|  |
| --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  федеральное государственное АВТОНОМНОЕ образовательное учреждение высшего образования  «Национальный исследовательский ядерный университет «МИФИ» |
| **Димитровградский инженерно-технологический институт –**  филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»  **(ДИТИ НИЯУ МИФИ)** |

Факультет информационно-технологический и социально-экономических наук

Кафедра Информационных технологий

Направление подготовки 09.03.01 Информатика и вычислительная техника

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**К КУРСОВОМУ ПРОЕКТУ НА ТЕМУ**

Разработка модуля авторизации для серверной инфраструктуры маркетплейса автопроизводителя

Студент

Группы ВТ-41 Д.Д. Кузин

(подпись)

Руководитель

ассистент М.С. Сутягина

(подпись)

Заведующий кафедрой

доцент, к.п.н. О.А. Ракова

(подпись)

Димитровград, 2025

|  |
| --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  федеральное государственное АВТОНОМНОЕ образовательное учреждение высшего образования  «Национальный исследовательский ядерный университет «МИФИ» |
| **Димитровградский инженерно-технологический институт –**  филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»  **(ДИТИ НИЯУ МИФИ)** |

**ФАКУЛЬТЕТ** Информационно-технологический и социально-экономических наук

**КАФЕДРА** Информационных технологий

**НАПРАВЛЕНИЕ ПОДГОТОВКИ** 09.03.01 **ГРУППА** ВТ-41

**ЗАДАНИЕ НА КУРСОВОЙ ПРОЕКТ**

1. Фамилия, имя, отчество Кузин Данила Денисович

2. Тема «Разработка модуля авторизации для серверной инфраструктуры маркетплейса автопроизводителя

3. Срок сдачи студентом готовой работы

4. Руководитель курсовой работы Сутягина Мария Сергеевна

Дата выдачи задания «\_18\_»\_апреля\_\_\_2025 г.

Руководитель курсовой работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись руководителя)

Задание принял к исполнению \_\_\_15 февраля\_2024\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата и подпись студента)

1. Исходные данные к работе:

*требования к уровню разработки программного продукта:*

*а) разработка базы данных на языке Transact-SQL;*

*а) современный пользовательский интерфейс;*

*б) язык программирования C#.*

1. Содержание работы:
   1. *теоретическая часть:*

* исследование предметной области;
* описание логики программы;
* проектирование элементов интерфейса.
  1. *практическая часть:*
* реализация интерфейса;
* реализация логического компонента программного продукта.

1. Основная литература по теме работы:
2. *Карпова, И.П. База данных. Курс лекций и материалы для практических занятий [Текст] // Учебное пособие. – М.: Питер, 2013. – 240 с.*
3. *Сергеев, С.Ф. Введение в проектирование интеллектуальных интерфейсов [Текст] / С.Ф. Сергеев, П.И. Падерно, Н.А. Назаренко. – СПб: СПбГУ ИТМО, 2011. – 108 с.*
4. Отчётный материал работы:
5. *пояснительная записка;*
6. *CD/DVD-диск с пояcнительной запиской и файлами проекта приложения.*

РЕФЕРАТ

Кузин Д.Д. «РАЗРАБОТКА МОДУЛЯ АВТОРИЗАЦИИ ДЛЯ СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ МАРКЕТПЛЕЙСА АВТОПРОИЗВОДИТЕЛЯ»: КУРСОВОЙ ПРОЕКТ / ДИТИ НИЯУ МИФИ № КП.09.03.01.71.2024 – Димитровград, 2024. – стр. 32, рис. 16, табл. 4, библ. назв. 5.

Ключевые слова: База данных ……

Объект исследования –.

Цель работы –

Задачи:.

Выводы: в ходе курсовой работы была изучена предметная область «Фирма по продаже запчастей», определили главные сущности и их свойства, создали базу данных в MS SQL Server. На основе исследований, а также создания базы данных разработана информационная система на языке программирования C# для платформы Windows.

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 5](#_Toc166279974)

[1.1 Понятие и определение базы данных 6](#_Toc166279975)

[1.2 Понятие модели данных 6](#_Toc166279976)

[1.3 Исследование методов проектирования 6](#_Toc166279977)

[1.4 Сценарий пользовательского интерфейса 6](#_Toc166279978)

[1.5 Исследование и обоснование выбора инструментальных средств разработки программного продукта 6](#_Toc166279979)

[2 ПРАКТИЧЕСКАЯ ЧАСТЬ 7](#_Toc166279980)

[2.1 Разработка базы данных 7](#_Toc166279981)

[2.2 Технология программирования интерфейса программы 7](#_Toc166279982)

[2.3 Описание инструментов программирования. 7](#_Toc166279983)

[2.4 Тестирование программного продукта. 7](#_Toc166279984)

[Заключение 8](#_Toc166279985)

[БИБЛИОГРАФИЧЕСКИЙ СПИСОК 9](#_Toc166279986)

ВВЕДЕНИЕ

В современном цифровом мире информационные технологии играют ключевую роль в обеспечении безопасности и эффективного функционирования бизнес-процессов. Для крупных компаний, таких как автопроизводители, надежная серверная инфраструктура является основой стабильной работы всех сервисов, включая маркетплейсы, которые обеспечивают взаимодействие с клиентами, дилерами и партнерами. Одним из критически важных компонентов такой инфраструктуры является система авторизации пользователей, позволяющая управлять доступом к различным сервисам и защищать конфиденциальные данные.

В данном курсовом проекте будет рассмотрен процесс разработки модуля авторизации пользователей для серверной инфраструктуры маркетплейса автопроизводителя. Будут проанализированы основные требования к системе авторизации, изучены современные методы аутентификации и защиты данных, а также реализованы механизмы управления правами пользователей.

Актуальность темы: Разработка безопасного и масштабируемого модуля авторизации позволит повысить уровень защиты пользовательских данных и предотвратить несанкционированный доступ к информационным ресурсам маркетплейса. Это особенно важно в условиях роста киберугроз и увеличения объемов персональных данных, обрабатываемых в цифровых экосистемах.

Цель проекта: Создание надежной и гибкой системы авторизации, обеспечивающей безопасный доступ пользователей к ресурсам маркетплейса, а также управление их ролями и правами.

Задачи проекта:

Анализ предметной области и изучение существующих решений в области авторизации пользователей.

* Разработка требований к модулю авторизации с учетом специфики маркетплейса автопроизводителя.
* Выбор технологий и инструментов для реализации системы аутентификации и управления доступом.
* Проектирование архитектуры модуля, разработка логической и физической моделей данных.
* Реализация механизма аутентификации пользователей с поддержкой многофакторной авторизации.
* Обеспечение безопасности хранения и передачи данных, внедрение современных криптографических методов.
* Тестирование и оптимизация модуля, интеграция с существующей серверной инфраструктурой маркетплейса.

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

## Основные понятия и принципы аутентификации и авторизации

Аутентификация — это процедура проверки подлинности пользователя, то есть подтверждение, что он действительно является тем, за кого себя выдает. Чаще всего это осуществляется с помощью пароля, пин-кода, биометрических данных или других методов [1].

​Авторизация — это процесс предоставления пользователю или группе пользователей определенных разрешений, прав доступа и привилегий в компьютерной системе [2].

​В сфере информационной безопасности аутентификация и авторизация являются ключевыми процессами, обеспечивающими контроль доступа к системам и данным. Существует несколько видов аутентификации и авторизации, применяемых в зависимости от требований безопасности и специфики системы. Далее рассмотрены некоторые виды аутентификации:

* + - 1. По количеству факторов два основных вида аутентификации: Однофакторная аутентификация: использует один метод проверки, например, ввод пароля. ​ Многофакторная аутентификация (MFA): предполагает использование нескольких независимых факторов для подтверждения личности, таких как знание: то, что знает пользователь (пароль, PIN-код);владение: то, что есть у пользователя (смартфон, смарт-карта);присутствие: биометрические данные пользователя (отпечаток пальца, распознавание лица) [3].
      2. По методам реализации:
* Парольная аутентификация является самым распространенным методом, при котором пользователь вводит статический или одноразовый пароль [4]. ​
* Биометрическая аутентификация: использует уникальные физиологические характеристики пользователя, такие как отпечатки пальцев или голос.
* Аутентификация с использованием токенов: предполагает применение физических или программных устройств, генерирующих одноразовые коды доступа. ​
* Аутентификация по сертификатам: основана на использовании цифровых сертификатов для подтверждения личности пользователя [5]. ​

Виды авторизации:

* + - 1. По моделям управления доступом:
* Ролевая (RBAC): пользователям назначаются определенные роли, каждая из которых имеет набор разрешений. ​
* Мандатная (MAC): доступ к ресурсам определяется на основе установленных меток безопасности и правил, заданных администратором. ​
* Дискреционная (DAC): владелец ресурса самостоятельно определяет, кто и какие действия может выполнять с его ресурсами. ​
  + - 1. По способу предоставления доступа:
* Онлайн-авторизация: требует постоянного соединения с сервером для проверки прав доступа. ​
* Офлайн-авторизация: позволяет пользователю получать доступ к ресурсам без постоянного подключения к сети, основываясь на ранее полученных данных. ​

1. По количеству проверок существует одноступенчатая авторизация. Предполагает единовременную проверку прав доступа; ​многоступенчатая авторизация: требует прохождения нескольких этапов проверки перед предоставлением доступа [6].

## Методы и протоколы аутентификации

Аутентификация — это процесс проверки подлинности пользователя, системы или устройства, направленный на подтверждение их идентичности перед предоставлением доступа к ресурсам. Существует множество методов и протоколов аутентификации, каждый из которых имеет свои особенности и области применения.

Существуют следующие методы аутентификации:

* + - Парольная аутентификация: Пользователь предоставляет секретный код (пароль), известный только ему и системе. Несмотря на свою распространенность, этот метод подвержен рискам, таким как подбор пароля и фишинг.​
    - Аутентификация с использованием одноразовых паролей (OTP): В этой системе для каждого входа генерируется уникальный пароль, который действует ограниченное время. Алгоритмы, такие как HOTP (HMAC-Based One-Time Password), используют счетчик событий для генерации паролей [7]. ​
    - Многофакторная аутентификация (MFA): Сочетание двух или более факторов: что-то, что знает пользователь (пароль), что-то, что он имеет (смарт-карта или мобильное устройство), и что-то, что он есть (биометрические данные). Это повышает уровень безопасности системы.​
* Биометрическая аутентификация: Использует уникальные физиологические или поведенческие характеристики пользователя, такие как отпечатки пальцев, радужка глаза, лицо или голос, для подтверждения его личности.

На данный момент популярными протоколами авторизации являются следующие:

* Basic Authentication: простой протокол, при котором имя пользователя и пароль передаются в заголовке HTTP-запроса в кодировке Base64. Он небезопасен без использования HTTPS, так как учетные данные могут быть перехвачены. ​
* Digest Authentication: предлагает более высокий уровень безопасности по сравнению с Basic Authentication. Сервер генерирует уникальное значение (nonce), которое используется клиентом для создания хэшированного пароля, защищая учетные данные от перехвата. Однако Digest Authentication также имеет свои уязвимости, такие как возможность атак "человек посередине". ​
* Kerberos: протокол аутентификации, использующий билеты для подтверждения личности. Он работает по принципу "единого входа" (SSO), позволяя пользователю аутентифицироваться один раз и получать доступ к различным сервисам без повторного ввода учетных данных. Kerberos широко используется в корпоративных сетях. ​
* OAuth 2.0: протокол авторизации, который позволяет сторонним приложениям получать ограниченный доступ к ресурсам пользователя без необходимости передачи его учетных данных. OAuth 2.0 часто используется для интеграции с социальными сетями и другими сервисами. ​
* OpenID Connect: надстройка над OAuth 2.0, добавляющая слой аутентификации. Она позволяет клиентским приложениям подтверждать личность пользователя на основе аутентификации, выполненной авторизационным сервером, и получать базовую информацию о профиле пользователя. ​
* SAML (Security Assertion Markup Language): стандартный протокол для обмена данными об аутентификации и авторизации между различными доменами безопасности. Часто используется в корпоративных приложениях для реализации единого входа [8].

Выбор метода и протокола аутентификации зависит от требований безопасности, удобства использования и специфики системы. Важно учитывать баланс между защитой данных и пользовательским опытом.

## Сценарий пользовательского взаимодействия с модулем авторизации

​Сценарий пользовательского взаимодействия с модулем авторизации описывает последовательность действий, которые пользователь выполняет для доступа к защищённым ресурсам системы. Эти сценарии помогают понять и спроектировать удобный и безопасный процесс аутентификации и авторизации. Далее рассмотрены основные этапы и лучшие практики разработки таких сценариев:

* + - 1. Регистрация пользователя:
* Инициация: Пользователь посещает страницу регистрации на платформе.
* Вводданных: Пользователь предоставляет необходимую информацию, такую как имя, адрес электронной почты и пароль.​
* Подтверждение: Система отправляет письмо с подтверждением на указанный адрес электронной почты. Пользователь должен перейти по ссылке в письме для активации учётной записи.
  + - 1. Авторизация пользователя происходит по следующему принципу: инициация, в рамках которой пользователь посещает страницу входа в систему. ​ Далее происходит вводучётныхданных, а именно пользователь вводит свой логин (или адрес электронной почты) и пароль. ​Последним этапом является аутентификация, где система проверяет введённые данные. В случае успеха: Пользователь получает доступ к личному кабинету или защищённым разделам сайта. В случае неудачи – отображается сообщение об ошибке с предложением повторить попытку.
      2. Выход из системы (Logout): Инициация: пользователь нажимает кнопку "Выход" в личном кабинете. Завершениесеанса: система завершает текущий сеанс и перенаправляет пользователя на страницу входа или главную страницу сайта [9].

## Исследование и обоснование выбора технологий и инструментов разработки

​При разработке системы авторизации для веб-приложений важно тщательно подойти к выбору технологий и инструментов, чтобы обеспечить безопасность, удобство и масштабируемость системы. Существует несколько подходов и технологий для реализации аутентификации и авторизации: ​

1. Cookie-based аутентификация использует файлы cookie для хранения информации о сессии пользователя, позволяя серверу идентифицировать пользователя при последующих запросах. Основные преимущества – удобство пользователь не требует повторного ввода учетных данных при каждом посещении сайта. Производительность так же является большим преимуществом, так как снижается нагрузка на сервер за счет хранения информации о сессии на стороне клиента.
2. OAuth 2.0 — это открытый стандарт для делегирования доступа, позволяющий сторонним приложениям получать ограниченный доступ к ресурсам пользователя без передачи его пароля. Вместо этого OAuth предоставляет приложению токен доступа после того, как пользователь аутентифицируется через поставщика идентификации. Преимуществами можно назвать тот факт, что пользователь может авторизоваться в приложении, используя уже существующие учетные данные от других сервисов. Сторонние приложения получают доступ к ресурсам без необходимости хранения пароля пользователя. Недостатками являются сложность настройки, так как требуется правильная интеграция с поставщиками идентификации. Зависимость от сторонних сервисов так же является одной из проблем, ведь в случае компрометации поставщика идентификации может возникнуть дополнительный риск.
3. JSON Web Tokens (JWT) — это компактные, безопасные для URL токены, которые содержат утверждения о пользователе и часто используются для управления сессиями в современных веб-приложениях. JWT может хранить информацию о пользователе, такую как идентификатор, роль и привилегии, и подписан для обеспечения целостности данных. Преимуществамиявляютсябессессионнаяаутентификация: сервер не хранит информацию о сессии, что снижает нагрузку на сервер. Легко интегрируется с одностраничными приложениями (SPA) и мобильными приложениями. Срединедостатковможновыделить безопасность**:** кража токена может привести к несанкционированному доступу, если токен не защищен должным образом. Такжетокены могут становиться слишком большими, если в них хранится много данных.

Таким образом, на основе проведённого исследования и анализа различных методов авторизации, можно сделать вывод, что для текущего проекта наибольшую эффективность и безопасность обеспечит использование cookie-based авторизации. Этот подход сочетает в себе простоту реализации, удобство для пользователя и высокую производительность, что делает его оптимальным выбором для данного случая.

# 2 ПРАКТИЧЕСКАЯ ЧАСТЬ

* 1. Проектирование и реализация структуры базы данных

При разработке систем авторизации с использованием Entity Framework (EF) в ASP.NET Core существуют два основных подхода к проектированию и взаимодействию с базой данных: Database First и Code First.

1. Database First

Database First предполагает, что разработка начинается с уже существующей базы данных. Схема базы данных создается заранее, и затем на ее основе генерируются классы моделей и контекст данных в приложении.

Преимуществами можно назвать интеграцию с существующими базами данных. Если база данных уже разработана и используется, этот подход позволяет быстро создать соответствующие модели в приложении. Визуальное проектирование: Возможность использовать инструменты для визуального проектирования схемы базы данных, что облегчает понимание структуры данных.

Среди недостатков ограниченная гибкость: изменения в модели данных требуют внесения изменений непосредственно в базу данных, после чего необходимо повторно генерировать или обновлять модели в коде. Зависимость от базы данных: Бизнес-логика может быть тесно связана с конкретной схемой базы данных, что затрудняет переносимость и тестирование [10].

Code First ориентирован на первичное создание моделей данных в коде. Разработчик определяет классы сущностей и их конфигурацию, после чего EF генерирует соответствующую схему базы данных.

Преимущества:

* Гибкость в разработке: Модели данных определяются в коде, что упрощает их изменение и поддержку.
* Миграции: EF предоставляет механизм миграций, позволяющий автоматически обновлять схему базы данных в соответствии с изменениями моделей, что облегчает управление версиями базы данных.
* Независимость от конкретной СУБД: Модели могут быть легко адаптированы для работы с различными базами данных.

Недостатки:

* Потенциальная сложность начальной настройки: Требуется тщательная настройка моделей и понимание механизмов EF для корректной генерации схемы базы данных.
* Возможные ограничения в сложных сценариях: Для очень сложных схем базы данных может потребоваться дополнительная конфигурация или отказ от некоторых автоматизированных возможностей EF [11].

На основании проведенного исследования был выбран подход Code First. В качестве базы взята PostgreSQL, а язык программирования – C#, с его фреймворком asp.net core по требованию заказчика (?).

При работе с удалёнными базами данных PostgreSQL важно выбрать подходящий инструмент для администрирования и управления. Существует несколько популярных решений, каждое из которых обладает своими особенностями и преимуществами.

1. DBeaver

DBeaver — это универсальный графический клиент для работы с различными СУБД, включая PostgreSQL.

Преимущества DBeaver:

* Кроссплатформенность: Работает на Windows, macOS и Linux.
* Поддержка множества СУБД: Совместим более чем с 80 различными базами данных.
* Визуальный интерфейс: Удобный графический интерфейс с поддержкой визуального построителя запросов, что облегчает работу с данными.
* Импорт и экспорт данных: Поддерживает различные форматы, включая CSV, HTML, XML, JSON, XLS, XLSX.
* Расширяемость: Возможность установки дополнительных плагинов для расширения функциональности.

2. pgAdmin

pgAdmin — это бесплатный и открытый графический пользовательский интерфейс для администрирования PostgreSQL.

Преимущества pgAdmin:

* Специализация на PostgreSQL: Разработан специально для работы с PostgreSQL, что обеспечивает глубокую интеграцию с особенностями этой СУБД.
* Веб-интерфейс: Позволяет управлять базой данных через браузер, что удобно для удалённого администрирования.
* Мощные инструменты разработки и отладки: Включает в себя редактор запросов, инструменты для мониторинга производительности и управления пользователями.

3. DataGrip

DataGrip — это коммерческий инструмент от компании JetBrains для работы с базами данных.

Преимущества DataGrip:

* Интеллектуальный редактор SQL: Поддерживает автодополнение, рефакторинг и анализ кода.
* Поддержка множества СУБД: Помимо PostgreSQL, совместим с MySQL, Oracle, SQL Server и другими.
* Интеграция с системой контроля версий: Упрощает совместную работу над проектами [12].

На основании проведенного исследования, в качестве СУБД для удаленного доступа к базе данных выбрана DBeaver.

Структура базы данных:

**Таблица Users:**

Id (long) — уникальный идентификатор пользователя.

Username (string) — логин пользователя (необходим для аутентификации).

PasswordHash (string) — хэш пароля (для безопасности).

Role (Role) — связь с ролью пользователя. Один пользователь может иметь одну роль.

FirstName (string) — имя пользователя.

LastName (string) — фамилия пользователя.

Avatar (string) — путь к изображению аватара (если используется).

Phone (string) — номер телефона (валидируется с помощью атрибута [Phone]).

Email (string) — email пользователя (валидируется с помощью атрибута [EmailAddress]).

Address (string) — домашний адрес пользователя.

Created (DateTime) — дата и время регистрации пользователя.

Updated (DateTime) — дата последнего обновления информации о пользователе.

IsActive (bool) — флаг активности пользователя (по умолчанию активен).

**Таблица Roles:**

Id (long) — уникальный идентификатор роли.

Name (string) — имя роли (например, "Admin", "User", "Manager").

IsActive (bool) — флаг активности роли (по умолчанию активна).

Чтобы отправить модели в базу данных с помощью Entity Framework Core в ASP.NET Core, нужно создать контекст базы данных, который будет содержать DbSet для каждой сущности, пример приведен ниже:

public class ApplicationDbContext : DbContext

{

public DbSet<User> Users { get; set; }

public DbSet<Role> Roles { get; set; }

public ApplicationDbContext(DbContextOptions<ApplicationDbContext> options): base(options) {}

protected override void OnModelCreating(ModelBuilder modelBuilder)

{ base.OnModelCreating(modelBuilder);

}}

В файле appsettings.json необходимо указать строку подключения к базе данных:

{"ConnectionStrings": {

"DefaultConnection": "Host=localhost;Port=5432;Database=mydb;Username=myuser;Password=mypassword"

}

}

Затем в Program.cs зарегистрировать контекст базы данных:

public void ConfigureServices(IServiceCollection services)

{

services.AddDbContext<ApplicationDbContext>(options =>

options.UseNpgsql(Configuration.GetConnectionString("DefaultConnection")));

}

Для создания миграции используется команда dotnet ef migrations add «Навазние миграции», а для того чтобы применить миграции команда dotnet ef database update.

На рисунке 2.1 изображены таблицы базы данных, что доказывает успешность отправленных моделей.

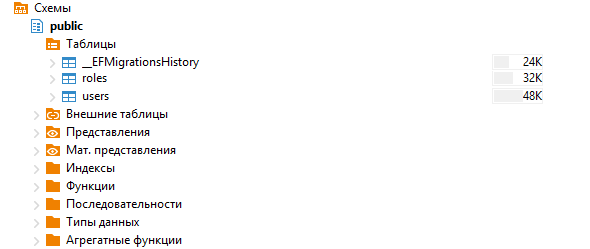


Рисунок 2.1 – Список таблиц в базе данных

* 1. Разработка серверной логики модуля авторизации

Для начала разработки необходимо определить контракт для работы с пользовательскими данными в контексте аутентификации. Данным контрактом является IAuthRepository.

public interface IAuthRepository

{

Task<User> GetByUsernameAsync(string username);

Task<User> CreateAsync(User user);

}

Далее необходимо реализовать данный интерфейс в классе AuthRepository. В рамках данного класса реализовано два метода: GetByUsernameAsync, в который передается переменная строкового типа и если в базе данных есть запись с таким Username, то возвращается данная запись. Второй же метод CreateAsync принимает модель пользователя, которая подготовлена к созданию и происходит создание и сохранение данного пользователя в БД:

public class AuthRepository: IAuthRepository

{

private readonly AppDbContext \_context;

public AuthRepository(AppDbContext context) {\_context = context;}

public async Task<User> GetByUsernameAsync(string username)

{

return await \_context.Users.Include(u => u.Role).FirstOrDefaultAsync(a => a.Username == username);

}

public async Task<User> CreateAsync(User auth)

{

\_context.Users.Add(auth);

await \_context.SaveChangesAsync();

return auth;

}

}

Класс AuthService реализует бизнес-логику аутентификации и регистрации пользователей в системе. Он работает через абстракции IAuthRepository и IRoleRepository, то есть не взаимодействует напрямую с базой данных, а использует репозитории, что соответствует принципам чистой архитектуры. Метод AuthenticateAsync получает на входе логин и пароля для их последующей проверки. Метод RegisterAsync создаёт пользователя в системе с хешированным паролем и назначенной ролью. Метод HashPassword хэширует пароль, что позволяет защитить хранимые пароли от компрометации.:

public class AuthService

{

private readonly IAuthRepository \_authRepository;

private readonly IRoleRepository \_roleRepository;

public AuthService(IAuthRepository authRepository, IRoleRepository roleRepository){

\_authRepository = authRepository;

\_roleRepository = roleRepository;

}

public async Task<User> AuthenticateAsync(string username, string password)

{

var auth = await \_authRepository.GetByUsernameAsync(username);

if (auth == null || auth.PasswordHash != HashPassword(password)){ return null; }

return auth;

}

public async Task<User> RegisterAsync(string firstname, string lastname, string username, string password, string email)

{

var existingUser = await \_authRepository.GetByUsernameAsync(username);

if (existingUser != null)

{

throw new Exception("Пользователь с таким именем уже существует");

}

var auth = new User

{

FirstName = firstname,

LastName = lastname,

Username = username,

PasswordHash = HashPassword(password),

Email = email,

Role = await \_roleRepository.GetByNameAsync("USER"),

Created = DateTime.UtcNow,

IsActive = true,

};

return await \_authRepository.CreateAsync(auth);

}

private string HashPassword(string password)

{

using var sha256 = SHA256.Create();

return Convert.ToBase64String(sha256.ComputeHash(Encoding.UTF8.GetBytes(password)));

}

}

ApiAuthController – API-контроллер для авторизации пользователей. Он предоставляет три HTTP-метода: регистрацию, вход и выход. Работает через сервис AuthService, который реализует бизнес-логику. Метод Register принимает JSON-объект с данными из RegisterViewModel (имя, фамилия, логин, пароль, email) и передает их сервису AuthService для последующей регистрации пользователя:

public async Task<IActionResult> Register([FromBody] RegisterViewModel request){

try{

var user = await \_authService.RegisterAsync(request.Firstname, request.Lastname, request.Username, request.Password, request.Email);

return Ok(new { user.Id, user.Username, user.Email });

}

catch (Exception ex)

{

return BadRequest(new { message = ex.Message });

}

}

Метод Login принимает JSON-объект с Username и Password, проверяет учетные данные через AuthenticateAsync и если пользователь найден, создаёт набор клеймов (Claims) и сохраняет их в куки через HttpContext.SignInAsync:

public async Task<IActionResult> Login([FromBody] LoginViewModel request)

{

var user = await \_authService.AuthenticateAsync(request.Username, request.Password);

if (user == null)

return Unauthorized(new { message = "Неверные учетные данные" });

var claims = new List<Claim>

{

new Claim(ClaimTypes.NameIdentifier, user.Id.ToString()),

new Claim(ClaimTypes.Name, user.Username),

new Claim(ClaimTypes.Email, user.Email),

new Claim(ClaimTypes.Role, user.Role.Name) // Добавляем роль в куки

};

var claimsIdentity = new ClaimsIdentity(claims, CookieAuthenticationDefaults.AuthenticationScheme);

var claimsPrincipal = new ClaimsPrincipal(claimsIdentity);

await HttpContext.SignInAsync(CookieAuthenticationDefaults.AuthenticationScheme, claimsPrincipal);

return Ok(new { user.Id, user.Username, user.Email });

}

Метод Logout удаляет аутентификационную куку .AspNetCore.Cookies, тем самым разлогинивает пользователя:

public async Task<IActionResult> Logout()

{

await Task.Run(() => Response.Cookies.Delete(".AspNetCore.Cookies")); // Асинхронно удаляем куку

return Ok(new { message = "Вы успешно вышли из системы" });

}

При запуске сайта отображается титульная форма (рисунок 2.2), на которой есть кнопки для входа и регистрации. На рисунке 2.3 и 2.4 приведен пример регистрации пользователя и ответ программы на успешную регистрацию.

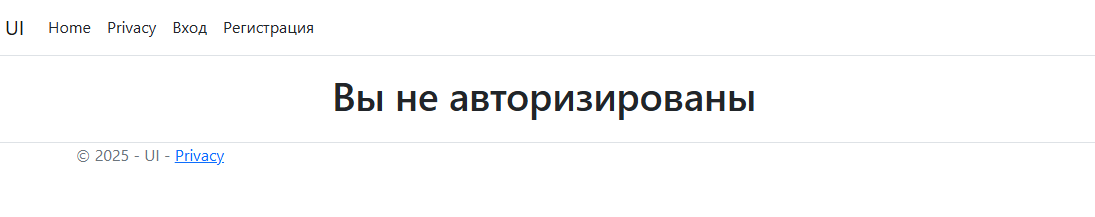


Рисунок 2.2 – Титульная форма

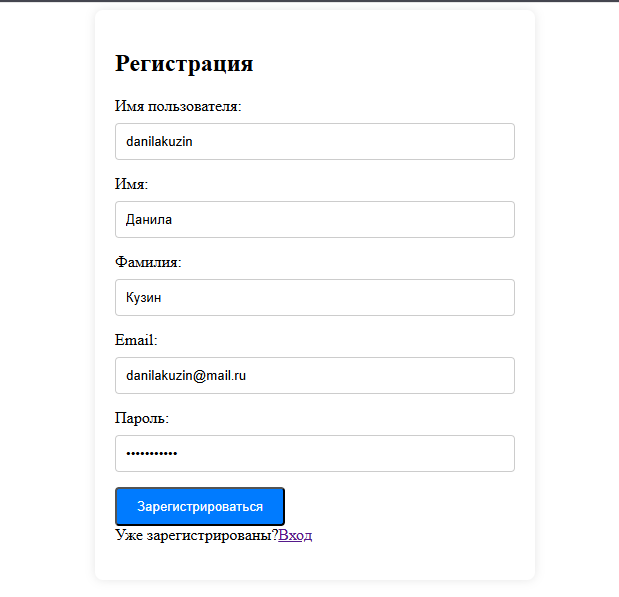


Рисунок 2.3 – Форма регистрации пользователя

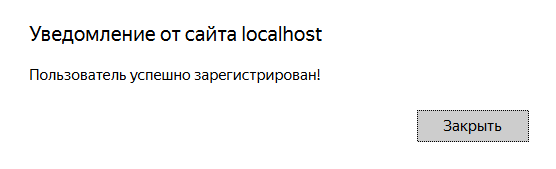


Рисунок 2.4 – Уведомление об успешной регистрации пользователя

На рисунке 2.5 продемонстрирован список пользователей после регистрации, где можно убедиться в наличии созданного пользователя, что об успешности работы методов, связанных с регистрацией пользователя

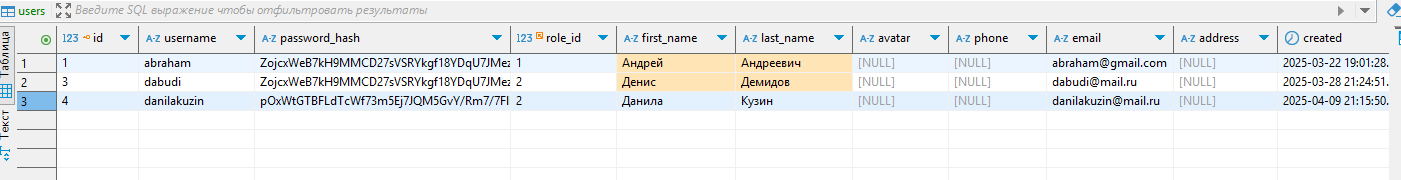


Рисунок 2.5 – Список пользователей в базе данных

По нажатию на кнопку входа отображается форма для ввода логина и пароля, показанная на рисунке 2.6. После успешного введения данных происходит отображение титульной формы, на которой будет отображаться приветствие пользователя. Результат продемонстрирован на рисунке 2.7.

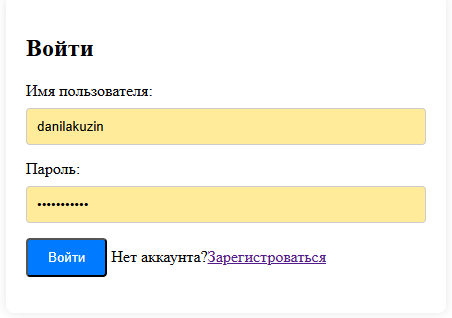


Рисунок 2.6 – Форма авторизации пользователя

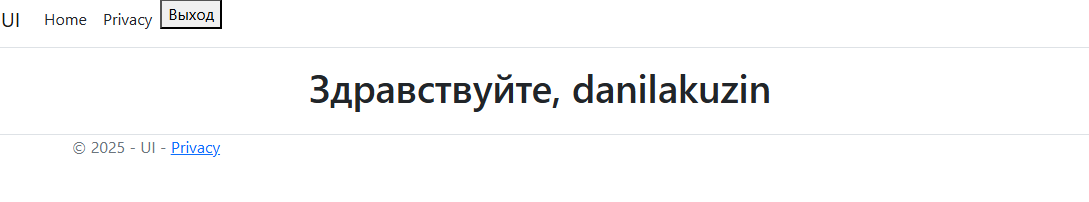


Рисунок 2.7 – Титульная форма для авторизованного пользователя

* 1. Используемые технологии и инструменты разработки.
  2. Тестирование модуля авторизации.

## Заключение

В рамках выполнения

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. <https://developers.sber.ru/help/sber-id/what-is-authentication>
2. <https://encyclopedia.kaspersky.ru/glossary/authorization/>
3. <https://rt-solar.ru/products/solar_inrights/blog/4518/>
4. <https://sendpulse.com/ru/support/glossary/authentication>
5. <https://ru.wikipedia.org/wiki/Аутентификация_в_Интернете>
6. <https://ekassir.com/blog/avtorizacziya-opredelenie-i-metody/>
7. <https://ru.wikipedia.org/wiki/HOTP>
8. <https://sky.pro/wiki/sql/protokoly-autentifikacii-kak-oni-rabotayut/>
9. <https://elma365.com/ru/help/platform/two-factor-integration.html>
10. <https://habr.com/ru/articles/413597/>
11. <https://habr.com/ru/articles/234827/>
12. <https://proglib.io/p/8-luchshih-gui-klientov-postgresql-v-2021-godu-2021-09-20>