Университет ИТМО

Факультет ПИиКТ

Информационная безопасность

Лабораторная работа №2

«Блочное симметричное шифрование»

Вербовой Александр

Группа P3400

Вариант 4

**Цель работы**

изучение структуры и основных принципов работы современных алгоритмов блочного симметричного шифрования, приобретение навыков программной реализации блочных симметричных шифров.

**Задание (вариант 4)**

Алгоритм – ГОСТ 28147-89. Режим шифрования - CFB

**Описание:**

Изображение выглядит как текст

Автоматически созданное описание

**Изображение выглядит как текст

Автоматически созданное описание**

**Вывод**

В ходе выполнения лабораторной работы были изучены структуры и основные принципы работы современных алгоритмов блочного симметричного шифрования.