**Задание на выпускную квалификационную работу**

**студента 4-го курса бакалавриата Денисова И.И.**

*Направление подготовки*: 01.03.02 – Прикладная математика и информатика.

*Студент*: Денисов И.И.

*Научный руководитель*: Мкртичян В.В.

*Год защиты*: 2023.

*Тема работы*: Модификация современного криптографического агрегата.

*Цели работы*: Целями работы являются построение модификации не интерактивного протокола доказательства знания с нулевым разглашением "ZK-SNARK" путём расширения полиномиальной базы его квадратичной арифметической программы и анализ параметров модифицированного протокола.

*Задачи работы*:

– Изучение и описание протокола ZK-SNARK.

– Модификация протокола ZK-SNARK.

– Построение модельного примера для изначальной и модифицированной версий ZK-SNARK.

– Анализ параметров модифицированного протокола.

Заведующий кафедрой Б.Я. Штейнберг

Научный руководитель В.В. Мкртичян

Студент И.И. Денисов

21 сентября 2022 г