Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Гайнуллин Никита Эдуардовчи Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

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

Руководитель практики: Кесель С. А ., к.т.н., доцент кафедры «Информационная безопасность»

Москва 2025

**Оглавление.**

**ОБЩАЯ ИНФОРМАЦИЯ О ПРОЕКТЕ**

Проектная деятельность: автоматизация внутренних бизнес-процессов университета (2ГИС).

Проект направлен на проектирование и разработку веб-сервисов и чат-ботов. Автоматизация бизнес-процессов в целом помогает повысить эффективность работы за счет экономии ресурсов и роста производительности, а также решает множество задач, такие как экономия времени, управление проектами и обеспечение прозрачности бизнес-процессов.

Главной целью проекта является перевод части или все повторяющиеся рабочие циклы в программы, что позволит сократить время на выполнение различный операций, улучшить качество продукции и оптимизировать затраты.

**ОБЩАЯ ХАРАКТЕРИСТИКА ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ**

Подразделения университета обращаются за автоматизацией тех или иных процессов, также приглашаются студенты профиля ФИТ.

При работе над проектами по автоматизации бизнес-процессов учитываются интересы и ожидания заказчика. Выявляется, что именно заказчик ожидает получить в итоге, в каком представлении или формате.

**Основные направления деятельности:** автоматизация процессов сбора, анализа и управления данными о клиентах, включая взаимодействие с ними, маркетинговые кампании и обработку заказов, управления запасами и закупок, а также автоматизация подбора персонала, ведения кадрового учета, оценки и управления их обучением.

**ОПИСАНИЕ ЗАДАНИЯ ПО ПРОЕКТНОЙ ПРАКТИКЕ**

В рамках проектной практики было поставлено комплексное задание, направленное на формирование и усвоение навыков работы с современными инструментами разработки, управления проектами и взаимодействия с организациями-партнёрами. Задания были даны и разделены на базовую и вариативные части. При этом каждые из них предусматривают выполнение определенных задач в назначенный срок.

**Базовая часть** проекта включала создание Git-репозитория на GitHub/GitVerse по заданному шаблону и освоение основных команд Git: клонирование, коммит, отправка изменений, управление ветками. Важно было регулярно фиксировать прогресс с понятными комментариями. Вместе с эим изучался Markdown для оформления проектной документации, включая описания и журналы.

Основной задачей было создание статического веб-сайта о проекте по «Проектной деятельности». Допускалось использование HTML/CSS, но также рекомендовался Hugo для упрощения. Сайт должен был включать: домашнюю страницу с аннотацией, разделы "О проекте", "Участники" (с личным вкладом каждого), "Журнал" (три записи) и "Ресурсы" (ссылки на материалы партнера). Оформление требовало более 50% уникальности и интеграцию графики и медиа.

Также одним из основных аспектов было взаимодействие с партнером: участие в мероприятиях (конференциях, семинарах, экскурсиях) и организация встреч/стажировок.

Итоговый отчёт о работе, включая описание опыта и знаний, нужно было оформить в PDF/DOCX и разместить в репозитории и на сайте.

**Вариативная часть**

При выполнении вариативной части возникли технические проблемы и сбои при установке дистрибутива Сканера вс на систему Astro Linux 1.7

Появляется ошибка смена носителя: вставьте диск с меткой <<OS Astra Linux 1.7.0 7\_86-64 DVD>> В устройство <</media/cdrim/>> и нажмите enter.

**ОПИСАНИЕ ДОСТИГНУТЫХ РЕЗУЛЬТАТОВ ПО ПРОЕКТНОЙ ПРАКТИКЕ**

В начале практики было выдано общее задание, которое включало в себя изучение и описание основных аспектов матрицы — Mitre Att&ck; изучение и описание информации с сайта OWASP; разбор реального инцидента произошедшего за последний год-полтора, с требованием расписать какие тактики, техники и процедуры были применены злоумышленниками. Что было успешно выполнено.

При выполнении задач, связанные с MITRE ATT&CK, OWASP и анализу реального инцидента, был получен опты и результат, который позволил не просто понять, а и углубить современные проблемы угроз информационной безопасности и методов борьбы с ними. При изучении матрицы MITRE ATT&CK были получены знания в области систематизации тактиках, техниках и процедурах (TTPs), используемые злоумышленниками при кибератаках на те или иные объеты.

При изучении материалов OWASP, включающие еще актуальную версию OWASP Top-10, было получено представление о наиболее уязвимых местах веб-приложений, таких как инъекции, недостаточная защита данных или misconfiguration, а также немного понять, как работают злоумышленники при кибератаках. Это опыт дал определенное представление о базовых принципах безопасной разработки. Отдельное внимание было уделено изучению рекомендаций по mitigations, что дало возможность дать конкретные меры защиты, такие как, внедрение валидации входных данных или использование prepared statements для предотвращения SQL-инъекций.

При разборе реального инцидента, произошедшего в 2024–2025 годах, были получены практические навыки, а также применены теоретические знания.В ходе выполнения работы было выявлена первоначальная цель злоумышленников— успешно перехватить исполнение одной из функций, отвечающей за работу с ключом RSA. Были получены сведения о вредоносном бэкдоре, который был встроен в дистрибутив и при этом очень хорошо замаскирован. Данный бэкдор имел определенные функциональные особенности, которые и позволили злоумышленникам внедрить его в систему. Он также обеспечивал удаленное выполнение кода, что позволяло выполнять любую системную команду на зараженном сервере дистанционно.\

Итог работы сформирован в виде комплексного отчета, данный файл можно увидеть ниже или в файле task1 папки task в Git репозитории (примерное выполнении задания по времени 5 часов)

**ИЗУЧЕНИЕ MITRE ATT&CK**

MITRE – некоммерческая американская организация, занимающаяся исследованиями в области регулирования и навигации в воздушном пространстве, систем глобального позиционирования (GPS), аэрокосмической промышленности, кибербезопасности и других. Создана в 2013 году.

MITRE ATT&CK — это глобально доступная база знаний о тактиках и методах противника, основанная на реальных наблюдениях. База знаний ATT&CK используется в качестве основы для разработки конкретных моделей и методологий угроз в частном секторе, в правительстве, а также в сообществе продуктов и услуг в области кибербезопасности.

С созданием ATT&CK MITRE выполняет свою миссию по решению проблем для более безопасного мира — объединяя сообщества для разработки более эффективной кибербезопасности. ATT&CK открыт и доступен для бесплатного использования любым лицом или организацией.

Эта своеобразная матрица, которая представляет из себя общедоступную базу данных. Основывается она на анализе реальных атак. В ней содержится список тактик и стратегии борьбы против злоумышленников, а также техник и подтехник для этой тактики. MITRE ATT&CK необходима также для анализа существующей защиты, своевременном реагировании на инциденты, расследования этих инцидентов, атрибуции атак, анализ деятельности и как действуют киберпреступники.

Имеется три матрицы MITRE ATT&CK – для корпоративных сетей и классических клиент-сервисных приложений (Enterprise), для мобильных приложений (Mobile) и для промышленных систем управления (ATT&CK for ICS).

Изображение выглядит как текст, снимок экрана, Параллельный, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 1 (матрица MITRE ATT&CK)

На данном рисунке показана матрица для предприятий. Различные этапы и их техники борьбы с киберпреступлениями.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 2 (Группы)

На данном рисунке изображены различные группы. Это кластеры активности, которые отслеживаются под общим именем в сообществе безопасности. В зависимости от типа угрозы и ее местонахождения работает та или иная группа.

**ИЗУЧЕНИЕ OWASP**

OWASP (Open Web Application Security Project) — открытый проект по безопасности веб-приложений, созданный и поддерживаемый некоммерческой организацией OWASP Foundation.

Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. Оно работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе.

Организация выступает за то, чтобы подходить к безопасности приложений как к проблеме людей, процессов и технологий, потому что наиболее эффективные подходы к безопасности приложений требуют улучшения в этих областях.

Один из флагманских проектов OWASP — Web Security Testing Guide (WSTG) — Руководство по тестированию безопасности веб-приложений. В нём описываются приёмы, методики, инструменты и ресурсы для тестирования наиболее распространённых уязвимостей веб-приложений.

Самое интересное, что все их материалы имеется в общем доступе, находятся они на их веб-сайте.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3. (10 основных рисков безопасности веб-приложений) Десятка лучших OWASP

Есть три новые категории, четыре категории с изменениями в названиях и области охвата, а также некоторая консолидация в Топ-10 на 2021 год.

Они формализовали процесс сбора данных OWASP Top 10 на саммите Open Security Summit в 2017 году. Лидеры OWASP Top 10 и сообщество потратили два дня на то, чтобы формализовать прозрачный процесс сбора данных. В 2021 году уже во второй раз используют эту методологию.

Каждое из этих веб – приложений постоянно тестируется, проверяется и улучшается и все они необходимы для улучшения кибербезопасности, защиты от сбоев, от угроз злоумышленников, нахождение уязвимых и устаревших компонентов.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 4 Дорожная карта (Проект безопасности OWASP API)

Основополагающим элементом инноваций в современном мире, управляемом приложениями, является API. От банков, розничной торговли и транспорта до Интернета вещей, автономных транспортных средств и интеллектуальных технологий города, API являются важной частью современных мобильных, SaaS и веб-приложений, а также можно найти в приложениях, ориентированных на клиентов, партнеров и внутренних приложениях. Около природа, API предоставляют логику приложения и конфиденциальные данные, такие как личные данные. Идентифицируемая информация (PII) и из-за этого все чаще становятся мишень для злоумышленников. Без безопасных API быстрые инновации были бы невозможны.

API Security фокусируется на стратегиях и решениях для понимания и смягчения последствий уникальные уязвимости и риски безопасности интерфейсов прикладного программирования (API).

Изображение выглядит как текст, снимок экрана, число, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 5 OWASP SamuraiWTF(Использование Katana из командной строки)

SamuraiWTF (Web Training Framework) — это не просто еще одно уязвимое приложение — это полноценный, надежный фреймворк для обучения тестированию безопасности приложений. Это проект OWASP (Open Web Application Security Project) и призван помочь людям улучшить свои навыки в области кибербезопасности. Фреймворк основан на базовом ящике на основе Ubuntu, что делает его довольно легким и простым в управлении.

SamuraiWTF — это система сборки, состоящая из нескольких проектов. Компания наиболее известна тем, что создала виртуальную машину, которая была предварительно настроена для работы в качестве веб-среды для тестирования на проникновение и обучения. Эта среда поддерживается в Hyper-V, VirtualBox и VMWare. Он создан с использованием Vagrant и Ansible, чтобы предоставить наиболее кроссплатформенный механизм для создания и улучшения учебной среды.

Проще говоря, это приложение, которое поможет каждому человеку обучиться и улучшить свои навыки в области кибербезопасности. А именно путем тестирования безопасности различных приложений.

**ИНЦИДЕНТ И ЕГО РАЗБОР**

Бэкдор в XZ: атака на цепочку поставок.

Первоначальная цель злоумышленников — успешно перехватить исполнение одной из функций, отвечающей за работу с ключом RSA.

29 марта 2024 года в рассылке Openwall Open Source Security (oss-security) было опубликовано сообщение об обнаружении вредоносного бэкдора в XZ, утилите для сжатия данных, встроенной во многие популярные дистрибутивы Linux. Библиотека, содержащая бэкдор, используется sshd — серверным процессом OpenSSH. В некоторых дистрибутивах Linux на основе systemd, таких как Ubuntu, Debian и RedHat/Fedora, для доступа к функциям systemd применяется модифицированный OpenSSH, зависящий от этой библиотеки (проблема не коснулась дистрибутивов Arch Linux и Gentoo). Код бэкдора внедрялся в феврале и марте 2024 года, в основном пользователем по имени Цзя Чон Тан (Jia Cheong Tan). Скорее всего, это вымышленное имя. Мы полагаем, что целью атаки было добавление в sshd возможности удаленного выполнения кода посредством вмешательства в процесс сборки XZ Utils и последующее внедрение вредоносного кода, содержащего бэкдор, в популярные дистрибутивы Linux в рамках крупномасштабной атаки на цепочку поставок.

Анализ выявил следующие интересные функциональные особенности бэкдора:

* Злоумышленник реализовал защиту от повторного воспроизведения (anti-replay), чтобы избежать возможного перехвата сообщений бэкдора.
* Для сокрытия открытого ключа шифрования автор применил собственную технику стеганографии в коде x86.
* Бэкдор скрывает логи несанкционированных подключений к SSH-серверу посредством перехвата функции логирования.
* Бэкдор перехватывает функцию аутентификации по паролю, позволяя злоумышленнику входить на зараженный сервер с любым именем пользователя и паролем без дополнительных проверок. То же самое происходит и с функцией аутентификации по открытому ключу.
* Бэкдор обеспечивает удаленное выполнение кода, что позволяет злоумышленнику выполнить любую системную команду на зараженном сервере.

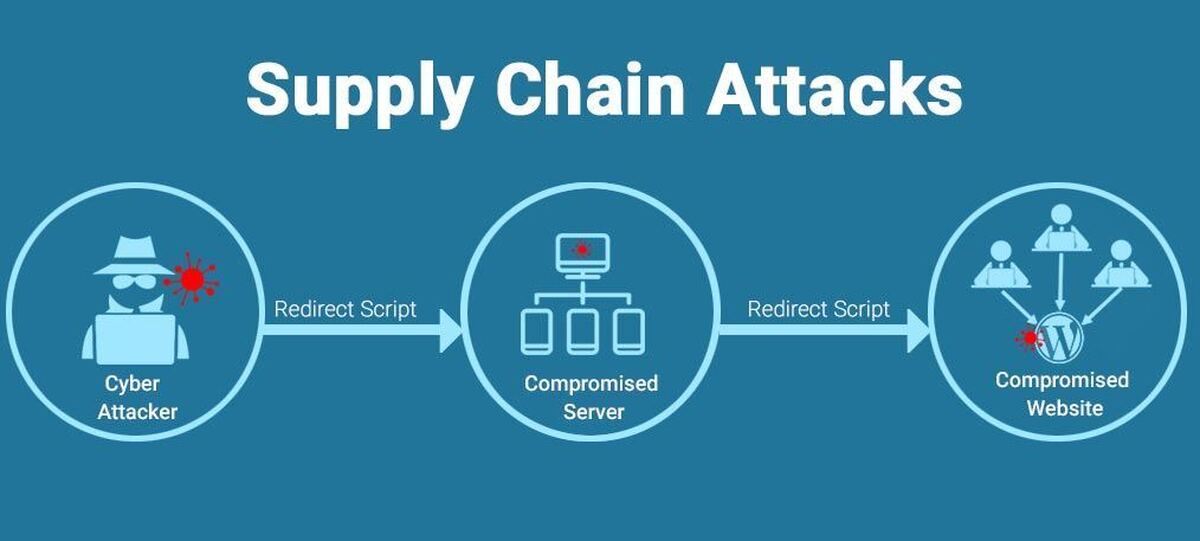


Рис.6 Схема кибератаки

Бэкдор в библиотеке liblzma был реализован на двух уровнях. В исходный код инфраструктуры сборки для получения финальных пакетов злоумышленники добавили файл build-to-host.m4, который извлекал скрипт следующего этапа, спрятанный в файле тестового примера (bad-3-corrupt\_lzma2.xz). Этот скрипт, в свою очередь, извлекал вредоносный бинарный компонент из другого тестового файла (good-large\_compressed.lzma), который в процессе компиляции прилинковывался к легитимной библиотеке и с ней попадал в репозитории Linux. В результате основные вендоры начали распространять вредоносный компонент в составе бета-версий и экспериментальных сборок. Эта уязвимость была зарегистрирована под номером CVE-2024–3094 с максимальным уровнем серьезности по десятибалльной шкале.

**Базовая часть**

После выполнения общей части была выполнена базовая часть, которая включала в себя следующие пункты: настройка Git и репозитория, написание документов в Markdown, создание статического веб-сайта. Выполнение базовой части задания позволило получить и закрепить навыки работы с современными инструментами разработки, управления версиями и документацией, а также создать статический сайт, который хорошо функционирует.

**Настройка Git и репозитория**

Была успешно организована работа с системой контроля версий Git: создан репозиторий на платформе GitHub, освоены базовые команды, включая клонирование, создание веток, фиксацию изменений с осмысленными комментариями и отправку кода в удалённое хранилище. Разделение задач через ветки дало эффективное распределение работу межды участниками команды. Репозиторий стал основной платформой для хранения всех материалов проектной практики, включая исходный код сайта, документацию и отчёты. (время на выполнение 4 часа).

**Создание статического веб-сайта**

Разработан статический веб-сайт, посвящённый проектной деятельности. Для разработки сайта было выбрано сочетание языка разметки HTML и CSS. Сайт включает:

* Главную страницу с краткой аннотацией проекта, участниках и его вкладе
* Страницу «style.css» где указано написание кода стилизации
* Страницу «Групповое задание», где находится информация о вариативной части
* Страницу «мастер класс», где находится отчет о посещении мероприятия (фото, видео).

Уникальность контента и дизайна была обеспечена за счёт авторских решений: адаптивной вёрстки на HTML/CSS, интеграции графики (фотографий) и медиаэлементов (видео). Сайт размещён в репозитории. (затрачено примерное 8 часов)

**Взаимодействие с организацией-партнёром**

В рамках взаимодействия с организацией-партнёром я посетил мастер-класс «Демо-собеседование». Подробнее можно узнать на сайте GIT, на странице мастер класс. Посетив данный мастер-класс, было получены знания, а также небольшой опыт в собеседовании и требования, которые необходимы для работы студентов.

**Итоговые навыки и достижения**

* Освоены инструменты DevOps: Git, GitHub, работа с ветками и pull-request.
* Получение опыта в демо-собеседовании.
* Развиты навыки фронтенд-разработки, включая вёрстку, работу с HTML и CSS и публикацию исходного кода проекта.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. **MITRE ATT&CK®** [Электронный ресурс]. – Режим доступа: <https://attack.mitre.org/> (дата обращения: 19.04.2025).
2. **OWASP Foundation** [Электронный ресурс]. – Режим доступа: <https://owasp.org/> (дата обращения: 18.04.2025).
3. **GitHub Docs** [Электронный ресурс]. – Режим доступа: <https://docs.github.com/> (дата обращения: 20.04.2025).