МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ (МАГИСТЕРСКУЮ ДИССЕРТАЦИЮ)

Студенту: Гусеву Виталию Евгеньевичу группы 09-335

| 1. Срок сдачи студентом законченной работы 2025 г. |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Тема работы: <u>Исследование методов дискретного логарифмирования.</u> |
| 3. Постановка задачи: <u>исследовать и реализовать модификации методов дискретного логарифмирования. Реализовать модификации, которые будут иметь большую скорость вычисления или меньше затраченной памяти по сравнению с базовыми алгоритмами. Провести эксперименты для проверки работы модифицированных алгоритмов на числах различной длины. Провести сравнительный анализ с результатами работы базовых алгоритмов.</u> |
| 4. Поэтапный план работы: |
| 1) исследование методов дискретного логарифмирования, |
| 2) реализация базовых алгоритмов дискретного логарифмирования, |
| 3) проведение экспериментов на базовых алгоритмах дискретного логарифмирования, |
| 4) исследование модификаций методов дискретного логарифмирования, |
| 5) реализация модифицированных методов дискретного логарифмирования, |
| 6) тестирование модифицированных методов дискретного логарифмирования, |
| 7) проведение экспериментов на модифицированных алгоритмах дискретного логарифмирования, |
| проведение сравнительного анализа работы базовых и модифицированных алгоритмов дискретного логарифмирования. |
| 5. Ожидаемые результаты работы: <u>в результате работы будут исследованы и реализованы модификации методов дискретного логарифмирования. Ожидается, что реализованные модификации будут иметь большую скорость вычисления или меньше затраченной памяти по сравнению с базовыми алгоритмами. Будут проведены эксперименты для проверки работы модифицированных алгоритмов на числах различной длины. Будет проведён сравнительный анализ с результатами работы базовых алгоритмов. 6. Особые замечания к работе:</u> |
| |

| 7. Руководитель работы: <u>доцент кафедры САИТ, канд. техн. наук Мубараков Булат Газинурович</u> 8. Рецензент работы: | | | |
|--------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------|--|
| | | | |
| | | | |
| М.П. | Дата выдачи задания « <u>10</u> |)» февраля 2025 г. | |
| | Руководитель работы | | |
| | Зав.кафедрой | Васильев А.В. | |
| «»2025 г. | | | |
| Задание принял к исполнению «» _ | | 2025 г. | |
| | | | |
| - | | - | |