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

Отчет по лабораторной работе №3

Дисциплина: «Технологии сетевого программирования»

Тема «Авторизация»

Выполнили: Новикова В.В., Мартынов О.И.

Группа: 6302-010302D

Самара, 2024

**1. Описание модели пользователя и JWT-аутентификации**

**Модель пользователя**

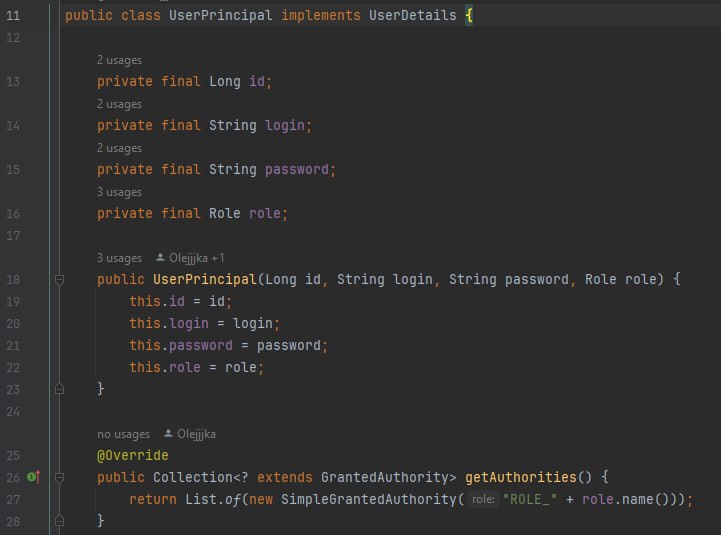
В системе реализованы две категории пользователей: Client и Master, каждая из которых имеет индивидуальные данные и используется в рамках авторизации и бизнес-логики. Обе сущности содержат следующие ключевые поля:

* id: Уникальный идентификатор;
* name: Имя пользователя;
* phone: Номер телефона (уникальный);
* login: Уникальный логин для авторизации;
* password: Пароль, хранимый в зашифрованном виде.

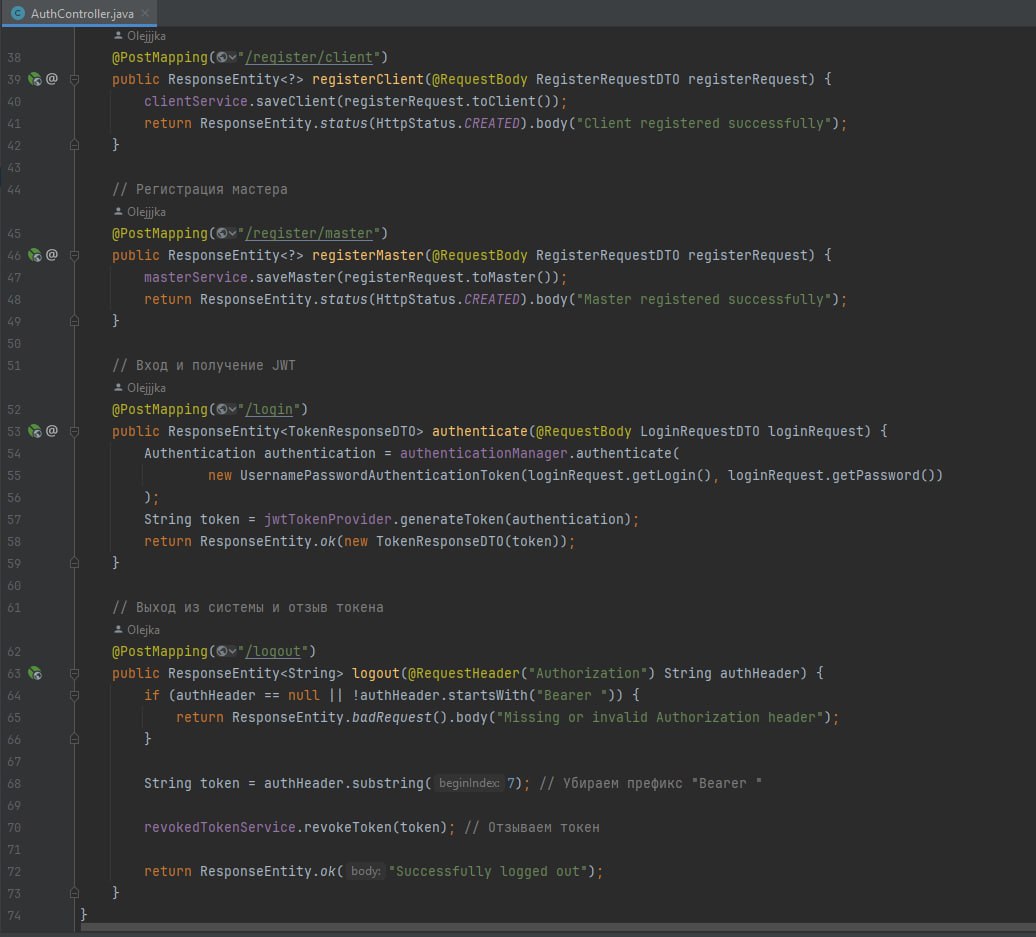
**Аутентификация и безопасность**

Для обеспечения безопасности и разграничения доступа используется механизм JWT-аутентификации. Пользователь проходит авторизацию через контроллер AuthController, получая JWT-токен. Токен включает роль пользователя (CLIENT или MASTER), определяется на этапе загрузки пользователя в UserPrincipal, а не хранится напрямую в сущностях.

UserPrincipal:

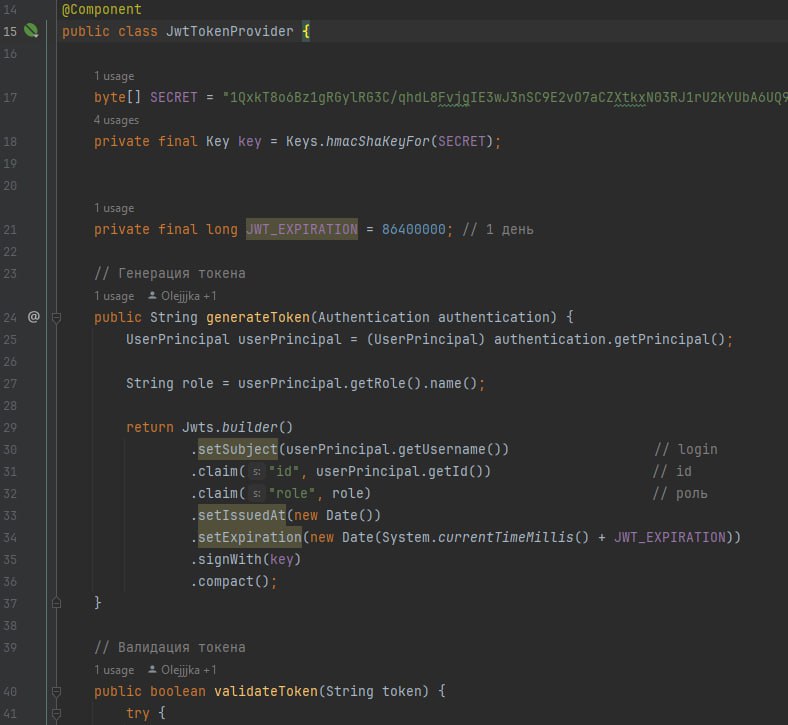


AuthController:



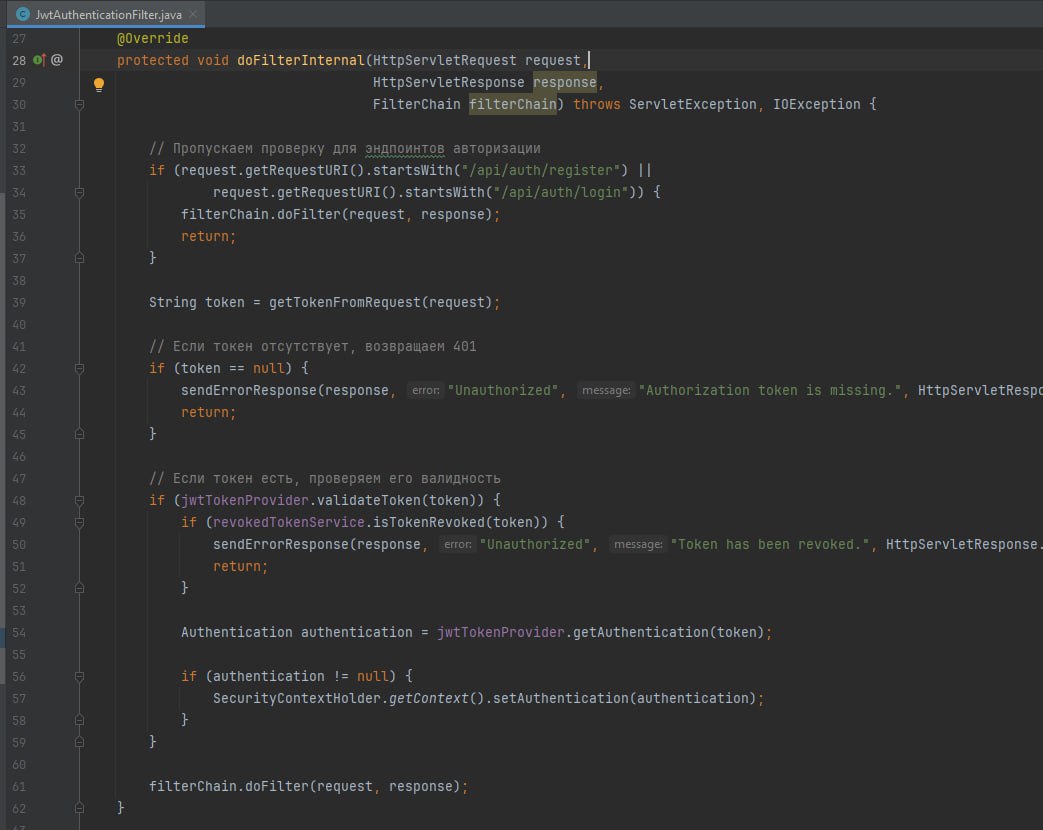
* **JWT включает:**
  + логин;
  + дату истечения;
  + роль (в claim);

JwtTokenProvider:

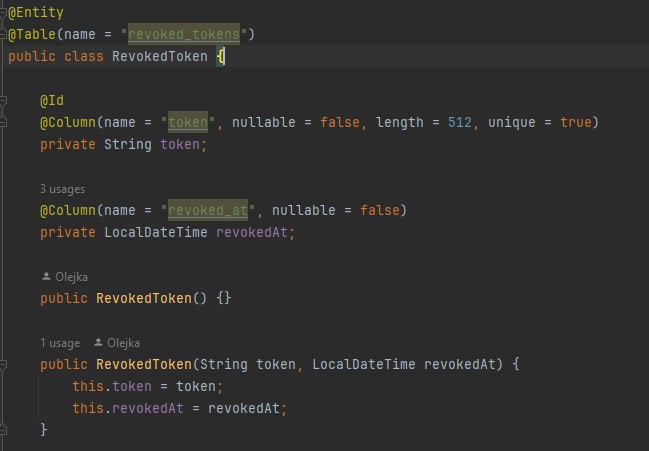


* **Проверка и защита:**
  + Каждый запрос проходит через JWT-фильтр;
  + Отзыв токенов реализован через сущность RevokedToken и сервис RevokedTokenService, который сохраняет отозванные токены и проверяет их актуальность при каждом запросе;

JwtAuthenticationFilter:



RevokedToken:

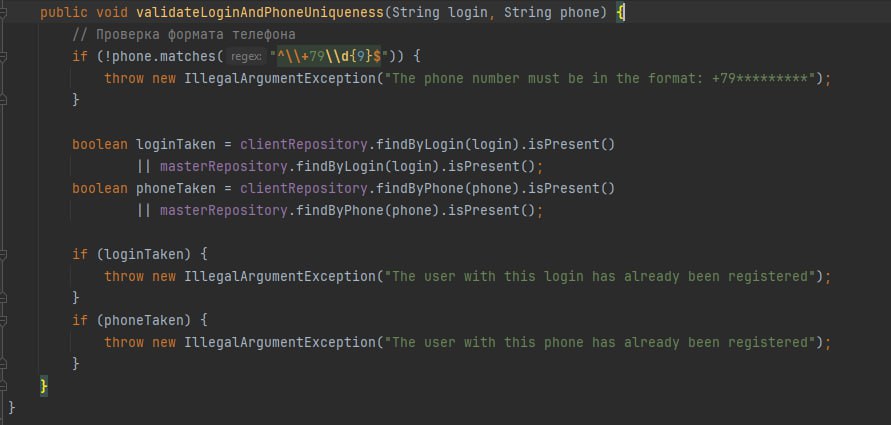


RevokedTokenService:

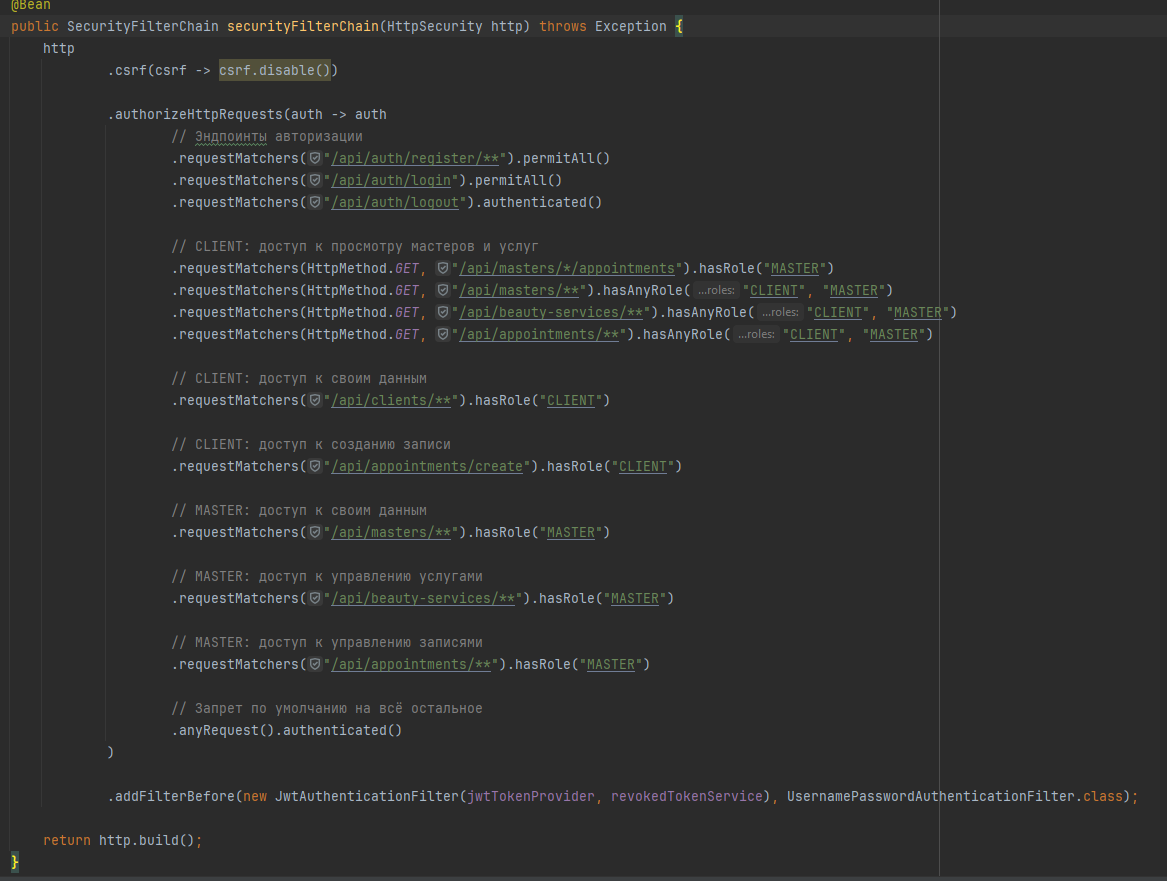


* **Валидация данных пользователя:**
  + Проверка уникальности логина и телефона через UserValidationService;
  + Валидация формата номера телефона: ^\+79\d{9}$;

UserValidationService:



* **Пример защиты эндпоинтов:**
  + Доступ к ресурсам ограничен на основе роли, роль определяется при загрузке UserDetails.

****

**2. Примеры запросов, ответов и их статусов**

#### Регистрация клиента

**POST** /api/auth/register/client

**Request body:**



**Response:**

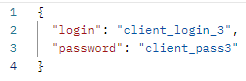


**HTTP Status:** 201 Created

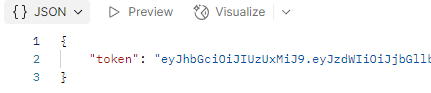
#### Вход клиента

**POST** /api/auth/login

**Request body:**



**Response:**



**HTTP Status:** 200 OK

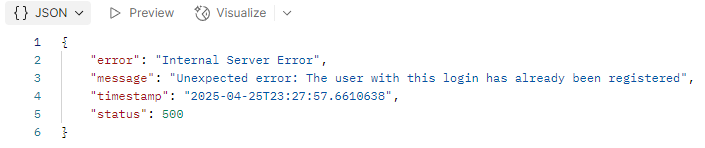
#### Попытка регистрации с уже занятым логином

**POST** /api/auth/register/master

**Request body:**



**Response:**

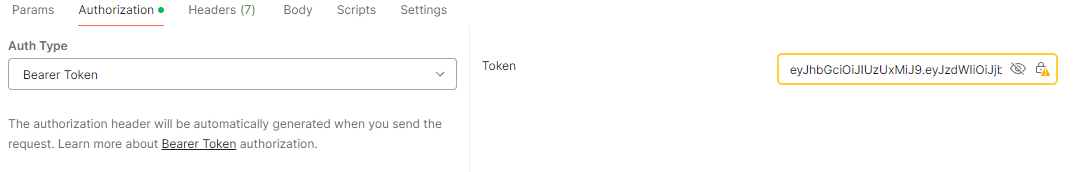


**HTTP Status:** 500 Internal Server Error

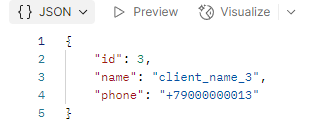
#### Доступ к защищенному эндпоинту

**GET** /client/{clientId}

**Header:**



**Response:**

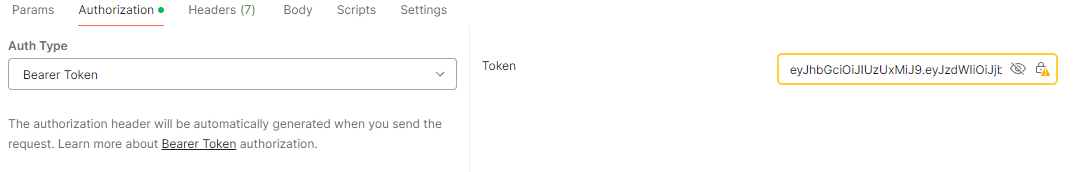


**HTTP Status:** 200 OK

#### Доступ к защищенному эндпоинту без прав

**GET** /master/{masterId}

**Header:**

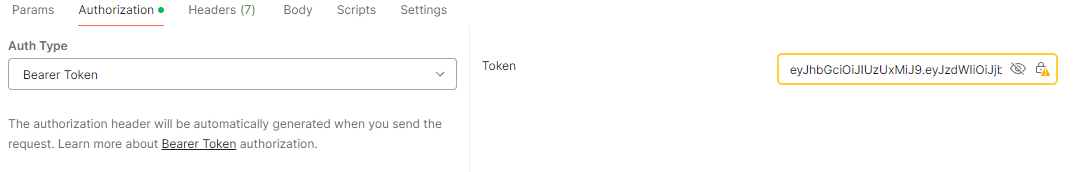


**HTTP Status:** 403 Forbidden

#### Логаут (отзыв токена)

**POST** /api/auth/logout

**Header:**



**Response:**

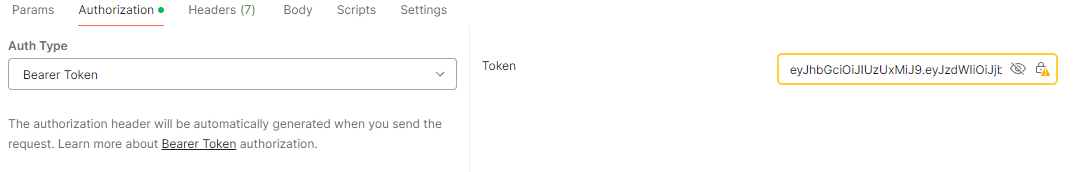


**HTTP Status:** 200 OK

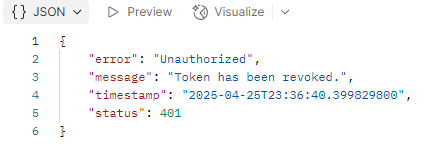
#### Попытка с отозванным токеном

**GET** /api/client/{clientId}

**Header:**



**Response:**



**HTTP Status:** 401 Unauthorized