|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Возведение в степень по модулю числа»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Дроздов А.Д.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[1. Теоретическая часть 3](#_Toc128233466)

[1.1. Основной метод вычисления степени по модулю числа 3](#_Toc128233467)

[1.2. Альтернативные методы вычисления 3](#_Toc128233468)

[1.3. Вопросы оценки сложности алгоритмов 3](#_Toc128233469)

[2. Практическая часть 3](#_Toc128233470)

[2.1. Результаты вычисление 3](#_Toc128233471)

[2.2. Сравнение сложности алгоритмов вычисления 3](#_Toc128233472)

[Заключение 3](#_Toc128233473)

# Теоретическая часть

## Бинарный алгоритм возведения в степень по модулю числа

Бинарный алгоритм – это один из методов, позволяющий возвести число в степень по заданному модулю с помощью разложения данной степени в двоичное число.

### 1.1.1. Описание бинарного алгоритма

## 1.2. Альтернативный алгоритм быстрого возведения в степень по модулю числа

## Вопросы оценки сложности алгоритмов

# Практическая часть

## Результаты вычисление

## Сравнение сложности алгоритмов вычисления

# Заключение

Текст заключения.