Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет «Высшая школа экономики»

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

Направление подготовки
«10.04.01 Информационная безопасность»
Образовательная программа **«Информационная безопасность киберфизических систем»**

О Т Ч Е Т
о прохождении
производственной практики

Студент Новиков В.С. МКБ 241
(Фамилия И.О.) номер группы

Руководитель практики студента:
тех. директор АО ТК Конвай Плюс Самиров Д.А.
должность и место работы Фамилия И.О. подпись

Руководитель практики от НИУ ВШЭ:
Зав. каф. информационной безопасности киберфизических систем департамента электронной инженерии МИЭМ НИУ ВШЭ Евсютин О.О.
должность и место работы Фамилия И.О. подпись

Практика пройдена с оценкой десять (10)
Дата 09.06.2025

Москва, 2025

СОДЕРЖАНИЕ

1. Введение

Целью прохождения производственной практики является получение профессиональных умений и опыта профессиональной деятельности, в первую очередь научно-исследовательской работы.

Задачи практики:

– закрепление и углубление теоретических знаний по прослушанным за время обучения в университете дисциплинам;

– адаптация студента к реальным условиям работы в различных учреждениях и организациях, приобретение опыта работы в трудовых коллективах, планирование работы в организации, коммуникация и общение в сфере будущей профессиональной деятельности;

– создание условий для практического применения знаний в области информационной безопасности;

– формирование и совершенствование базовых профессиональных навыков и умений в области применения современных информационных технологий к задачам информационной безопасности;

– выполнений обязанностей на первичных должностях в области обеспечения информационной безопасности;

– диагностика профессиональной пригодности студента к профессиональной деятельности;

– формирование информационной компетентности с целью успешной работы в профессиональной деятельности;

– обеспечение успеха дальнейшей профессиональной карьеры.

2. Краткая характеристика организации

АО «Телекоммуникационная компания «Конвей Плюс» является центром IT-компетенций для компаний международной транспортной группы, которые осуществляют транспортировку грузов водным транспортом и их перевалку в российских портах, а также оказывают услуги в логистике и судостроении. Компания реорганизована в 2018 г. с целью концентрации в единой структуре профессионалов и технических мощностей в области IT. Центральный офис расположен в Санкт-Петербурге, обособленные подразделения - в Москве, Нижнем Новгороде, Таганроге и Туапсе.

3. Описание профессиональных задач

В период производственной практики студент выполнял комплекс прикладных задач, направленных на повышение киберустойчивости телекоммуникационной компании «Конвей Плюс». Все задачи соответствовали целям магистерской программы «Информационная безопасность» и индивидуальному заданию, обеспечивая развитие как технических, так и организационных компетенций.

1. **Аудит внешнего периметра организации.**
    - Проведена полно-текстовая инвентаризация публичных ИТ-активов: сканирование диапазонов IP-адресов и доменных имён компании с помощью *nmap* и дополнительных скриптов, что позволило выявить полный перечень опубликованных сервисов.
    - Выполнено стратифицированное тестирование узлов (баннер-граббинг, проверка версий ПО, быстрая атака словарными паролями), после чего составлен детализированный отчёт о рисках с категоризацией уязвимых сервисов по CVSS и бизнес-критичности.
    - Совместно с ИТ-департаментом разработан и реализован план сокращения поверхности атаки: закрытие избыточных портов, миграция критичных сервисов во внутренние DMZ/VPN-сегменты, настройка WAF-правил.
2. **Аудит учётных записей в домене компании.**
    - Через hashcat запущено пассивное сравнение хешей с базами утекших паролей; выполнение *Kerberoasting*-процедур позволило выявить скомпрометированные и предсказуемые пароли.
    - Инициирована принудительная смена слабых паролей и усилена политика паролей (длина, сложность, срок действия), о чём издан внутренний приказ.
3. **Освоение и практическое применение специализированных средств защиты информации.**
    - **MaxPatrol VM:** настройка скан-профилей, интерпретация отчётов, формирование задач на устранение уязвимостей.
    - **Kaspersky KUMA (SIEM):** построение корреляционных правил на основе MITRE ATT&CK для обнаружения сетевой разведки и попыток перебора паролей.
    - **Kaspersky Endpoint Security:** настройка политик антивирусной защиты и контроля устройств.
    - **nmap и Wireshark:** углублённое сканирование пакетов и разбор аномального трафика при расследовании инцидентов.

Реализация указанных задач позволила студенту не только оценить и снизить технические риски предприятия, но и получить практический опыт полного цикла управления уязвимостями — от выявления до подтверждённого устранения — с применением современных инструментов СЗИ.

4 Исполненное индивидуальное задание

4.1 Аудит внешнего периметра компании

В течение первых двух недель практики выполнена сплошная инвентаризация публичных ИТ-активов АО «Телекоммуникационная компания «Конвей Плюс».

Методология включала: сканирование диапазонов IP-адресов и доменных имён с помощью **nmap** (режимы -sS, -sV, -O); идентификацию версий сервисов; экспресс-оценку доступных веб-приложений на предмет OWASP Top-10 (скрипты **nmap–scripts** + вспомогательные утилиты).

Результаты: выявлено **новых 66** активов вместо **134**, то есть расхождение **49 %**; избыточных/устаревших сервисов — **89**; подготовлен отчёт о рисках, рекомендации по миграции в DMZ/VPN.

Совместно с ИТ-департаментом выполнены корректирующие действия: закрыты избыточные порты, а критичные сервисы перенесены во внутренние сегменты. В результате риск-профиль внешнего периметра снижен с *High* до *Medium*.

4.2 Аудит доменных учётных записей и парольной политики

Целью второго этапа практики было выявление слабых и скомпрометированных паролей.

Действия: выгрузка списка учётных записей **Active Directory** (*dsquery*, *Get-ADUser*); анализ паролей с помощью **hashcat** + скрипт «Kerberoasting»; проверка хешей на совпадения с утекшими базами (*Have I Been Pwned*, **CrackStation**).

Результаты: обнаружено **1439** скомпрометированных и **‹705›** слабых паролей; инициирована их принудительная смена; устаревших учётных записей (более 90 дн. неактивности) — 6.

4.3 Внедрение процесса управления уязвимостями

- Сконфигурированы скан-профили **MaxPatrol VM** под серверы Windows Server 2019/2022, Linux.
- По итогам первых циклов зарегистрировано **12,100** критических и **65,000** High-уязвимостей; к концу практики устранено **8,200** критических и **30,000** High-уязвимостей, что соответствует **67,8 %** закрытия критических и **46,2 %** High-уязвимостей.
- Разработан проект регламента «Управление уязвимостями».

4.4 Освоение и применение средств СЗИ

Инструмент	Выполненные действия	Полученные компетенции
MaxPatrol VM	настройка профилей, приоритизация CVE, формирование задач в 1С	полный цикл VMT: скан-аналитика → remediation
Kaspersky KUMA (SIEM)	созданы 6 корреляционных правил (MITRE ATT&CK T1046, T1059, T1110)	реагирование через playbook
Kaspersky Endpoint Security	разработаны политики AV + Device Control	централизованное управление агентами
nmap / Wireshark	анализ трафика инцидента	разбор TCP-сессий, pcap-фильтрация
Python (Scapy, Volatility)	анализ дампов памяти, дисков, журналов, pcap файлов	сетевой парсинг, анализ дампов памяти

5 Заключение

Производственная практика в АО «Телекоммуникационная компания „Конвей Плюс“» позволила студенту в полной мере реализовать поставленные цели и задачи магистерской программы «Информационная безопасность». В ходе работы:

Проведён комплексный аудит внешнего периметра предприятия, в результате которого площадь атаки снижена до приемлемого уровня, а выявленные критичные сервисы перемещены во внутренние сегменты сети.

Внедрён непрерывный процесс управления уязвимостями: настроены регулярные сканы MaxPatrol VM, определены приоритеты устранения, разработан проект регламента взаимодействия ИТ-подразделений и службы кибербезопасности.

Проведён аудит доменных учётных записей, выявлены и устранены слабые либо скомпрометированные пароли, что повысило общий уровень аутентикационной безопасности корпоративной среды.

Освоены и практически применены современные инструменты СЗИ (MaxPatrol VM, Kaspersky KUMA, Kaspersky Endpoint Security, nmap, Wireshark, Python-скрипты), что подтвердило готовность студента к профессиональной деятельности в роли руководителя службы ИБ.

Полученный опыт углубил технические знания студента, расширил навыки межфункционального взаимодействия и управления проектами информационной безопасности. Практика оказала ощутимое позитивное влияние на киберустойчивость предприятия и стала ценным этапом профессионального становления магистранта.