Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования

«Пермский национальный исследовательский

политехнический университет»

(ПНИПУ)

Электротехнический факультет
Кафедра «Информационные технологии и автоматизированные системы»
Направление: 09.03.04 «Программная инженерия»

УТВЕРЖДАЮ

Зав. кафедрой ИТАС

Профессор, Доктор

экономических наук

_____ Р.А. Файзрахманов

«___» _____ 2024г.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

на распределенную производственную практику

студента группы РИС-21-1бзу

Дерябина Кирилла Николаевича

---

1. Тема индивидуального задания: Исследование утилиты автоматического тестирования на проникновение «Deep Exploit» и разработка методов противодействия

2. Цель: Анализ работы утилиты «Deep Exploit», принципов работы RCE уязвимостей.

3. Календарный план проведения производственной практики

№	Наименование этапа	Наименование работ	Сроки		Отметка о выполнении работы
			начало	окончание	
1	**1 этап (основной)**	Изучение и анализ утилиты автоматического тестирования на проникновение «Deep Exploit» Анализ принципов работы RCE уязвимостей, их недопущения при написании кода. Анализ механизмов защиты от RCE уязвимостей (stack canary, DEP, NX-bit, ASLR) Изучение и анализ принципа обхода механизма защиты ASLR.	19.02.2024	05.03.2024	
2	**2 этап (итоговый)**	Составление отчета по практике	06.03.2024	08.03.2024	

4. Место прохождения производственной практики:
ООО «Бигпринтер цифровые инновации»

5. Срок сдачи студентом отчета по производственной практике и отзыва руководителя практики от профильной организации руководителю практики от кафедры:

_____

6. Содержание отчета: введение, основная часть, заключение, список использованных источников

7. Требования к разрабатываемой отчетной документации

Результаты производственной практики должны быть оформлены в форме отчета по практике в соответствии с требованиями ГОСТ 7.32–2017 «Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления».

Руководитель практики

от кафедры _____ (Д.Б. Кузнецов)

(подпись)

Руководитель практики

от профильной организации _____ (М.А. Попов)

(подпись)

Задание принял к исполнению _____ (К.Н. Дерябин)

(подпись) (Ф.И.О)

«___» _____ 2024 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

«Пермский национальный исследовательский политехнический университет»

(ПНИПУ)

Электротехнический факультет
Кафедра «Информационные технологии и автоматизированные системы»
Направление: 09.03.04 «Программная инженерия»

ДНЕВНИК

производственной практики студента

РИС-21-1бзу учебной группы 3го курса

Дерябина Кирилла Николаевича

Начат 19.02.2024

Окончен 08.03.2024

Пермь 2024

Место прохождения практики: ООО «Бигпринтер цифровые инновации»

Должность, Ф.И.О. непосредственного руководителя практики от профильной организации:

Руководитель департамента разработки программно-аппаратных комплексов, Главный специалист по программному обеспечению: Попов М.А.

УЧЕТ ВЫПОЛНЕННОЙ РАБОТЫ

Дата	Краткое содержание работы практиканта и указания руководителей практики	Отметка о выполнении работы (оценка и подпись руководителя практики)
19.02.2024	Изучение утилиты Metasploit framework	
20.02.2024	Изучение утилиты DeepExploit	
21.02.2024	Изучение архитектуры x86	
22.02.2024	Изучение архитектуры x64	
23.02.2024	Изучение процесса трансляции кода	
26.02.2024	Изучение конструкций, генерируемых компиляторами msvc и gcc с языка C.	
27.02.2024	Изучение принципов работы и видов RCE уязвимостей.	
28.02.2024	Изучение механизмов защиты от последствий переполнения буфера (ASLR, DEP, NX-bit, stack canary).	

29.02.2024	Изучение уязвимости утечки адресов. Изучение методов обхода механизма ASLR	
01.03.2024	Изучение ROP (oriented programming) и принципа использования гаджетов	
04.03.2024	Изучение документации и примеров по сетевому программированию. Реализация демо клиента на UDP сокете для отправки команд локальному уязвимому серверу.	
05.03.2024	Реализация уязвимого демо сервера на UDP сокете, для выполнения RCE локально.	
06.03.2024	Подготовка отчета по практике	
07.03.2024	Подготовка отчета по практике	
08.03.2024	Подготовка отчета по практике	

Студент-практикант Дерябин К.Н. / _____

подпись

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

«Пермский национальный исследовательский политехнический университет»

(ПНИПУ)

Электротехнический факультет
Кафедра «Информационные технологии и автоматизированные системы»
Направление: 09.03.04 «Программная инженерия»

О Т Ч Е Т

по производственной практике

Выполнил студент гр.
РИС-21-1бзу
Дерябин К.Н.

_____
(подпись)

Проверили:

Гл. специалист по ПО
М.А. Попов

_____ _____
(оценка) (подпись)

_____
(дата)

Ст.пр. Д.Б. Кузнецов

_____ _____
(оценка) (подпись)

_____
(дата)

Пермь 2024

ОТЗЫВ-ХАРАКТЕРИСТИКА

о результатах прохождения практики

Обучающийся Дерябин Кирилл Николаевич проходил производственную практику (по получению первичных профессиональных умений и навыков) в период с. 19.02.2024 по 08.03.2024 в ООО «Бигпринтер цифровые инновации».

На время прохождения практики Дерябину Кириллу Николаевичу поручалось решение следующих задач:

Ознакомление с научной литературой, составление отчета по заданной теме практики, изучение и анализ утилиты автоматического тестирования на проникновение «DeepExploit», изучение архитектур x86/x64, конструкций генерируемых компиляторами языков высокого уровня, принципов работы уязвимостей удаленного выполнения кода (RCE), их эксплуатации и предотвращения. Изучить механизмы защиты DEP, NX-bit, ASLR, stack canary. Реализовать уязвимое демо приложение и продемонстрировать работу уязвимости. Исправить проблему безопасности.

За время прохождения практики обучающийся проявил активность, дисциплину, место проведения практики посещал регулярно.

(навыки, активность, дисциплина, помощь организации, качество и достаточность собранного материала для отчета и выполненных работ, поощрения и т. п.)

Индивидуальное задание выполнено, решения по порученным задачам предложены, материал собран полностью.

Руководитель практики

от профильной организации _____ (М.А. Попов)

(подпись)

«___» _____2024г.