Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий
Кафедра «Информационной безопасности»

Направление подготовки: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Пак Алексей Витальевич Группа: 241-352

Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____

Руководитель практики: Кесель Сергей Александрович

Москва 2025

ОГЛАВЛЕНИЕ

1. Введение

В эпоху цифровой трансформации и учащающихся кибератак обеспечение безопасности веб-серверов становится ключевым приоритетом для компаний любого размера.

Согласно данным BI.ZONE EDR, 67% хостов в российских организациях подвержены кибератакам из-за некорректных настроек оборудования, что ведет к утечкам данных, финансовому ущербу и репутационным рискам. Универсальные операционные системы, такие как Ubuntu или CentOS, часто включают избыточные компоненты, увеличивающие поверхность атаки, что снижает их надежность в специализированных средах с повышенными требованиями к безопасности.

В связи с этим возрастает спрос на минималистичные решения, ориентированные строго на выполнение узкоспециализированных задач — например, хостинг веб-приложений — с повышенной защитой от современных киберугроз.

2. Общая информация о проекте:

Название проекта: Киберполигон

Цель: на проекте «Киберполигон» есть задачи по разработке фронтенда на React и бэкенда на Django, а также по программированию интерфейсов для работы с системами виртуализации и контейнеризации (VirtualBox, KVM, Docker).

Актуальность проекта обусловлена необходимостью практического обучения студентов, развития исследований в сфере кибербезопасности и укрепления сотрудничества с индустрией. Киберполигон позволит:

- Отрабатывать навыки противодействия реальным киберугрозам.
- Проводить исследования и разрабатывать новые методы защиты.
- Привлекать партнёров из IT-сектора для совместных проектов.
- Повышать уровень подготовки специалистов, востребованных на рынке труда.

3. Общая характеристика деятельности организации

Наименование заказчика: Московский политехнический университет

Организационная структура:

- **Руководство**:
  - Ректор
  - Проректоры
- **Академические подразделения**:
  - Институты и факультеты
  - Кафедры
- **Административные и вспомогательные подразделения**:
  - Учебный отдел
  - Научно-исследовательский
  - Центр карьеры и трудоустройства
  - Бухгалтерия
- **Проектные и инновационные структуры**:
  - Центры компетенций и лаборатории

Описание деятельности:

- Образовательная деятельность
- Научно-исследовательская деятельность

4. Описание задания по проектной практике

Задание на проектную (учебную) практику разработано для студентов первого курса, обучающихся по направлениям подготовки, связанным с информационными технологиями и информационной безопасностью. Трудоёмкость практики составляет 72 академических часа. Задание может выполняться индивидуально или в составе группы до 3 человек. Для управления версиями будет использоваться Git, для написания документации — Markdown, а для создания статического веб-сайта — языки разметки HTML и CSS, но опционально допускается использовать генераторы статических сайтов, такие, как Hugo. В качестве платформы для размещения репозиториев допустимо использовать как GitHub, так и GitVerse, что обеспечивает гибкость в выборе инструментов. Также предусмотрено взаимодействие с организациями-партнёрами, включая стажировки, которые будут приниматься к зачёту при оценке. Задание состоит из двух частей. Первая часть(базовая) является общей и обязательной для всех студентов. Вторая часть вариативная.

Базовая часть задания включает в себя:

1. Настройка Git и репозитория;
2. Написание документов в Markdown;
3. Создание статического веб-сайта;
4. Взаимодействие с организацией-партнёром;
5. Отчёт по практике.

Вариативная часть представляют собой кафедральное задание: Система мониторинга и предотвращения веб-атак с сетевым анализом трафика.

Вариативная часть задания включает в себя:

— Развернуть тестовое веб-приложение (например, на Flask/Django) и имитировать атаки (SQL-инъекции, XSS, DDoS).
— Настроить сетевой анализатор (на основе Suricata, Snort или собственного скрипта на Python/Go) для детектирования аномалий.

— Реализовать автоматическое блокирование подозрительных IP через iptables/nftables или API облачного фаервола (например, Cloudflare).
— Интегрировать SIEM-систему (например, Wazuh или ELK Stack) для централизованного управления угрозами.

5. Описание достигнутых результатов по проектной практике

В ходе выполнения базовой части практики был написан веб-сайт, а также посещен курс лекций «Введение в специальность» и мастер-класс от компании «Инфосистемы Джет» - "Как развиваться в ИБ". На рисунках 1-5 показан статический веб-сайт.

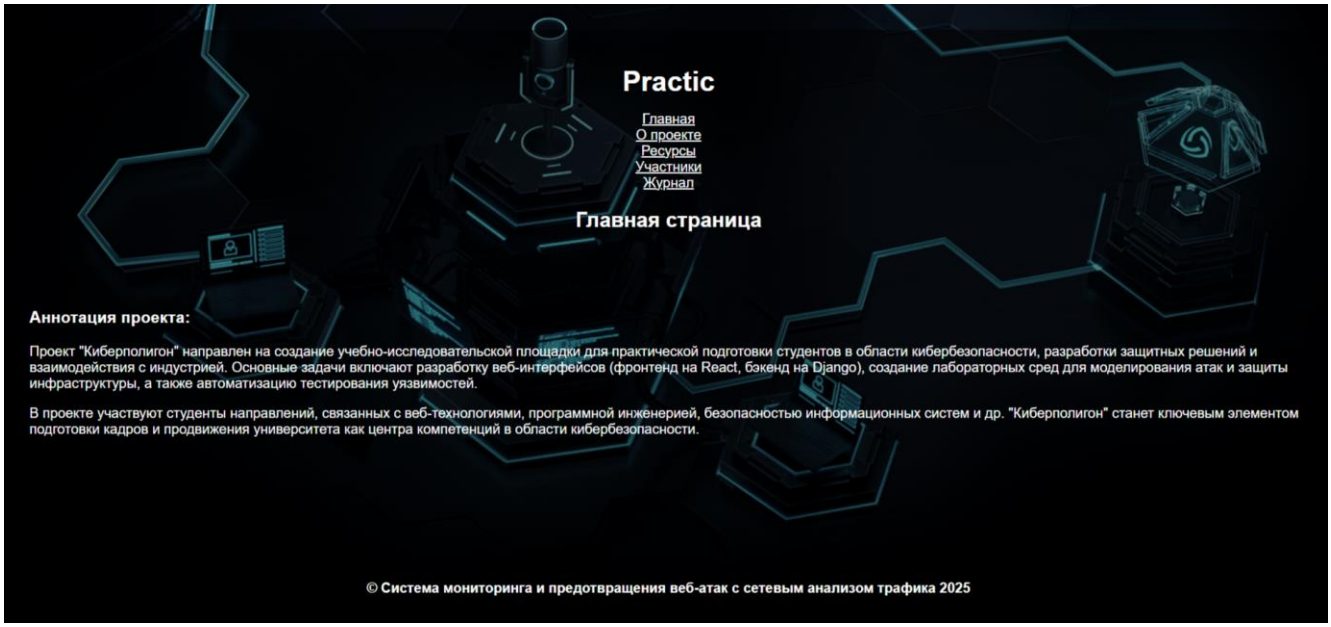

Рис.1. страница «Главная страница»

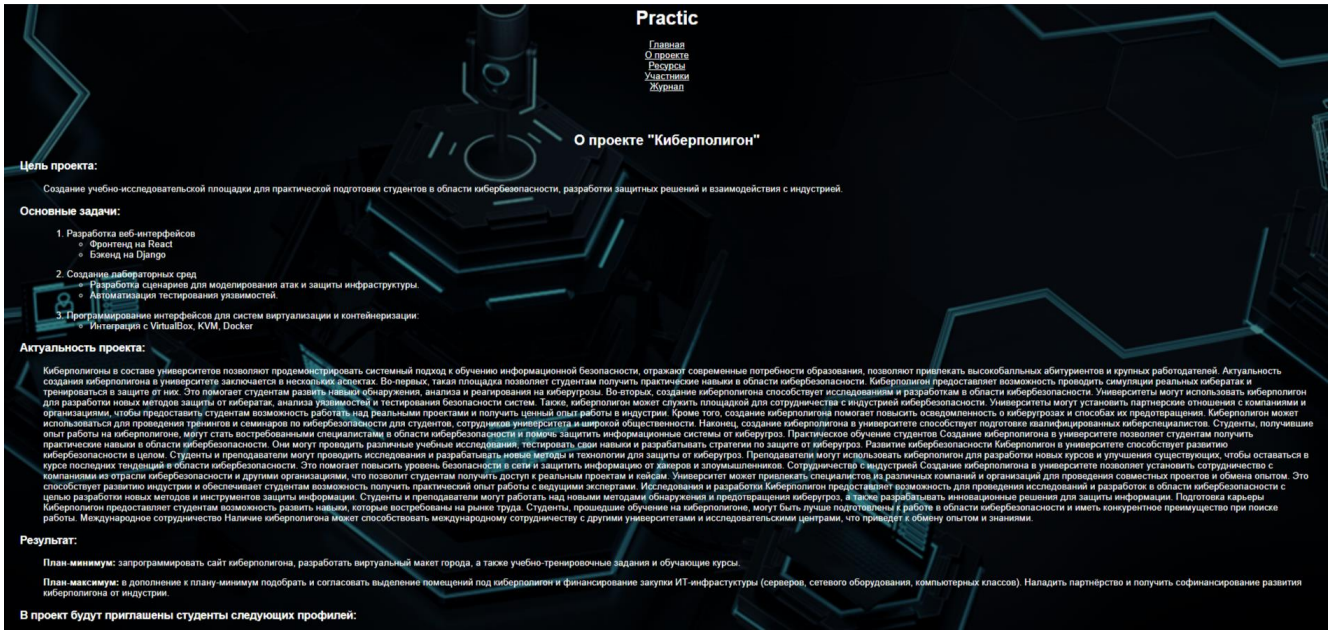

Рис.2. страница «О проекте «Киберполигон»»

Рис.3. страница «Ресурсы»

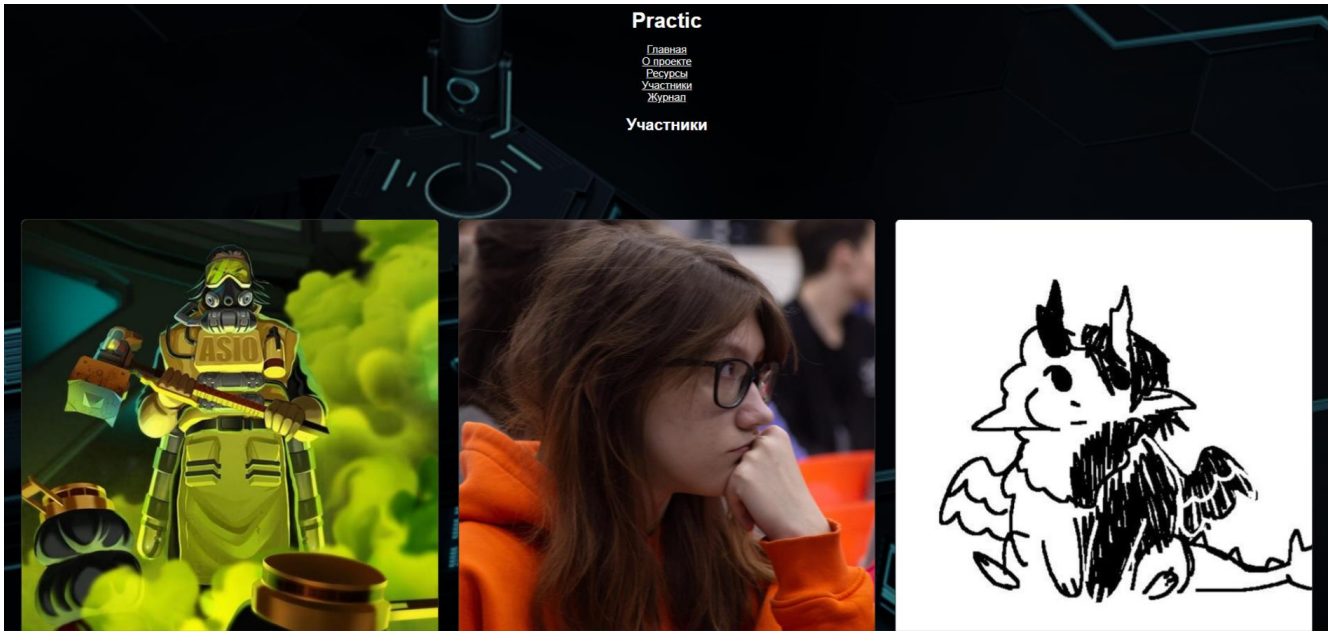

Рис.4. страница «Участники»

Рис.5. страница «Журнал»

На Рис.6 показано фото с мастер-класса.

Рис.6. Фото с мастер-класса

На выполнение базовой части практики было уделено 42 часа в это время я изучил языка разметки HTML (17 часов), языка описания CSS (8 часов), Git (5 часов), Markdown (5 часов), а также на взаимодействие с организацией-партнером было уделено 3 часа.

В ходе выполнения вариативной части было реализовано автоматическое блокирование подозрительных IP через iptables.

Для этого был создан набор для хранения подозрительных ip-адресов, которые заблокированы, для этого была написана команда "sudo ipset create banned_ip hash:ip" в терминал.

После была написана команда "sudo iptables -A INPUT -m set --match-set banned_ip src -j DROP" , которая устанавливает правило, что если ip-адрес есть в наборе benned_ip, то пакет с таким адресом отправителя блокируется.

После была написана команда "sudo iptables -A INPUT -p tcp --syn -m hashlimit --hashlimit-name syn_flood --hashlimit-mode srcip --hashlimit-above 10/second -j SET --add-set banned_ip src", которая устанавливает правило, что максимальный лимит приема tcp syn-пакетов равен 10 пакетам в секунду, то есть если от ip-адреса пришло больше 10 tcp syn-пакетов в секунду то он заисывается в набор banned_ip.

Также была написана команда "sudo iptables -A INPUT -p icmp --icmp-type echo-request -j SET --add-set banned_ip src", которая устанавливает правило, что icmp-пакеты блокируются.

После была написана команда "sudo iptables -A INPUT -p udp -m hashlimit --hashlimit-name nmap_udp --hashlimit-mode srcip --hashlimit-above 5/second -j SET --add-set banned_ip src", которая устанавливает правило, что максимальный лимит приема udp syn-пакетов равен 5 пакетам в секунду, то есть если от ip-адреса пришло больше 5 udp syn-пакетов в секунду то он заисывается в набор banned_ip.

После была вписана команда "sudo iptables -A INPUT -p tcp --dport 0:1024 -m hashlimit --hashlimit-name port_scan --hashlimit-mode srcip --hashlimit-above 5/minute -j SET --add-set banned_ip src", которая блокирует IP, если он отправляет больше 5 запросов в минуту на системные порты (0-1024).

После была вписана командs «sudo iptables -A INPUT -p tcp --dport 22 -m recent --name ssh_brute –set» и «sudo iptables -A INPUT -p tcp --dport 22 -m recent --name ssh_brute --update --seconds 60 --hitcount 5 -j SET --add-set banned_ip src», которое блокирует IP, если он совершает более 5 попыток подключения к SSH за 60 секунд.

Таким образом получилось добиться того, что блокируются ip, если от ip-адреса пришло больше 10 tcp syn-пакетов в секунду, если от ip-адреса пришло больше 5 udp syn-пакетов в секунду, если он отправляет больше 5 запросов в минуту на системные порты, если он совершает более 5 попыток подключения к SSH за 60 секунд, а также блокируются icmp-пакеты.

На вариативную часть было уделено 30 часов, в течение которых был изучен инструмент iptables, для настройки брэндмауэра ОС linux.

6. Заключение

В ходе проектной практики на тему «Киберполигон» были успешно выполнены поставленные задачи, включая как базовую, так и вариативную части. В рамках базовой части был создан статический веб-сайт, изучены ключевые технологии, такие как HTML, CSS, Git и Markdown, а также посещены лекции и мастер-классы, что позволило углубить понимание современных тенденций в области информационной безопасности.

Вариативная часть практики была посвящена разработке системы мониторинга и предотвращения веб-атак. Были достигнуты следующие результаты:

— Реализовано автоматическое блокирование подозрительных IP-адресов с использованием `iptables`, что позволило эффективно защитить систему от таких угроз, как DDoS-атаки, сканирование портов и попытки подбора паролей через SSH.
— Настроены правила для фильтрации сетевого трафика, включая ограничение количества запросов к системным портам и блокировку ICMP-пакетов.
— Освоен инструмент `iptables`, что значительно расширило практические навыки в области настройки сетевой безопасности.

Практика позволила не только закрепить теоретические знания, но и получить ценный опыт работы с реальными инструментами защиты информации. Выполненные задачи соответствуют актуальным требованиям рынка кибербезопасности и демонстрируют готовность к решению сложных профессиональных задач. Полученные результаты могут быть использованы в дальнейшем для развития проекта «Киберполигон» и других инициатив в сфере информационной безопасности.