Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Воробьёв Игорь Валерьевич Группа: 241-352

Место прохождения практики: Московский Политех, кафедра информационная безопасность

Отчет принят с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

ВВЕДЕНИЕ

1. Общая информация о проекте
2. Общая характеристика деятельности организации (заказчика проекта)
3. Описание задания по проектной практике
4. Описание достигнутых результатов по проектной практике

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

**ВВЕДЕНИЕ**

В рамках проектной практики была выполнена работа по исследованию безопасности протоколов удалённого доступа (RDP) и создан сайт об основном проекте по дисциплине «Проектная деятельность» — создании 3D-тренажёра для проведения пусконаладочных испытаний на оборудовании автоматизированных систем (АС) для I курса. Актуальность темы обусловлена растущим использованием удалённого доступа в корпоративных и образовательных средах, где уязвимости RDP могут привести к серьёзным инцидентам безопасности, таким как несанкционированный доступ, утечки данных или атаки типа ransomware. Кроме того, в условиях цифровизации образования создание интерактивных 3D-тренажёров позволяет моделировать реальные сценарии испытаний оборудования без риска повреждения реальных систем, повышая эффективность обучения. Целью проекта стала разработка и внедрение анализа уязвимостей RDP с рекомендациями по защите, а также интеграция результатов в репозиторий и сайт, посвящённый основному проекту по «Проектной деятельности». В ходе практики были изучены лучшие практики безопасности, проведены тесты на виртуальных машинах и собраны данные о распространённых угрозах, что позволило углубить понимание интеграции безопасности в образовательные инструменты.

**3.Общая информация о проекте**

Название проекта: Создание 3D-тренажёра для проведения пусконаладочных испытаний на оборудовании АС (I курс). Цели проекта: развитие навыков моделирования и симуляции автоматизированных систем; создание интерактивной платформы для виртуальных испытаний оборудования, включая датчики, контроллеры и интерфейсы; автоматизация проверки сценариев пусконаладки; повышение безопасности и эффективности обучения студентов I курса без использования реального оборудования; интеграция элементов информационной безопасности для симуляции угроз в виртуальной среде. Проект включает использование инструментов вроде Unity или Blender для 3D-моделирования, с акцентом на реалистичную симуляцию процессов, таких как калибровка сенсоров, тестирование цепей управления и диагностика неисправностей.

**2.Общая характеристика деятельности организации (заказчика проекта)**

Заказчиком проекта выступает кафедра «Информационная безопасность» Московского Политехнического Университета. Организация занимается подготовкой специалистов в области информационной безопасности, включая разработку образовательных программ, научные исследования и практические проекты. Деятельность включает анализ уязвимостей систем, разработку защитных мер, а также интеграцию IT в образовательный процесс. В контексте проекта акцент делается на создании инструментов для симуляции реальных сценариев, что способствует повышению квалификации студентов и минимизации рисков в реальных системах АС. Университет сотрудничает с промышленными партнёрами для тестирования разработок, обеспечивая соответствие современным стандартам безопасности (например, ISO 27001).

**3.Описание задания по проектной практике**

Базовая часть задания: настройка репозитория в Git для хранения кода, документации и ресурсов проекта; написание документов в Markdown для описания процессов, структуры и сроков; создание статического веб-сайта об основном проекте по дисциплине «Проектная деятельность» — 3D-тренажёре для пусконаладочных испытаний на оборудовании АС; составление отчета по проектной практике с детальным анализом выполненных работ.

Вариативная часть задания: индивидуальное отдельное задание — исследование безопасности протоколов удалённого доступа (RDP), включая анализ уязвимостей, тестирование на виртуальных машинах и разработку рекомендаций по защите; интеграция результатов индивидуального задания и отчета по нему в репозиторий и сайт, созданные в базовой части, с добавлением разделов о безопасности RDP в контексте образовательных симуляций.

**4.Описание достигнутых результатов по проектной практике**

4.1Базовая часть

Был создан репозиторий на GitHub под названием "3D-AS-Trainer-Project". Изучена основная документация по Git, включая команды для ветвления, слияния и разрешения конфликтов, а также Markdown для форматирования текстов, таблиц и вставки изображений. Репозиторий структурирован для удобства: корневая папка содержит README.md с общим описанием проекта, включая цели, технологии и инструкции по запуску; папка docs включает README.md с пошаговым процессом выполнения практики, включая этапы моделирования 3D-объектов и интеграции скриптов; папка task содержит README.md с детальным заданием, git\_structure.md с предложенной структурой репозиторияи terms.md с контрольными сроками

4.2.Вариативная часть.

Было проведено исследование безопасности протоколов удалённого доступа (RDP), основанное на анализе стандарта Microsoft RDP (Remote Desktop Protocol). Для тестирования установлена виртуальная среда на базе VirtualBox с ОС Windows Server 2022 как сервером RDP и Ubuntu как клиентом. Изучены ключевые уязвимости: BlueKeep (CVE-2019-0708) — удалённое выполнение кода без аутентификации; Credential Security Support Provider (CredSSP) уязвимости, позволяющие MITM-атаки; слабые шифрования (RC4) и отсутствие многофакторной аутентификации по умолчанию.

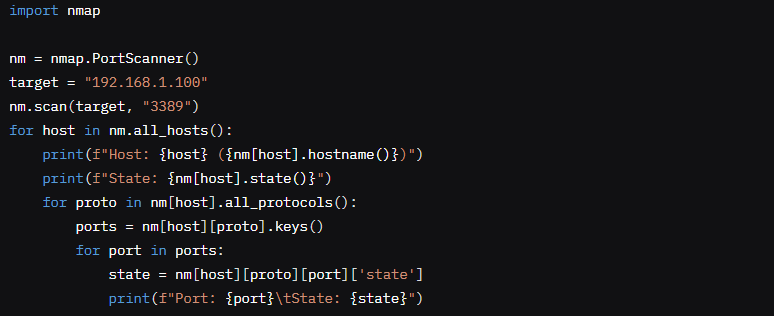
Проведены практические тесты: сканирование портов (3389/TCP) с помощью Nmap; симуляция brute-force атак с Metasploit; анализ трафика Wireshark для выявления незащищённых сессий. Разработаны рекомендации по защите: активация Network Level Authentication (NLA); использование VPN (например, OpenVPN) для туннелирования RDP; настройка firewall (Windows Defender Firewall) для ограничения IP; внедрение сертификатов TLS 1.3; регулярные обновления и мониторинг с помощью инструментов вроде Fail2Ban. Результаты интегрированы в репозиторий: добавлена папка security\_rdp с отчётом в Markdown, скриптами тестов (Python для автоматизированного сканирования) и рекомендациями. На сайте добавлен раздел "Безопасность в симуляциях", где описано, как RDP может использоваться для удалённого доступа к 3D-тренажёру, с акцентом на защиту от угроз в образовательной среде.

**ЗАКЛЮЧЕНИЕ**

В ходе проектной практики были успешно выполнены все поставленные задачи, включая базовую часть с созданием репозитория и сайта, а также вариативную с глубоким исследованием RDP. Полученные результаты способствуют повышению осведомлённости о безопасности удалённого доступа и могут быть применены в дальнейших проектах по симуляции АС. Проект продемонстрировал интеграцию теоретических знаний с практическими навыками, подтвердив актуальность темы в контексте цифровизации образования и IT-безопасности.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. Официальная документация Git // git-scm URL: <https://git-scm.com/book/ru/v2> (дата обращения: 10.05.2025).
2. Основы HTML // MDN Web Docs URL: <https://developer.mozilla.org/ru/docs/Learn/Getting_started_with_the_web/HTML_basics> (дата обращения: 11.05.2025).
3. Основы CSS // MDN Web Docs URL: <https://developer.mozilla.org/ru/docs/Web/CSS> (дата обращения: 12.05.2025).
4. Руководство по оформлению Markdown файлов // GitHub URL: <https://gist.github.com/Jekins/2bf2d0638163f1294637> (дата обращения: 13.05.2025).
5. Документация по RDP // Microsoft Docs URL: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/remote-desktop-protocol> (дата обращения: 15.05.2025).
6. Уязвимости RDP: BlueKeep // NIST CVE URL: <https://nvd.nist.gov/vuln/detail/CVE-2019-0708> (дата обращения: 18.05.2025).
7. Руководство по Unity для 3D-моделирования // Unity Documentation URL: <https://docs.unity3d.com/Manual/index.html> (дата обращения: 20.05.2025).
8. Безопасность автоматизированных систем // ISO/IEC 27001 URL: <https://www.iso.org/standard/27001> (дата обращения: 22.05.2025).



Приложение 1.