МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

ОНК «Институт высоких технологий»

ОТЧЁТ

О ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ ТЕХНОЛОГИЧЕСКОЙ

(ПРОЕКТНО-ТЕХНОЛОГИЧЕСКОЙ) ПРАКТИКИ

на базе Высшей школы компьютерных наук и прикладной математики образовательно-научного кластера “Институт высоких технологий”

Выполнил Шаманов Юрий Альбертович \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

студент очной формы обучения 5 курса

специальности 10.05.01 – «Компьютерная безопасность», специализации "Математические методы защиты информации"

Руководитель практики от университета

доцент ОНК «ИВТ», к.т.н., доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ветров И.А.

г. Калининград 2024 г.

## СОДЕРЖАНИЕ

[Введение 2](#_sxvjgeza2zj4)

[Основная часть 3](#_to8ncbkz5apx)

[Заключение 6](#_gl1s8f6y41jy)

[Список литературы 7](#_1clqq8bycsje)

## Введение

Место прохождения практики – «Высшая школа компьютерных наук и искусственного интеллекта». В должностные обязанности практиканта входит исследование предложенного научного подхода к решению актуальных проблем криптографии, а именно исследование существующих подходов к построению PKI инфраструктуры на базе технологий блокчейн, а также создание обоснования к проведению дальнейшей работы по разработке собственных подходов к построению представителей данного семейства PKI инфраструктур.

**Целью** производственной практики является систематизация, обобщение и углубление теоретических знаний, формирование практических умений, общекультурных, профессиональных компетенций и профессиональных компетенций в сфере информационной безопасности и математических методов защиты информации. Исходя из должностных обязанностей и целей производственной практики, перед практикантом были поставлены следующие **задачи**:

* изучение существующей литературы в соответствии с целью и должностными обязанностями практиканта;
* перечисление существующих подходов к решению проблем, входящих в должностные обязанности практиканта;
* выявление актуальных нерешённых проблем в сфере исследования, согласно должностным обязанностям практиканта;
* создание обоснования проведения исследовательской работы;

## Основная часть

На сегодняшний день инфраструктура открытых ключей (Public Key Infrastructure - PKI) является одной из наиболее важных и эффективных систем, обеспечивающих аутентификацию, целостность данных (с помощью электронной подписи) и построение защищенных каналов передачи данных. РКІ касается практически каждого.

PKI - это комплексная система, основанная на использовании пары ключей - открытого и закрытого. Открытый ключ доступен всем пользователям и применяется для шифрования данных, в то время как закрытый ключ известен только владельцу и используется для расшифровки данных.

Важной составляющей PKI являются удостоверяющие центры (Certificate Authority - CA), которые отвечают за выпуск и управление сертификатами открытых ключей. Сертификаты являются электронными документами, подтверждающими подлинность открытых ключей и идентифицирующими их владельцев.

Некорректно утверждать, что PKI сама по себе представляет собой инфраструктуру безопасности, однако она может служить основой для создания всеобъемлющей инфраструктуры безопасности. Основная цель PKI заключается в управлении открытыми ключами и сертификатами, что позволяет организации поддерживать надежную сетевую среду. PKI предоставляет возможность использования сервисов шифрования и электронной подписи в соответствии с различными приложениями, функционирующими в среде открытых ключей.

Использование подписанных сертификатов даже крупнейшими центрами сертификации не исключает возможность атаки типа Man-in-the-Middle (MitM). Сущность проблемы заключается в том, что при использовании протоколов SSL/TLS браузер (и другие приложения) безоговорочно доверяет подписанным сертификатам. Для того чтобы браузер доверял сертификату, требуется присутствие отпечатка сертификата конкретного центра сертификации в браузере или операционной системе в качестве корневого. Все сертификаты, подписанные данным центром, автоматически становятся доверенными и валидными (при условии корректности временных рамок действия, имени домена и некоторых других, менее значимых параметров) для пользователя. Другими словами, если центр сертификации подпишет подставной сертификат на определенный домен (с технической точки зрения, выпустит легитимный сертификат), то его можно будет предъявить пользователю и осуществить атаку MitM.



Также существует атака на сертификационный центр. Если злоумышленник сможет скомпрометировать сертификационный центр, он сможет выпускать поддельные сертификаты, которые будут выглядеть подлинными. Однако, благодаря тому, что цепочка сертификатов хранится не в одном месте, а распределена между различными узлами сети, злоумышленник должен будет обладать контролем над более чем 51% мощностей сети, что делает атаку крайне дорогостоящей и сложно реализуемой.

Большая часть современных реализаций процесса выпуска сертификатов представляют собой "чёрный ящик", что создаёт неопределённость и непрозрачность в процессе генерации сертификатов. Благодаря блокчейн технологиям процесс создания, хранения и распространения сертификатов будут полностью прозрачны, что сильно повышает уровень доверия.

**Актуальность** темы заключается в поиске решения проблемы доверия в сети. Это особенно важно в контексте современных технологий, где конфиденциальность и безопасность данных становятся все более значимыми. Совмещение технологий блокчейн и инфраструктуры PKI (Public Key Infrastructure) предлагают инновационные подходы к решению этой проблемы. Это может привести к созданию более безопасных и надежных систем, которые будут способствовать развитию цифровых технологий и улучшению качества жизни людей.

**Целью** настоящей работы является исследование возможности разработать алгоритмы для системы, позволяющей решить проблему доверия в сети, используя технологию блокчейн и инфраструктуру PKI. Блокчейн представляет собой децентрализованную базу данных, которая позволяет хранить и передавать информацию без необходимости доверия к центральному органу. Каждый участник сети имеет доступ к полной истории транзакций, что обеспечивает прозрачность и надежность.

Для достижения указанной цели необходимо решить следующие **задачи**:

* Изучить алгоритмы создания сертификатов
* Изучить алгоритмы размещени в сети блокчейн
* Изучить алгоритмы идентификации и аутентификации владельца сертифика в сети блокчейн

PKI инфраструктура построенная на базе блокчейн технологий позволит осуществлять безопасное соединение без предварительного обмена сертификатами, что решит проблему недоверия полученного сертификата и возможную его фальсификацию во время передачи второму участнику обмена сообщениями в сети.

## Заключение

В ходе проделанной работы был проведён анализ существующих подходов к построению инфраструктуры открытых ключей (Public Key Infrastructure, PKI). В результате были выявлены основные недостатки этих подходов. Кроме того, было предложено обоснование актуальности дальнейшего исследования построения PKI инфраструктуры с использованием технологий блокчейн. Это необходимо для создания системы, которая позволит решить проблему доверия в сети.

Данная практика была необходима для систематизации, обобщения и углубления теоретических знаний, формирования практических умений, общекультурных, профессиональных компетенций и профессиональных компетенций в сфере информационной безопасности и математических методов защиты информации.

## Список литературы

1. Александр Кудрявцев. «Архитектура PKI» [Электронный ресурс]: <https://docs.google.com/presentation/d/1GqfF1bJ2gEFJ5TTDtJ9vIV24-9dKTY0nDcabEiwXKNQ/htmlpresent>
2. «LINUX.ORG.RU Проблема доверия центрам сертификации» [Электронный ресурс]: <https://www.linux.org.ru/forum/security/9591765>
3. «Первый ОФД Принцип работы ЭЦП» [Электронный ресурс]: <https://www.1-ofd.ru/blog/news/princip-raboty-ecp/>
4. «SC Labs | Networking notes» [Электронный ресурс]: <http://sclabs.blogspot.com/2012/10/ccna-security-chapter-7-cryptographic.html>
5. «What is a Public Key Infrastructure (PKI)?» [Электронный ресурс]: <https://www.essendi.ch/en/what_is_a_pki/>
6. «Информационная безопасность. Практика Информационной безопасности» [Электронный ресурс]: <http://dorlov.blogspot.com/2010/09/issp-06-4.html>
7. «The SSL Store» [Электронный ресурс]: <https://www.thesslstore.com/blog/how-pki-works/>

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

ОНК «Институт высоких технологий»

ДНЕВНИК

ПРОИЗВОДСТВЕННОЙ

ПРАКТИКИ

г. Калининград 2024 г.

**1.Информационная часть**

Шаманов Юрий Альбертович, студент очной формы обучения \_\_\_курса группы 05\_КБ\_19\_О\_/

специальности 10.05.01 – «Компьютерная безопасность», специализации "Математические

методы защиты информации" в соответствии с приказом № \_\_\_ от \_\_\_ \_\_\_\_\_ 2024 г.

направляется на производственную практику в Высшую школу компьютерных наук и

прикладной математики образовательно-научного кластера “Институт высоких технологий”

Период практики – с 24.06.2024 г. по 06.07.2024 г.

Руководитель практики от университета – доцент ОНК «ИВТ», к.т.н., доцент Ветров Игорь Анатольевич

ОНК «Институт высоких технологий»

Контактный номер телефона +7 (4012) 338 217

Первый заместитель

директора ОНК «ИВТ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шпилевой А.А.

**2. Программа практики**

**2.1. План работы**

| **№ п.п.** | **Рабочее место практиканта, вид работы** | **Продолжительность**  **(в днях)** |
| --- | --- | --- |
| **1.** | Компьютерный класс 315А | **10 дней** |

**2.2. Индивидуальное задание по профилю подготовки/специальности**

1. Пройти инструктаж по технике безопасности.
2. Ознакомиться с должностными обязанностями.
3. Изучить существующую литературу в соответствии с должностными обязанностями практиканта.
4. Создать обоснование проведения дальнейшей исследовательской работы.
5. Написать отчет по практике.

Руководитель практики от университета –

доцент ОНК «ИВТ», к.т.н., доцент Ветров И.А. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3. Ход выполнения практики**

| **№ п.п.** | **Дата** | **Описание выполненной работы** | **Отметки**  **руководителя практики**  **(руководителя ВКР)** |
| --- | --- | --- | --- |
|  | 24.06.24 | Инструктаж по технике безопасности, ознакомление с правилами внутреннего трудового распорядка, обязанностями специалиста и с требованиями охраны труда. |  |
|  | 25.06.24 | Изучение нормативно-правовой документации места проведения практики |  |
|  | 26.06.24 | Изучение существующей литературы для выполнения должностных обязанностей практиканта |  |
|  | 27.06.24 | Изучение существующей литературы для выполнения должностных обязанностей практиканта |  |
|  | 28.06.24 | Анализ существующих подходов к решению проблем, согласно должностным обязанностям практиканта |  |
|  | 01.07.24 | Анализ существующих подходов к решению проблем, согласно должностным обязанностям практиканта |  |
|  | 02.07.24 | Выявление нерешённых проблем, согласно должностным обязанностям практиканта |  |
|  | 03.07.24 | Сбор и систематизация полученной в ходе выполнения практики информации |  |
|  | 04.07.24 | Создание обоснования к проведению дальнейшей исследовательской работы, согласно должностным обязанностям практиканта |  |
|  | 05.07.24 | Создание обоснования к проведению дальнейшей исследовательской работы, согласно должностным обязанностям практиканта |  |
|  | 06.07.24 | Оформление отчета по практике, систематизация и обобщение полученной информации. |  |

**4. Отзыв руководителя практики**

**Отзыв о работе студента руководителя практики от университета**

Шаманов Юрий Альбертович, студент очной формы обучения \_\_ курса группы 05\_КБ\_19\_О\_/

специальности 10.05.01 – «Компьютерная безопасность», специализации "Математические методы защиты информации" в соответствии с приказом № \_\_\_\_ от \_\_ \_\_\_\_ 2024 г. направлен на производственную практику в Высшую школу компьютерных наук и прикладной математики образовательно-научного кластера “Институт высоких технологий”

Период практики – с 24.06.2024 г. по 6.07.2024 г.

Программа практики и индивидуальное задание на практику выполнены. Отчёт по практике сдан и защищён на отчётной конференции.

Производственная практика оценена на оценку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики от университета –

доцент ОНК «ИВТ», к.т.н., доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ветров И.А.

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.