Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

ОТЧЕТ

по лабораторной работа №2

по курсу «Защита информации»

на тему: «Алгоритм AES»

Вариант № 2

Студент ИУ7-73Б _____ Лысцев Н. Д.
(Группа) (Подпись, дата) (И. О. Фамилия)

Преподаватель _____ Чиж И. С.
(Подпись, дата) (И. О. Фамилия)

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **3**

ВВЕДЕНИЕ

Целью данной лабораторной работы является реализация программы шифрования симметричным алгоритмом AES с применением режима CFB.

Для достижения поставленной цели необходимо решить следующие задачи:

1) описать алгоритм AES с режимом CFB;

2) выбрать средства программной реализации;

3) реализовать данный алгоритм.