Университет ИТМО

Факультет ПИиКТ

Информационная безопасность

Лабораторная работа №3

«Поточное симметричное шифрование»

Вербовой Александр

Группа P3400

Вариант 4

**Цель работы**

изучение структуры и основных принципов работы современных алгоритмов поточного симметричного шифрования, приобретение навыков программной реализации поточных симметричных шифров

**Задание (вариант 4)**

20

89

…

…

. . .

91

89

20

γ

4. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы РС

&

**v**

Управление тактированием, если бит=0, то управляемый ЛРС сдвигается вправо, если 1 - нет

ЛРС1 (89,6,5,3,0)

ЛРС2 (91,8,5,1,0)

**Описание:**

**Изображение выглядит как текст

Автоматически созданное описание**

**Изображение выглядит как текст

Автоматически созданное описание**

**Вывод**

В ходе лабораторной работы были изучены структура и основные принципы работы современных алгоритмов поточного симметричного шифрования, приобретены навыков программной реализации поточных симметричных шифров.