**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ**

(национальный исследовательский университет)»

**Институт (Филиал)** №8«Компьютерные науки и прикладная математика» **Кафедра** 806

**Группа** М8О-407Б-18 **Направление подготовки** 01.03.02 Прикладная математика и информатика

**Профиль**  Информатика

**Квалификация**  **бакалавр**

**УТВЕРЖДАЮ**

Заведующий кафедрой 806 \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

(№ каф.) (подпись) (инициалы, фамилия)

\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ 20 г.

**ЗАДАНИЕ**

**на выпускную квалификационную работу бакалавра**

**Обучающийся** Гамов Павел Антонович

(фамилия, имя, отчество полностью)

**Руководитель** Ухов Петр Александрович \_\_\_\_\_\_\_\_

(фамилия, имя, отчество полностью

Доцент. Кандидат технических наук

ученая степень, ученое звание, должность и место работы)

**1. Наименование темы**  Алгоритмы факторизации больших чисел

**2. Срок сдачи обучающимся законченной работы** 24.05.2022

**3. Задание и исходные данные к работе**

Реализовать алгоритм факторизации p Полларда а также алгоритма квадратичного решета. Сравнить алгоритмы. Улучшить алгоритм квадратичного решета.

**Перечень иллюстративно-графических материалов:**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество листов** |
| 1 | Раздаточный материал | 21 |

**4. Перечень подлежащих разработке разделов и этапы выполнения работы**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/п | Наименование раздела или этапа | Трудоёмкость в % от полной трудоёмкости ВКРБ | Срок выполнения | Примечание |
| 1 | Прорабатывание теоретической части работы, чтение литературы. | 8% | 09.2.2022-16.2.2022 |  |
| 2 | Формирование скелета алгоритма квадратичного решета. | 12% | 17.2.2022-29.02.2022 |  |
| 3 | Внедрение улучшений в алгоритм квадратичного решета. | 22% | 30.02.2022- 23.03.2022 |  |
| 4 | Сбор метрик, составления графиков скорости алгоритмов на разных данных. | 10% | 24.03.2022-4.04.2022 |  |
| 5 | Ознакомление с ГОСТ. | 3% | 5.04.2022-6.04.2022 |  |
| 6 | Написание ВКР. | 32% | 7.04.2022-10.05.2022 |  |
| 7 | Оформление ВКР. | 3% | 11.05.2022-13.05.2022 |  |
| 8 | Создание презентации на основе текста ВКР. | 10% | 14.05.2022-24.05.2022 |  |

# 5. Исходные материалы и пособия 1. Шнайер Б. Прикладная криптография. —Москва: Триумф, 2013. 2. Коблиц Н. Курс теории чисел и криптографии. —Москва: Научное издательство «ТВП», 2001. 3. Василенко О.Н. Теоретико – числовые алгоритмы в криптографии. —М.: МЦНМО, 2003. 4. ИшмухаметовШ.Т. Методы факторизации натуральных чисел: учебное пособие —Казань: Казан. Ун., 2011. 5. Brent R. P.Some parallel algorithms for integer factorization—Proc. Fifth International Euro-Par Conference, Lecture Notes in Computer Science 1685, Springer, 1999. 6. Koblitz N.A. Course in number theory and cryptography — Springer-Verlag, 1987. 7. Gerver J.L. Factoring large numbers with a quadratic sieve. — Math. Comp., 1983. — Vol. 41. — P. 287—294. 8. Коэн А. A Course in Computational Algebraic Number Theory — 4th Print Edition — Берлин, Гейдельберг. 9. Montgomery P., Silverman R. D. An FFT extension to the P-1 factoring algorithm Math. Comp.— AMS, 1990.10. Pollard J. M. Theorems on factorization and primality testing Mathematical Proceedings of the Cambridge Philosophical Society B. J. Green — Cambridge University Press, 1974.

**6. Дата выдачи задания** 09.02.2022

Руководитель (Ухов П.А*.*)

(подпись)

Задание принял к исполнению (Гамов П.А.)

(подпись)