Федеральное государственное автономное образовательное

учреждение высшего образования   
"Национальный исследовательский университет   
"Высшая школа экономики"

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

ЖУРНАЛ

производственной (преддипломной) практики студента

группы СКБ-171 5 курса

|  |
| --- |
| Компьютерная безопасность |
| (образовательная программа) |
| 10.05.01 |
| (код, наименование направления подготовки/специальности) |
| Астраханцев Роман Геннадьевич |
| (фамилия, имя, отчество студента) |

Начат 05.07.2021

Окончен 31.07.2021

Москва 2021 г.

|  |
| --- |
| Место прохождения практики: |
| Кафедра компьютерной безопасности |
| Должность, Ф.И.О. руководителя практики: |
| Доцент, Нестеренко Алексей Юрьевич |
| Инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка проведен: |

05.07.2021

Инструктирующий \_\_\_\_\_\_\_\_\_\_\_\_\_ / Нестеренко А.Ю (руководитель практики)

Инструктируемый \_\_\_\_\_\_\_\_\_\_\_\_\_ / Астраханцев Р.Г. (студент)

УЧЕТ ВЫПОЛНЕННОЙ РАБОТЫ

|  |  |  |
| --- | --- | --- |
| Дата | Содержание работы практиканта | Отметка о выполнении  в  выполнении |
| 5 июля | Изучение задач, решаемых пороговой подписью и принципов её построения | ✓ |
| 6 июля | Изучение задач, решаемых пороговой подписью и принципов её построения | ✓ |
| 7 июля | Изучение различных схем разделения секрета (Шамира, VSS, Блэкли и др.), их свойств | ✓ |
| 8 июля | Формирование базовой схемы генерации долей закрытого ключа с доверенным дилером на основе секрета Шамира | ✓ |
| 9 июля | Формирование базовой схемы генерации долей закрытого ключа с доверенным дилером на основе секрета Шамира | ✓ |
| 10 июля | Изучение различных методов выработки долей секрета с акцентом на генерацию без дилера | ✓ |
| 11 июля | Изучение различных методов выработки долей секрета с акцентом на генерацию без дилера | ✓ |
| 12 июля | Формирование требований к базовому алгоритму распределенной выработки ключа ключу на основе аддитивных свойств | ✓ |
| 13 июля | Формирование требований к базовому алгоритму распределенной выработки ключа ключу на основе аддитивных свойств | ✓ |
| 14 июля | Изучение схемы подписи Эль-Гамаля | ✓ |
| 15 июля | Изучение схемы подписи Эль-Гамаля | ✓ |
| 16 июля | Изучение возможности создания подписи в пороговой схеме на основе подписи Эль-Гамаля и проблем, возникающих при совместной выработки подписи | ✓ |
| 17 июля | Изучение возможности создания подписи в пороговой схеме на основе подписи Эль-Гамаля и проблем, возникающих при совместной выработки подписи | ✓ |
| 18 июля | Модификация схемы с генерацией долей закрытого ключа схемы Эль-Гамаля без дилера | ✓ |
| 19 июля | Модификация схемы с генерацией долей закрытого ключа схемы Эль-Гамаля без дилера | ✓ |
| 20 июля | Изучение алгоритмов получения произведения секретов на основе их долей без раскрытия самих секретов | ✓ |
| 21 июля | Изучение алгоритмов получения произведения секретов на основе их долей без раскрытия самих секретов | ✓ |
| 22 июля | Изучение алгоритмов получения произведения секретов на основе их долей без раскрытия самих секретов | ✓ |
| 23 июля | Реализация наиболее эффективного метода получения произведения секретов на основе из долей без раскрытия самих секретов | ✓ |
| 24 июля | Реализация наиболее эффективного метода получения произведения секретов на основе из долей без раскрытия самих секретов | ✓ |
| 25 июля | Формирование итогового алгоритма выработки пороговой подписи на основе схемы Эль-Гамаля с учетом всех рассмотренных вопросов | ✓ |
| 26 июля | Формирование итогового алгоритма выработки пороговой подписи на основе схемы Эль-Гамаля с учетом всех рассмотренных вопросов | ✓ |
| 27 июля | Анализ степени защищённости полученной пороговой схемы от раскрытия секретов | ✓ |
| 28 июля | Анализ степени защищённости полученной пороговой схемы от раскрытия секретов | ✓ |
| 29 июля | Написание отчёта с описанием принципов работы и построения пороговых схем | ✓ |
| 30 июля | Написание отчёта с описанием принципов работы и построения пороговых схем | ✓ |
| 31 июля | Написание отчёта с описанием принципов работы и построения пороговых схем | ✓ |

Студент практикант \_\_\_\_\_\_\_\_\_\_\_\_\_ /Астраханцев Р.Г./