Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет «Высшая школа экономики»

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

ОТЧЁТ

о прохождении производственной практики

Студент: Новиков Виталий Сергеевич

Группа: 241

Направление подготовки: 10.04.01 – «Информационная безопасность»

Образовательная программа: Информационная безопасность

База практики: АО «Телекоммуникационная компания «Конвей Плюс»

Период практики: 04.04.2025 – 16.06.2025

Санкт‑Петербург • 2025

# 1  Введение

Цель практики — получение практического опыта в области организации и управления службой кибербезопасности на примере телекоммуникационной компании, а также закрепление теоретических знаний, полученных в магистратуре.

Краткая характеристика компании:

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.

# 2  Выполненные работы

## 2.1  Проведен аудит внешнего периметра компании

Проведен аудит внешнего периметра компании (идентификация всех открытых внешних активов, анализ публичных сервисов и служб, подготовка отчёта о рисках).

## 2.2  Совместно с ИТ‑департаментом уменьшена поверхность атаки путём удаления из публичного доступа ряда сервисов и их переноса в DMZ/VPN‑сегменты.

Совместно с ИТ‑департаментом уменьшена поверхность атаки путём удаления из публичного доступа ряда сервисов и их переноса в DMZ/VPN‑сегменты.

## 2.3  Проведён аудит ИТ‑активов и внедрён процесс управления уязвимостями

Проведён аудит ИТ‑активов и внедрён процесс управления уязвимостями (приоритизация и устранение критичных/высоких уязвимостей).

## 2.4  Проведён аудит учётных записей с целью выявления слабых и скомпрометированных паролей и инициирована их срочная смена.

Проведён аудит учётных записей с целью выявления слабых и скомпрометированных паролей и инициирована их срочная смена.

## 2.5  Организована работа службы кибербезопасности: распределены роли, внедрено взаимодействие с ИТ‑службой, составлены регламенты.

Организована работа службы кибербезопасности: распределены роли, внедрено взаимодействие с ИТ‑службой, составлены регламенты.

## 2.6  Освоены и использованы инструменты: MaxPatrol VM, Kaspersky KUMA

Освоены и использованы инструменты: MaxPatrol VM, Kaspersky KUMA (SIEM), Kaspersky Endpoint Security, nmap, Wireshark, Python‑скрипты (Volatility, Scapy).

# 3  Результаты и показатели эффективности

В результате выполнения поставленных задач достигнуты следующие показатели (конкретные числовые значения будут добавлены):

* \_\_\_[Указать количество убранных/перемещённых во внутренний сегмент сервисов]\_\_\_
* \_\_\_[Указать количество закрытых критических и высоких уязвимостей]\_\_\_
* \_\_\_[Указать количество слабых или скомпрометированных паролей]\_\_\_

# 4  Выводы

Практика способствовала развитию профессиональных компетенций в области кибербезопасности, включая аудит периметра, управление уязвимостями и организацию процессов защиты информации. Полученный опыт будет полезен как в дальнейшем обучении, так и в профессиональной деятельности.

# 5  Приложения

1. Скриншоты отчётов MaxPatrol VM, Kaspersky KUMA и nmap.  
2. Таблицы устранённых уязвимостей.  
3. Примеры Python‑скриптов (Volatility, Scapy).