

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра автоматизированных систем управления (АСУ)

АЛГОРИТМЫ ДОНАУЧНОЙ КРИПТОГРАФИИ

Лабораторная работа №1
по дисциплине «Защита информации»

Обучающийся гр. 437-2:

_____ Тимофеев Д.О.

___. ___. 2021

Руководитель

Д.т.н. каф. АСУ:

_____ Горитов А.Н.

___. ___. 2021

1. Цель лабораторной работы.

Познакомиться и научиться работать с алгоритмами донаучной криптографии.

2. Индивидуальное задание.

Вариант 2. Перестановочный шифр.

Написать программу, позволяющую зашифровать и расшифровать сообщения с использованием перестановочного шифра. Количество столбцов и строк задается в программе. Входные и выходные данные запишите в файл типа .txt.

3. Описание алгоритма шифрования.

Перестановочный шифр - это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами.

В данной лабораторной работе шифр перестановками основан на заполнении таблицы в одном порядке (слева-направо сверху-вниз) и считыванием в другом (сверху-вниз слева-направо).

4. Листинг программы.

Листинг программы представлен в приложении А

5. Примеры работы программы.

Примеры работы программы представлены в приложении А

6. Вывод о проделанной работе.

В ходе выполнения лабораторной работы №1, я освоил на практике алгоритм донаучной криптографии – Перестановочный шифр.