Учреждение образования

«Белорусский государственный технологический университет»

**Отчеты по практическим работам**

По дисциплине: «Основы защиты информации»

Студентки 2 курса 1 группы ФИТ

Шимчёнок Елизаветы Константиновны

**2022 г.**

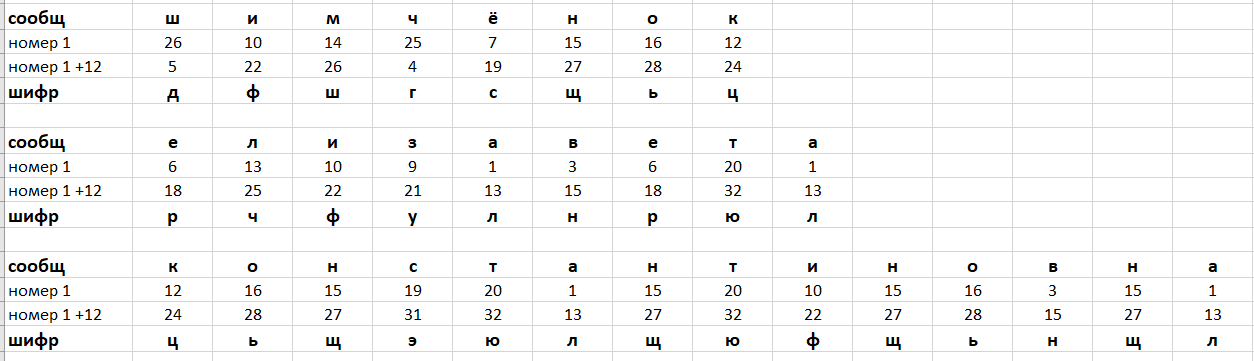
**Цель работы:** Овладение основными криптографическими алгоритмами симметричного шифрования.

# **Выполнение заданий**

## **Зашифровать сообщение с использованием шифра Цезаря**

Сообщение: Шимчёнок Елизавета Константиновна

Ключ: 12



## **Зашифровать сообщение с использованием шифра Трисемуса**

Сообщение: Шимчёнок Елизавета Константиновна

Ключ: “Защита”



Шифр: АЙХЗПЦЧУ ПФЙДЕМПКЕ УЧЦЫКЕЦКЙЦЧМЦЕ

## **Зашифровать сообщение с использованием шифра Плейфейра**

Сообщение: Шимчёнок Елизавета Константиновна

Ключ: «Защита»

Разбитое на биграммы сообщение: ши мч ён ок ел из ав ет ак он ст ан ти но вн а



ши –> ыа (прямоугольник)

мч –> дю (прямоугольник)

ен –> жд (строка)

ок –> уд (прямоугольник)

ел –> жм (строка)

из –> та (строка)

ав –> щг (строка)

ет –> ка (прямоугольника)

ак –> те (прямоугольник)

он –> цд (прямоугольник)

ст –> уи (прямоугольник)

ан –> ге (прямоугольник)

ти –> бт (строка)

но –> дц (прямоугольник)

вн –> гм (прямоугольник)

а’х’ –> вп (прямоугольник)

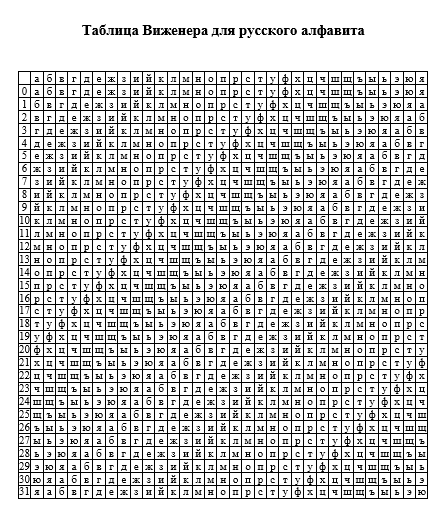
Итог: ЫАДЮЖМТАЩГКАТЕЦДЖДУДУИГЕБТДЦГМВП

## **Зашифровать сообщение с использованием шифра Вижинера**

Сообщение: Шимчёнок Елизавета Константиновна

Ключ: «Защита»

Человек, посылающий сообщение, записывает ключевое слово («Защита») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:



защитазащитазащитазащитазащитаз

Шимчёнок Елизавета Константиновна

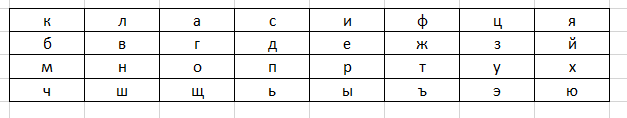
Защитаза щитазащит азащитазащитаз

ЯИЕЯЧНХК ЮУЪЗЗВЮЪТ КХНКЪТНЩИЖЦФНЗ

Итог: ЯИЕЯЧНХКЮУЪЗЗВЮЪТКХНКЪТНЩИЖЦФНЗ

## **Расшифровать с помощью шифра Плейфейра**

Ключ: КЛАССИФИКАЦИЯ



Рп -> по

Пд -> дс

Оф -> та

Бл -> вк

Гщ -> ао

Мф -> тк

Ыи -> ры

Мф -> тк

Цг -> аз

Гн -> во

Оп -> но

См -> кп

Тп -> ро

Гн -> во

Въ -> дш

Ив -> ле

Жя -> йф

Итог: подставка открытка звонок провод шлейф

**Вывод:** были освоены основные криптографические алгоритмы симметричного шифрования на примерах шифров Цезаря, Трисемуса, Плейфера и Вижинера.