

# Информационная безопасность

## Презентация к лабораторной работе № 8

---

Живцова Анна

14 сентября 2023

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Факультет физико-математических и естественных наук, Москва, Россия

Кафедра теории вероятности и кибербезопасности, Москва, Россия

## Информация

---

- Живцова Анна Александровна
- Студент IV курса
- Группа НКНбд-01-20
- Российский университет дружбы народов имени Патриса Лумумбы
- 1032201673
- <https://github.com/AnnaZhiv>

- Схема однократного гаммирования является простой, но надёжной схемой шифрования данных
- Практическая реализация криптографических методов и знакомство с теоретической частью их применения важно для полноценного освоения материала

- Схема однократного гаммирования
- Зашифрованный текст в различной кодировке

- Для двух текстов, зашифрованных одним ключом, разработать программу вычисления одного из исходных текстов при известном втором тексте и двух шифротекстах

- Язык программирования питон

- Изучение теоретического описания схемы однократного гаммирования
- Реализация программ кодирования и декодирования по заданным компонентам криптографического алгоритма



- Программно реализована и протестирована схема однократного гаммирования и ее дешифровка при повторном использовании ключа и одном известном шифротексте