Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное   
образовательное учреждение высшего образования   
«Самарский национальный исследовательский университет   
имени академика С.П. Королева»

Институт информатики и кибернетики

Кафедра технической кибернетики

**Краткая документация по проекту   
«FluffyTailClinic»**

Выполнили:

Рыбалко Ф. А. 6305-010302D

Мурзина А. Е. 6305-010302D

Самара, 2025

**Задачи**

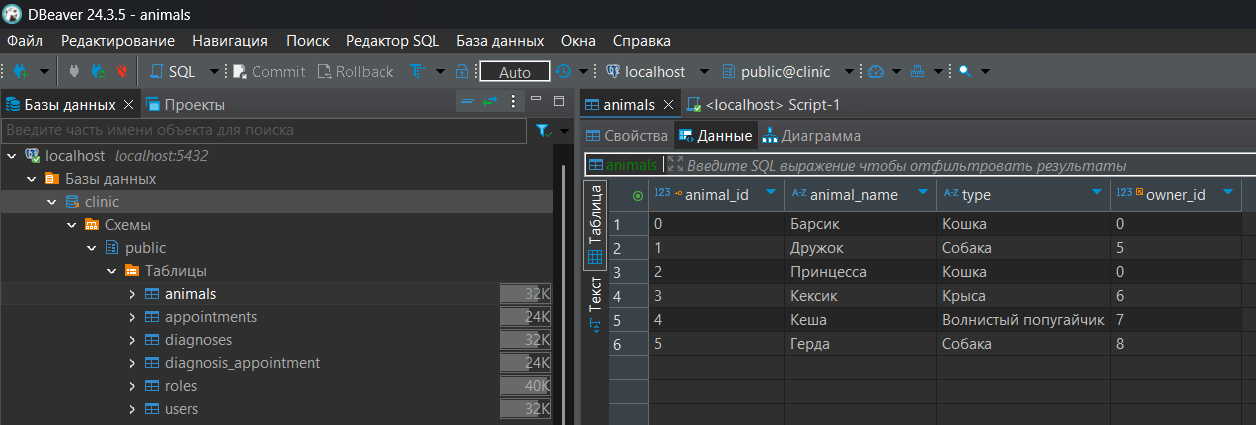
1. **Настройка базы данных**:

* **Развернуть PostgreSQL в Docker;**

Для развертывания PostgreSQL в Docker на сервере с Ubuntu через PuTTY был выполнен ряд шагов. Сначала произведено подключение к серверу Ubuntu с использованием PuTTY, где был введен IP-адрес сервера и выполнена аутентификация через SSH. После успешного подключения на сервере была установлена среда Docker: обновлены пакеты системы, установлены необходимые зависимости, добавлен GPG-ключ Docker и его репозиторий, а затем выполнена установка Docker. После установки Docker была создана директория для хранения данных PostgreSQL, чтобы обеспечить их сохранность после остановки контейнера. Затем был запущен контейнер PostgreSQL с использованием Docker, где указаны параметры для создания пользователя, пароля и базы данных, а также настроено монтирование директории для хранения данных и проброс порта 5432 для доступа к базе данных. Для проверки работоспособности контейнера использовалась команда `docker ps`, которая отобразила запущенный контейнер с именем `postgres`. Для подключения к базе данных был установлен клиент PostgreSQL, после чего выполнено подключение к базе данных с использованием команды `psql`. Для обеспечения удаленного доступа к PostgreSQL были отредактированы конфигурационные файлы `pg\_hba.conf` и `postgresql.conf`, чтобы разрешить подключение с любого IP-адреса, и контейнер был перезапущен. В завершение была проверена возможность подключения к базе данных с другого компьютера с использованием клиента PostgreSQL, что подтвердило корректность настройки и доступность базы данных.

* **Подключиться к БД через DBeaver.**

Для подключения к базе данных PostgreSQL через DBeaver был выполнен следующий процесс. Сначала в DBeaver создано новое соединение с базой данных, где был выбран тип СУБД — PostgreSQL. В настройках соединения указаны параметры: хост (IP-адрес сервера), порт (5432 по умолчанию), имя базы данных, а также логин и пароль пользователя (clinic), которые были заданы при запуске контейнера PostgreSQL в Docker. После заполнения всех необходимых полей выполнено тестирование соединения, чтобы убедиться в корректности настроек. После успешного теста соединение было сохранено, и в DBeaver отобразилась структура базы данных, включая таблицы и схемы. Это позволило выполнять SQL-запросы, просматривать и редактировать данные, а также управлять объектами базы данных через удобный графический интерфейс DBeaver.



1. **Разработка ORM-моделей:**

* **Определить сущности и связи между ними;**

При разработке ORM-моделей сущности и связи между ними были определены на основе анализа предметной области и структуры базы данных. Каждая сущность (например, `User`, `Animal`, `Role`, `Appointment`, `Diagnosis`, `DiagnosisAppointment`) была представлена в виде класса, где поля класса соответствовали столбцам таблиц в базе данных. Аннотации, такие как `@Entity`, `@Table`, `@Id`, `@GeneratedValue`, использовались для указания, что класс является сущностью, а его поля — атрибутами таблицы. Связи между сущностями (один-ко-многим, многие-ко-многим) были описаны с помощью аннотаций, таких как `@OneToMany`, `@ManyToOne`, `@ManyToMany`, и `@JoinColumn`, которые определяют, как сущности связаны между собой на уровне базы данных. Например, связь между `User` и `Animal` была определена как один-ко-многим, так как один пользователь может иметь несколько животных, а связь между `Appointment` и `Diagnosis` через промежуточную таблицу `DiagnosisAppointment` — как многие-ко-многим. Таким образом, ORM-модели точно отражают структуру базы данных и связи между таблицами, что позволяет удобно работать с данными на уровне объектов в коде.

* **Реализовать модели с использованием SQLAlchemy/Django ORM** (Hibernate);

Для реализации моделей с использованием Hibernate был выполнен следующий процесс. Каждая сущность (например, `User`, `Animal`, `Role`, `Appointment`, `Diagnosis`, `DiagnosisAppointment`) была описана в виде Java-класса с аннотациями Hibernate, такими как `@Entity`, `@Table`, `@Id`, `@GeneratedValue`, которые указывают, что класс является сущностью и соответствует таблице в базе данных. Поля классов были аннотированы как `@Column`, чтобы связать их с соответствующими столбцами таблиц. Связи между сущностями (один-ко-многим, многие-ко-многим) были реализованы с помощью аннотаций `@OneToMany`, `@ManyToOne`, `@ManyToMany` и `@JoinColumn`, которые определяют, как сущности связаны между собой на уровне базы данных. Например, связь между `User` и `Animal` была описана как один-ко-многим, а связь между `Appointment` и `Diagnosis` через промежуточную таблицу `DiagnosisAppointment` — как многие-ко-многим. Для работы с базой данных был настроен файл `hibernate.cfg.xml`, где указаны параметры подключения к PostgreSQL, диалект базы данных и автоматическое создание/обновление таблиц. В коде использовался `SessionFactory` для создания сессий и выполнения операций с базой данных, таких как сохранение, обновление, удаление и выборка данных. Таким образом, Hibernate позволил удобно работать с базой данных через объекты Java, автоматически генерируя SQL-запросы и управляя связями между сущностями.

* Настроить миграции.

Для настройки миграций с помощью Hibernate в Spring Boot был использован механизм автоматического управления схемой базы данных через параметр `spring.jpa.hibernate.ddl-auto`. В файле конфигурации `application.properties` было указано значение `update`, что позволяет Hibernate автоматически создавать или обновлять таблицы в базе данных на основе описанных сущностей. Это означает, что при запуске приложения Hibernate проверяет структуру базы данных и вносит изменения, если сущности были изменены (например, добавлены новые поля или таблицы). Для более сложных сценариев миграций можно использовать инструменты, такие как Flyway или Liquibase, которые позволяют управлять изменениями базы данных через SQL-скрипты или конфигурационные файлы, обеспечивая контроль версий и возможность отката изменений. В нашем случае Hibernate автоматически обрабатывал миграции, что упростило разработку на ранних этапах проекта.

1. **Разработка модели пользователя:**

* **Определить структуру модели (email, пароль, имя и т. д.);**

Структура модели пользователя была определена на основе требований к данным, которые необходимо хранить и обрабатывать в системе. Класс `User` был создан как сущность с аннотацией `@Entity`, что указывает на его соответствие таблице в базе данных. Поля класса, такие как `email`, `password`, `name`, `phone` и `description`, были аннотированы с помощью `@Column`, чтобы связать их с соответствующими столбцами таблицы. Поле `id` было помечено аннотациями `@Id` и `@GeneratedValue`, чтобы указать, что это первичный ключ с автоматической генерацией значения. Для обеспечения связи с другими сущностями, например, с ролью пользователя (`Role`), было добавлено поле `role` с аннотацией `@ManyToOne`, что отражает отношение "многие-к-одному". Таким образом, модель пользователя включает основные атрибуты, такие как уникальный идентификатор, имя, пароль, email, телефон и описание, а также связи с другими сущностями, что позволяет эффективно управлять данными пользователя в системе.

* **Настроить хеширование паролей.**

Хеширование паролей было настроено с использованием библиотеки `BCryptPasswordEncoder` из Spring Security. В коде создан экземпляр `BCryptPasswordEncoder`, который используется для преобразования исходного пароля (например, `"562"`) в хешированное значение. Хешированный пароль был получен с помощью метода `encoder.encode(rawPassword)` и выведен в консоль. Для сохранения хешированного пароля в базе данных PostgreSQL был выполнен SQL-запрос `INSERT` через psql, где хешированное значение было вставлено в соответствующее поле таблицы пользователей. Например:

INSERT INTO users (username, password, email) VALUES ('user1', '$2a$10$exampleHashedPassword', 'user1@example.com');

Таким образом, пароль хранится в базе данных в безопасном хешированном виде, что обеспечивает защиту данных пользователей.

1. **Функционал для работы с моделями:**

* **Написать скрипты для заполнения базы данных тестовыми данными;**

Для создания структуры базы данных и последующего заполнения тестовыми данными был использован следующий подход. Сначала структура базы данных была автоматически создана при запуске приложения с использованием Hibernate. Это было сделано через параметр `spring.jpa.hibernate.ddl-auto=update` в конфигурации Spring Boot, который позволяет Hibernate генерировать таблицы на основе Java-моделей (`@Entity`). После этого был создан dump-файл, содержащий только структуру базы данных (без тестовых данных), с помощью команды `pg\_dump`:

pg\_dump -U your\_username -d fluffytailclinic --schema-only -f path/to/structure\_dump.sql

Этот dump-файл содержал SQL-команды для создания таблиц, индексов и связей, но без данных. Для заполнения базы тестовыми данными был написан отдельный SQL-скрипт, содержащий команды `INSERT`, который выполнялся после восстановления структуры из dump-файла. Таким образом, структура базы данных была создана через Hibernate, а тестовые данные добавлены вручную через SQL-скрипты.

* **Реализация функционала для работы с данными в соответствии с тематикой выбранного приложения.**

Для реализации CRUD (Create, Read, Update, Delete) операций для каждого класса (`User`, `Animal`, `Role`, `Appointment`, `Diagnosis`, `DiagnosisAppointment`) был использован Spring Data JPA в сочетании с Hibernate. Для каждого класса создан репозиторий, расширяющий `JpaRepository`, что предоставило готовые методы для работы с базой данных, такие как `save`, `findById`, `findAll`, `deleteById`. В сервисном слое (`Service`) были реализованы методы, которые вызывают соответствующие методы репозитория и добавляют необходимую бизнес-логику. В контроллерах (`Controller`) были созданы REST-эндпоинты для обработки HTTP-запросов (GET, POST, PUT, DELETE), которые вызывают методы сервисов. Например, для класса `User`:

- Create: `POST /users` — создание нового пользователя через `userRepository.save(user)`.

- Read: `GET /users` — получение списка всех пользователей через `userRepository.findAll()`.

- Update: `PUT /users/{id}` — обновление данных пользователя через `userRepository.save(existingUser)`.

- Delete: `DELETE /users/{id}` — удаление пользователя через `userRepository.deleteById(id)`.

Аналогичная структура была реализована для остальных классов, что обеспечило полный набор CRUD операций для каждой сущности.

1. **Оформление отчета:**

* Описать структуру базы данных;
* Подготовить скрипты создания таблиц и миграции;
* Создать презентацию с результатами работы.

## **Лабораторная работа 2: Разработка API**

### **Задачи**

1. Разработка RESTful API
2. Тестирование API с помощью Postman или cURL

**Разработка RESTful API**

**Определение API**

В ходе работы были разработаны REST API для взаимодействия с системой ветеринарной клиники FluffyTailClinic. API включает следующие сущности:

* **User (Пользователь)** — управление пользователями системы (ветеринары, владельцы животных).
* **Animal (Животное)** — информация о питомцах, привязанных к пользователям.
* **Appointment (Запись на приём)** — хранение данных о записях к ветеринарам.
* **Diagnosis (Диагноз)** — справочник возможных диагнозов.
* **DiagnosisAppointment (Связь диагнозов и записей)** — привязка диагнозов к записям на приём.

**Структура API**

**1. API Пользователей (/api/users):**

* GET /api/users — получение списка пользователей
* GET /api/users/{id} — получение информации о пользователе
* POST /api/users/registration — регистрация пользователя
* PUT /api/users/{id} — обновление данных пользователя
* DELETE /api/users/{id} — удаление пользователя

**2. API Животных (/api/animals):**

* GET /api/animals — получение списка животных
* GET /api/animals/{id} — получение информации о конкретном животном
* POST /api/animals — добавление нового животного
* PUT /api/animals/{id} — обновление информации о животном
* DELETE /api/animals/{id} — удаление животного

**3. API Записей на приём (/api/appointments):**

* GET /api/appointments — получение списка записей
* GET /api/appointments/{id} — получение информации о конкретной записи
* POST /api/appointments — создание новой записи
* PUT /api/appointments/{id} — обновление информации о записи
* DELETE /api/appointments/{id} — удаление записи

**4. API Диагнозов (/api/diagnoses):**

* GET /api/diagnoses — получение списка диагнозов
* GET /api/diagnoses/{id} — получение информации о диагнозе
* POST /api/diagnoses — добавление нового диагноза
* PUT /api/diagnoses/{id} — обновление диагноза
* DELETE /api/diagnoses/{id} — удаление диагноза

**5. API Связи диагнозов с приёмами (/api/diagnosis-appointments):**

* GET /api/diagnosis-appointments — получение всех связей диагнозов и записей
* GET /api/diagnosis-appointments/{id} — получение информации о связи
* POST /api/diagnosis-appointments — добавление связи диагноза к записи
* PUT /api/diagnosis-appointments/{id} — обновление связи
* DELETE /api/diagnosis-appointments/{id} — удаление связи

**Разработка DTO для предотвращения зацикливания**

Для предотвращения бесконечной рекурсии в JSON-ответах были использованы **Data Transfer Objects (DTO)**:

* UserDTO — содержит только основные поля пользователя, без списка животных.
* AnimalDTO — содержит ownerId вместо объекта User.
* DiagnosisAppointmentDTO — вместо полных объектов Diagnosis и Appointment содержит их id.

Пример DTO для DiagnosisAppointment:

public class DiagnosisAppointmentDTO {

private Long id;

private Long appointmentId;

private Long diagnosisId;

public DiagnosisAppointmentDTO(DiagnosisAppointment diagnosisAppointment) {

this.id = diagnosisAppointment.getId();

this.appointmentId = diagnosisAppointment.getAppointment().getId();

this.diagnosisId = diagnosisAppointment.getDiagnosis().getId();

}

}

Использование DTO позволило разорвать циклы сериализации и избежать ошибок в API.

**Тестирование API с помощью Postman**

Для тестирования API использовались **Postman**. Были проверены следующие сценарии:

1. **Создание нового пользователя** (POST /api/users/registration)
2. **Добавление животного пользователю** (POST /api/animals)
3. **Запись животного на приём** (POST /api/appointments)
4. **Добавление диагноза к приёму** (POST /api/diagnosis-appointments)
5. **Обновление диагноза** (PUT /api/diagnoses/{id})
6. **Удаление записи на приём** (DELETE /api/appointments/{id})

**Пример запроса в Postman**

POST /api/appointments

{

"animalId": 5,

"vetId": 2,

"date": "2025-03-15T10:30:00",

"description": "Вакцинация"

}

**Пример ответа**

{

"id": 12,

"animalId": 5,

"vetId": 2,

"date": "2025-03-15T10:30:00",

"description": "Вакцинация"

}

**Вывод**

В ходе лабораторной работы было разработано RESTful API для системы управления ветеринарной клиникой FluffyTailClinic. API реализует все основные CRUD-операции, а также использует DTO для предотвращения зацикливания при сериализации. API протестировано с использованием Postman, все запросы работают корректно.

**Отчёт по лабораторной работе №3**

**Тема:** Добавление аутентификации с JWT в Spring Boot

**Цель работы**

Настроить аутентификацию пользователей в Spring Boot приложении с использованием JSON Web Token (JWT). Реализовать защиту API, используя Spring Security.

**Этапы работы**

**1. Добавление зависимостей в build.gradle**

Для работы с JWT добавлены необходимые зависимости:

implementation 'io.jsonwebtoken:jjwt-api:0.11.5'  
implementation 'io.jsonwebtoken:jjwt-impl:0.11.5'  
implementation 'io.jsonwebtoken:jjwt-jackson:0.11.5'

**2. Настройка фильтра JWT**

Создан фильтр JwtFilter, который перехватывает запросы и проверяет наличие JWT в заголовке:

@Component  
public class JwtFilter extends OncePerRequestFilter {  
  
 private final JwtUtil jwtUtil;  
 private final UserDetailsService userDetailsService;  
  
 public JwtFilter(JwtUtil jwtUtil, UserDetailsService userDetailsService) {  
 this.jwtUtil = jwtUtil;  
 this.userDetailsService = userDetailsService;  
 }  
  
 @Override  
 protected void doFilterInternal(HttpServletRequest request,  
 HttpServletResponse response,  
 FilterChain chain) throws ServletException, IOException {  
 String authHeader = request.getHeader("Authorization");  
  
 if (authHeader == null || !authHeader.startsWith("Bearer ")) {  
 chain.doFilter(request, response);  
 return;  
 }  
  
 String token = authHeader.substring(7);  
 String email = jwtUtil.extractEmail(token);  
  
 if (email != null && SecurityContextHolder.*getContext*().getAuthentication() == null) {  
 UserDetails userDetails = userDetailsService.loadUserByUsername(email);  
  
 if (jwtUtil.validateToken(token)) {  
 UsernamePasswordAuthenticationToken authentication =  
 new UsernamePasswordAuthenticationToken(userDetails, null, userDetails.getAuthorities());  
 authentication.setDetails(new WebAuthenticationDetailsSource().buildDetails(request));  
  
 SecurityContextHolder.*getContext*().setAuthentication(authentication);  
 }  
 }  
 chain.doFilter(request, response);  
 }  
}

**3. Реализация утилиты JwtService**

Сервис для генерации и проверки токенов:

@Component  
public class JwtUtil {  
 private static final String *SECRET\_KEY* = "SuperSecretKeyForJWTTokenSuperSecretKey";  
 private static final long *EXPIRATION\_TIME* = 86400000; // 24 часа  
  
 private final Key key = Keys.*hmacShaKeyFor*(*SECRET\_KEY*.getBytes());  
  
 // Генерация токена  
 public String generateToken(String email) {  
 return Jwts.*builder*()  
 .setSubject(email)  
 .setIssuedAt(new Date())  
 .setExpiration(new Date(System.*currentTimeMillis*() + *EXPIRATION\_TIME*))  
 .signWith(key, SignatureAlgorithm.*HS256*)  
 .compact();  
 }  
  
 // Получение email из токена  
 public String extractEmail(String token) {  
 return Jwts.*parserBuilder*()  
 .setSigningKey(key)  
 .build()  
 .parseClaimsJws(token)  
 .getBody()  
 .getSubject();  
 }  
  
 // Проверка токена  
 public boolean validateToken(String token) {  
 try {  
 Jwts.*parserBuilder*().setSigningKey(key).build().parseClaimsJws(token);  
 return true;  
 } catch (JwtException e) {  
 return false;  
 }  
 }  
}

**4. Настройка Spring Security**

В файле SecurityConfig добавлена проверка JWT-токенов:

@Bean  
public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {  
 return http  
 .csrf(csrf -> csrf.disable())  
 .sessionManagement(session -> session.sessionCreationPolicy(SessionCreationPolicy.*STATELESS*))  
 .authorizeHttpRequests(auth -> auth  
 .requestMatchers("/login").permitAll()  
 .requestMatchers( "/register", "/css/\*\*", "/js/\*\*", "/images/\*\*","login.html","register.html","/error","error.html","/dashboard","dashboard.html").permitAll() // Разрешаем доступ  
 .requestMatchers("/api/\*\*").authenticated() // Все пользователи должны быть авторизованы  
 .anyRequest().authenticated()  
 )  
 .formLogin(form -> form  
 .loginPage("/login") // Указываем страницу входа  
 .permitAll()  
 .defaultSuccessUrl("/dashboard")  
 )  
 .logout((logout) -> logout.permitAll())  
 .sessionManagement(session -> session  
 .sessionCreationPolicy(SessionCreationPolicy.*ALWAYS*) // Открываем сессию для каждого запроса  
 )  
 .exceptionHandling(ex -> ex  
 .accessDeniedPage("/error") // Перенаправление на кастомную страницу ошибки  
 )  
 .addFilterBefore(jwtFilter, UsernamePasswordAuthenticationFilter.class)  
 .build();  
}

**5. Создание контроллера аутентификации**

Контроллер для входа пользователей и генерации токенов:

@PostMapping("/login")  
public ResponseEntity<?> loginUser(@RequestParam String email, @RequestParam String password) {  
 Optional<User> userOpt = userRepository.findByEmail(email);  
  
 if (userOpt.isEmpty()) {  
 return ResponseEntity.*status*(401).body("Invalid email or password");  
 }  
  
 User user = userOpt.get();  
  
 if (!passwordEncoder.matches(password, user.getPassword())) {  
 return ResponseEntity.*status*(401).body("Invalid email or password");  
 }  
  
 String token = jwtUtil.generateToken(user.getEmail());  
 return ResponseEntity.*ok*(token);  
}

**6. Тестирование API с Postman**

Примеры запросов:

**Регистрация пользователя:**

POST http://localhost:8081/api/auth/register

{

"username": "testuser",

"password": "password123",

"email": "test@example.com"

}

**Авторизация:**

POST http://localhost:8081/api/auth/login

{

"username": "testuser",

"password": "password123"

}

Ответ:

{

"token": "eyJhbGciOiJIUzI1NiIsInR5..."

}

**Доступ к защищённому API:**

GET http://localhost:8081/api/protected

Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5...

**Вывод**

Настроена аутентификация с JWT, защищены маршруты API. Теперь пользователи могут получать токены и использовать их для доступа к защищённым ресурсам.

**Отчёт по лабораторной работе №4**

**Тема:** Разработка клиентской части приложения FluffyTail Clinic

**Цель работы:** Создание интерфейса для взаимодействия с REST API через Spring Thymeleaf. Реализация обработки ошибок (401, 403, 404) и работа с Fetch API.

**Выполненные этапы работы**

**1. Создание интерфейса с использованием Thymeleaf**

* Разработаны шаблоны:
  + /login
  + /register
  + /dashboard
  + /add-pet
  + /add-appointment
* Формы созданы на HTML + CSS и используют Fetch API для отправки запросов.

**2. Взаимодействие с API**

* JWT-токен сохраняется в localStorage.
* Fetch-запросы добавляют Authorization-заголовок.

**3. Обработка ошибок**

* Создана кастомная страница /error с динамическим выводом статус-кода.
* Обработаны ошибки 401, 403, 404.

**4. Дополнительная защита**

* Доступ к личному кабинету и управлению питомцами только по JWT-токену.
* При отсутствии токена перенаправление на /login.

**Стек использованных технологий**

* **Frontend:** Spring Thymeleaf + HTML5 + CSS3
* **Backend API:** Spring Boot + REST API + JWT
* **JS:** Fetch API
* **База данных:** PostgreSQL
* **Обработка ошибок:** Spring MVC error handling

**Выводы**

В ходе лабораторной работы был реализован полноценный клиентский интерфейс, организовано безопасное взаимодействие с API через JWT, реализована корректная обработка ошибок.

**Отчёт по лабораторной работе №5**

**Тема:** Упаковка и развёртывание приложения FluffyTail Clinic в Docker-контейнерах

**Цель работы:** Организовать сборку и запуск проекта в Docker, настроить хранение данных PostgreSQL в volume, обеспечить соединение между сервисами.

**Описание структуры контейнеризации и настройки окружения**

**Dockerfile**

* Создан Dockerfile для сборки Spring Boot приложения.
* Сборка jar-файла через Gradle.
* Копирование готового jar-файла в контейнер.

**Dockerfile простой:**

FROM openjdk:21-jdk-slim

WORKDIR /app

COPY target/app.jar app.jar

ENTRYPOINT ["java", "-jar", "app.jar"]

**docker-compose.yml**

* Связь сервисов:
  + app - Spring Boot приложение.
  + db - PostgreSQL.
* Томы для PostgreSQL (сохранение данных при перезапусках).

**docker-compose.yml:**

version: '3.8'

services:

db:

image: postgres:15

container\_name: clinic-db

environment:

POSTGRES\_DB: clinic

POSTGRES\_USER: clinic

POSTGRES\_PASSWORD: clinic

volumes:

- db\_data:/var/lib/postgresql/data

ports:

- "5432:5432"

app:

build:

context: .

dockerfile: Dockerfile

container\_name: clinic-app

depends\_on:

- db

environment:

SPRING\_DATASOURCE\_URL: jdbc:postgresql://db:5432/clinic

SPRING\_DATASOURCE\_USERNAME: clinic

SPRING\_DATASOURCE\_PASSWORD: clinic

ports:

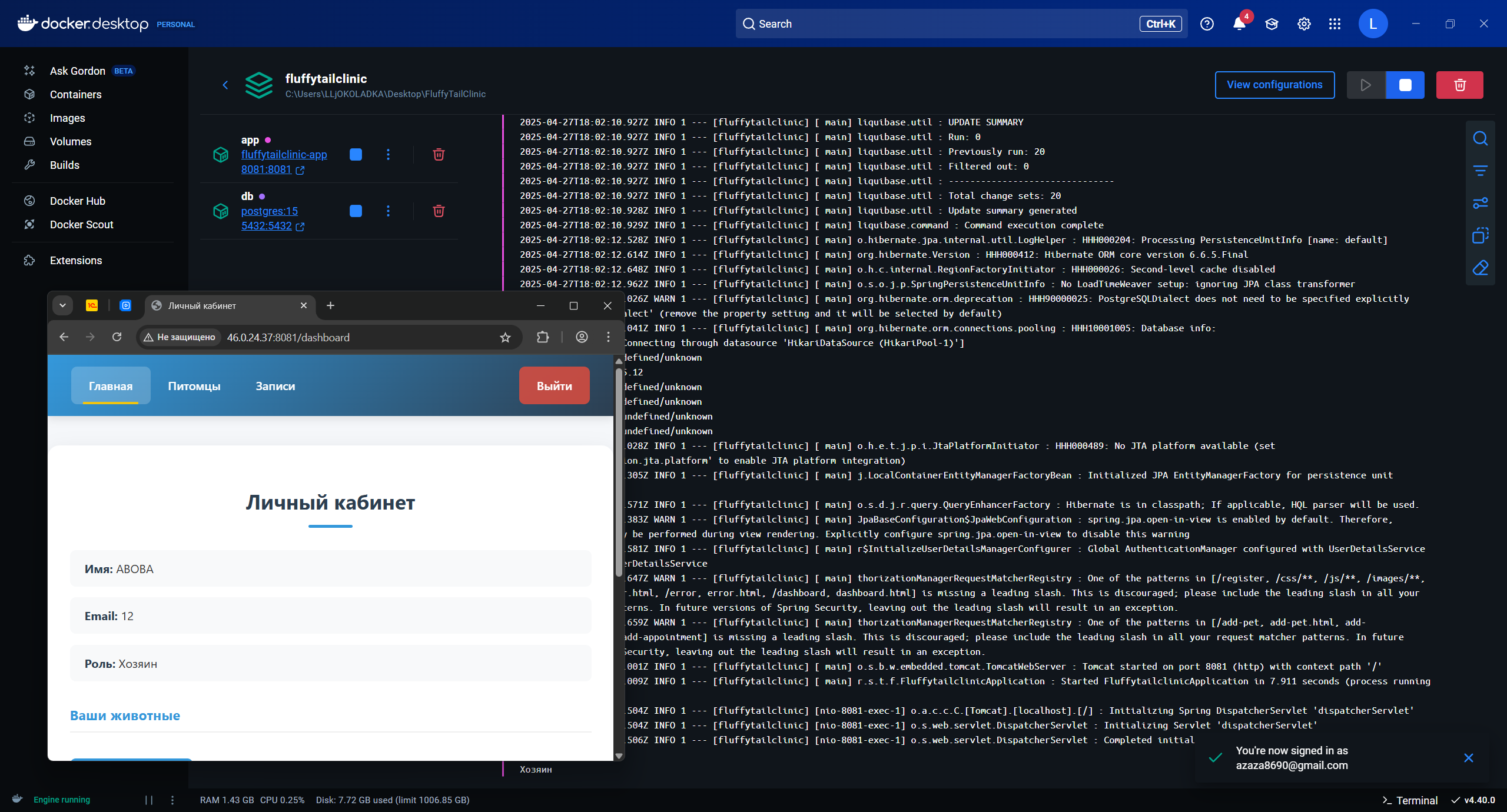
- "8081:8081"

restart: on-failure

volumes:

db\_data:

**Скриншот работающего приложения**



**Описание API**

|  |  |  |
| --- | --- | --- |
| **Метод** | **URL** | **Описание** |
| POST | /login | Авторизация, получение JWT |
| POST | /registration | Регистрация нового пользователя |
| GET | /me | Данные текущего пользователя |
| GET | /api/animals | Список всех животных |
| POST | /api/animals | Добавить животное |
| GET | /api/appointments | Список записей на приём |
| POST | /api/appointments | Запись на приём |

**Архитектура приложения**

**Frontend:**

* Spring Boot + Thymeleaf
* HTML5 + CSS + JS
* Fetch API

**Backend:**

* Spring Boot (REST Controllers)
* Spring Security (JWT)
* Hibernate ORM (JPA)
* Liquibase (миграции)

**Database:**

* PostgreSQL 15
* Хранение данных через Docker volume

**Docker контейнеры:**

* app - Spring Boot приложение
* db - PostgreSQL