ПРИЛОЖЕНИЕ № 3

к Порядку организации

практической подготовки обучающихся,

утверждённому приказом от

«\_\_\_\_»\_\_\_\_\_\_\_20\_\_\_г. № \_\_\_\_\_\_\_\_\_\_\_

Федеральное государственное автономное образовательное  
учреждение высшего образования   
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт математики, механики и компьютерных наук им И.И. Воровича

*структурное подразделение*

*01.03.02 Прикладная математика и информатика*

*специальность/направление подготовки (код, наименование)*

**ОТЧЁТ**

**о прохождении практики**

обучающегося 4 курса

Фамилия \_\_\_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_\_*Денисов*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Имя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Илия\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Отчество (при наличии) \_\_\_\_\_Игоревич\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Место практики Институт математики, механики и компьютерных наук им И.И. Воровича

*наименование профильной организации /структурного подразделения Университета*

Вид практики: производственная

*учебная/производственная*

Тип практики: преддипломная

*указывается в соответствии с ОПОП*

Способ проведения практики: стационарная

*стационарная/выездная*

Сроки прохождения практики: *с 23.05.2023 по 05.06.2023*

**I. ЗАДАНИЕ ОБУЧАЮЩЕГОСЯ НА ПРАКТИКУ**

1. Провести обзор протокола Ethereum
2. Провести обзор протокола ZK-SNARK.
3. Модифицировать протокол ZK-SNARK.
4. Проанализировать модификацию протокола ZK-SNARK.

**II. ИНСТРУКТАЖ ПО ОЗНАКОМЛЕНИЮ С ТРЕБОВАНИЯМИ ОХРАНЫ ТРУДА, ТЕХНИКИ БЕЗОПАСНОСТИ, ПОЖАРНОЙ БЕЗОПАСНОСТИ, ПРАВИЛАМ ВНУТРЕННЕГО РАСПОРЯДКА**

|  |  |  |
| --- | --- | --- |
|  | **Инструктаж проведен** | **Ознакомлен** |
| по требованиям охраны труда | / Мкртичян В.В.  *(подпись и Ф.И.О руководителя практики университета)*  23 мая 2023 г. | / Денисов И.И.  *(подпись и Ф.И.О. обучающегося)*  23 мая 2023 г. |
| по техники безопасности |
| по пожарной безопасности |
| по правилами внутреннего трудового распорядка |

**III. ДНЕВНИК ПРАКТИКИ**

|  |  |
| --- | --- |
| Дата | Выполненные мероприятия в соответствии с заданием на практику |
| 23.05-01.06 | Изучен протокола Ethereum и проведен обзор протокола ZK-SNARK. Модифицирован протокол ZK-SNARK. |
| 02.06-05.06 | Проведен сравнительный анализ модификация протокола ZK-SNARK. |
|  |  |

**IV. АНАЛИЗ ПРОВЕДЁННОЙ РАБОТЫ В ПЕРИОД ПРОХОЖДЕНИЯ ПРАКТИКИ ОБУЧАЮЩИМСЯ**

*Раздел заполняется обучающимся в соответствии со спецификой практики (может содержать таблицы, графики, статистические данные и т.п.)*

|  |  |  |
| --- | --- | --- |
| № п/п | Выполненные мероприятия в соответствии с заданием на практику | Анализ проведенной работы |
| 1 | Изучен протокола Ethereum и проведен обзор протокола ZK-SNARK. Модифицирован протокол ZK-SNARK. | Был изучен протокола Ethereum, который является децентрализованной платформой для создания и запуска смарт-контрактов на базе блокчейна.  В рамках работы был также рассмотрен протокол ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Он используется в Ethereum для улучшения приватности и масштабируемости сети. ZK-SNARK позволяет проводить доказательства взаимодействия с данными без раскрытия самих данных, обеспечивая конфиденциальность и анонимность участников.  По результатам исследования был сделан вывод о возможности модифицировать процесс разбиения вычисления многочлена на действия. Описаны следствия модификации для построения системы векторов ограничений, квадратичной арифметической программы, случайного сдвига многочленов, а также протокола Пиноккио. |
| 2 | Проведен сравнительный анализ модификация протокола ZK-SNARK. | По результатам сравнительного анализа модификация протокола ZK-SNARK было выявлено, что размер достимого набора присваиваний сократился, однако увеличился объем данных в канале, необходимый для коммуникаций между двумя сторонами в рамках протокола ZK-SNARK. Также увеличился размер общей ссылочной строки. |

**ОТЗЫВ РУКОВОДИТЕЛЯ ПРАКТИКИ от УНИВЕРСИТЕТА**

*Отзыв оформляется руководителем практики от Университета в свободной форме с указанием полноты, своевременности и качества проведенной обучающимся работы*

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

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*зачтено/отлично/хорошо/удовлетворительно*

Руководитель практики

от Университета      / Мкртичян В.В

подпись Ф.И.О.