sФедеральное государственное автономное образовательное учреждение

высшего образования

«Национальный исследовательский университет «Высшая школа экономики»

Московский институт электроники и математики им. А.Н. Тихонова

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ, ВЫПОЛНЯЕМОЕ В ПЕРИОД ПРАКТИКИ**

студенту 5 курса очной формы обучения

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Астраханцеву Роману Геннадьевичу | | | | | | | |
| *(фамилия, имя, отчество при наличии)* | | | | | | | |
| образовательной программы | | | | | Компьютерная безопасность | | |
| уровня | | специалитет | | | | | |
| по специальности | | | 10.05.01 КБ | | | | |
| Вид практики | | | производственная | | | | |
| Тип практики | | | производственная | | | | |
| Место практики | | | МИЭМ НИУ ВШЭ | | | | |
| Срок прохождения практики | | | | | | с | 01.07.2021 |
|  |  |  | |  | | по | 31.07.2021 |

Цель прохождения практики[[1]](#footnote-1):

|  |
| --- |
| Построение модели пороговой схемы подписи с нулевым доверием |
|  |
|  |
|  |
| Задачи практики[[2]](#footnote-2): |
| 1. Построение алгоритма распределённой генерации ключа |
| 1. Построение распределённого алгоритма выработки подписи |
| 1. Модификация полученных алгоритмов в схему с нулевым доверием |
|  |
|  |
|  |
|  |

Содержание практики (вопросы, подлежащие изучению):

|  |  |
| --- | --- |
| 1. | Схемы разделения секрета (Шамира, VSS и др.) |
| 2. | Схема подписи Эль-Гамаля |
| 3. | Вычисление произведений секретов на основе их долей |
| 4. | Инверсия секретов на основе их долей |
| 5. | Мультиподпись блокчейна |
| 6. |  |
| 7. |  |
| Планируемые результаты: | |
| 1. | Уметь строить пороговые схемы с нулевым доверием |
| 2. | Уметь анализировать степень защищённости пороговых схем от раскрытия секретов |
| 3. |  |
| 4. |  |
| 5. |  |
| 6. |  |
| 7. |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Руководитель практики от НИУ ВШЭ: | | | | | | | | | | | | | | |
| Доцент | | | | | |  |  | | |  | Лось А.Б. | | | |
| *(должность)* | | | | | |  | *(подпись)* | | |  | *(фамилия, инициалы)* | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| СОГЛАСОВАНО | | | | | | | | | | | | | | |
| Руководитель практики студента от профильной организации/НИУ ВШЭ | | | | | | | | | | | | | | |
| Доцент | | | | | |  |  | | |  | Нестеренко А.Ю. | | | |
| *(должность)* | | | | | |  | *(подпись)* | | |  | *(фамилия, инициалы)* | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Задание принято к исполнению | | | | | | | | \_\_\_.\_\_\_.20\_\_\_ | | | | | | |
| Студент | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | | | |  | Астраханцев Р.Г. | | | | | | |  |
|  |  | *(подпись)* | | | |  | *(фамилия, инициалы)* | | | | | | |  |

1. В соответствии с программой практики. [↑](#footnote-ref-1)
2. В соответствии с программой практики. [↑](#footnote-ref-2)