|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| logoМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| **ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)** | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| **Департамент информационной безопасности** | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | | |
| о прохождении Производственной практики. Организационно-управленческой практики | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнил студент  гр. Б9123-10.03.01отзи | | | | | | | | | |
|  |  |  | | | | | | | Брустовский А.М. | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | | |  | |
|  | | | | | | | | | |  |  | Доцент департамента  информационной безопасности ИМКТ | | | | | | | | | |
|  | | | |  | | Боршевников А.Е. | | | |  |  |  | | | | |  | Боршевников А.Е. | | | |
| (подпись) | | | |  | | (И.О. Фамилия) | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | | |
| « |  | » |  | | | | | | 2024 г. |  |  |  | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | | |
| « |  | » |  | | | | | | 2024 г. |  |  | с | « | 22 | » | июля | | | | | 2024 г. |
|  | | | | | | | | | |  |  | по | « | 03 | » | августа | | | | | 2024 г. |
|  | | | | |  | | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | | |
| (подпись) | | | | |  | | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | Департамент информационной | | | | | | | | | |
|  | | | | | | | | | |  |  | безопасности ИМиКТ ДВФУ | | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | | |
| 2024 | | | | | | | | | | | | | | | | | | | | | |

**Содержание**

[Цели практики 3](#_Toc173532533)

[Введение 4](#_Toc173532534)

[Задание 1 5](#_Toc173532535)

[Задание 2 9](#_Toc173532536)

[Заключение 19](#_Toc173532537)

[Список используемых источников 20](#_Toc173532538)

# **Цели практики**

1. Научиться работать с электронными подписями;
2. Провести исследование одной из предложенных специальностей, связанных с компьютерной безопасностью;

# **Введение**

Учебная практика. Ознакомительная практика проходила в департаменте информационной безопасности ИМиКТ ДВФУ в период с 22 июля 2024 по 03 августа 2024 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности.

Задачи практики:

1. Выполнение заданий, представленных преподавателем.
2. Подготовка доклада о выполненных заданиях и его защита.

# **Задание 1**

**Работа с цифровыми подписями**

1. Подготовлен файл для отправки. Результат работы представлен на рисунке 1.

A person in a black dress

Description automatically generated

Рисунок 1 – Файл для отправки

1. Файл подписан и зашифрован. Результат работы представлен на рисунке 2.

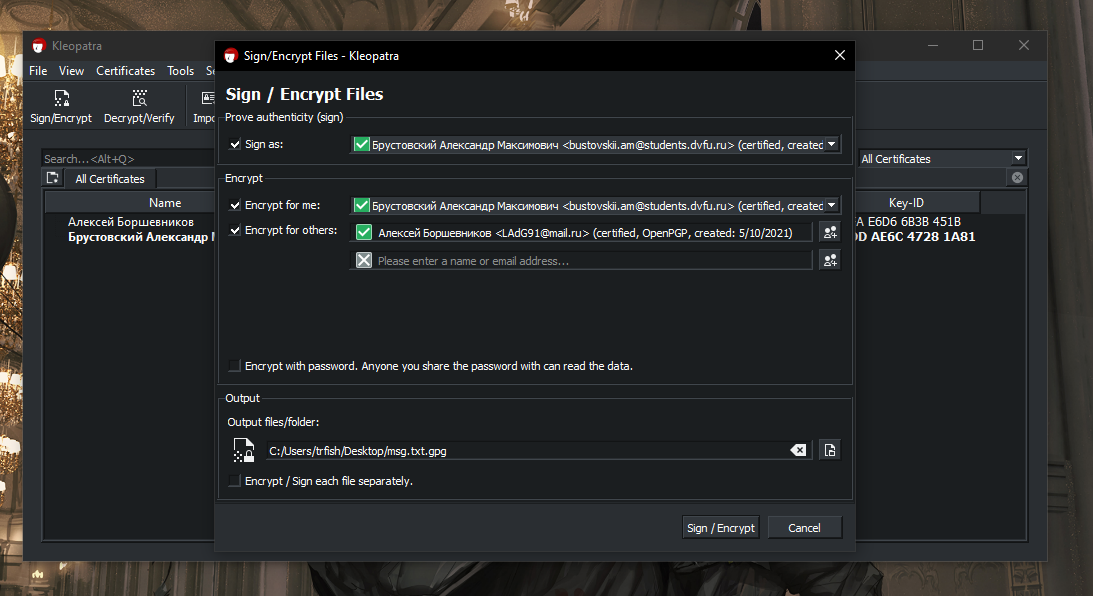


Рисунок 2 – Зашифрованный файл

1. Зашифрованный файл и открытый ключ отправлены научному руководителю. Результат работы представлен на рисунке 3.

A screenshot of a computer

Description automatically generated

Рисунок 3 – Зашифрованный файл и открытый ключ

1. Получен ответ. Результат работы представлен на рисунке 4.

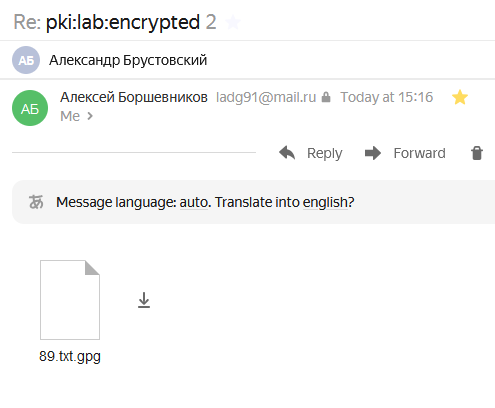


Рисунок 4

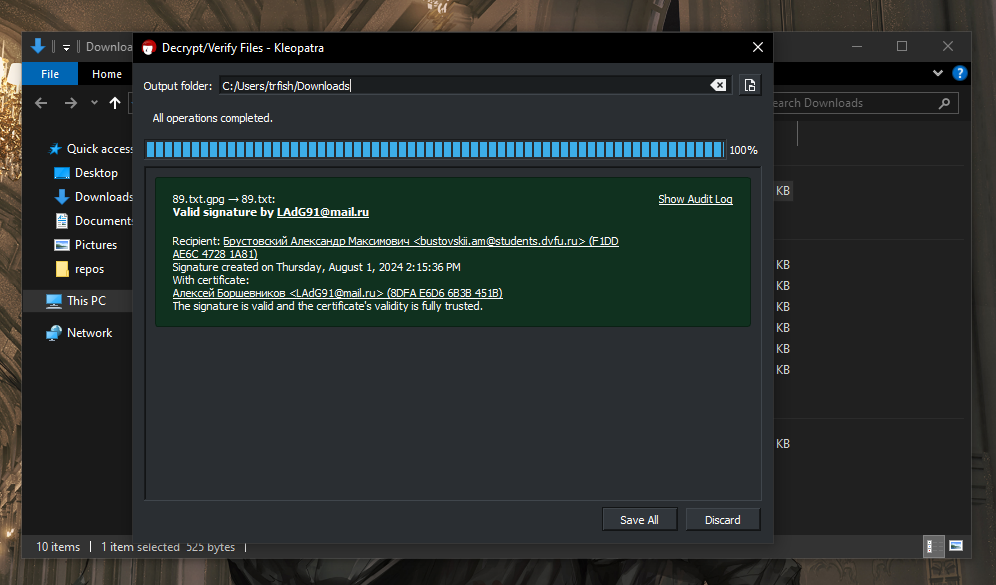
1. Расшифрован файл. Результат работы представлен на рисунке 5 и 6.

Рисунок 5

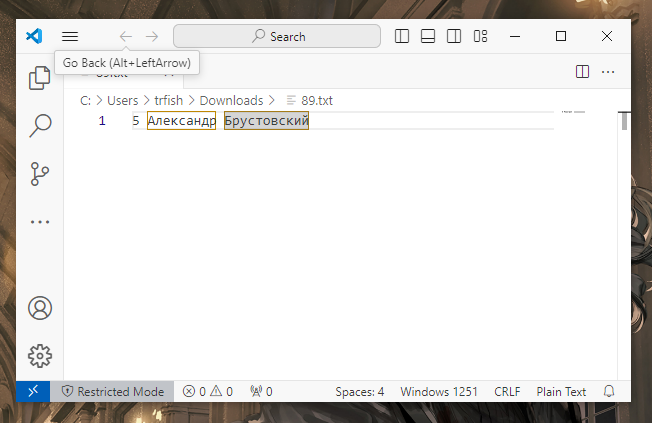


Рисунок 6

1. Задание выполнено. Результат работы представлен на рисунке 6.  
   A screenshot of a computer

   Description automatically generated

Рисунок 7

# **Задание 2**

**Ознакомление с профессией DevSecOps-разработчика.**

DevSecOps-разработчик – это высококвалифицированный специалист IT-сферы. Он отвечает за автоматизацию процесса создания приложений на каждом из этапов и обеспечивает взаимодействие программистов и системных администраторов. DevSecOps-инженер должен быть ответственным и грамотным специалистом, знать операционные системы и владеть навыками программирования, понимать, как устроена и по каким принципам работает методология DevSecOps, знать принципы работы ИБ-практик.

Аббревиатура DevSecOps расшифровывается как **Development Security Operations** (Разработка Безопастность Эксплуатация). Эта методология дополняет практику создания и поддержки программного обеспечения (DevOps), которая устраняет разрыв между интересами разработчиков, тестировщиков и пользователей, повышает эффективность производства программных продуктов и ускоряет разработку их новых версий.

**Обязанности DevSecOps-разработчика:**

1. Разработка безопасной архитектуры приложений: Проектирование и разработка архитектуры приложений с учетом требований безопасности. Обеспечение надежной защиты информации и мер противодействия различным атакам и утечкам данных.
2. Внедрение и автоматизация процессов безопасности: Создание и внедрение автоматизированных процессов безопасности в рамках команды разработки. Оптимизация процессов и обеспечение безопасности на всех этапах разработки и эксплуатации приложений.
3. Проведение аудитов безопасности: Проведение аудитов безопасности, включая проверку уязвимостей в коде приложений и инфраструктуре. Анализ угроз и рисков, разработка рекомендаций по устранению уязвимостей.
4. Обеспечение безопасности DevOps-процессов: Контроль безопасности всего цикла разработки, включая использование инструментов и технологий DevOps. Разработка и внедрение архитектуры безопасной поставки программного обеспечения.
5. Развитие инфраструктуры безопасности: Обновление и развитие инфраструктуры безопасности, включая инструменты и технологии для обеспечения безопасности программных продуктов и процессов разработки.
6. Анализ безопасности системы: Анализ безопасности разрабатываемой системы, проведение аудита кода, идентификация уязвимостей. Использование инструментов автоматизации для сканирования и обнаружения уязвимостей.
7. Внедрение безопасности на всех этапах разработки: Интеграция безопасности в каждый этап разработки ПО. Применения безопасных методов разработки, таких как тестирование безопасности и кодирование безопасности.
8. Разработка безопасных процедур: Разработка и внедрение безопасных процедур в рамках разработки ПО. Определение требований безопасности для работы команды разработчиков и создание систем мониторинга и оповещения.
9. Отладка и исправление уязвимостей: Участие в процессе отладки и исправления уязвимостей в разрабатываемом ПО. Тестирование на безопасность и анализ результатов для выявления и устранения возможных уязвимостей.
10. Сотрудничество с командой эксплуатации: Сотрудничество с командой эксплуатации для обеспечения безопасной эксплуатации разработанного программного обеспечения. Разработка и внедрение мониторинга и аналитики безопасности.

**Исследование рынка труда:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Организация | Вакансия | Требования | Заработная плата |
| 1 | [Межрегиональный ТранзитТелеком (АО МТТ)](https://hh.ru/employer/12034?hhtmFrom=vacancy) | DevSecOps | **Задачи:**  Разрабатывать технические требования по применению практик безопасной разработки;  Реализовать контроль dev/test/prod окружений в части compliance требований и best practice;  Разрабатывать гайды, инструкции, архитектурные и процессные схемы;  Участвовать в реализация концепции Zero-trust;  Участвовать в выстраивании взаимодействия продуктовых команд и команд DevSecOps, AppSec;  Контролировать соблюдение практик безопасной разработки;  Контролировать соблюдение выставленных требований;  Осуществлять взаимодействие, оказывать экспертную продуктовым командам по вопросам безопасной разработки;  Заниматься настройкой, интеграцией и развитием инструментов безопасности;  Исследовать вопросы безопасности различных технологий.  Вы нам подходите, если у Вас есть:  Опыт разворачивания и применения инструментов безопасной разработки (SAST, DAST, CS и др);  Опыт построения и развития инженерных практик DevSecOps, их масштабирования в pipeline;  Опыт разработки архитектур, проектирования информационных систем, систем безопасной разработки;  Опыт работы с docker/podman, k8s;  Опыт работы с одним или несколькими инструментами CI/CD (Gitlab/Teamcity/Jenkins);  Опыт работы с системами коллективного взаимодействия, администрирования проектов и репозиториев (Git, Confluence, Jira );  Опыт работы с продуктовыми командами разработки по Agile методологии;  Понимание концепций Shift-Left, Zero-Trust.  **Желательно:**  Английский язык уровня B1 и выше;  Опыт разработки на одном из языков: Go, JS;  Умение писать скрипты на Python / Bash / Powershell. | [з/п не указана](https://ufa.hh.ru/vacancy/105066946?hhtmFromLabel=similar_vacancies_sidebar&hhtmFrom=vacancy" \t "_blank) |
| 2 | [СберСпасибо](https://hh.ru/employer/4315301?hhtmFrom=vacancy) | DevSecOps | **Основные обязанности:**  Проектирование ИБ-решений по направлению DevSecOps;  Консультирование и поддержка команд разработки по вопросам КБ и практикам написания безопасного кода;  Разработка архитектуры решений и методов реализации;  Сбор и анализ предварительной информации о исходном коде АС;  Разработка политик, правил технических требований к интеграции с репозиториями исходного кода и системами разработки;  Настройка анализаторов и проведение сканирования исходных кодов, приложений (SAST/DAST);  Автоматизация процессов сканирования;  Выявления ложных срабатываний, разработка/корректировка правил;  Подготовка отчетов об уязвимостях и рекомендаций по их устранению;  Участие в разработке проектной, эксплуатационной документации, подготовке инструкций и формирования базы знаний;  Взаимодействие с разработчиками прикладного ПО и профильными специалистами при внедрении нового функционала и устранении уязвимостей.  **Что ждем от вас:**  Образование высшее техническое/либо профильные курсы повышения квалификации;  Опыт работы на должностях: инженер, специалист по направлению AppSec/DevSecOps;  Опыт разработки на Java;  Опыт внедрения, администрирования и сопровождения решений DevSecOps, Application Security, понимание принципов CI/CD;  Опыт участия в проектах внедрения решений по КБ, в частности в построении, внедрении, поддержки и модернизации подходов SSDLC или DevSecOps;  Знание стандартов и практик обеспечения безопасности ПО и выявления уязвимостей;  Опыт работы с решениями класса SAST, DAST, опыт анализа и интерпретации отчетов об обнаруженных уязвимостях;  Английский язык (чтение технической литературы).  **Будет плюсом:**  Опыт построения CI/CD с использованием DevSecOps продуктов;  Опыт разработки проектных решений и рабочей документации. | [з/п не указана](https://ufa.hh.ru/vacancy/105066946?hhtmFromLabel=similar_vacancies_sidebar&hhtmFrom=vacancy" \t "_blank) |
| 3 | Finbridge | DevSecOps | Твои задачи:  Формирование и контроль выполнения требований ИБ к процессам CI/CD и инфраструктуре разработки;  Внедрение, настройка и управление средствами информационной безопасности в средах CI/CD: инструменты анализа уязвимостей в образах docker, анализа open-source библиотек, анализа кода приложений и т.д.;  Организация, поддержка и развитие процесса безопасной разработки (SSDLC);  Проведение анализа кода разрабатываемых в компании продуктов на наличие уязвимостей, подготовка рекомендаций по их устранению и контроль выполнения;  Внедрение метрик работоспособности в готовые приложения для повышения эксплуатационного качества сервисов;  Создание и поддержка в актуальном состоянии документации по обеспечению информационной безопасности приложений.  Наши ожидания:  Высшее образование в области информационных технологий, кибербезопасности, информационной безопасности, или смежных областях;  Знание и опыт администрирования операционных систем семейства Linux;  Знание стека протоколов TCP/IP, модели OSI;  Знание уязвимостей из OWASP Top 10, OWASP Mobile Top 10, CWE;  Знание современных методов безопасного кодирования;  Знание архитектуры и понимание принципа работы микросервисных приложений;  Понимание принципов организации безопасности API, опыт тестирования безопасности;  Знание и опыт работы с методологиями Secure SDLC, DevSecOps;  Понимание принципов работы CI/CD;  Опыт работы с инструментами безопасности SCA/OSA, SAST, DAST, Fuzzing, SBOM, Secret management, Vulnerability management и т.д., встраивание их в процесс разработки;  Опыт работы с системами контейнеризации (Docker) и оркестрации (Docker-compose, Kubernetes), знания методов по обеспечению безопасности в них;  Опыт работы с инструментами DevOps (Gitlab (пайплайны), Vault, Ansible и др.);  Опыт встраивания процессов и практик безопасной разработки в жизненный цикл программного обеспечения;  Опыт настройки мониторинга (Zabbix, ELK, Prometheus и др.);  Знание НПА в области информационной безопасности (PCI DSS, ФЗ-152 и др.);  Знание английского языка не ниже уровня чтения технической документации; Опыт работы от 2-х лет. | [з/п не указана](https://ufa.hh.ru/vacancy/105066946?hhtmFromLabel=similar_vacancies_sidebar&hhtmFrom=vacancy" \t "_blank) |

**На основе анализа рынка труда можно выделить следующее:**

1. **Образование и квалификация**:

Необходимо иметь высшее техническое образование в области информационных технологий, кибербезопасности, информационной безопасности или смежных областях.

Необходимо пройти курсы повышения квалификации в профильной области.

1. **Опыт работы**:

Необходимо иметь опыт работы на должностях DevSecOps, AppSec или инженера по информационной безопасности.

Необходимо иметь опыт внедрения и администрирования решений DevSecOps, CI/CD и инструментов безопасности.

Необходимо иметь опыт работы с контейнеризацией (Docker, Kubernetes) и оркестрацией.

Необходимо иметь опыт разработки на различных языках программирования (Java, Go, JS) и написания скриптов (Python, Bash, Powershell).

1. **Технические знания**:

Необходимо знать и иметь опыт работы с методологиями Secure SDLC, DevSecOps.

Необходимо знать уязвимости из OWASP Top 10, OWASP Mobile Top 10, CWE.

Необходимо знать протоколы TCP/IP, модель OSI, принципы безопасности API.

Необходимо знать архитектуру микросервисных приложений и современные методы безопасного кодирования.

1. **Дополнительные навыки**:

Необходимо знать английский язык для чтения технической документации.

Необходимо знать НПА в области информационной безопасности (PCI DSS, ФЗ-152 и др.).

Необходимо иметь навыки встраивания процессов и практик безопасной разработки в жизненный цикл программного обеспечения.

#### Задачи и обязанности

1. **Технические требования и архитектура**:

Требуется разрабатывать и контролировать соблюдение технических требований по применению практик безопасной разработки.

Требуется создавать и поддерживать документацию, гайды, инструкции.

Требуется проектировать ИБ-решения, архитектуру систем и методы реализации.

1. **Инструменты безопасности**:

Требуется настраивать и управлять инструментами анализа уязвимостей (SAST, DAST, CS и др.).

Требуется интегрировать средства информационной безопасности в процессы CI/CD.

1. **Анализ и автоматизация**:

Требуется автоматизировать процессы сканирования исходного кода и приложений.

Требуется проводить анализ кода на наличие уязвимостей и разрабатывать рекомендации по их устранению.

1. **Взаимодействие с командами**:

Требуется консультировать и поддерживать команды разработки по вопросам кибербезопасности.

Требуется взаимодействовать с продуктовыми командами разработки по Agile методологии.

1. **Документация и compliance**:

Требуется разрабатывать и поддерживать документацию по обеспечению информационной безопасности.

Требуется контролировать выполнение требований безопасности и compliance.

**Как сертифицироваться в данной области?**

Для сертификации специалистов существует множество популярных крупных организаций, имеющих свои сертификационные программы.

Некоторые из самых распространенных сертификаций в области информационной безопасности включают:

1. CompTIA Security+. Сертификат начального уровня, который охватывает основы кибербезопасности, от угроз и уязвимостей до протоколов управления рисками.

2. CompTIA Linux+. Сертификат, который поможет освоить управление дистрибутивами Linux, от управления программным обеспечением и сервисами до сценариев и безопасности.

3. AWS Certified Developer — Associate. Сертификат, который демонстрирует навыки разработки и управления приложениями на основе AWS для реальных случаев использования DevSecOps.

4. Certified Kubernetes Administrator (CKA). Сертификат, который подтверждает способность управлять кластерами Kubernetes.

5. Сертифицированный менеджер по информационной безопасности (CISM). Сертификация Certified Information Security Manager (CISM) проводится ISACA. Она была разработана для руководителей, которые занимаются управлением программой информационной безопасности компании. Это еще один сертификат, который не относится строго к DevSecOps, но он охватывает элементы управления безопасностью и рисками, которые имеют решающее значение в средах DevSecOps.

6. Сертифицированный специалист по безопасному программному обеспечению жизненного цикла (CSSLP). Сертификация Certified Secure Software Lifecycle Professional (CSSLP) - еще одно предложение ISC2. Оно ориентировано на лучшие практики разработки безопасного программного обеспечения. CSSLP охватывает множество тем, которые имеют решающее значение для обеспечения разработки программного обеспечения с учетом безопасности в качестве первого шага.

7. Сертифицированный специалист по облачной безопасности (CCSP). Сертификат Certified Cloud Security Professional (CCSP) - еще одно предложение ISC2. Основное внимание в нем уделяется облачной безопасности, что является преимуществом, поскольку многие проекты DevSecOps размещаются в облачных средах.

# **Заключение**

Для достижения данной цели, в процессе прохождения Учебной практики. Ознакомительной практики были рассмотрены электронные подписи, профессия DevSecOps-разработчика.

В ходе работы были выполнены все практические задания от руководителя, а также были изучены требования на рынке труда к специалистам для того, чтобы занять должность DevSecOps-разработчика.

В результате был подготовлен данный отчёт, а также доклад с презентацией.

По итогам прохождения практики все задачи были выполнены, а цель достигнута. Данный отчёт планируется защищать перед руководителем практики.

# **Список используемых источников**

1. О профессии - <https://it-vacancies.ru/blog/vakansiia-devsecops-inzener/>
2. Вакансия 1 - <https://hh.ru/vacancy/101714582?hhtmFromLabel=similar_vacancies&hhtmFrom=vacancy>
3. Вакансия 2 - <https://hh.ru/vacancy/103595059?hhtmFromLabel=similar_vacancies&hhtmFrom=vacancy>
4. Вакансия 3 – <https://ufa.hh.ru/vacancy/102704871?query=DevSecOps&hhtmFrom=vacancy_search_list>
5. О сертификации – <https://www.developer.com/project-management/devsecops-project-management-certifications/>