**Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации**

**ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникации им. проф. М.А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра Защищенных систем связи

Дисциплина «Основы криптографии»

# Лабораторная работа № 12

**решение задач по дискретной математике**

Выполнил: ст. г. ИКТЗ-83

Громов А.А.

Проверил: Яковлев В. А.

Цель лабораторной работы:

* Приобретение навыков выполнения вычислений дискретной математики

**Выполнение работы:**

Задание №1

Найти наибольший общий делитель.

Четные номера. Найти НОД (8888,2404)

Ответ: НОД (8888,2404) = 4

Задание №2

Используя алгоритм быстрого возведения в степень, вычислить:

Четные номера. .

Ответ:

Задание №3

Найти обратный элемент к числу *а* по *mod b*,

где *a* соответствует числу в таблице 1, порядковый номер которого совпадает с Вашим номером по журналу, *b* с номером большим на 10 порядковый номер числа *а*.

Таблица1

23 29 31 37 41 43 47 53 59 61

67 71 73 79 83 89 97 101 103 107

109 113 127 131 137 139 149 151 157 163

167 173 179 181 191 193 197 199 211 223

1) Находим НОД:

.

2 = 2\*1 + 0

НОД (79,37) = 1

2)

3)

4) Проверка

Ответ:

Задание №4

Используя тест Ферма, проверить является ли число р простым.

Таблица 2

179 183 191 193 197 199 213 223 227 229

233 239 247 251 257 263 269 271 277 281

283 299 307 311 311 317 331 337 347 349

Вероятность ошибки, т. е. вероятность принять составное число за простое составляет 0.25.

Ответ: число 193 – простое

Выводы:

В ходе данной лабораторной работы, мы закрепили навыки вычисления наибольшего общего делителя, быстрого возведения в степень по модулю, вычисления обратного элемента к числу по модулю, а также проверки простого числа используя тест Ферма.