

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РТФ

ОТЧЕТ

о проектной работе

по теме: Web-разработка Digital Portfolio 2024

по дисциплине: Проектный практикум 1A

Команда: «МЫ»

Тимлид: Жмайло Михаил Александрович РИ-130934

Аналитик: Пономарева Анастасия Юрьевна РИ-130934

Дизайнер: Пономарева Анастасия Юрьевна РИ-130934

Фронтенд-разработчик: Репин Михаил Евгеньевич РИ-130934

Бэкенд-разработчик: Саетбатталов Павел Равильевич РИ-130933

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc165369900)

[1. Целевая аудитория 5](#_Toc165369901)

[2. Определение проблемы 6](#_Toc165369902)

[3. Подходы к решению проблемы 8](#_Toc165369903)

[4. Анализ аналогов 9](#_Toc165369904)

[5. Календарный план проекта 12](#_Toc165369905)

[6. Сценарии использования 13](#_Toc165369906)

[7. Требования к продукту и к MVP 14](#_Toc165369907)

[8. Стек для разработки 16](#_Toc165369908)

[9. Проектирование и разработка системы 17](#_Toc165369910)

[ЗАКЛЮЧЕНИЕ 20](#_Toc165369911)

[СПИСОК ЛИТЕРАТУРЫ 21](#_Toc165369912)

[ПРИЛОЖЕНИЕ А 22](#_Toc165369913)

ПРИЛОЖЕНИЕ Б 23

ПРИЛОЖЕНИЕ B 24

ВВЕДЕНИЕ

Современное программное обеспечение представляет собой сложный многогранный продукт, для стабильной работы которого требуются различные сервисы, десятки тысяч строк кода, своевременная поддержка и обновление инфраструктуры, на ресурсах которой осуществляется развертывание и выполнение программы. Однако продукт, либо хостинг-платформа, либо обслуживающие сервисы зачастую имеют внутри себя уязвимости: о каких-то уже давно известно, какие-то еще даже не обнаружены. Уязвимостью, в самом простом ее проявлении, можно считать некоторый недокументированный, нестандартный, отличающийся от задуманного разработчиком, поток исполнения программы. В свою очередь, при правильной эксплуатации (в некоторых случаях — злоупотреблении) уязвимости появляется возможность воздействия на развернутый программный продукт. Например, если присутствует уязвимость Command Injection, то существует риск компрометации сервера, на котором осуществляет свою работу соответствующее программное обеспечение. Уязвимости обнаруживают исследователи информационной безопасности. Абсолютно безопасный программный код, не имеющий ни одной уязвимости, написать практически невозможно.

В связи с уходом иностранных вендоров у разработчиков отечественного программного обеспечения пропала возможность своевременного отслеживания появления новых уязвимостей в их программных продуктах. В свою очередь, ландшафт угроз кибербезопасности лишь возрос: количество атак на российскую инфраструктуру стремительно увеличилось за последний год. На текущий момент новые уязвимости регистрируются в банке данных угроз (далее — «БДУ») Федеральной службы по техническому и экспортному контролю России (далее — «ФСТЭК»), однако нет ни одного программного обеспечения с открытым исходным кодом, которым могли бы пользоваться все разработчики с целью своевременного получения оповещений о новых уязвимостях в своих программных продуктах. Подобный функционал зачастую идет вместе с более обширным коммерческим продуктом, приобретение которого доступно далеко не каждой компании.

Таким образом, проект «Sploit2Me» решает проблему отсутствия программного обеспечения с открытым исходным кодом, которое позволяет своевременно получать информацию о новых уязвимостях, изучать уже опубликованные уязвимости и настраивать точечную фильтрацию для отображения данных по уязвимостям в конкретном программном продукте.

Перед созданием проекта перед командой «МЫ» были поставлены следующие цели:

– Создать программный продукт, умеющий извлекать данные (далее — «парсинг», «парсить») из базы данных БДУ ФСТЭК России;

– Реализовать функционал оповещения пользователей о появлении новой уязвимости посредством отправки уведомления через чат-бот в Telegram;

– Разработать механизм применения фильтров к отображаемым на главной странице уязвимостям и к программным продуктам, об уязвимостях в котором желает получать уведомления пользователь;

– Предусмотреть механизм регистрации, аутентификации пользователей.

Цель достигалась путем решения следующих поставленных задач:

– Изучить необходимый набор навыков и инструментарий для создания WEB-ресурса с базовым функционалом: аутентификация, регистрация, добавление информации в базу данных, вывод информации на страницу;

– Подготовить графическую составляющую, разработать пользовательский интерфейс;

– Написать программный код с необходимым функционалом;

– Провести тестирование продукта.

1. Целевая аудитория

Для определения целевой аудитории мы использовали методику 5W Марка Шеррингтона. Продуктом проекта является исходный код веб-сервиса «Sploit2Me», который можно развернуть на собственном стенде. Потенциально есть возможность добавления механизма подписки на уязвимости, покупки аккаунтов для использования сервиса, но изначально проект не рассматривался как коммерческое решение, поэтому исходный код опубликован на интернет-ресурсе Github.Com и доступен всем желающим абсолютно бесплатно.

В использовании продукта заинтересованы разработчики отечественного программного обеспечения, специалисты по информационной безопасности, SOC-аналитики, Threat Intelligence эксперты и иные сотрудники, отвечающие за информационную безопасность в организации.

Наш продукт решает важную проблему, заключающуюся в отсутствии программного обеспечения, способного взаимодействовать с базой ФСТЭК России и имеющего встроенный функционал уведомления о новых уязвимостях посредством отправки сообщения в Telegram.

Основной мотивацией потенциального пользователя веб-сервиса является желание своевременного получения информации о вышедшей уязвимости в интересующем его программном продукте.

В России не так много специалистов по информационной безопасности, поэтому присутствует некоторое ограниченное количество точек контакта с потенциальным пользователем. Однако отмечу, что идея проекта родилась после разговора с ведущими специалистами по анализу защищенности и тестированию на проникновение компании УЦСБ (Уральский Центр Систем Безопасности). Таким образом, принцип «сарафанного радио» будет работать как нельзя кстати и проект сможет обрести популярность.

1. Определение проблемы

Согласно последним данным и отчетам компаний, связанных с информационной безопасностью, в частном случае, с поиском угроз информационной безопасности (от англ. — Threat Hunting), возможно заметить тенденцию увеличения числа атак на российскую инфраструктуру, совершаемых политически мотивированными, либо финансово мотивированными хакерскими группировками. Ситуация усложнилась тем, что большинство иностранных решений по определению уязвимостей в программном обеспечении ушли с российского рынка. Помимо того, с сентября 2024 года, согласно новому пакету санкций, было запрещено осуществление различных услуг, в том числе консультационных, связанных с вопросами сектором IT-индустрии, в частности, информационной безопасности.

В связи с чем, у владельцев информационных систем пропала возможность отслеживания появления новых уязвимостей в собственном программном обеспечении. Однако существует БДУ ФСТЭК России, где своевременно появляется информация о новых уязвимостях программного обеспечения. Проблема заключается в отсутствии бесплатных, некоммерческих решений по интеграции взаимодействия с БДУ ФСТЭК России. Ситуация осложняется тем, что ресурс не предоставляет никакого программного интерфейса (так называемый API — Application Programming Interface), что приводит к сложности интеграции с базой.

Наш сервис позволяет решить обе этих проблемы. Во-первых, разработчики создали программный код, умеющий извлекать всю базу с ресурса БДУ ФСТЭК России и представлять его в виде электронной таблицы, что упрощает взаимодействие и извлечение требуемых данных. Во-вторых, пользователи сервиса могут собственноручно использовать фильтры, необходимые им для получения информации о новых уязвимостях. В-третьих, присутствует возможность настройки уведомления посредством Telegram-бота.

Таким образом, благодаря нашему продукту, у разработчиков отечественного программного обеспечения появляется возможность отслеживания уязвимостей в собственных продуктах абсолютно бесплатно, что решает поставленную проблему.

1. Подходы к решению проблемы

Осуществление функционала поиска и своевременного уведомления об уязвимостях возможно несколькими способами. Изначально проект основывался на извлечении уязвимостях с иностранного ресурса nsa.gov, который был доступен из российского сегмента сети «Интернет». Однако, на момент написания отчета ресурс недоступен. Способ извлечения информации заключался в создании механизма, именуемым «каруселью прокси-серверов». Механизм позволяет совершать каждый запрос на веб-ресурс с альтернативного IP-адреса, что обходит поставленную блокировку.

Способ был отклонен нашей командой. Первый фактор — финансовый. Поддерживать такой механизм потребует определенных вложений, как следствие, потребуется чтобы эти вложения себя окупали. Проект задумывался как некоммерческий инструмент для решения современной проблемы IT-специалистов, поэтому мотивации извлечения финансовой выгоды не было. Второй фактор — обнаружение аналогичной базы данных в российском сегменте интернета. Отсутствие публично доступного кода для интеграции с БДУ ФСТЭК стало основной мотивацией нашей команды по созданию проекта.

Таким образом, для решения проблемы наша команда приняла решение использовать отечественный аналог базы с уязвимостями вместо иностранного ресурса nsa.gov.

Итоговый подход заключался в настройке интеграции с БДУ ФСТЭК с целью извлечения информации об уязвимостях в удобном для чтения пользователем и программным кодом формате. Добавление функционала по уведомлению о новой уязвимости в Telegram позволит не пропустить выход ни одной новой уязвимости.

Для структурирования и грамотному подходу к обучению наша команда использовала механизм Zettelkasten. [1]

1. Анализ аналогов

Функционал нашего продукта можно назвать уникальным. В основном подобные механизмы присутствуют в коммерческих продуктах, подписки на которые стоят несколько миллионов рублей в месяц, что несколько сужает целевую аудиторию. Как следствие, получать возможность о наличии уязвимостей могут далеко не все компании. Подобных проектов с открытым исходным кодом нет. Однако, существуют косвенные конкуренты, разрабатываемые отечественными компаниями, связанными с информационной безопасностью. В них функционал интеграции с БДУ ФСТЭК осуществлен в качестве дополнения к более сложному механизму. Например, механизм определения поверхности атаки (от англ. — Attack Surface Discovery) может включать в себя интеграцию с БДУ ФСТЭК. Однако, отдельно это дополнение не продается.

В таблице 1 представлен анализ конкурентов по нескольким критериям.

Таблица 1 – Анализ конкурентов

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Название продукта | Описание | Уведомление | Статистические данные | Открытый исходный код | Цена |
| PT MaxPatrol 8 | Система MaxPatrol 8 предназначена для обеспечения контроля защищенности и соответствия стандартам безопасности информационных систем. Присутствует интеграция с БДУ ФСТЭК | Отсутствует возможность настройки уведомления о появлении новой уязвимости. | Присутствуют статистические данные об уязвимостях в текущей инфраструктуре, но нет возможности просмотра суммарной (общей) ситуации | - | NDA |
| CICADA8 | Сервис управления уязвимостями и возможностью отслеживания киберугроз в реальном времени. Интеграция с cve.mitre.org, отсутствует взаимодействие с БДУ ФСТЭК | Присутствует уведомление о новой уязвимости на почту. | Доступны статистические данные об уязвимостях внешнего периметра | - | NDA |
| BI.ZONE CPT | Решение для управления поверхностью атаки и непрерывного мониторинга IT‑активов. Интеграция с attack.mitre.org, отсутствует взаимодействие с БДУ ФСТЭК | Нет информации об уведомлениях о новых уязвимостях. | Статистические данные представлены в виде обработанных графиков с приятным пользовательским интерфейсом. Информация об уязвимостях в текущей инфраструктуре. | - | NDA |
| Sploit2Me | Сервис специализируется именно на БДУ ФСТЭК. Присутствует простая расширяемость и встроенная возможность по уведомлению об уязвимостях в Telegram-бота, добавление фильтров к информации, которая будет поступать пользователям | Telegram | Представлены графики, описывающие общую информацию об уязвимостях, представленных в БДУ ФСТЭК | + | 0 руб |

Полученные данные свидетельствуют об отсутствии решений с открытым исходным кодом по извлечению информации из БДУ ФСТЭК. Помимо этого, далеко не у каждого продукта присутствует возможность уведомления о новой уязвимости в мессенджере Telegram. Наконец, наше решение абсолютно бесплатное, так как является продуктом с открытым исходным кодом. Совокупность этих факторов позволяет продукту «Sploit2Me» отличаться в лучшую сторону от существующих решений.

1. Календарный план проекта

Календарный план проекта, учитывающий все важнейшие этапы и временные рамки, представлен в приложении А документа, что позволяет более подробно ознакомиться с каждым аспектом предстоящих работ и убедиться в их соответствии запланированным срокам.

Следует отметить, что под календарным планом проекта понимается детализированный график проведения работ, разработанный для обеспечения эффективности управления проектом. В рамках создания такого плана учитываются доступные ресурсы, объемы задач, последовательность выполнения работ и временные ограничения. Таким образом, календарный план представляет собой неотъемлемую часть планирования проекта и является инструментом, позволяющим оперативно реагировать на изменения и максимально рационально использовать все имеющиеся ресурсы для достижения поставленных целей.

Календарный план выполняет ключевую роль в успешной реализации проекта, поскольку он помогает не только планировать ресурсы и распределять обязанности среди членов команды, но и мониторить прогресс выполнения задач. С его помощью можно своевременно выявлять потенциальные риски и корректировать действия, чтобы избежать незапланированных задержек и других проблем, способных негативно сказаться на итоговом результате проекта.

Представленный в приложении А документа план охватывает полный спектр задач, начиная с первоначальной фазы подготовки и заканчивая финальной стадией завершения проекта. Он включает в себя установленные сроки для каждой задачи, а также взаимосвязи между различными этапами работ, что позволяет обеспечить последовательное и бесперебойное выполнение всех необходимых действий.

1. Сценарии использования

Сценарии использования продукта «Sploit2Me» представлены в приложении Б текущего документа. Основной целью проекта является возможность интеграции с БДУ ФСТЭК с возможностью пользователем добавления фильтров к отображаемым данным. Помимо этого, важным фактором считается оповещение о новой уязвимости посредством чат-бота на платформе Telegram.

Однако, следует уделить должное внимание обработке всех возможных случаев поведения пользователя. В частности, механизму аутентификации и применению фильтров к передаваемым данным.

1. Требования к продукту и к MVP

В ходе работы аналитика были созданы следующие требования к продукту:

Требования клиентов

Следует решать задачи по:

* обеспечению механизма аутентификации, авторизации и контроля доступа пользователей;
* предоставление возможности извлечения обработанного массива данных с информационного ресурса БДУ ФСТЭК;
* осуществлять фильтрацию массива данных по требованию пользователя;
* гарантировать своевременное уведомление пользователей о появившейся уязвимости посредством извещения в мессенджере «Telegram»

Функциональные требования

Каждая страница системы должна отображать в верхней правой части вкладку информации о пользователе, при нажатии на которую возможно просмотреть профиль пользователя. Система должна предоставлять возможность пользователю изменять пароль учетной записи, обновлять аккаунт для уведомлений об уязвимостях, отключать аккаунт, применять фильтры.

Нефункциональные требования

Функционирование системы должно осуществляться посредством размещения в сети Интернет на доменном имени. Хранение, запуск и управление функциональным составляющим информационной системы должно осуществляться внутри изолированных Docker-контейнеров. Помимо этого, система должна поддерживать бота в мессенджере «Telegram», посредством которого будет осуществляться уведомление пользователя о новой уязвимости.

Интерфейс пользователя должен быть простым в освоении, минималистичным. Во время работы пользователь может подключить аккаунт, на который будут отсылаться уведомления, отключить аккаунт, применить правила фильтрации. Пользователи могут быть ограничены в возможности добавления аккаунтов для уведомления об уязвимостях.

Механизм аутентификации и авторизации пользователей, а также хранения информации о подключенных аккаунтах для уведомления об уязвимостях должен быть осуществлен с использованием реляционной базы данных. В частности, разрешается использование SQLite, PostgreSQL.

MVP должен представлять собой веб-сайт со следующим функционалом:

* Регистрация пользователя
* Аутентификация пользователя
* Механизм подключения Telegram-аккаунта
* Механизм изучения статистики по уязвимостям
* Механизм добавления фильтров к получаемым данным

1. Стек для разработки

Проект задумывался как решение с открытым исходным кодом, обеспечивающее возможность интеграции с БДУ ФСТЭК. Таким образом, решение не должно иметь «под капотом» множество сервисов, сложность в запуске и иных механизмов, усложняющих развертывание программного продукта, что сужает количество пользователей, способных использовать проект.

Большинство членов команды были знакомы с языком программирования Python, поэтому он был выбран в качестве основного для написания проекта. Помимо этого, в течение второго семестра студенты проходили курс по веб-технологиям, что позволило им эффективно использовать HTML, CSS и JS. В качестве базы была выбрана SQLite [2], однако в коде используются стандартные параметризированные запросы, что упрощает интеграцию с иными реляционными базами, например, PostgreSQL.

В качестве веб-фреймворка был выбран Flask[3]-[5], опять-таки по причине простоты его использования, наличия множества технической литературы и быстроты изучения разработчиками проекта этого инструмента.

Платформа Github использовалась как система управления версиями.

Использование данных технологий позволило создать минимальный жизнеспособный продукт, также именуемый как Proof Of Concept, что позволит без особых проблем добавлять в инструмент собственный функционал, в зависимости от потребностей конечного пользователя.

1. Проектирование и разработка системы

**9.1 Общая структура программного комплекса**

На этапе проектирования и разработки веб-сервиса по изучению существующих уязвимостей из базы данных ФСТЭК формируется общая структура программного комплекса. В соответствии с технологией нисходящего структурного программирования, программный комплекс разбивается на несколько программных модулей, каждый из которых отвечает за определенные функции. Основными модулями являются:

1. Модуль аутентификации и регистрации пользователей

2. Модуль управления уведомлениями

3. Модуль взаимодействия с базой данных ФСТЭК

4. Модуль управления подписками на уведомления

5. Модуль обработки ошибок

Подобная систематизация была выстроена после изучения соответствующей литературы. [5]

**9.2 Модуль аутентификации и регистрации пользователей**

Этот модуль отвечает за обработку регистрации новых пользователей и аутентификацию уже существующих. Основная задача модуля – надежное управление учетными записями пользователей, включая создание, проверку и удаление учетных записей. Модуль также отвечает за обработку ошибок при регистрации и аутентификации, а также за проверку на дублирование аккаунтов. Алгоритм работы:

1. Пользователь инициирует процесс регистрации.

2. Система проверяет введенные данные на корректность и дублирование.

3. В случае успешной проверки создается новый аккаунт.

4. Пользователь проходит аутентификацию, которая включает проверку логина и пароля.

5. В случае успешной аутентификации пользователь получает доступ к системе.

**9.3 Модуль управления уведомлениями**

Этот модуль ответственен за формирование и отправку уведомлений пользователям о новых уязвимостях. Уведомления формируются на основе подписок пользователей, а также могут содержать информацию о критических изменениях или новых данных по уязвимостям. Алгоритм работы:

1. Проверка списка уязвимостей на наличие новых записей.

2. Формирование уведомления на основе данных об уязвимости и настроенных пользователями фильтров.

3. Отправка уведомления пользователю.

**9.4 Модуль взаимодействия с базой данных ФСТЭК**

Основная задача этого модуля – обеспечение получения и обновления информации об уязвимостях из базы данных ФСТЭК. Модуль осуществляет регулярные HTTP-запросы [6] к базе данных, обрабатывает ответ и вносит обновления в локальную базу данных. Алгоритм работы:

1. Инициируется запрос на получение информации об уязвимостях из базы данных ФСТЭК.

2. Обработка ответа и проверка данных на корректность.

3. Обновление локальной базы данных.

4. Обработка возможных ошибок при получении данных.

**9.5 Модуль управления подписками на уведомления**

Этот модуль обеспечивает функционал подписки пользователей на уведомления о новых уязвимостях. Модуль позволяет пользователям настраивать предпочтения уведомлений, подписываться и отписываться от определенных типов уведомлений. Алгоритм работы:

1. Пользователь настраивает подписки на уведомления.

2. Система проверяет и сохраняет изменения в настройках подписок.

3. При поступлении новой информации проверяется необходимость уведомления подписчиков.

4. Уведомления формируются и отправляются в соответствии с заданными предпочтениями.

**9.6 Модуль обработки ошибок**

Данный модуль отвечает за корректную обработку всех возможных ошибок, возникающих в процессе работы системы. Включает логирование ошибок и предоставление пользователям информации о характере возникших проблем.

**9.7 Взаимодействие программных модулей**

Модуль аутентификации и регистрации пользователей взаимодействует как с пользователями, так и с модулем обработки ошибок. Модуль управления уведомлениями обрабатывает события из модуля взаимодействия с базой данных ФСТЭК и отсылает уведомления, сформированные на основе настроек подписок, хранящихся в соответствующем модуле. Модули аутентификации, управления подписками и уведомлений тесно связаны посредством кросс-взаимодействий для обеспечения целостности данных и синхронизации операций. Схема в графическом представлении представлена в приложении В.

ЗАКЛЮЧЕНИЕ

В ходе работы над проектом команда «МЫ» успешно достигла поставленных целей. Был создан программный продукт, который извлекает данные из базы данных БДУ ФСТЭК России, оповещает пользователей о новых уязвимостях через чат-бот в Telegram, предоставляет возможность применения фильтров к отображаемым уязвимостям и программным продуктам, а также предусматривает механизм регистрации и аутентификации пользователей. Продукт прошел этап тестирования и готовится к запуску на реальных пользователях.

Мы уверены, что наш сервис станет полезным инструментом для мониторинга уязвимостей и оперативного информирования пользователей о новых угрозах. В дальнейшем мы планируем продолжать работу над улучшением продукта, расширением его функционала и повышением надежности.

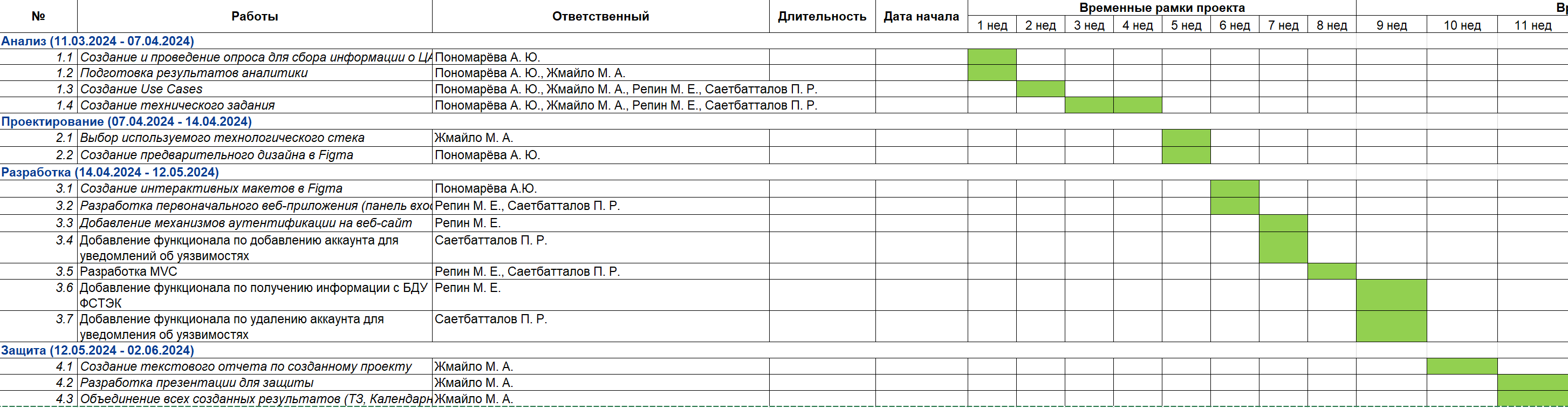
СПИСОК ЛИТЕРАТУРЫ

1. Productivity Zettelkasten в Obsidian. – 2021. – URL: <https://www.youtube.com/watch?v=PiS3pRRj994> (дата обращения: 19.02.2024).
2. Прохоренок К., Дронов В. HTML, JavaScript, PHP и MySQL Джентльменский набор Web-мастера / Николай Прохоренок, Владимир Дронов. – 5-е изд. – Санкт-Петербург: «БХВ-Петербург», 2019. – 913 с. – ISBN 978-5-9775-3986-9.
3. Grinberg M. Flask Web Development Developing Web Application With Python / Miguel Grinberg. – 2-е изд. – O’Reilly Media, 2022. – 314 с. – ISBN 978-1-491-99173-2.
4. Введение во Flask. – 2021. – URL: https://pythonru.com/uroki/1-vvedenie-vo-flask (дата обращения: 20.03.2024).
5. Коберн А. Современные методы описания функциональных требований к системам / А. Коберн. – Москва: Издательство «Лори», 2012. – 264 с. – ISBN 978-5-85582-326-4.
6. Мидоус Ф. Введение в протоколы HTTP и HTTPS / Филлип Мидоус. – 2022. – URL: https://docs.microsoft.com/ru-ru/azure/rtos/netx-duo/netx-duo-web-http/chapter1 (дата обращения: 05.05.2022).

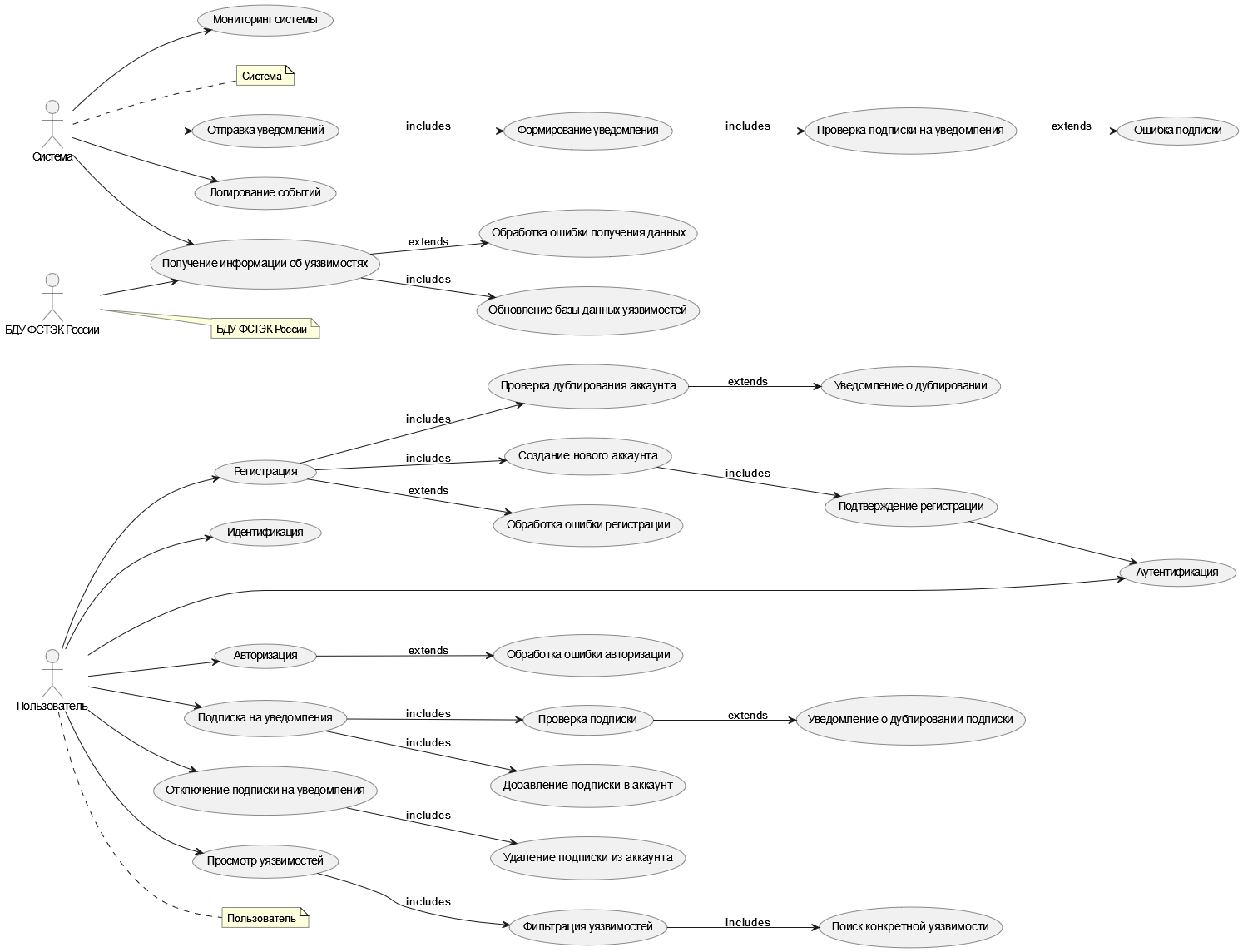
ПРИЛОЖЕНИЕ А

Название проекта: «Sploit2Me»

Руководитель проекта: Жмайло Михаил Александрович



ПРИЛОЖЕНИЕ Б



ПРИЛОЖЕНИЕ В

