

# Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

---

Мануэл Марсия Педру

2026

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

- Мануэл Марсия Педру
- Студент группы НФИмд-02-25
- Студ. билет 1032255503
- Российский университет дружбы народов имени Патриса Лумумбы



## Цель работы

---

Изучить шифры простой замены и научиться их реализовывать.

## Выполнение лабораторной работы

---

Шифр Цезаря — это древнейший шифр подстановки, в котором каждая буква исходного текста заменяется другой буквой, сдвинутой на фиксированное число позиций в алфавите. Этот метод очень прост: например, при сдвиге на 3, А становится Г, Б — Д и так далее. Для восстановления исходного текста нужно сдвинуть буквы в обратном направлении.

## Реализация шифра Атбаш

Шифр Атбаш — это простейший шифр замены, в котором буквы алфавита заменяются в обратном порядке: первая буква становится последней, вторая — предпоследней и так далее. Например, А становится Z, В — Y, а С — X. Этот метод изначально применялся для еврейского алфавита, откуда и получил свое название от первых букв «алеф» и «тав»:

Выполним реализацию этого алгоритма на языке Python (рис. (fig:001?)):

```
# =====  
# Шифр Цезаря с произвольным ключом K  
# =====  
def cesar_cipher(text: str, k: int) -> str:  
  
    mapping = {  
        'n': 'y',  
        'p': 'ф',  
        'и': 'и',  
        'в': 'к',  
        'е': 'к',  
        'т': 'ц'  
    }  
  
    result = ""  
    for char in text.lower():  
        if char == 'т':  
            result += 'и'  
        elif char in mapping:
```

## Вывод

---



- В ходе выполнения лабораторной работы были изучены шифры простой замены, а также написаны их алгоритмы на языке Python.