Знакомство и реализация шифра Цезаря и шифра Атбаш.

## Ход работы

### 1. Шифр Цезаря.

Рис. 1 Реализация шифра Цезаря:

```
[1]: function ceasar(text::String, k::Int; alphabet::String="абвгдежзийклмнопрстуфхцчщъыьэюя")
    alphabet_chars = collect(alphabet)
    text_chars = collect(text)
    result = ""
    for char in text_chars
        idx=findfirst(isequal(char), alphabet_chars)
        if idx !==nothing
            new_idx = mod1(idx+k, length(alphabet_chars))
            result *= string(alphabet_chars[new_idx])
        else
            result *= string(char)
        end
    end
    return result
end

function ceasar_de(de_text::String, k::Int; alphabet::String="абвгдежзийклмнопрстуфхцчщъыьэюя")
    return ceasar(de_text, -k, alphabet=alphabet)
end
```

```
[1]: ceasar_de (generic function with 1 method)
```

Рис. 2 Тестирование шифра Цезаря:

```
[3]: text1="привет"  
    key1=3  
    encrypted1=  
    ceasar(text1, key1)  
    descrypted1=  
    ceasar_de(encrypted1, key1)  
    println("Исходный текст'$text1'")  
    println("зашифрованный текст'$encrypted1'")  
    println("дешифрованный текст'$descrypted1'")
```

```
Исходный текст'привет'  
зашифрованный текст'тулеих'  
дешифрованный текст'привет'
```

## 2. Шифр Атбаш.

Рис. 3 Реализация шифра Атбаш:

```
[4]: function atbash(text::String, alphabet::String="абвгдежзийклмнопрстуфхцчшщъыьэюя")
    alphabet_chars = collect(alphabet)
    text_chars = collect(text)
    result = ""
    for char in text_chars
        idx=findfirst(isequal(char), alphabet_chars)
        if idx !=nothing
            new_idx = length(alphabet_chars)-idx+1
            result *= string(alphabet_chars[new_idx])
        else
            result *= string(char)
        end
    end
    return result
end
atbash_de = atbash
```

[4]: atbash (generic function with 2 methods)

Рис. 4 Тестирование шифра Атбаш:

```
[5]: text2="привет"  
encrypted2=  
atbash(text2)  
descrypted2=  
atbash_de(encrypted2)  
println("Исходный текст'$text2'")  
println("зашифрованный текст'$encrypted2'")  
println("дешифрованный текст'$descrypted2'")
```

```
Исходный текст'привет'  
зашифрованный текст'рпчэън'  
дешифрованный текст'привет'
```

Вывод: В ходе данной работы мной были изучены шифры простой замены: шифр Цезаря и шифр Атбаш. Были получены теоретические и практические навыки реализации этих шифров. Написан программный код на языке Julia для шифрования, дешифрования и тестирования каждого метода.