**Министерство образования и науки Российской Федерации**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Владимирский государственный университет имени Александра Григорьевича

и Николая Григорьевича Столетовых» (ВлГУ)

Институт информационных технологий и электроники

Кафедра информатики и защиты информации

**ОТЧЕТ**

**О ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ**

**Разработка удаленного хранилища с мандатной и ролевой моделью управления доступом**

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к.т.н. доцент кафедры ИЗИ

подпись, дата Ю.М. Монахов

Исполнитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ студент группы ИБ-122

подпись, дата Д.С. Чугров

Владимир 2024

Оглавление

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Стр. |
| Введение | | | 4 |
| Глава 1. «Уточнение требований» | | | 6 |
| 1.1. |  | Анализ и декомпозиция предметной области | 6 |
| 1.2. |  | Обзор аналогов | 9 |
|  | 1.2.1. | Synology DiskStation Manager | 9 |
|  | 1.2.2. | QNAP QTS | 9 |
|  | 1.2.3. | WD My Cloud OS | 9 |
|  | 1.2.4. | Сравнение аналогов | 9 |
|  | 1.2.5. | Вывод из сравнения аналогов | 10 |
| 1.3. |  | Техническое задание | 10 |
|  | 1.3.1. | Требования к файловой системе | 10 |
|  | 1.3.2. | Требования к ролевой модели доступа | 10 |
|  | 1.3.3. | Требования к протоколу обмена данными | 10 |
|  | 1.3.4. | Требования к веб-сервису | 10 |
|  | 1.3.5. | Требования к основным страницам сервиса | 10 |
|  |  | 1.3.5.1. Страница аутентификации | 10 |
|  |  | 1.3.5.2. Основная страница хранилища | 11 |
|  |  | 1.3.5.3. Страница добавления файла | 11 |
|  |  | 1.3.5.4. Панель управления владельца | 11 |
|  |  | 1.3.5.5. Панель управления администратор | 11 |
|  | 1.3.6. | Допустимые размеры файлов | 11 |
|  | 13.7. | Требования к серверу | 12 |
| 1.4. |  | Техническое задание к MVP | 12 |
|  | 1.4.1. | Требования к файловой системе | 12 |
|  | 1.4.2. | Требования к ролевой модели доступа | 12 |
|  | 1.4.3. | Требования к протоколу обмена данными | 12 |
|  | 1.4.4. | Требования к веб-сервису | 12 |
|  | 1.4.5. | Требования к основным страницам сервиса | 12 |
|  |  | 1.4.5.1. Страница аутентификации | 12 |
|  |  | 1.4.5.2. Основная страница хранилища | 12 |
|  |  | 1.4.5.3. Страница добавления файла | 13 |
|  |  | 1.4.5.4. Панель управления владельца | 13 |
|  |  | 1.4.5.5. Панель управления администратор | 13 |
|  | 1.4.6. | Допустимые размеры файлов | 13 |
|  | 1.4.7. | Требования к серверу | 13 |
|  | Глава 2. «Удаленное хранилище с мандатной и ролевой моделью управления доступом» | | 14 |
| 2.1. |  | Обоснование выбора языка разработки и фрэймворка | 14 |
| 2.2. |  | Обоснование выбора СУБД | 14 |
| 2.3. |  | Протокол обмена данными | 14 |
| 2.4. |  | План разработки | 14 |
| 2.5. |  | Описание страниц веб-сервиса | 15 |
|  | 2.5.1. | /login | 15 |
|  | 2.5.2. | /files | 15 |
|  | 2.5.3. | /folders | 15 |
|  | 2.5.4. | Страница папки пользователя | 16 |
|  | 2.5.5. | /profile | 17 |
|  | 2.5.6. | /addAdmin и /addUser | 17 |
|  | 2.5.7. | /users | 17 |
| 2.6. |  | Расчет необходимой памяти жесткого диска | 19 |
|  | Глава 3. «Тестирование веб-сервиса» | | 20 |
| 3.1. |  | Результаты функционального тестирования | 20 |
| 3.2. |  | Результаты нагрузочного тестирования | 20 |
|  |  | 3.2.1. Тест №1 «Имитация попытки неавторизированных пользователей войти в систему» | 20 |
|  |  | 3.2.2. Тест №2 «Имитация попытки авторизированных пользователей войти в систему» | 22 |
|  |  | 3.2.3. Тест №3 «Имитация попытки авторизированных пользователей загрузить файлы в папку» | 23 |
| 3.3. |  | Результаты тестирования работы веб-сервиса в различных браузерах | 24 |
|  | Список использованной литературы | | 25 |
|  | Ссылка на исходный код веб-сервиса | | 26 |

Введение

На первых этапах развития бизнеса, когда ресурсы ограничены и каждый их расход тщательно контролируется, одним из наиболее экономически выгодных решений для хранения данных является использование локального хранилища. Как правило локальное хранилище основано на отдельных жестких дисках, представляет собой доступный и простой в реализации способ управления информацией.

Однако, по мере того как компания начинает расти и объем данных увеличивается, локальное хранилище может создавать определенные сложности. Во-первых, возникает риск замедления бизнес-процессов из-за ограниченной пропускной способности и необходимости регулярного обслуживания оборудования. Внезапное увеличение нагрузки на систему может привести к снижению скорости доступа к данным, что негативно скажется на эффективности работы сотрудников и на многое другое.

Во-вторых, использование локального хранилища без должной защиты несет риск несанкционированного доступа к информации. Так конфиденциальная информация может оказаться под угрозой утечки, что в свою очередь может причинить серьезный финансовый и репутационный ущерб для компании.

В-третьих, локальное хранилище не в состоянии обеспечить качественную работу отделов компании, находящиеся в различных точках мира. За счет этого становится невозможно построить эффективное взаимодействие с между собой.

Учитывая все вышеперечисленное, становится очевидной необходимость перехода к более продвинутым решениям, таким как удаленная система хранения данных. Такая система предоставляет множество преимуществ, включая возможность доступа к информации для авторизованных пользователей из любой точки мира, что особенно актуально в условиях современной мобильности и удаленной работы. Веб-сервис, обеспечивающий доступ к файлам, позволяет эффективно управлять правами пользователей, разграничивая уровни доступа и обеспечивая высокий уровень безопасности данных.

Таким образом, анализируя все факторы, становится понятно, что создание удаленной системы хранения данных является актуальным и неотъемлемым шагом для растущей компании, стремящейся к повышению безопасности и эффективности своих бизнес-процессов.

Предметной областью данного проекта является разработка удаленного хранилища данных.

Цель данной разработки за время производственной практики создать веб-сервис удаленного хранилища с моделью ролевого управления доступа, которое способно успешно выполнять свой функционал и обеспечивает доступ авторизированным пользователям к файловой системе в соответствии с их ролью. Для достижения этой цели должны быть решены следующие задачи:

1) Разработать веб- сервис удаленного хранилища данных, позволяющий взаимодействовать с файлами дистанционно;

2) Реализовать систему авторизации для недопущения сторонних лиц;

3) Создать систему ролей и мандатную модель разграничения прав доступа субъектов к файловым объектам;

4) Реализовать панель владельца и администратора для создания, удаления субъектов, изменения их ролей и уровня доступа.

Глава 1. «Уточнение требований»

1.1. Анализ и декомпозиция предметной области

Удаленное хранилище с ролевым управлением доступа - это система хранения данных, находящаяся на виртуальном сервере, реализованная вместе с моделью ролевого управления доступа, где доступ к объекту осуществляется в зависимости от роли субъекта. Данный сервис представляет собой частное хранилище.

Отличительная особенность удаленных хранилищ данных заключается в их доступности законным пользователям независимо от их местоположения, имея стабильное Интернет- подключение. Такую возможность предоставляет веб-сервис, позволяющий сохранять различные документы, фотографии и видео для хранения их за пределами рабочего устройства.

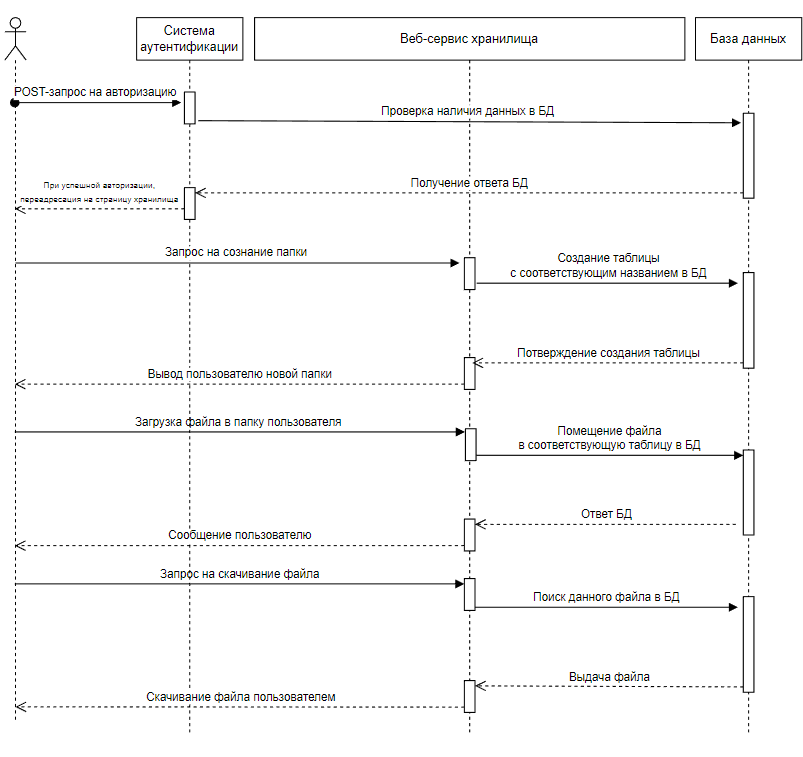
Удаленное хранилище предусматривает реализацию следующую систему разделения ролей:

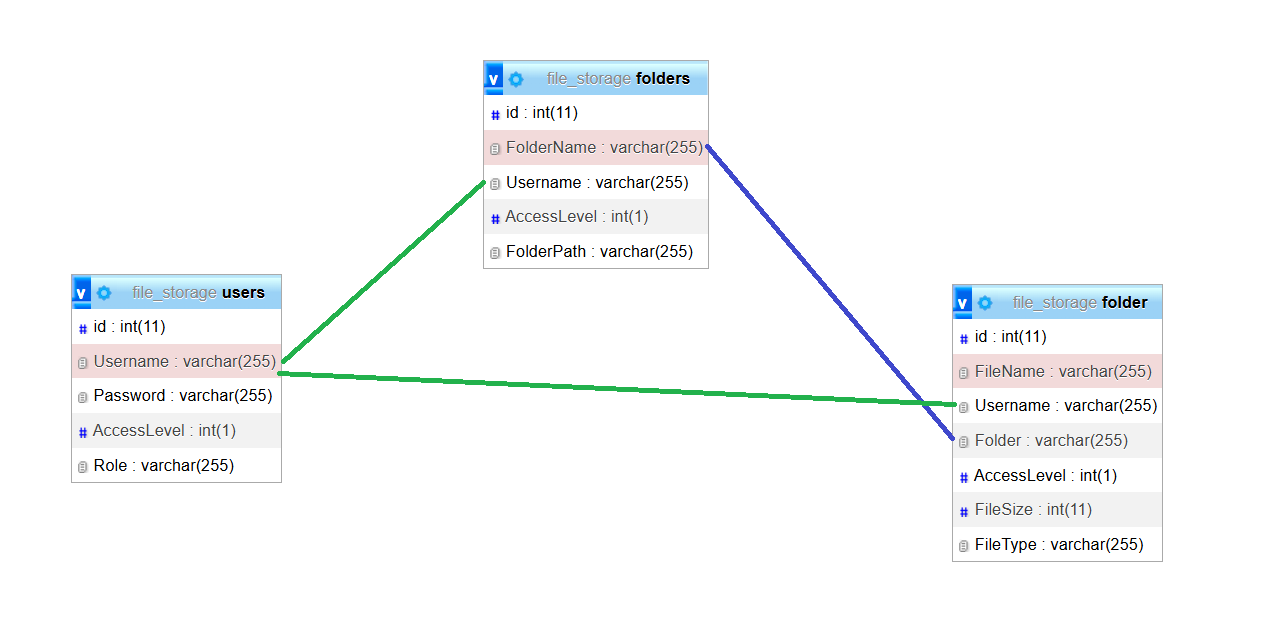
|  |  |  |
| --- | --- | --- |
| Название роли | Функции | Количество пользователей |
| Владелец | 1) Удаление папок других пользователей  2) Удаление файлов других пользователей  3) Назначение администраторов | 1 пользователь |
| Администратор | 1) Создание субъектов (регистрация нового пользователя)  2) Изменение уровня доступа субъекта к файлам  3) Удаление субъектов (пользователей) | Не менее 1 пользователя |
| Авторизированный пользователь | 1) Загрузка новых файлов  2) Удаление собственных папок и файлов  3) Добавление собственных файлов в чужие папки  4) Скачивание/Удаление чужих файлов в соответствии с уровнем доступа | Не ограничено |
| Неавторизированный пользователь | Не имеет доступ к системе | Не ограничено |

Также предполагается наличие у авторизированных пользователей уровня доступа к файлам. Система по мере возрастания: Public, Secret, Top secret. Важно отметить, что владелец системы по умолчанию имеет уровень доступа Top Secret. Также администратором может стать пользователь только с уровнем Top Secret.

|  |  |
| --- | --- |
| Уровень доступа | Возможности |
| Public | - Загрузка файлов в папки с соответствующим уровнем доступа  - Просмотр и удаление папок с соответствующим уровнем доступа  - Скачивание, удаление файлов с соответствующим уровнем доступа  - Загрузка файлов в папки с уровнем Secret без возможности просмотра содержимого папки |
| Secret | - Загрузка файлов в папки с соответствующим уровнем доступа  - Просмотр и удаление папок с соответствующим уровнем доступа  - Скачивание, удаление файлов с соответствующим уровнем доступа  - Просмотр содержимого папок с уровнем Public  - Скачивание файлов с уровнем Public  - Загрузка файлов в папки с уровнем Top Secret без возможности просмотра содержимого папки |
| Top Secret | - Загрузка файлов в папки с соответствующим уровнем доступа  - Просмотр и удаление папок с соответствующим уровнем доступа  - Скачивание, удаление файлов с соответствующим уровнем доступа  - Просмотр содержимого папок с уровнями Public и Secret  - Скачивание файлов с уровнем Public и Secret |

Общая диаграмма-последовательности и структура базы данных для удаленного хранилища





1.2. Обзор аналогов

1.2.1. Synology DiskStation Manager

Synology DiskStation Manager - это программное обеспечение на основе веб-интерфейса, совместимая со всеми устройствами Synology NAS и обеспечивающая управление цифровыми ресурсами во всех сетевых размещениях. Оно представляет собой простую интеграцию устройства NAS в любую среду благодаря обширной поддержке браузеров.

1.2.2. QNAP QTS

QNAP QTS - это программный пакет, разработанная для управления NAS-устройствами от компании QNAP. Она предлагает пользовательский интерфейс с обширным набором функций для эффективного управления данными и обеспечения безопасности. QTS поддерживает интеграцию с различными сетевыми протоколами и облачными сервисами, делая её подходящей для широкого спектра задач — от домашнего использования до корпоративных сред.

1.2.3. WD My Cloud OS

WD My Cloud OS - это программное обеспечение, созданное для управления NAS-устройствами компании Western Digital. Оно предоставляет простой интерфейс для управления цифровыми данными. My Cloud OS ориентирована на домашних пользователей и малые офисы, предлагая базовые функции для доступа к данным через веб-интерфейс, что делает управление данными удобным и доступным с любого устройства.

1.2.4. Сравнение аналогов

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | Synology DiskStation Manager | QNAP QTS | WD My Cloud OS |
| Интерфейс | Веб-сервис | Веб-сервис | Веб-сервис |
| Наличие ролевой модели доступа | Есть | Есть | Нет |
| Наличие мандатного управления доступа | Нет | Нет | Нет |
| Наличие системы аутентификации | Есть | Есть | Есть |
| Наличие журнала событий | Есть | Есть | Есть |
| Возможность установки на ПК или устройства сторонних компаний | Есть | Нет | Нет |

1.2.5. Вывод из сравнения аналогов

Исходя из сравнения аналогов можно сделать вывод о отсутствии у выше перечисленных программных обеспечений возможности удобного развертывания системы на любом устройстве (ПК или специальном хранилище) и мандатной модели управления доступом, которая способна обеспечить высокий уровень безопасности.

1.3. Техническое задание

1.3.1. Требования к файловой системе

1) Файлы должны быть видимы и доступны для скачивания только тем субъектам, которые имеют соответствующий уровень доступа.

2) Субъекты имеют право загружать файлы со указанием соответствующего уровня доступа.

1.3.2. Требования к ролевой модели доступа

Должна быть реализована модель доступа со следующими ролями: владелец, администратор и авторизированный пользователь.

1.3.3. Требования к протоколу обмена данных

Протокол обмена данными должен соответствовать современным стандартам безопасности, производительности и совместимости.

1.3.4. Требования к веб-сервису

Веб-сервису должен содержать следующие страницы:

1) Страница аутентификации;

2) Основная страница хранилища;

3) Страница добавления файла;

4) Панель управления владельца;

5) Панель управления администратора;

1.3.5. Требования к основным страницам сервиса

1.3.5.1. Страница аутентификации

Страница аутентификации должна предусматривать возможность авторизации пользователя. При положительном результате происходит переадресация на основную страницу хранилища. При ином - пользователю предлагается ввести данные заново.

1.3.5.2. Основная страница хранилища

Основная страница хранилища выводит доступные для просмотра/скачивания файлы в соответствии с уровнем доступа пользователя и журнал событий для отслеживания изменений. Также она должна содержать такие ссылки:

1) Ссылка на панель управления владельца (если пользователь владеет директорией);

2) Ссылка на панель управления администратора (если пользователь является администратором);

3) Ссылка на страницу добавления файла в директорию.

1.3.5.3. Страница добавления файла

Страница добавления файла предоставляет возможность загрузить допустимый размером файл и задать ему имя.

1.3.5.4. Панель управления владельца

Панель управления владельца должна быть доступна для взаимодействия пользователю со соответствующей ролью. Здесь он может:

1) Создать или удалить директорию;

2) Назначить администраторов;

3) Передать права над директорией другому пользователю;

4) Видеть на сколько заполнен диск.

1.3.5.5. Панель управления администратора

Панель управления администратора должна быть доступна для взаимодействия пользователю со соответствующей ролью. Здесь он может:

1) Создать субъекты (регистрация нового пользователя);

2) Задать или изменить уровень доступа к файлам;

3) Удалить субъекта (пользователя);

4) Удалить файлы.

1.3.6. Допустимые размеры файлов

Для документов: не более 50 Мб.

Для таблиц: не более 100 Мб.

Для видеоматериалов: не более 400 Мб.

1.3.7. Требования к серверу

* Не менее 4 ядер процессора;
* Не менее 256 Гб дискового пространства;
* Не менее 8 Гб ОЗУ;
* Операционная система: Ubuntu.

1.4. Техническое задание к MVP

1.4.1. Требования к файловой системе

1) Файлы должны быть видимы и доступны для скачивания только тем субъектам, которые имеют соответствующий уровень доступа.

2) Субъекты имеют право загружать файлы со указанием соответствующего уровня доступа.

1.4.2. Требования к ролевой модели доступа

Должна быть реализована модель доступа со следующими ролями: владелец, администратор и авторизированный пользователь.

1.4.3. Требования к протоколу обмену данными

Протокол обмена данными должен соответствовать современным стандартам безопасности, производительности и совместимости.

1.4.4. Требования к веб-сервису

Веб-сервис должен содержать следующие страницы:

1) Страница аутентификации;

2) Основная страница хранилища;

3) Страница добавления файла;

4) Панель управления владельца;

5) Панель управления администратора;

1.4.5. Требования к основным страницам сайта;

1.4.5.1. Страница аутентификации

Страница аутентификации должна предусматривать возможность авторизации пользователя. При положительном результате происходит переадресация на основную страницу хранилища. При ином - пользователю предлагается ввести данные заново.

1.4.5.2. Основная страница хранилища

Основная страница хранилища выводит доступные для просмотра/скачивания файлы в соответствии с уровнем доступа. Также она должна содержать такие ссылки:

1) Ссылка на панель управления владельца (если пользователь владеет директорией);

2) Ссылка на панель управления администратора (если пользователь является администратором);

3) Ссылка на страницу добавления файла в директорию.

1.4.5.3. Страница добавления файла

Страница добавления файла предоставляет возможность загрузить допустимый размером файл и задать ему имя.

1.4.5.4. Панель управления владельца

Панель управления владельца должна быть доступна для взаимодействия пользователю со соответствующей ролью. Здесь он может:

1) Создать или удалить директорию;

2) Назначить администраторов;

3) Передать права над директорией другому пользователю;

4) Видеть на сколько заполнен диск.

1.4.5.5. Панель управления администратора

Панель управления администратора должна быть доступна для взаимодействия пользователю со соответствующей ролью. Здесь он может:

1) Создать субъекты (регистрация нового пользователя);

2) Задать или изменить уровень доступа к файлам;

3) Удалить субъекта (пользователя);

4) Удалить файлы.

1.4.6. Допустимые размеры файлов

Для документов: не более 10 Мб.

Для таблиц: не более 10 Мб.

Для видеоматериалов: не более 100 Мб.

1.4.7. Требования к серверу

* Не менее 10 Гб дискового пространства;
* Не менее 2 Гб ОЗУ;
* Операционная система: Ubuntu.

Глава 2. Удаленное хранилище с мандатной и ролевой моделью управления доступом

2.1. Обоснование выбора языка разработки и фрэймворка.

Для реализации удаленного хранилища был выбран язык разработки Java, т.к. он позволяет запускать приложения на различных платформах без необходимости вносить изменения в код, что особенно важно для данного веб-сервиса. Более того, Java работает на виртуальной машине (JVM), которая эффективно управляет ресурсами и предоставляет высокую производительность приложений. Также в качестве фрэймворка был выбран Spring Framework, т.к. он построен по модульному принципу, что позволяет использовать только те его компоненты, которые необходимы для конкретного проекта. Это повышает гибкость и уменьшает зависимость от ненужных модулей.

2.2. Обоснование выбора СУБД

В качестве СУБД был выбран Redis, т.к. она поддерживает не только простые ключ-значение пары, но и более сложные структуры данных, такие как списки, множества, хеши. Более того, она работает в оперативной памяти, что позволяет обрабатывать запросы с минимальной задержкой (обычно в пределах миллисекунд). Для визуализации данных базы данных используется RedisInsight.

2.3. Протокол обмена данными

Для обмена данных удаленное хранилище использует протокол Http/2. Он демонстрирует гораздо более значительное технологическое превосходство над своим предшественником, чем HTTP 1.x в своё время. Более того, использование HTTP/2 — это шаг на пути к увеличению скорости загрузки страниц.

Для передачи данных используется протокол TLS 1.3. Соединение сервиса зашифровано и проверено с помощью AES\_128\_GSM. В качестве механизма обмена ключами используется X25519.

2.4. План разработки

Этап 1: Реализация страниц создания папки и загрузки/скачивания файла.

Этап 2: Создании системы авторизации пользователя.

Этап 3: Реализация функций удаления папок и файлов.

Этап 4: Создание системы ролей, соответствующих страниц и распределение функционала.

Этап 5: Реализация мандатной модели управления доступа.

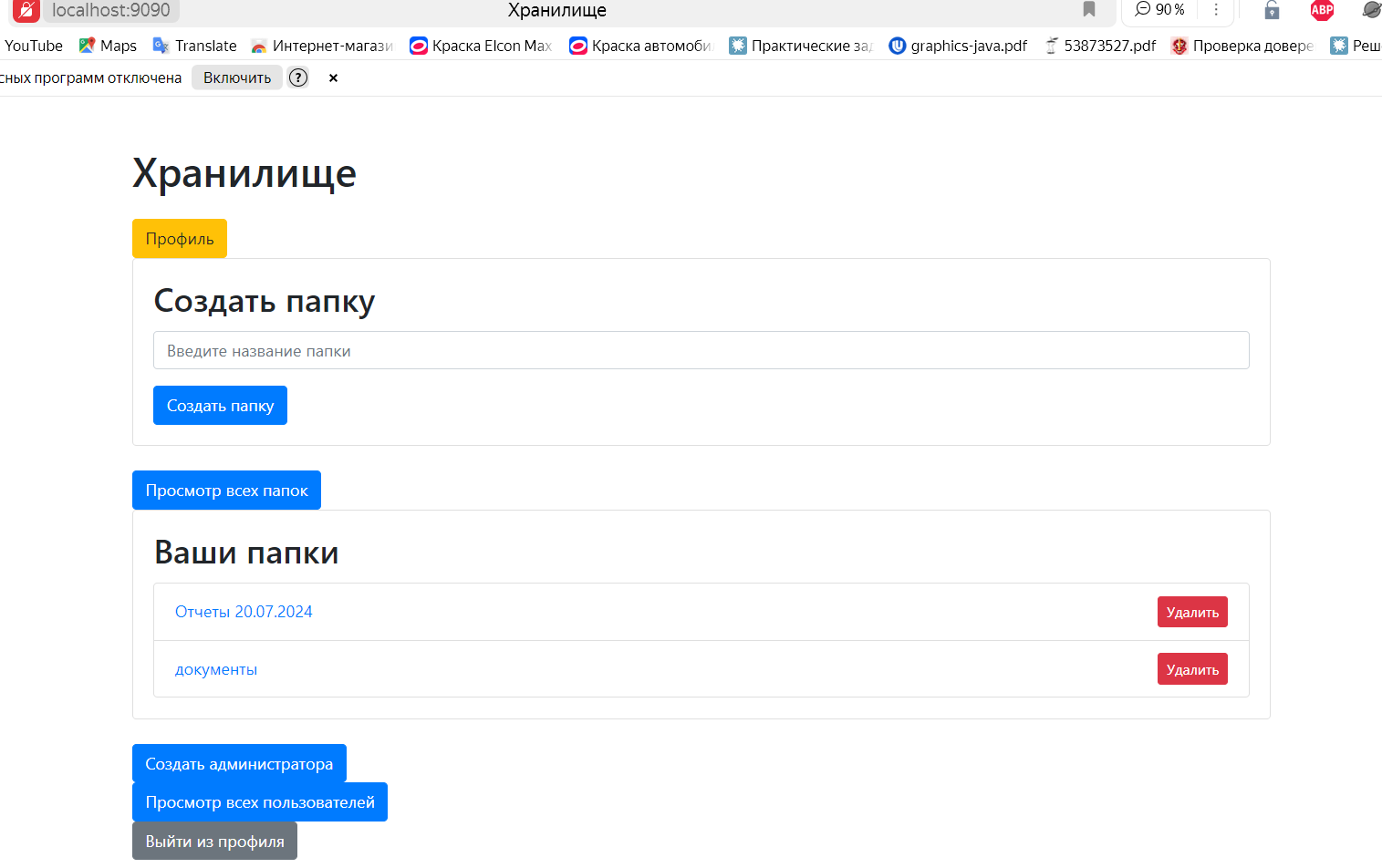
2.5. Описание страниц веб-сервиса

2.5.1. /login

Страница /login позволяет пользователю войти в систему. Если были введены неверные данные, то сервис предлагает произвести авторизацию заново.

2.5.2. /files

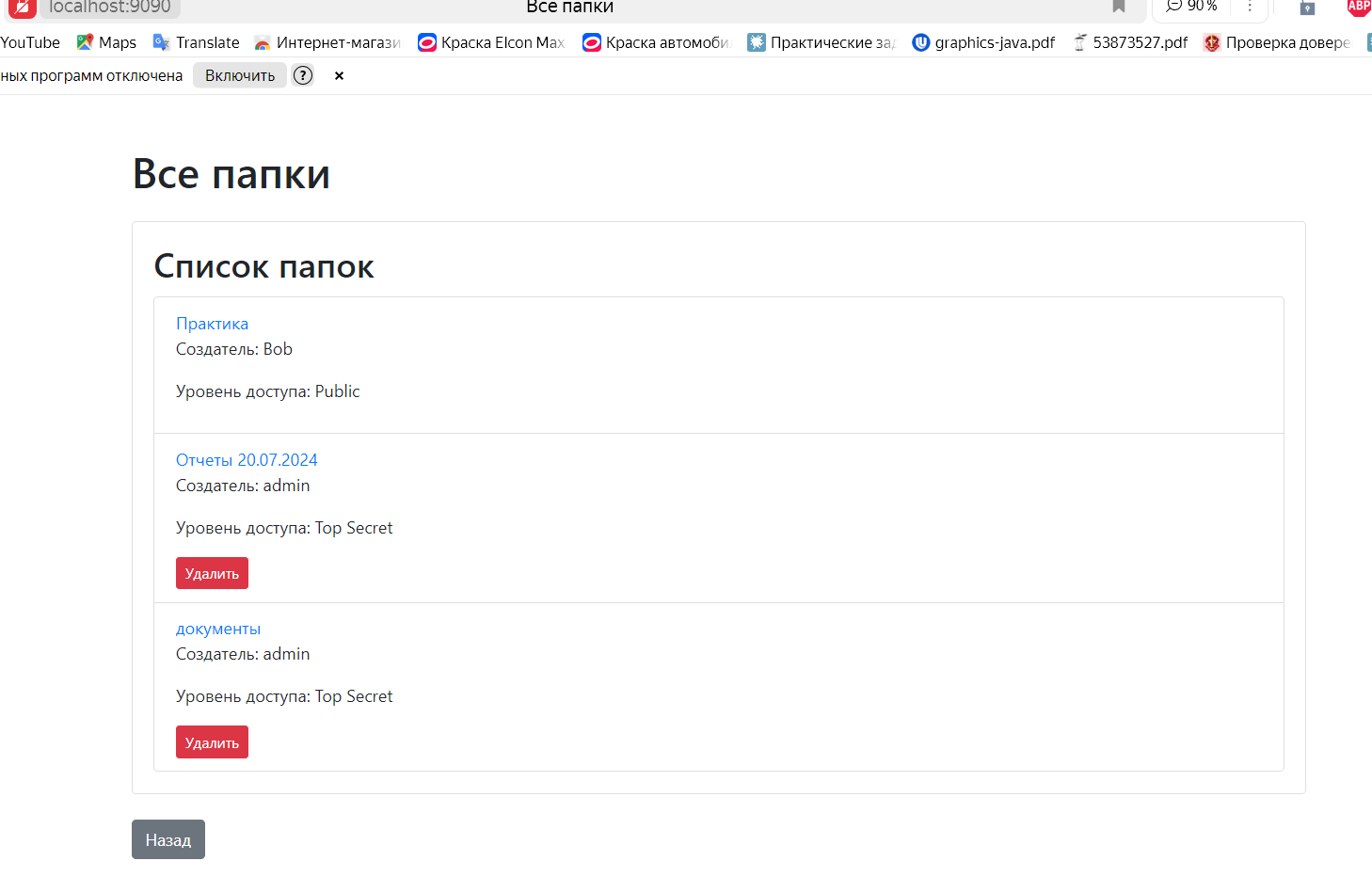
Эта страница является основной. Здесь пользователь может создавать собственные папки с соответствующим уровнем доступом. Кроме того, отсюда можно перейти в собственный профиль, просмотреть чужие папки и открывать собственные, создать пользователя с ролью администратор (доступно только для владельца), создать обычного пользователя (доступно только для администратора), просмотреть всех существующих пользователей и выйти из системы.



Пример страницы /files для владельца.

2.5.3. /folders

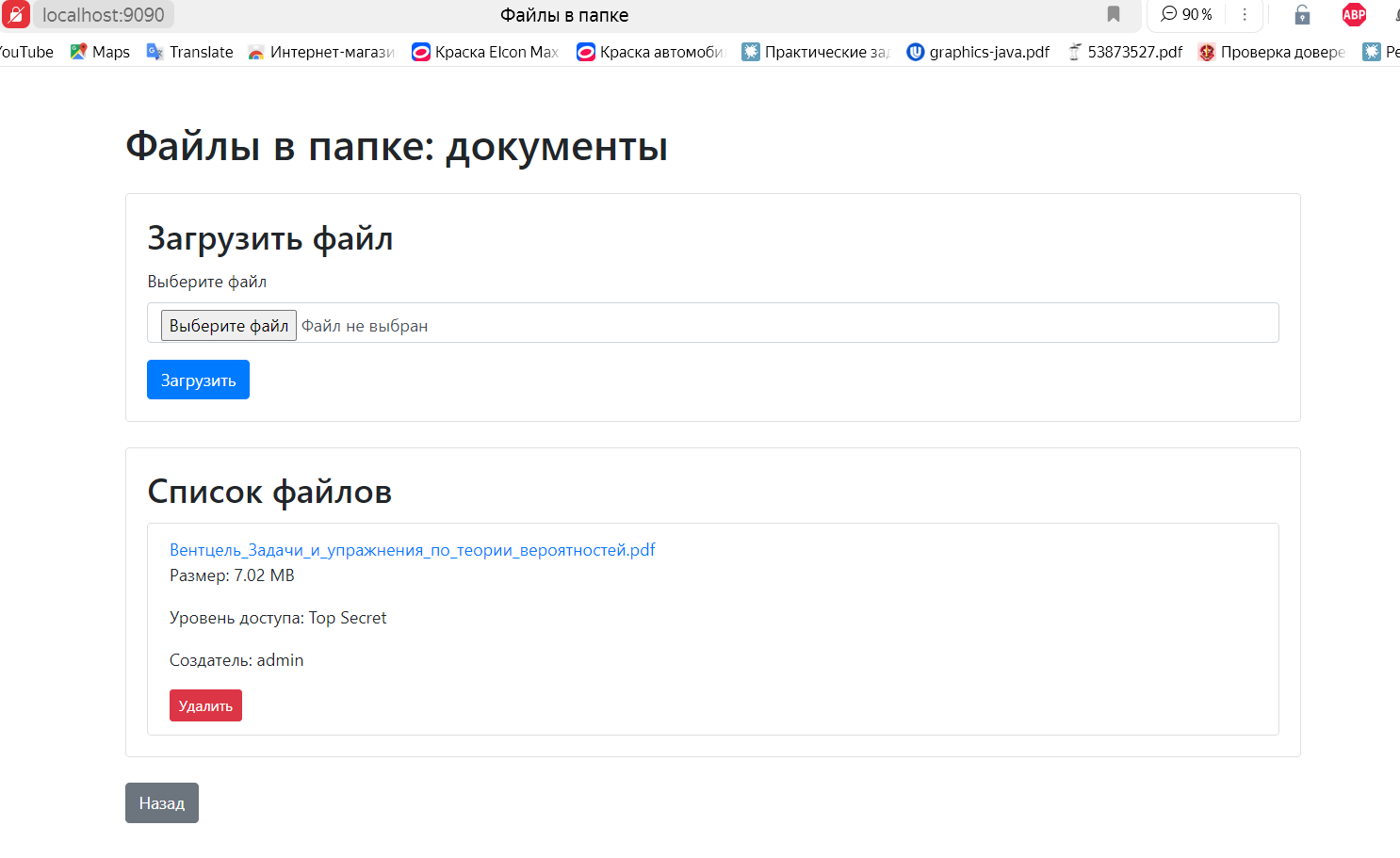
На данной странице пользователю отображаются все существующие папки, в соответствии с его уровнем доступа. Также здесь он может удалить как собственную, так и чужую папку, если такое возможно.



Пример страницы /folders для администратора

2.5.4. Страница папки пользователя

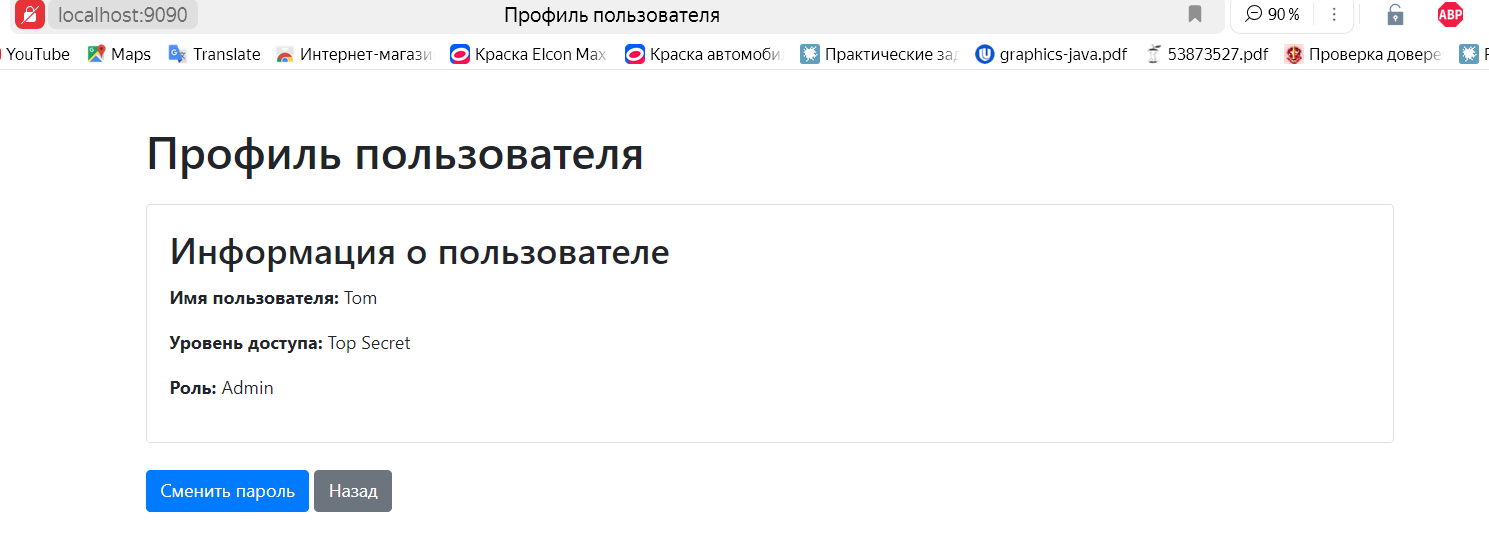
Благодаря этой странице пользователь может ознакомится с содержимым папки. Здесь доступно удаление, загрузка и скачивание файла в зависимости от уровня доступа пользователя.



Пример содержания папки «документы»

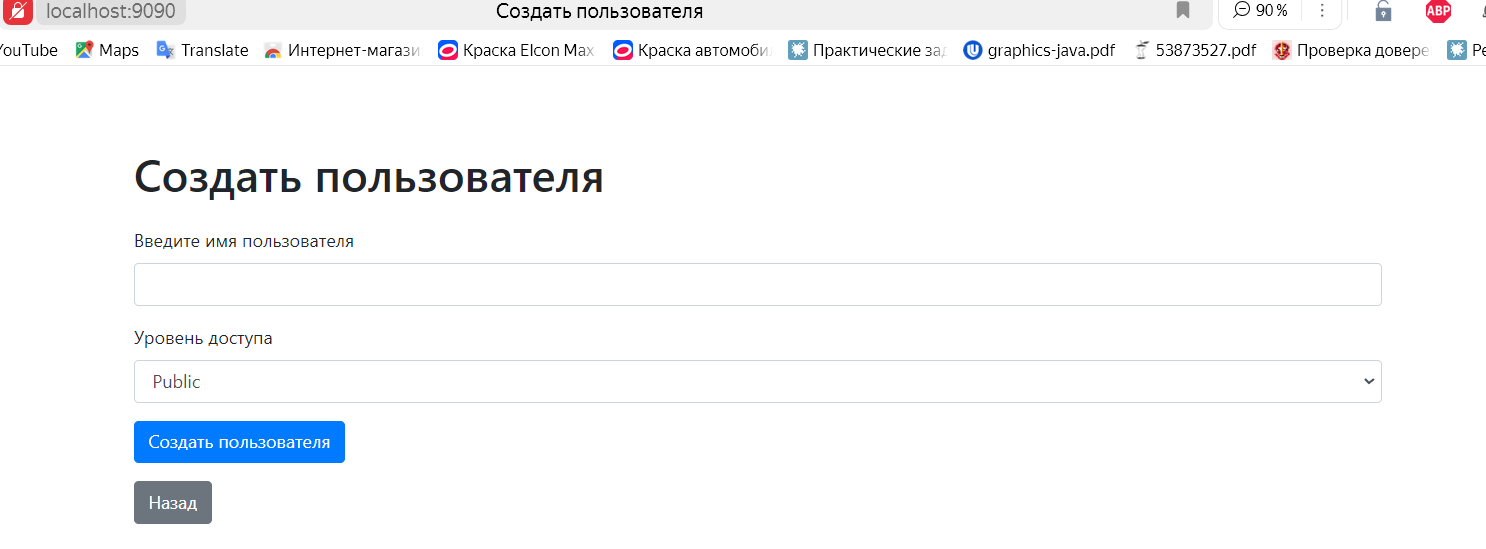
2.5.5. /profile

Данная страница является профилем пользователя. Здесь он может ознакомится со своим уровнем доступа и роль. Более того, здесь пользователь может сменить пароль для своей учетной записи.



2.5.6. /addAdmin и /addUser

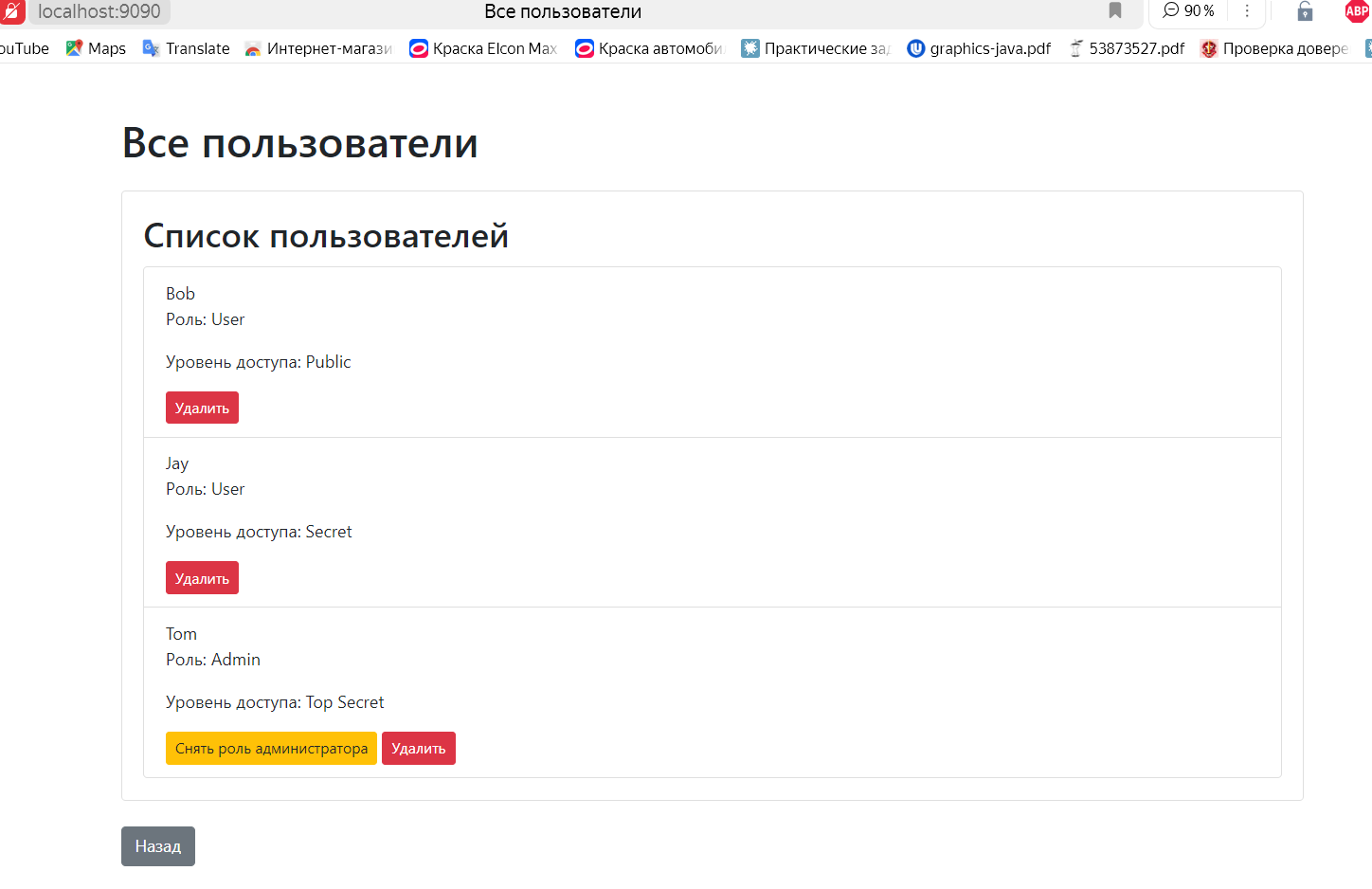
Данные страницы предоставляют возможность зарегистрировать в систему администратора или обычного пользователя. Они доступны только для владельца и для администратора соответственно.



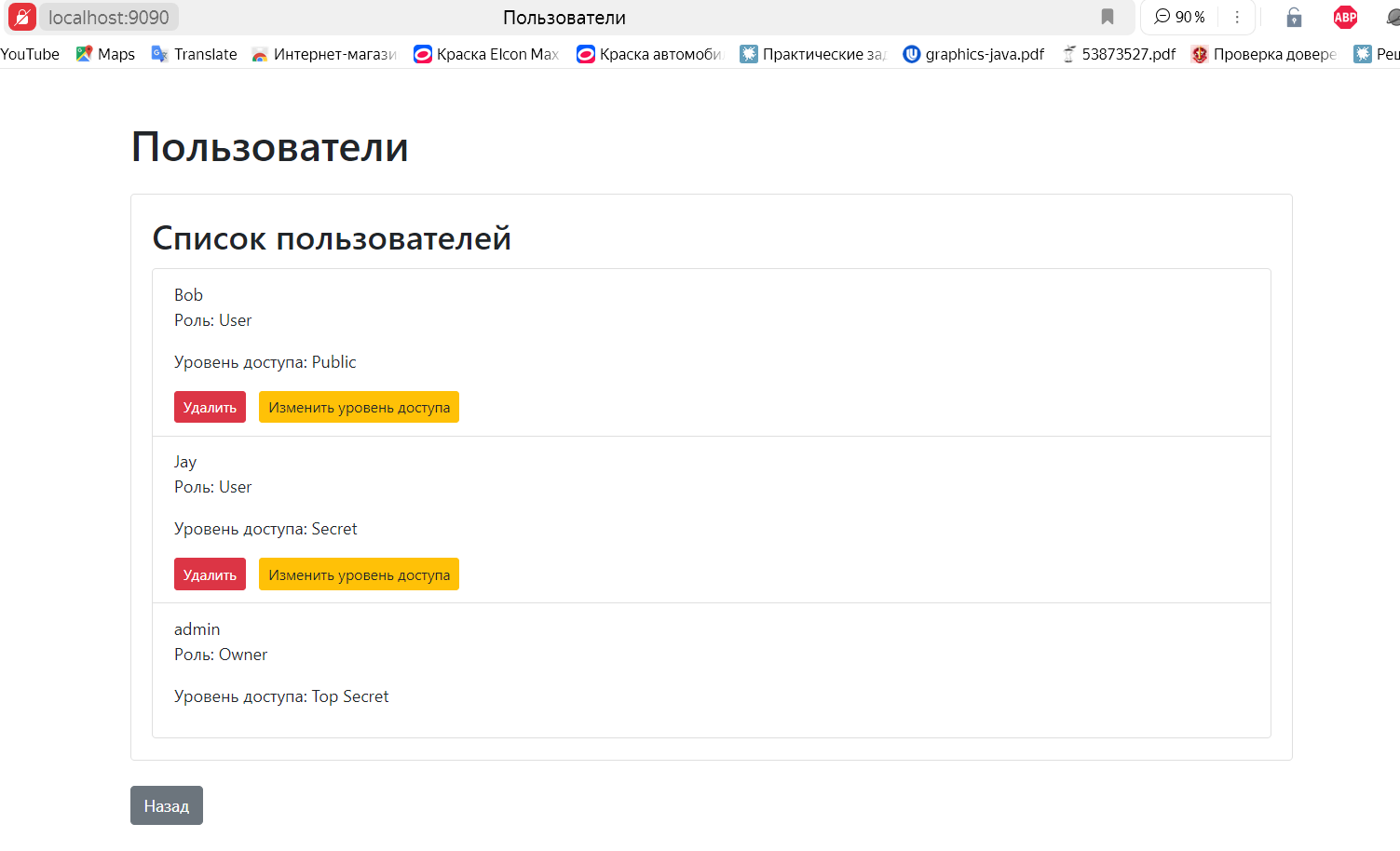
Пример заполнения формы для регистрации обычного пользователя

2.5.7. /users

Данная страница доступна только для владельца и администратора. Здесь можно ознакомится со списком пользователей, зарегистрированных в системе и произвести необходимые операции с ними.



Пример страницы /user для владельца



Пример страницы /user для администратора

2.6. Расчет необходимой памяти жесткого диска

Для расчета необходимо перечислить все необходимые компоненты для функционирования системы:

1) Java JDK (185 МБ);

2) Зависимости для Java (26 МБ);

3) Ubuntu OC (5,7 ГБ);

4) СУБД Redis (5 МБ).

5) Папка с исходным кодом (8 МБ)

Значит,

185 МБ + 26 МБ + 5,7 ГБ + 5 МБ + 8 МБ ≈ 6 ГБ.

Итого: для работы веб-сервиса необходимо пример 6 ГБ памяти жесткого диска. Однако, при выборе накопителя нужно учитывать объем предполагаемый данных, которые будут на нем находится.

Глава 3. Тестирование веб-сервиса

3.1. Результаты функционального тестирования

Функционального тестирование заключалось в проверке работоспособности всех функций, доступных пользователям. Испытания показали, что все процессы выполняются корректно.

3.2. Результаты нагрузочного тестирования

В процессе тестирования будет проверятся способность обработки веб-сервисом запросов на авторизацию и загрузки файлов в папку при пиковой нагрузке. Для этого будут использоваться такие программы, как JMeter (позволяет моделировать трафик от пользователей) и VisualVM (инструмент для мониторинга, анализа и профилирования Java-приложений в реальном времени.).

3.2.1. Тест №1 «Имитация попытки неавторизированных пользователей войти в систему»

Для данного теста созданы 100 потоков, пытающихся с неверными логинами и/или паролями войти в систему. В результате, все запросы были обработаны, все потоки были перенаправлены на страницу повторного ввода данных.

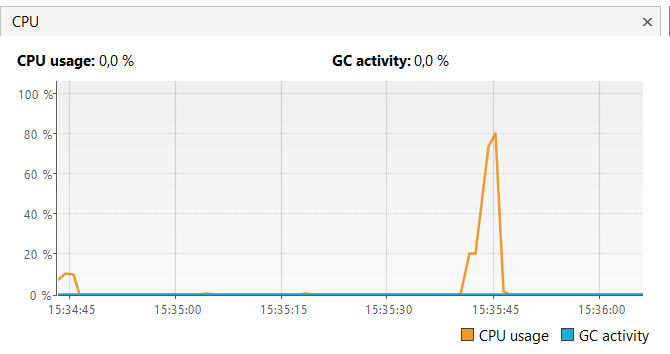


График нагрузки CPU

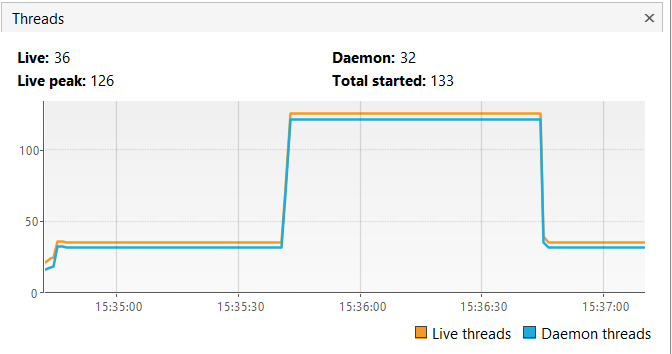
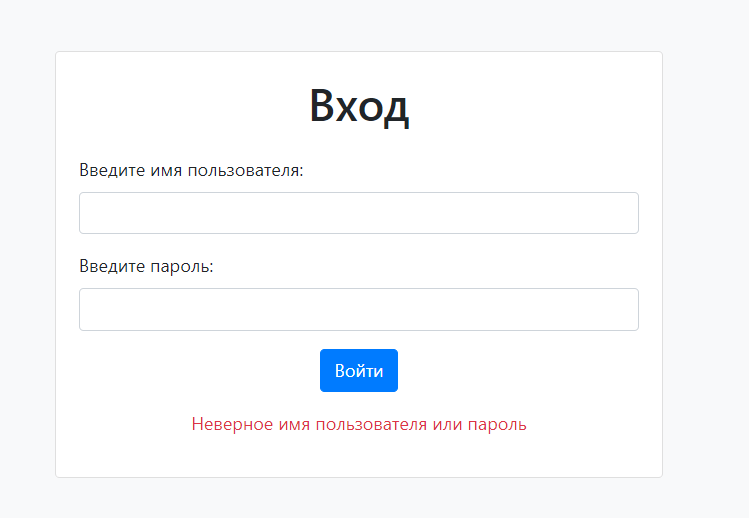


График создания потоков для обработки запросов



Страница авторизации при использовании неверных данных

3.2.2. Тест №2 «Имитация попытки авторизированных пользователей войти в систему»

Для данного теста созданы 100 потоков, пытающихся с верными логинами и паролями войти в систему. В результате, все запросы были обработаны, все потоки были перенаправлены на основную страницу хранилища.

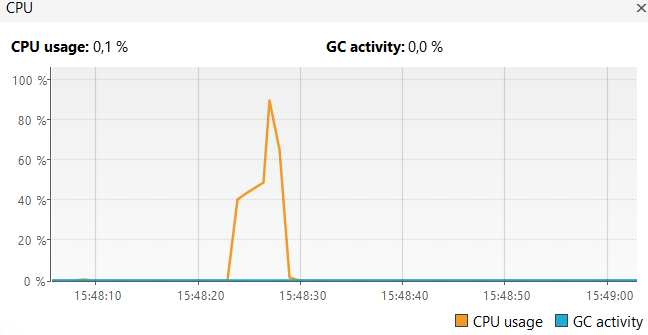
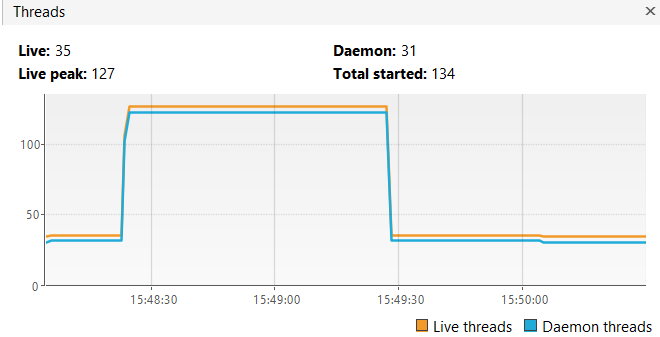


График нагрузки CPU

 График создания потоков для обработки запросов

3.2.3. Тест №3 «Имитация попытки авторизированных пользователей загрузить файлы в папку»

Для данного теста созданы 100 потоков, один из которых создает папку, а остальные пытаются загрузить в нее файлы. Каждый файл представляет собой картинку форматом .img размером в 32 КБ. В результате, все запросы были обработаны, папка была создана, файлы успешно загружены, все потоки были перенаправлены на страницу результата загрузки.

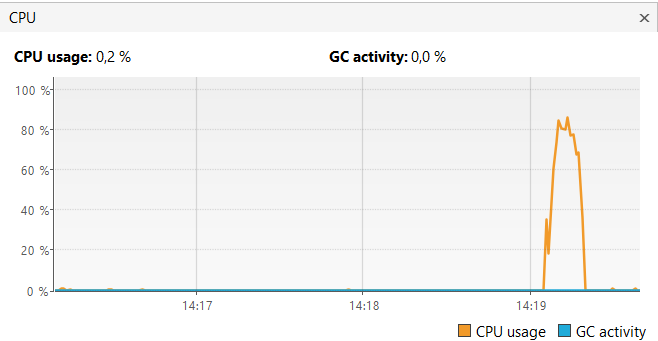


График нагрузки CPU

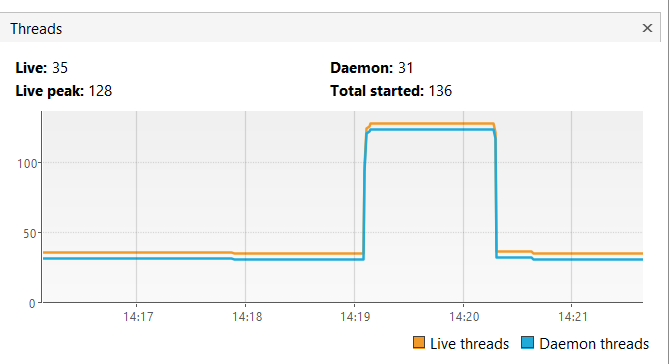


График создания потоков для обработки запросов

3.3. Результаты тестирования работы веб-сервиса в различных браузерах

Данное тестирование необходимо для доказательства работоспособности системы в различных браузерах. Для теста использовались Yandex, Google Chrome, Opera и Microsoft Edge. Результаты показали, что веб-сервис отображался во всех выше перечисленных браузерах корректно.

Список использованной литературы

1) Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками.

2) Menezes A. J, Oorschot P.C, Vanstote S.A.Handbook of applied cryptography.

3) Ferraiolo D. F., Kuhn D. R. Role Based Access Control.

4) Walls C. Spring in Action.

5) Deck P. Spring MVC: A Tutorial.

6) Dr. Josiah L Carlson. Redis in Action.

7) Acetozi J. Pro Java Clustering and Scalability.

8) Rushtoh N. The Little Book of QNAP QTS.

9) Prof Philip M. Parker Ph.D. The 2021-2026 World Outlook for Small and Medium-Sized Business Network-Attached Storage.

10) W. Curtis Preston. Using SANs and NAS.

Ссылка на исходный код веб-сервиса

