

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»  
Обнинский институт атомной энергетики –  
филиал федерального государственного автономного образовательного учреждения  
высшего образования «Национальный исследовательский ядерный университет «МИФИ»  
(ИАТЭ НИЯУ МИФИ)  
Отделение интеллектуальных и кибернетических систем

## **Отчет по преддипломной практике**

по направлению подготовки: 09.03.02 Информационные системы и технологии  
Направленность (профиль): Информационные технологии

### **«Разработка серверной части приложения «ShoppingAssistant»»**

Выполнил:

студент гр. \_ИС-Б16-з\_

\_\_\_\_\_  
(подпись, дата)

Галиханов А. Ф.

Руководитель практики,  
к.т.н., доцент ОИКС

\_\_\_\_\_  
(подпись, дата)

Грицюк С.В.

Обнинск, 2021 г

## Реферат

Работа 25 с., 1 табл., 5 рис., 7 ист., 1 прил.

API, АРХИТЕКТУРА REST, СУБД, JSON , FLASK, JSON Web Token.

Объектом исследования является архитектурный стиль REST для реализации клиент-серверного приложения.

Цель работы – разработка серверной части приложения «ShoppingAssistant».

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ . . . . .	3
ГЛАВА 1. ПОСТАНОВКА ЗАДАЧИ . . . . .	4
1.1 Функциональные требования . . . . .	4
1.2 Системные требования . . . . .	5
ГЛАВА 2. ОБЗОР ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ . . . . .	6
2.1 Архитектура REST . . . . .	6
2.2 Формат передачи данных JSON . . . . .	8
2.3 Стандарт JSON Web Token . . . . .	8
ГЛАВА 3. ПРОЕКТИРОВАНИЕ . . . . .	10
3.1 База данных . . . . .	10
3.2 RestAPI . . . . .	12
ГЛАВА 4. РЕАЛИЗАЦИЯ ПРОЕКТА . . . . .	16
4.1 Выбор инструментов разработки . . . . .	16
4.1.1 Выбор инструментов разработки . . . . .	16
4.1.2 Описание реализованного RestAPI . . . . .	17
ЗАКЛЮЧЕНИЕ . . . . .	19
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ . . . . .	20
ПРИЛОЖЕНИЕ А . . . . .	22

## ВВЕДЕНИЕ

Питание является одним из основных факторов, влияющих на здоровье человека. В настоящее время заметно возрастает понимание того, что пища оказывает на человека значительное влияние. Она даёт энергию, силу, развитие, а при грамотном её употреблении – и здоровье. Без всякого сомнения, можно утверждать, что здоровье человека на 65% зависит от питания. Вредная пища зачастую является основным источником большинства заболеваний. Повышенное содержание холестерина в крови, ожирение, кариес, диабет, нарушение жирового обмена веществ, гипертония, повышенное содержание мочевой кислоты в крови – вот неполный перечень болезней вызванных неправильным питанием. Исключив из своего рациона вредные продукты, можно не только предотвратить эти заболевания, но и избавиться от большинства хронических недугов. С каждым годом увеличивается ассортимент готовых продуктов питания и усложняется их состав. Вместе с тем растут и проблемы выбора здоровой пищи возле прилавков магазина. Ведь не всегда просто разобрать состав продукта, написанный мелким шрифтом, и определить подходит ли данный товар вам. Особенно эта проблема актуальна для людей со слабым зрением или имеющие аллергию на определенные продукты. Для облегчения процесса выбора продуктов питания, было принято решение, реализовать приложение «ShoppingAssistant»(Помощник по покупкам).

ShoppingAssistant ускоряет и облегчает процесс покупок в любых продовольственных магазинах. Просто отсканировав штрих-код продукта с помощью камеры на смартфоне, через приложение, получаешь полную информацию о составе и пищевой ценности продукта в удобочитаемом виде. В приложении можно заранее составлять список нежелательных продуктов в составе товара, которые будут подсвечиваться определенным цветом предупреждая вас. Также ведется подсчет калорий и соотношения белков, жиров и углеводов в корзине для соблюдения баланса энергетической ценности.

## ГЛАВА 1. ПОСТАНОВКА ЗАДАЧИ

Разработать серверную часть приложения «ShoppingAssistant», которая планируется реализовать в рамках выпускной квалификационной работы. Приложение «ShoppingAssistant» ориентирована на людей следящих за своим питанием:

- 1) Людей имеющих аллергию на определенные продукты;
- 2) Вегетарианцев;
- 3) Людей соблюдающих пост по религиозным или иным причинам;
- 4) Людей соблюдающих диету для похудения или для набора мышечной массы.

При релизации сервера придерживаться архитектурного стиля REST(Representational State Transfer — «передача состояния представления»). Для взаимодействия с клиентом сервер должен предоставлять API(Application Programming Interfaces — «интерфейс прикладного программирования»). Использовать данные полученные и подготовленные в рамках курса «Нереляционные базы данных».

### 1.1 Функциональные требования

Реализуемый RestAPI сервер должен удовлетворять следующим функциональным требованиям:

- 1) Регистрация пользователя. Все данные пользователя должны храниться в БД. Для обеспечения безопасности, пароль доступа должен храниться в зашифрованном виде;
- 2) Авторизация пользователя. Процесс аутентификации пользователя должна происходить с помощью токенов доступа. Сервер должен иметь возможность обновления токена;
- 3) У каждого зарегистрированного пользователя в базе данных, должен храниться список недопустимых продуктов. Пользователь должен иметь возможность добавлять и удалять необходимые продукты;

- 4) По штрих-коду товара сервер должен предоставить пользователю:
- состав товара;
  - пищевую и энергетическую ценность товара;
  - список недопустимых продуктов входящих в состав товара.

## 1.2 Системные требования

Для реализуемого RestAPI сервера предъявляются следующие системные требования:

- 1) При проектировании сервера использовать архитектурный стиль REST;
- 2) Для передачи данных клиенту и взаимодействия с базой данных использовать формат JSON;
- 3) Для реализации системы авторизации использовать технологию и стандарт JWT(JSON Web Token). На сервере не должна храниться никакая информация о состоянии клиента;
- 4) Импортировать в базу данных разрабатываемого сервера данные, полученные и подготовленные в рамках курса «Нереляционные базы данных».

## ГЛАВА 2. ОБЗОР ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ

### 2.1 Архитектура REST

Термин REST ввел Рой Филдинг, один из создателей протокола HTTP, в своей докторской диссертации "Архитектурные стили и дизайн сетевых программных архитектур" ("Architectural Styles and the Design of Network-based Software Architectures") в 2000 году. REST — это акроним, сокращение от английского Representational State Transfer — передача состояния представления. Архитектурный стиль взаимодействия компонентов распределенной системы в компьютерной сети. REST определяет стиль взаимодействия (обмена данными) между разными компонентами системы, каждая из которых может физически располагаться в разных местах. Данный архитектурный стиль представляет собой согласованный набор ограничений, учитываемых при проектировании распределенной системы. Эти ограничения иногда называют принципами REST:

- 1) Приведение архитектуры к модели клиент-сервер. В основе данного ограничения лежит разграничение потребностей. Необходимо отделять потребности клиентского интерфейса от потребностей сервера, хранящего данные. Данное ограничение повышает переносимость клиентского кода на другие платформы, а упрощение серверной части улучшает масштабируемость системы. Само разграничение на "клиент" и "сервер" позволяет им развиваться независимо друг от друга;
- 2) Отсутствие состояния. Архитектура REST требует соблюдения следующего условия. В период между запросами серверу не нужно хранить информацию о состоянии клиента. Все запросы от клиента должны быть составлены так, чтобы сервер получил всю необходимую информацию для выполнения запроса и идентификации клиента. Таким образом и сервер, и клиент могут "понимать" любое принятое сообщение, не опираясь при этом на предыдущие сообщения;

- 3) Кэширование. Клиенты могут выполнять кэширование ответов сервера. У тех, в свою очередь, должно быть явное или неявное обозначение как кэшируемых или некэшируемых, чтобы клиенты в ответ на последующие запросы не получали устаревшие или неверные данные. Правильное использование кэширования помогает полностью или частично устранить некоторые клиент-серверные взаимодействия, ещё больше повышая производительность и расширяемость системы;
- 4) Единообразие интерфейса. К фундаментальным требованиям REST архитектуры относится и унифицированный, единообразный интерфейс. Клиент должен всегда понимать, в каком формате и на какие адреса ему нужно слать запрос, а сервер, в свою очередь, также должен понимать, в каком формате ему следует отвечать на запросы клиента. Этот единый формат клиент-серверного взаимодействия, который описывает, что, куда, в каком виде и как отсылать и является унифицированным интерфейсом. Каждый ресурс в REST должен быть идентифицирован посредством стабильного идентификатора, который не меняется при изменении состояния ресурса. Идентификатором в REST является URI;
- 5) Слои. Под слоями подразумевается иерархическая структура сетей. Иногда клиент может общаться напрямую с сервером, а иногда — просто с промежуточным узлом. Применение промежуточных серверов способно повысить масштабируемость за счёт балансировки нагрузки и распределённого кэширования;
- 6) Код по требованию (необязательное ограничение). Данное ограничение подразумевает, что клиент может расширять свою функциональность, за счёт загрузки кода с сервера в виде апплетов или сценариев.

В общем случае REST является очень простым интерфейсом управления информацией без использования каких-то дополнительных внутренних прослоек. Каждая единица информации однозначно определяется глобальным идентификатором, таким как URL. Каждая URL в свою очередь имеет строго заданный формат. Как происходит управление информацией сервиса — это целиком и полностью основывается на протоколе передачи данных. Для HTTP



действие над данными задается с помощью методов: GET (получить), PUT (добавить, заменить), POST (добавить, изменить, удалить), DELETE (удалить).

## 2.2 Формат передачи данных JSON

JSON (JavaScript Object Notation) – это текстовый формат представления данных в нотации объекта JavaScript. Предназначен JSON, также как и некоторые другие форматы такие как XML и YAML, для обмена данными. Несмотря на происхождение от JavaScript, формат считается независимым от языка и может использоваться практически с любым языком программирования. JSON основан на двух структурах данных:

- 1) Коллекция пар ключ/значение;
- 2) Упорядоченный список значений.

Это универсальные структуры данных. Почти все современные языки программирования поддерживают их в какой-либо форме. Объект JSON представляет собой заключённый в фигурные скобки список из пар ключ/значение. В коллекции ключ отделяется от значения с помощью знака двоеточия (:), а одна пара от другой - с помощью запятой (,). При этом ключ в JSON обязательно должен быть заключен в двойные кавычки. Значение ключа в JSON можно задать только в одном из следующих форматов: string (строкой), number (числом), object (объектом), array (массивом), boolean (логическим значением true или false) или null. Массив JSON представляет собой заключённый в квадратные скобки список из нуля или более значений, разделённых запятыми. Эти структуры могут быть вложенными.

## 2.3 Стандарт JSON Web Token

JSON Web Token (JWT) — это открытый стандарт (RFC 7519) представления данных для передачи между двумя или более сторонами в виде JSON-объекта. В клиент-серверных приложениях токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в

дальнейшем использует данный токен для подтверждения своей личности. Как правило, структурно JWT состоит из трех частей:

- 1) header — заголовок;
- 2) payload — полезная нагрузка;
- 3) signature — подпись.

Заголовок и полезная нагрузка — обычные JSON-объекты, которые необходимо дополнительно закодировать при помощи алгоритма base64url. Закодированные части соединяются друг с другом, и на их основе вычисляется подпись, которая также становится частью токена. Заголовок — служебная часть токена. Он помогает приложению определить, каким образом следует обрабатывать полученный токен:

```
{  
  "typ": "JWT",  
  "alg": "HS256"  
}
```

Поле `typ` определяет тип токена. Поле `alg` определяет алгоритм, использованный для генерации подписи. В приведенном случае был применен алгоритм HS256, в котором для генерации и проверки подписи используется единый секретный ключ. В полезной нагрузке передается любая информация, которая помогает приложению тем или иным образом идентифицировать пользователя и время жизни токена. Заголовок и полезная нагрузка кодируются при помощи алгоритма base64url, после чего объединяются в единую строку с использованием точки (".") в качестве разделителя. Генерируется подпись, которая добавляется к исходной строке так же через точку:

header.payload.signature

Получив JWT от пользователя, приложение самостоятельно вычислит значение подписи и сравнит его с тем значением, которое было передано в токене. Если эти значения не совпадут, значит, токен был модифицирован или сгенерирован недоверенной стороной, и принимать такой токен и доверять ему приложение не будет.

## ГЛАВА 3. ПРОЕКТИРОВАНИЕ

Для проектирования системы использовался универсальный язык моделирования UML с использованием редактора диаграмм Visual Paradigm Community Edition v.16.2. При проектировании системы, соответствующая вышеописанным требованиям, были разработаны следующие диаграммы:

- 1) диаграмма вариантов использования платформы;
- 2) диаграммы описания ресурсов RestAPI

### 3.1 База данных

В качестве базы данных было решено использовать NoSQL СУБД MongoDB. Подробное изучение данной СУБД позволило выявить ряд нижеописанных преимуществ для нашей системы:

- 1) Документоориентированность – СУБД предназначена для хранения иерархических структур данных (документов).
- 2) Представление в формате JSON – формат данных JSON удобен в интерпретации и использовании. В виду того, что серверная составляющая должна предоставлять RestAPI, MongoDB отлично подходит для реализации нашего сервиса.
- 3) Гибкость и динамичность данных – MongoDB способен хранить как структурированные, так и не структурированные данные.
- 4) Документация и ПО – данная СУБД является ПО с открытым исходным кодом, с отличной документацией и реализацией драйверов для подавляющего большинства языков программирования.

Исходя из системных требований к проектируемому сервису, представление данных в формате JSON стал решающим фактором в выборе данного СУБД. Это позволит исключить использование дополнительных прослоек в виде ORM для преобразования данных.

Контейнерами сущностей (документов) в MongoDB являются коллекции. Ниже описаны используемые коллекции с перечислением ключевых свойств документов.

### Продукты

```
product = {
  "name": string,      - название продукта
  "barcode": string,   - штрих-код продукта
  "composition": [array], - состав продукта
  "comment": string,   - комментарии к продукту
  "gost": string,      - номер ГОСТ-стандарта
  "net mass": string,  - масса-нетто продукта
  "keeping time": string, - срок годности
  "storage conditions": string, - условия хранения
  "esl": {              - пищевая ценность продукта
    "protein": number, - количество белков на 100 грамм продукта
    "fats": number,   - количество жиров на 100 грамм продукта
    "carbohydrates": number, - количество углеводов на 100 грамм
    "calorie": number, - количество калорий на 100 грамм продукта
  }
  "packing type": string - тип упаковки
}
```

### Пользователи

```
users = {
  "_id": Objectid, - уникальный идентификатор пользователя
  "name": string,   - имя пользователя (логин)
  "password": string, - хеш пароля пользователя
  "unacceptable_products": [array] - список недопустимых продуктов
}
```

### Черный список токенов обновления

```
token_blacklist = {
  "_id": Objectid, - уникальный идентификатор
  "jti": string,   - токен обновления
  "created_at": date, - время добавления токена в формате UTC
  "user_id": Objectid - уникальный идентификатор пользователя
}
```

В черном списке будут храниться токены обновления пользователей с истекшим сроком жизни, чтобы исключить возможность повторного использования для получения токена доступа. По истечении срока жизни токены автоматически удаляются из коллекции.

### 3.2 RestAPI

Для описания общего представления о функциональном назначении платформы была разработана диаграмма вариантов использования представленная на рисунке 1. С платформой взаимодействует два актера:

- 1) гость – пользователь не авторизованный в системе;
- 2) авторизованный пользователь.

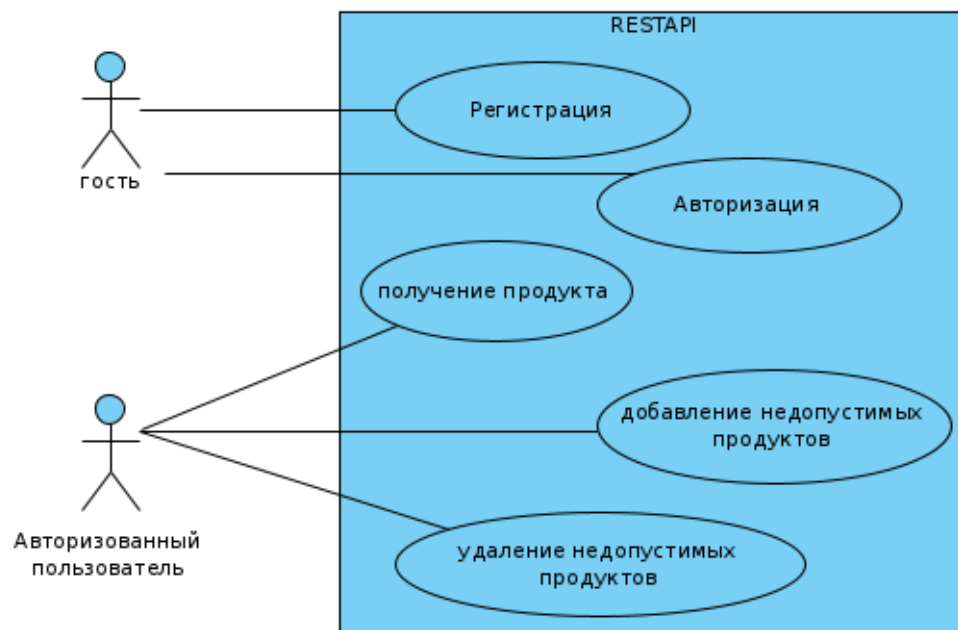


Рисунок 1 – Архитектура полной виртуализации

Гость платформы имеет следующие варианты использования:

- 1) регистрация в системе;
- 2) авторизация в системе.

Авторизованный пользователь имеет следующие варианты использования:

- 1) получение продукта – получение полной информации о продукте по штрих-коду и списка недопустимых продуктов присутствующих в составе;
- 2) добавление недопустимых продуктов – добавление нежелательного продукта в коллекцию;
- 3) удаление недопустимых продуктов – удаление нежелательного продукта из коллекции.

Для дальнейшего проектирования необходимо ввести понятие «ресурс». Ресурс в REST-архитектуре является ключевой абстракцией информации. Любая информация, которая может быть названа, может быть ресурсом. Сам Рой Филдинг в своей диссертации дает такое определение: «Любая информация, которая может быть названа, может быть ресурсом». Другими словами, любое понятие, которое может быть объектом гипертекстовой ссылки, должно вписываться в определение ресурса. Исходя из требований к реализуемому проекту можно выделить следующие ресурсы:

- 1) пользователи;
- 2) продукты;
- 3) недопустимые продукты;
- 4) токены.

Проектирование будем производить в среде visual paradigm, который предоставляет сервис для моделирования RestAPI. На рисунке 2 представлен модель RestAPI для ресурса пользователь. Для данного ресурса доступны два действия: регистрация и авторизация. На модели белая стрелка в черном квадрате направленная внутрь блока действия, обозначает запрос(request) к серверу, а обратная ответ(response). В заголовке блока действия указывается тип HTTP-запроса и URL. В синих блоках указываются параметры запроса и формат передаваемых параметров. При регистрации пользователя на сервер отправляется POST-запрос с необходимыми параметрами по указанному URL. В зависимости успешности действия возвращается соответствующий ответ. На рисунках представлены модели для остальных ресурсов. Не будем приводить описание для каждого ресурса, так как они аналогичны приведенному выше.

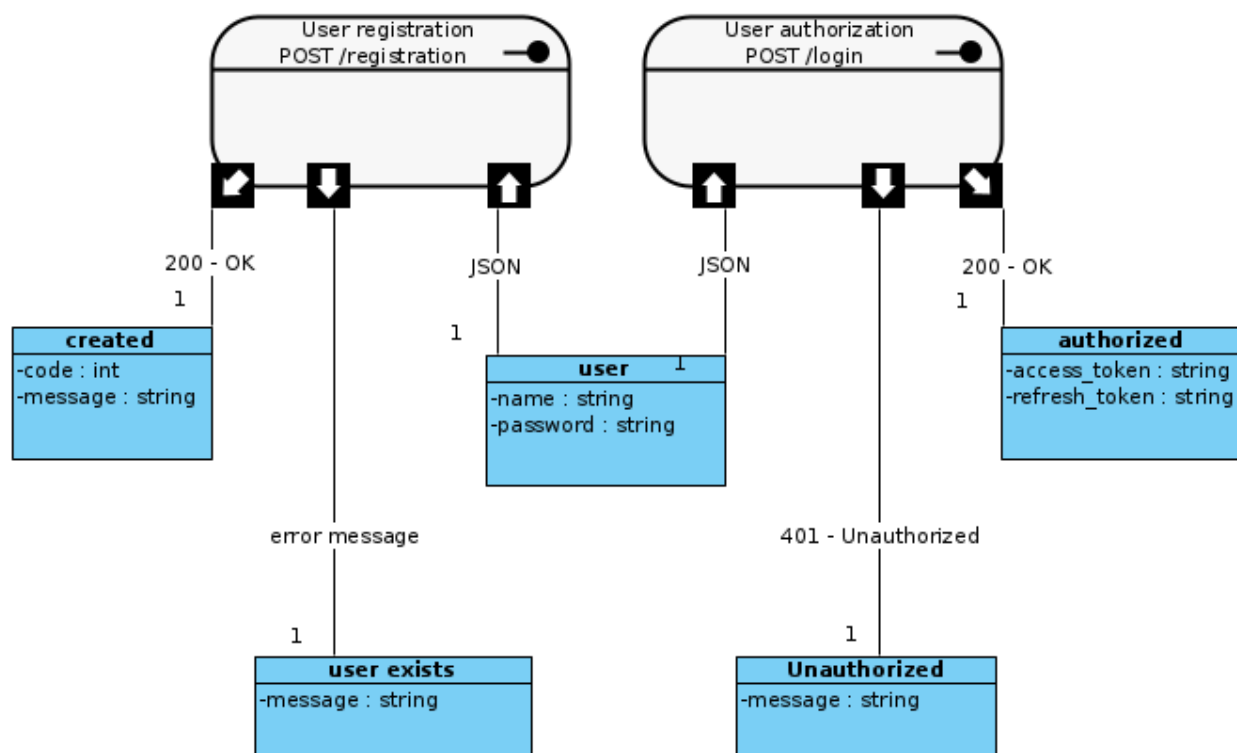


Рисунок 2 – Модель RestAPI для ресурса Пользователи

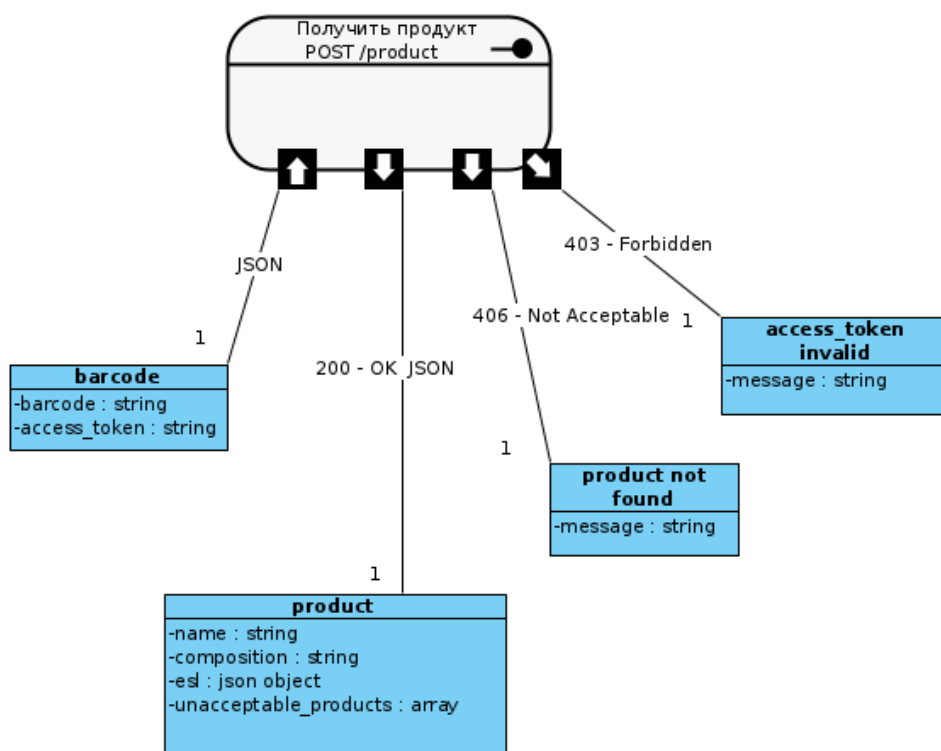


Рисунок 3 – Модель RestAPI для ресурса Продукты

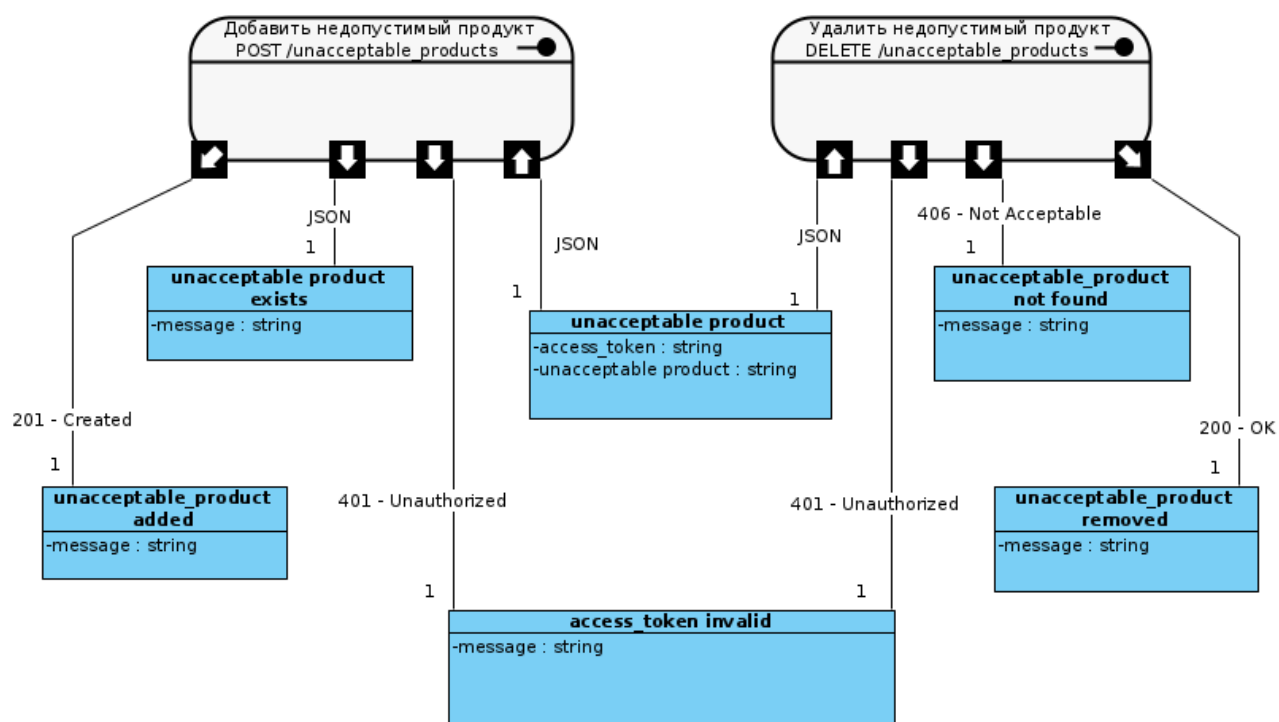


Рисунок 4 – Модель RestAPI для ресурса Недопустимые продукты

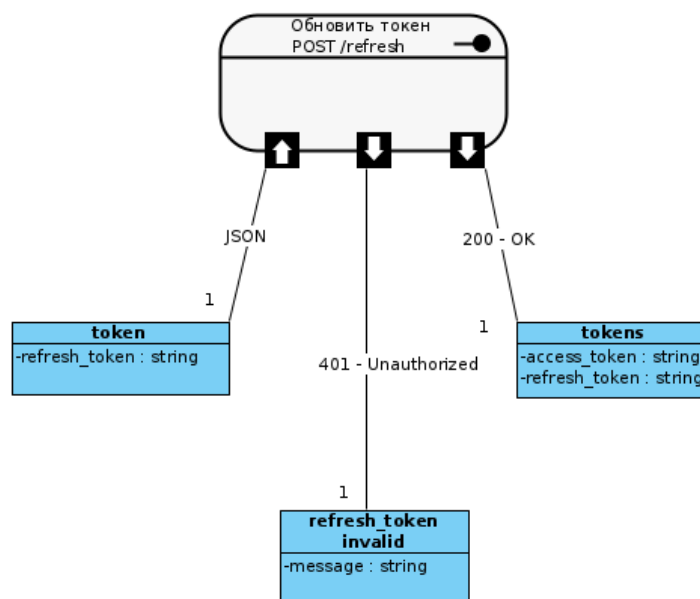


Рисунок 5 – Модель RestAPI для ресурса Токены

В данной главе представлено подробное описание компонентов RestAPI. В соответствии с функциональными требованиями к платформе была спроектирована диаграмма вариантов использования платформы. Разработаны модели для каждого ресурса, в соответствии с которыми будет реализован будущий сервер.



## ГЛАВА 4. РЕАЛИЗАЦИЯ ПРОЕКТА

### 4.1 Выбор инструментов разработки

Исходя из системных требований предъявляемых к реализуемому серверу, к выбору инструментов разработки накладываются следующие ограничения:

- 1) Поддержка формата передачи данных JSON;
- 2) Наличие библиотек для работы со стандартом JWT;
- 3) Возможность реализации архитектурного стиля REST.

#### 4.1.1 Выбор инструментов разработки

Для реализации сервера используется язык программирования Python версии 3.8.5 и фреймворк для создания веб-приложений Flask. Flask предоставляет гибкую настройку веб-приложения с минимальным количеством зависимостей. Пакетный менеджер `pip` предоставляет множество расширений для языка Python, благодаря чему реализация взаимодействия между компонентами системы сводится к написанию бизнес логики. Процесс написания программного кода и его отладки осуществлялся в интегрированной среде разработки PyCharm версии 2020.3.3. Для взаимодействия с базой данных используется рекомендованный способ для работы с MongoDB из среды Python пакет PyMongo. Пример подключения к базе данных:

```
app.config["MONGO_URI"] = "mongodb://localhost:27017/barcode"
mongo = PyMongo(app)
```

Создается экземпляр класса клиента базы данных, который используется для обращения к данным. Благодаря тому, что данная база является документоориентированной с представлением объектов в типе BSON отсутствует миграция базы данных.

Для реализации стандарта аутентификации используется расширение Flask-JWT-Extended, которое реализует весь необходимый функционал. Для встраивания данного функционала в программный код, достаточно добавить к методам ресурсов соответствующие декораторы доступа. При возникновении ошибки декоратор прерывает выполнение обработки запроса и возвращает соответствующее сообщение. По умолчанию access-токен валиден в течение 15 минут, а refresh-токен в течение 30 дней. Для авторизованного запроса необходимо передать параметр Authorization в заголовке запроса с содержимым: Bearer <соответствующий токен доступа (access/refresh)>.

#### 4.1.2 Описание реализованного RestAPI

Описание основных параметров конфигурации реализованного сервера:

- 1) SECRET KEY – секретный ключ, который использует Flask при вычислении хэша паролей. Пакетное расширение jwt extended использует его для генерации подписи при создании токенов. Секретный ключ хранится отдельно от программного кода и передается посредством переменных окружения (environment variables), при развертке данного приложения на сервере;
- 2) JWT ACCESS TOKEN EXPIRES – срок жизни для токена доступа. Задаем равной 30 минутам;
- 3) JWT REFRESH TOKEN EXPIRES – срок жизни для токена обновления. Задаем равной 24 часам;
- 4) MONGO URI – URL сервера с MongoDB с необходимыми данными авторизации;

Опираясь на модели спроектированные в предыдущей главе, были разработаны методы для каждого ресурса требуемые для полноценной работы сервиса, которым присвоены соответствующие маршруты. В таблице 1 приводится описание всех реализованных методов. Листинг кода реализованного сервера приведен в приложении А.

Таблица 1 – Описание реализованного RestAPI

URL	Метод	Описание
/registration	POST	Регистрация пользователя с переданными аргументами. Результатом является сообщение об успешной регистрации пользователя, либо сообщение о соответствующей ошибке с HTTP-кодом.
/login	POST	Аутентификация пользователя по логину и паролю. Результатом является access- и refresh-токены, либо сообщение о соответствующей ошибке с HTTP-кодом.
/refresh	POST	Обновление access-токена на основе переданного refresh-токена. Результатом является access-токен.
/unacceptable products	POST	Добавление недопустимого продукта для пользователя. Необходим заголовок авторизации. Результатом является сообщение об успешном добавлении продукта, либо сообщение о соответствующей ошибке с HTTP-кодом.
/unacceptable products	DELETE	Удаление недопустимого продукта из списка хранимой в базе данных. Необходим заголовок авторизации. Результатом является сообщение об успешном удалении продукта, либо сообщение о соответствующей ошибке с HTTP-кодом.
/product	POST	Получение информации о продукте по переданному штрих-коду. Необходим заголовок авторизации. Результатом является полная информация о продукте, либо сообщение о соответствующей ошибке с HTTP-кодом.

Источник: собственная разработка

Все ресурсы на стороне сервера требуют авторизации с использованием токенов доступа, за исключением ресурсов, необходимых для аутентификации. Refresh-токен позволяет клиентам запрашивать новые access-токены по истечении их времени жизни. Refresh-токен выдается на более длительный срок, чем access-токен, и по истечению времени его жизни клиенту необходимо вновь пройти процесс аутентификации.

## ЗАКЛЮЧЕНИЕ

Целью данной работы являлась разработка серверной части приложения «ShoppingAssistant», которая планируется реализовать в рамках выпускной квалификационной работы. В ходе выполнения работы были решены следующие задачи:

- 1) Определены требования к сервису;
- 2) Выполнен обзор требуемых технологий;
- 3) Выполнено проектирование;
- 4) Разработана серверная часть приложения полностью соответствующая предъявленным требованиям.

В результате выполнения работы были решены все поставленные задачи, таким образом, цель данной работы достигнута.

Планируется дальнейшее развитие проекта в рамках выпускной квалификационной работы, а именно реализация клиентской части приложения.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Roy Thomas Fielding Architectural Styles and the Design of Network-based Software Architectures [Электронный ресурс] Режим доступа: <https://www.ics.uci.edu/fielding/pubs/dissertation/top.htm>
- 2 Flask Documentation [Электронный ресурс] Режим доступа: <https://flask.palletsprojects.com/en/1.1.x/>
- 3 Flask-JWT-Extended's Documentation [Электронный ресурс] Режим доступа: <https://flask-jwt-extended.readthedocs.io/en/stable/>
- 4 Postman | API Development Environment [Электронный ресурс] Режим доступа: <https://www.postman.com/api-documentation-tool/>
- 5 MongoDB Documentation [Электронный ресурс] Режим доступа: <https://docs.mongodb.com/>
- 6 Visual Paradigm User's Guides [Электронный ресурс] Режим доступа: <https://www.visual-paradigm.com/support/documents/>
- 7 Flask-PyMongo 2.3.0 documentation [Электронный ресурс] Режим доступа: <https://flask-pymongo.readthedocs.io/en/latest/>

## ПРИЛОЖЕНИЯ

## ПРИЛОЖЕНИЕ А

### Листинг кода реализованного RestApi

```
import datetime
import os
import re

from bson.objectid import ObjectId
from flask import Flask, jsonify, request, make_response
from flask_jwt_extended import JWTManager
from flask_jwt_extended import create_access_token,
    create_refresh_token, get_jwt
from flask_jwt_extended import get_jwt_identity
from flask_jwt_extended import jwt_required
from flask_pymongo import PyMongo
from werkzeug.security import generate_password_hash,
    check_password_hash

app = Flask(__name__)
app.config['SECRET_KEY'] = os.getenv('SECRET_KEY', '
    DefaultValue_d5049c7d')
app.config["JWT_ACCESS_TOKEN_EXPIRES"] = datetime.timedelta(minutes
    =30)
app.config["JWT_REFRESH_TOKEN_EXPIRES"] = datetime.timedelta(hours
    =24)
app.config["MONGO_URI"] = "mongodb://localhost:27017/barcode"
app.config['DEBUG'] = True

mongo = PyMongo(app)
jwt = JWTManager(app)
current_time = datetime.datetime.utcnow()

# Регистрация пользователя
@app.route('/registration', methods=['POST'])
def create_user():
```

```

data = request.get_json()
existing_user = mongo.db.users.find_one({'name': data['name']})
if existing_user is None:
    hash_pass = generate_password_hash(data['password'], method='sha256
        ')
    user = {
        'name': data['name'],
        'password': hash_pass,
        "unacceptable_products": [],
    }
    mongo.db.users.insert(user)
    return 'You have successfully registered'
    return 'User exist'

```

```

# Авторизация пользователя
@app.route('/login', methods=['POST'])
def user_login():
    data = request.get_json()
    if not data or not data['name'] or not data['password']:
        return make_response('Could not verify', 401)
    user = mongo.db.users.find_one({'name': data['name']}, {'_id': 1, '
        name': 1, 'password': 1})
    if not user:
        return make_response('Could not verify', 401)
    if check_password_hash(user['password'], data['password']):
        access_token = create_access_token(identity=str(user['_id']))
        refresh_token = create_refresh_token(identity=str(user['_id']))
        return jsonify(access_token=access_token, refresh_token=
            refresh_token)
    return make_response('Could not verify', 401)

```

```

# Обновление токена доступа
@app.route("/refresh", methods=["POST"])
@jwt_required(refresh=True)
def refresh():

```



```

current_user = get_jwt_identity()
jti = get_jwt()["jti"]
existing_jti = mongo.db.token_blacklist.find_one({'user_id':
    current_user, 'jti': jti})
if existing_jti:
    return jsonify('this token invalid')
token_blacklist = {
    'jti': jti,
    'created_at': current_time,
    'user_id': current_user
}
mongo.db.token_blacklist.insert(token_blacklist)
access_token = create_access_token(identity=current_user)
refresh_token = create_refresh_token(identity=current_user)
return jsonify(access_token=access_token, refresh_token=
    refresh_token)

# Добавление и удаление недопустимых продуктов
@app.route("/unacceptable_products", methods=['POST', 'DELETE'])
@jwt_required()
def add_unacceptable_products():
    current_user = get_jwt_identity()
    unacceptable_products = request.json['unacceptable_products']
    if request.method == 'POST':
        mongo.db.users.update({"_id": ObjectId(current_user)},
            {'$addToSet': {'unacceptable_products': {'$each':
                unacceptable_products}}})
        return jsonifyУказанные(" продуктыдобавленывсписокнежелательных
            ")
    if request.method == 'DELETE':
        mongo.db.users.update({"_id": ObjectId(current_user)},
            {'$pullAll': {'unacceptable_products': unacceptable_products}})
        return jsonifyУказанные(" продуктыудаленыизсписканежелательных
            ")

```

```

# получение продукта по штрих-коду
@app.route("/product", methods=['POST'])
@jwt_required()
def test_req():
    current_user = get_jwt_identity()
    barcode = request.json['barcode']
    product = mongo.db.goods.find_one_or_404({"barcode": barcode},
    {'composition': 1, '_id': 0, 'name': 1, 'esl': 1})
    unacceptable_products = mongo.db.users.find_one_or_404({"_id":
        ObjectId(current_user)},
    {'unacceptable_products': 1})
    # result = list(set(product['composition']) & set(
        unacceptable_products['unacceptable_products']))
    result = []
    for unacceptable in unacceptable_products['unacceptable_products']:
    for composition in product['composition']:
    temp = re.search(f'(?i){unacceptable}', composition)
    if temp is not None:
    result.append(composition)
    return_result = {
    "name": product['name'],
    "composition": product['composition'],
    "unacceptable_products": result,
    "esl": product['esl']
    }
    return jsonify(return_result)

if __name__ == '__main__':
    app.run()

```