Реализация механизма авторизации пользователя

Описание задачи:

Необходимо реализовать механизм авторизации пользователя, который обеспечивает безопасный доступ к защищённым разделам системы по паре логин/пароль. При успешной авторизации создаётся сессия или выдается JWT-токен. В случае ошибок выводятся соответствующие сообщения.

Цель:

Обеспечить проверку подлинности пользователей, зарегистрированных в системе, и предоставить им доступ к функционалу на основе их роли и статуса.

Критерии готовности (Definition of Done):

- Страница авторизации реализована на frontend.
- Реализован API эндпоинт POST /auth/login.
- Проверка логина и пароля с использованием безопасного хеширования.
- Генерация и возврат токена (JWT) или установка сессионного cookie.
- Реализована обработка ошибок: "Неверный логин или пароль".
- Покрытие unit и интеграционными тестами ≥ 80%.
- Обновлена документация API и пользовательская инструкция.

Технические детали:

Frontend:

- Форма с валидацией логина и пароля.
- Отправка данных на backend (AJAX/Fetch).
- Отображение сообщений об ошибках.
- Хранение токена в localStorage или cookie (по решению архитектуры).

Backend:

- Эндпоинт /auth/login:
    - Получает login и password.
    - Ищет пользователя в базе по логину.
    - Сравнивает введённый пароль с хешем.
    - В случае успеха: возвращает JWT / создаёт сессию.
    - В случае ошибки: HTTP 401 + сообщение.

- Поддержка стандартных алгоритмов хеширования (например, bcrypt).

Безопасность:

- Пароли хранятся в БД только в виде хеша.
- Все соединения идут через HTTPS.
- Ограничение количества попыток входа (rate limit).

Диаграмма последовательности: