Правительство Санкт-Петербурга

Комитет по науке и высшей школе

**Санкт-Петербургское государственное бюджетное**

**профессиональное образовательное учреждение**

**«Политехнический колледж городского хозяйства»**

**ДИПЛОМНЫЙ ПРОЕКТ**

Разработка локального WinForms приложения «BiblioLand»

Пояснительная записка

Листов 63

**СОДЕРЖАНИЕ**

[Введение 2](#_Toc771599615)

[1 Анализ предметной области 4](#_Toc690766167)

[1.1 Описание предметной области 5](#_Toc1110338466)

[1.2 Обзор аналогов 6](#_Toc1999476609)

[1.3 Требования к разрабатываемой ИС 9](#_Toc2012133059)

[1.4 Обоснование выбора стека технологий 12](#_Toc965165984)

[2 Проектирование 15](#_Toc1353332560)

[2.1 Проектирование системы 16](#_Toc787233217)

[2.2 Разработка модели базы данных 19](#_Toc2015017396)

[2.3 Проектирование интерфейсов 23](#_Toc1306836856)

[3 Реализация 27](#_Toc1294951494)

[3.1 Реализация основных функций 28](#_Toc1565918795)

[3.2 Реализация интерфейсов 32](#_Toc414348881)

[3.3 Тестирование 33](#_Toc1280741983)

[4 Руководство администратора/пользователя 36](#_Toc621005000)

[4.1 Руководство для администратора 37](#_Toc231994965)

[4.2 Руководство для пользователя 39](#_Toc515675300)

[5 Мероприятия по информационной безопасности 42](#_Toc1357142628)

[5.1 Определение угроз при эксплуатации приложения «GameEnergy» 43](#_Toc375293718)

[5.2 Реализованные меры защиты 43](#_Toc1939665110)

[5.3 Рекомендации пользователям по безопасной работе 46](#_Toc1111558871)

[Заключение 48](#_Toc574994094)

[Список источников 51](#_Toc293080336)

[Приложение А 54](#_Toc1399035305)

[Приложение Б 58](#_Toc828927205)

## Введение

В условиях стремительного развития цифровых технологий и роста объёма информационных ресурсов всё большее значение приобретают локальные, автономные программные решения, не зависящие от постоянного подключения к глобальной сети. Это особенно актуально для сфер образования, библиотечного дела и частного использования, где требуется надёжная, безопасная и удобная система управления цифровыми материалами без рисков, связанных с облачными сервисами или веб-платформами.

Современные пользователи всё чаще сталкиваются с необходимостью хранения, систематизации и удобного доступа к личным или профессиональным коллекциям электронных книг в форматах PDF и EPUB. Однако большинство существующих решений либо требуют постоянного подключения к интернету, либо ограничены базовыми функциями просмотра, не предоставляя инструментов для персонализации, аналитики, модерации контента и гибкого администрирования.

В связи с этим возникает потребность в многофункциональной локальной платформе, сочетающей в себе функции цифровой библиотеки, социальной сети и системы управления контентом. Такая система должна поддерживать работу в полностью офлайн-режиме, обеспечивать защиту персональных данных, предоставлять расширенные возможности для пользователей и администраторов, а также быть адаптируемой под различные сценарии использования — от личного чтения до корпоративного или учебного применения.

Целью данного дипломного проекта является разработка программного продукта «BiblioLand» — локального десктопного приложения на платформе C# WinForms, предназначенного для комплексного управления электронной библиотекой. Приложение реализует поддержку трёхуровневой системы ролей (обычный пользователь, администратор, суперадминистратор), работу с локальной базой данных MS SQL Server, хранение PDF-файлов на диске, а также предоставляет богатый пользовательский интерфейс с возможностями закладок, отзывов, оценок, жалоб, приватности профиля и уведомлений.

Проект разработан с учётом принципов современной инженерии ПО: использованы архитектурные паттерны MVC и Repository, реализованы механизмы валидации и защиты от угроз информационной безопасности, применены современные UI-библиотеки (Guna UI2, MaterialSkin) и библиотека SixLabors.ImageSharp для динамического формирования эстетически привлекательного фона.

Исходный код проекта доступен на GitHub: <https://github.com/L2MBO/BiblioLand.git>

## Анализ предметной области

## 1.1 Описание предметной области

Предметной областью проекта BiblioLand является локальная цифровая библиотечная система, ориентированная на работу с электронными книгами в формате PDF. В отличие от веб-аналогов, приложение функционирует полностью автономно: все данные — пользовательские профили, метаданные книг, закладки, отзывы, уведомления — хранятся в локальной базе данных Microsoft SQL Server, а сами PDF-файлы размещаются в выделенной папке на жёстком диске.

BiblioLand предназначен для трёх основных категорий пользователей:

* **Обычные пользователи** могут:
* регистрироваться и авторизовываться в системе;
* выполнять поиск и фильтрацию книг по названию, автору и жанру;
* просматривать подробную информацию о книге (обложка, описание, оценка, статистика);
* добавлять книги в закладки с выбором категории: читаю, буду читать, прочитано, брошено, отложено;
* оставлять текстовые отзывы и оценивать книги по 10-балльной шкале;
* ставить лайки комментариям других пользователей;
* отправлять жалобы на книги, комментарии или пользователей;
* настраивать приватность своего профиля (скрывать закладки от других);
* отправлять обратную связь администрации по категориям: мне нравится, мне не нравится, нашёл баг, есть предложение;
* читать книги через стандартный PDF-просмотрщик операционной системы, при этом файл автоматически открывается на последней просмотренной странице (благодаря встроенному механизму браузера).
* **Администраторы** обладают всеми правами обычных пользователей и дополнительно могут:
* добавлять, редактировать и удалять книги (включая загрузку обложки и PDF-файла);
* просматривать и управлять жалобами от пользователей;
* отправлять системные уведомления (например, о технических работах);
* просматривать профили любых пользователей;
* банить нарушителей с указанием срока и причины;
* управлять пользователями через админ-панель (поиск, сортировка, фильтрация по наличию описания, статусу бана и роли).
* **Суперадминистраторы** обладают всеми правами администраторов и дополнительно могут:
* назначать другим пользователям роль администратора или обычного пользователя (роль суперадминистратора назначается только вручную в БД для защиты от несанкционированного доступа).

Таким образом, **BiblioLand — это не просто читалка, а гибкая, многофункциональная и безопасная платформа**, которая может быть успешно внедрена:

* в **образовательных учреждениях** — для предоставления студентам доступа к учебной литературе;
* в **библиотеках** — как цифровой каталог с возможностью удалённого чтения;
* в **корпоративной среде** — для внутреннего обмена знаниями и документацией;
* в **личном использовании** — как удобный менеджер личной коллекции PDF-книг.

## 1.2 Обзор аналогов

На современном рынке программного обеспечения существует ряд решений, ориентированных на управление и чтение электронных книг. Наиболее известные из них — **Calibre**, **FBReader** и **Adobe Digital Editions**. Рассмотрим их ключевые особенности, а также выделим преимущества разрабатываемого приложения **BiblioLand**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Приложение** | **Тип** | **Интернет-зависимость** | **Основные функции** | **Ограничения** |
| **Calibre** | Кроссплатформенный менеджер библиотеки | Нет (полностью офлайн) | Импорт/экспорт книг, конвертация форматов, метаданные, ридер | Нет социальных функций, сложный для новичков интерфейс, отсутствие ролевой модели и администрирования |
| **FBReader** | Кроссплатформенная читалка | Частичная (для каталогов и синхронизации) | Чтение EPUB, PDF, поддержка словарей, закладки | Нет локального каталога с управлением, нет отзывов, оценок, жалоб, приватности профиля |
| **Adobe Digital Editions** | Десктопное приложение для DRM-контента | Да (требуется авторизация) | Чтение защищённых книг, синхронизация | Поддержка только DRM-контента, отсутствие локального управления, нет социальных функций |
| **BiblioLand** (разрабатываемое приложение) | **Локальное WinForms-приложение** | **Минимальная** (только восстановление пароля) | **Полноценная библиотека с ролями, закладками по категориям, отзывами, оценками, жалобами, приватностью, уведомлениями, бан-системой, админ-панелью** | Только PDF, нет конвертации форматов |

Ключевые преимущества BiblioLand перед аналогами:

* **Полная автономность**
* Все данные — пользователи, книги, отзывы, уведомления — хранятся локально в **MS SQL Server**. PDF-файлы размещаются в защищённой папке на диске. Приложение не требует подключения к интернету для основного функционала.
* **Поддержка трёхуровневой ролевой модели**

В отличие от большинства аналогов, BiblioLand реализует гибкую систему прав:

* **Обычный пользователь** — чтение, закладки, отзывы.
* **Администратор** — управление книгами, пользователями, жалобами.
* **Суперадминистратор** — назначение ролей (кроме своей собственной).
* **Социальные функции и модерация**

BiblioLand объединяет функции читалки и социальной платформы:

* Оценки по 10-балльной шкале.
* Отзывы с возможностью лайков.
* Жалобы на книги, комментарии и пользователей.
* Система банов с указанием срока и причины.
* **Гибкость использования**

Приложение может быть развёрнуто:

* в **образовательных учреждениях** — как цифровая библиотека учебной литературы;
* в **библиотеках** — для удалённого доступа к фондам;
* в **корпоративной среде** — для внутреннего документооборота;
* в **личном пользовании** — как удобный менеджер PDF-книг с закладками и статистикой.
* **Безопасность и контроль**
* Хеширование паролей через **BCrypt**.
* Ограничение типов и размеров загружаемых файлов (обложки, аватары).
* Приватность профиля — возможность скрыть закладки от других пользователей.
* Защита от брутфорс-атак (блокировка после 5 неудачных попыток входа).

Таким образом, **BiblioLand** не просто заменяет существующие аналоги, а предлагает новый подход к управлению цифровыми книгами — как **локальной**, **безопасной и социально-ориентированной платформе**, способной адаптироваться под потребности самых разных пользователей.

## 1.3 Требования к разрабатываемой ИС

### 1.3.1 Функциональные требования

Приложение **BiblioLand** должно обеспечивать следующие функции для трёх категорий пользователей: **обычный пользователь**, **администратор** и **суперадминистратор**.

#### **Для обычного пользователя:**

* **Регистрация и авторизация**
* Регистрация с указанием: никнейма, email, пароля и подтверждения пароля.
* Авторизация по никнейму/email и паролю.
* Восстановление пароля через отправку кода подтверждения на email (требует интернета).
* Блокировка входа на **5 минут** после **5 неудачных попыток**.
* **Управление профилем**
* Редактирование аватарки (хранится в БД в формате Base64).
* Смена никнейма, описания, email и пароля.
* Настройка **приватности профиля**: при включении — закладки скрыты от других пользователей.
* **Работа с библиотекой**
* Поиск книг по названию или автору.
* Фильтрация по жанру.
* Сортировка по: новизне добавления, популярности, количеству оценок, среднему рейтингу (возрастание/убывание).
* Открытие PDF-файла книги через стандартный просмотрщик ОС.
* Автоматическое добавление книги в категорию «**читаю**» при первом нажатии «Читать».
* **Закладки**
* Возможность добавления книги в одну из 5 категорий: читаю, буду читать, прочитано, брошено, отложено.
* Просмотр всех закладок на отдельной форме.
* **Социальное взаимодействие**
* Оценка книги по **10-балльной шкале**.
* Написание текстового отзыва (от 50 до 1000 символов).
* Постановка лайков комментариям других пользователей.
* Просмотр профиля другого пользователя (с ограничениями при включённой приватности).
* **Модерация и обратная связь**
* Отправка жалобы на книгу по категориям: дубль, несоответствие жанра, другое.
* Отправка обратной связи администрации по категориям: мне нравится, мне не нравится, нашёл баг, есть предложение.
* **Уведомления**
* Просмотр системных уведомлений от администрации (например, о технических работах).
* Удаление прочитанных уведомлений.

#### **Для администратора (все функции пользователя + дополнительные):**

* **Управление книгами**
* Добавление новой книги с загрузкой обложки и PDF-файла.
* Редактирование и удаление существующих книг.
* **Модерация контента**
* Просмотр и удаление жалоб от пользователей.
* Удаление комментариев к книгам.
* Просмотр профиля отправителя жалобы с возможностью скопировать его email в буфер обмена.
* **Работа с пользователями**
* Просмотр списка всех пользователей с сортировкой (по нику, дате регистрации, роли) и фильтрацией (забанен/не забанен, с описанием/без).
* Бан пользователя с указанием срока (через календарь) и причины.
* Разбан забаненного пользователя.
* **Рассылка уведомлений**
* Создание и отправка системных уведомлений всем пользователям.

#### **Для суперадминистратора (все функции администратора и пользователя +):**

* **Управление ролями**
* Назначение роли администратора или пользователя любому аккаунту (роль суперадминистратора назначается только вручную в БД).

### 1.3.2 Требования к пользовательскому интерфейсу

* **Современный и единый дизайн**
* Использование библиотек Guna UI2 и MaterialSkin для создания согласованного визуального стиля.
* Единая цветовая палитра, шрифты, отступы и анимации на всех формах.
* **Кастомные контролы**
* Реализация 13 пользовательских контролов для повторного использования (например, MainBookControl, UserCommentsControl, CartAndOrderItemsControl).
* **Адаптивность**
* Поддержка разрешений экрана от 1280×720 и выше.
* Корректное отображение интерфейса в оконном и полноэкранном режимах.
* **Визуальная обратная связь**
* Анимации при наведении и нажатии на кнопки.
* Отображение ошибок валидации (например, красная рамка у поля с неверным email).
* Уведомления об успешных действиях («Данные обновлены»).
* **Динамический фон**
* Использование библиотеки SixLabors.ImageSharp для создания размытого фона на основе обложки книги (размытие по Гауссу).

### 1.3.3 Требования к производительности и надёжности

* **Автономность**
* Полная работа без интернета для всех функций, кроме восстановления пароля.
* **Производительность**
* Время отклика на действия пользователя ≤ 1 секунда.
* Оптимизированные SQL-запросы через Entity Framework Core.
* **Безопасность**
* Хеширование паролей и кодов восстановления через BCrypt.Net-Next.
* Ограничение загружаемых файлов по типу (только JPG, PNG для изображений; только PDF для книг) и размеру.
* Защита от SQL-инъекций (параметризованные запросы).

## 1.4 Обоснование выбора стека технологий

Разработка приложения **BiblioLand** выполнена с использованием современного, стабильного и хорошо документированного стека технологий, ориентированного на создание локальных десктопных решений под операционные системы семейства Windows. Выбор каждой технологии обоснован требованиями к функциональности, безопасности, производительности и удобству сопровождения.

#### **Язык программирования: C#**

* Выбор языка **C#** обусловлен следующими факторами:
* Является стандартом де-факто для разработки Windows-приложений.
* Обладает высокой **типобезопасностью**, **производительностью** и **мощной экосистемой**.
* Имеет **нативную интеграцию** с .NET Framework и Visual Studio, что ускоряет разработку и отладку.
* Поддерживает современные парадигмы: ООП, LINQ, асинхронное программирование.

#### **Фреймворк: Windows Forms (WinForms)**

* Несмотря на наличие более новых UI-фреймворков (WPF, MAUI), для проекта выбран **WinForms** по следующим причинам:
* **Простота и скорость разработки** графического интерфейса для локальных приложений.
* **Отличная поддержка кастомных контролов**, что позволило реализовать 13 повторно используемых компонентов (например, MainBookControl, UserCommentsControl).
* **Полная совместимость** с библиотеками **Guna UI2** и **MaterialSkin**, обеспечивающими современный визуальный стиль.
* **Низкие требования к ресурсам** и стабильность на всех версиях Windows 10/11.

#### **СУБД: Microsoft SQL Server (локальный экземпляр)**

* Для хранения данных использована **Microsoft SQL Server**, так как:
* Это **надёжная реляционная СУБД** с поддержкой транзакций, ограничений и триггеров.
* Обеспечивает **высокую целостность данных** за счёт внешних ключей, ограничений и каскадных операций.
* Позволяет хранить **BLOB-данные** (аватары в формате Base64) непосредственно в таблицах.
* Имеет **простую интеграцию** с Entity Framework и поддержку локального развёртывания (включая SQL Server Express).

#### **ORM: Entity Framework Core**

* Работа с базой данных осуществляется через **Entity Framework Core**, что даёт следующие преимущества:
* **Автоматическая генерация SQL-запросов** с защитой от SQL-инъекций.
* **Чёткое разделение слоёв** (Model–View–Controller), упрощающее поддержку и расширение кода.
* **Поддержка паттерна Repository**, что изолирует бизнес-логику от UI и упрощает модификацию.
* Возможность **ленивой и явной загрузки связанных сущностей**, оптимизируя производительность.

#### **Безопасность: BCrypt.Net-Next**

* Для защиты учётных данных применена библиотека **BCrypt.Net-Next**:
* Обеспечивает **надёжное хеширование** паролей и кодов восстановления с автоматической «солью».
* **Адаптивный алгоритм** — время хеширования увеличивается со временем, что защищает от брутфорс-атак.
* Даже при компрометации базы данных **восстановление исходных паролей вычислительно невозможно**.

#### **Дополнительные библиотеки**

* **Guna UI2 и MaterialSkin** — использованы для создания современного, визуально привлекательного интерфейса с анимациями, тенями и согласованной цветовой палитрой.
* **SixLabors.ImageSharp** — применена для динамического формирования фона на формах книг: обложка автоматически обрезается под размеры окна и размывается по Гауссу, создавая эстетичный эффект глубины без нагрузки на производительность.
* **System.Net.Mail** — используется для отправки кода восстановления пароля на email (единственная функция, требующая интернета).

**Примечание**: Приложение **полностью автономно**. Все данные — пользователи, книги, отзывы, закладки — хранятся локально. Интернет требуется **только для отправки кода восстановления пароля**. При отсутствии сети эта функция недоступна, но **основной функционал (поиск, чтение, отзывы, закладки)** **работает без ограничений**.

## Проектирование

## 2.1 Проектирование системы

**Проектирование программного продукта BiblioLand выполнено с учётом требований к функциональности, безопасности и удобству использования. Система спроектирована как локальное десктопное приложение с чётким разделением на слои: представление (View), бизнес-логика (Controller/Service) и данные (Model), что обеспечивает высокую читаемость, расширяемость и сопровождаемость кода.**

### 2.1.1 Определение группы пользователей

В приложении **BiblioLand** реализована **трёхуровневая система ролей**, что является ключевым архитектурным решением, отличающим проект от большинства аналогов:

#### **Обычный пользователь**

* Основная целевая аудитория приложения. Может:
* регистрироваться и авторизовываться;
* выполнять поиск и фильтрацию книг;
* добавлять книги в закладки с выбором категории: читаю, буду читать, прочитано, брошено, отложено;
* оставлять текстовые отзывы (50–1000 символов) и ставить оценки по **10-балльной шкале**;
* ставить лайки комментариям других пользователей;
* отправлять жалобы на книги, комментарии или пользователей;
* настраивать приватность профиля;
* отправлять обратную связь администрации;
* читать книги через стандартный PDF-просмотрщик ОС, при этом файл автоматически открывается на последней просмотренной странице (благодаря встроенному механизму браузера).

#### **Администратор**

* Обладает всеми правами обычного пользователя. Дополнительно может:
* добавлять, редактировать и удалять книги (включая загрузку обложки и PDF-файла);
* просматривать и управлять жалобами от пользователей;
* отправлять системные уведомления (например, о технических работах);
* просматривать профили любых пользователей;
* банить нарушителей с указанием срока и причины;
* управлять пользователями через админ-панель (поиск, сортировка, фильтрация по наличию описания, статусу бана и роли).

#### **Суперадминистратор**

* Обладает всеми правами администратора и пользователя. Дополнительно может:
* назначать другим пользователям роль администратора или обычного пользователя.

**Важно**: роль суперадминистратора назначается **только вручную в базе данных** для защиты от несанкционированного повышения привилегий.

Таким образом, система гибко адаптируется под различные сценарии использования: от личного чтения до корпоративного или учебного управления библиотекой.

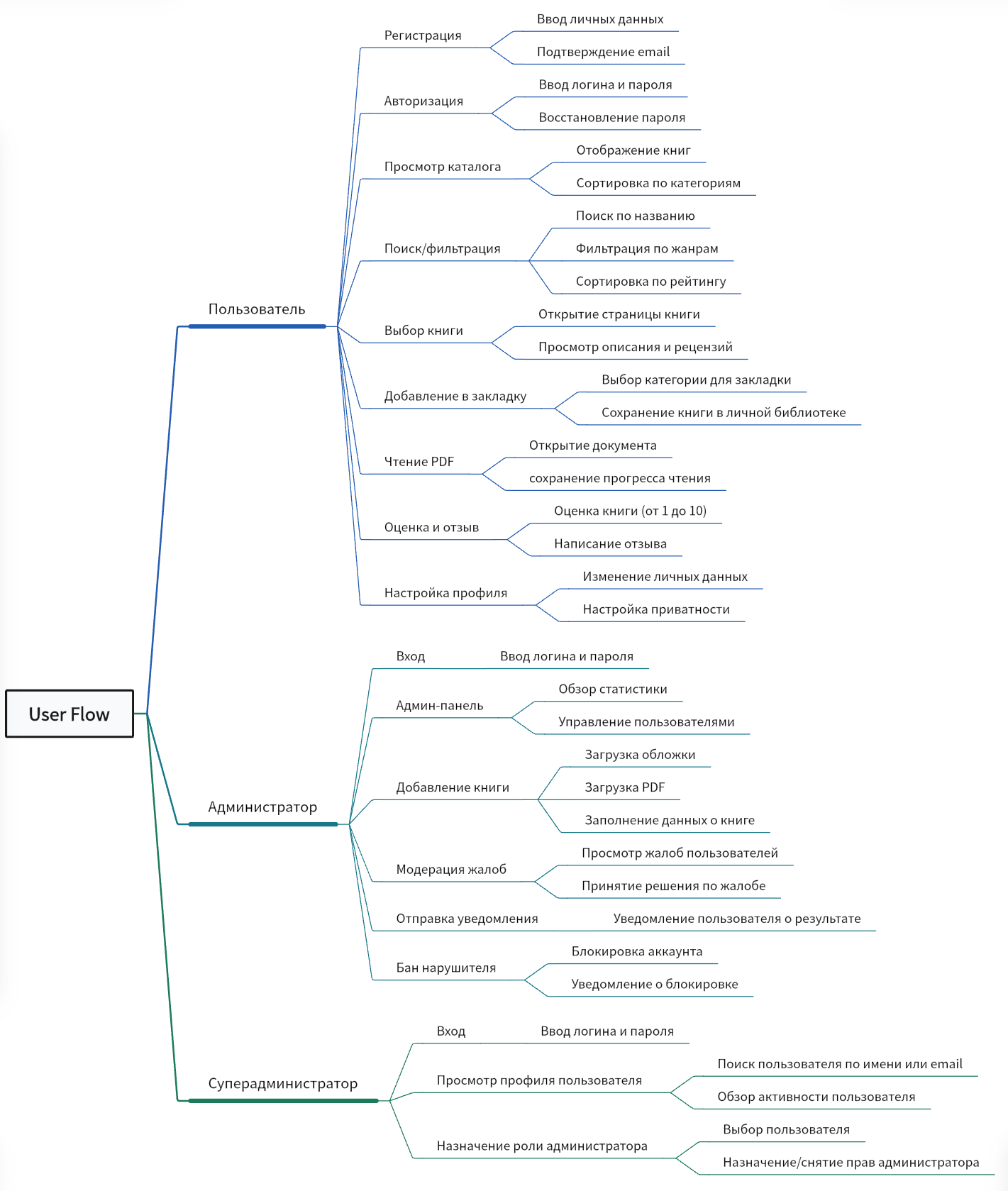
### 2.1.2 Функциональное моделирование

Для описания взаимодействия пользователей с системой разработана **диаграмма прецедентов**.



*Рисунок 1 - Диаграмма прецедентов*

**User Flow:**

*Рисунок 2 – User Flow*

Такая структура обеспечивает полную автономность приложения: все действия, кроме восстановления пароля, выполняются без подключения к интернету.

## 2.2 Разработка модели базы данных

База данных приложения **BiblioLand** разработана на платформе **Microsoft SQL Server** и представляет собой реляционную структуру, оптимизированную для хранения информации о пользователях, книгах, отзывах, закладках и системных уведомлениях. Все данные хранятся **локально**, что обеспечивает полную автономность приложения и защиту от внешних угроз.

Модель спроектирована с учётом **трёхуровневой ролевой системы** (пользователь, администратор, суперадминистратор) и поддерживает ключевые бизнес-процессы: управление библиотекой, оценку книг, модерацию контента и персонализацию профиля.

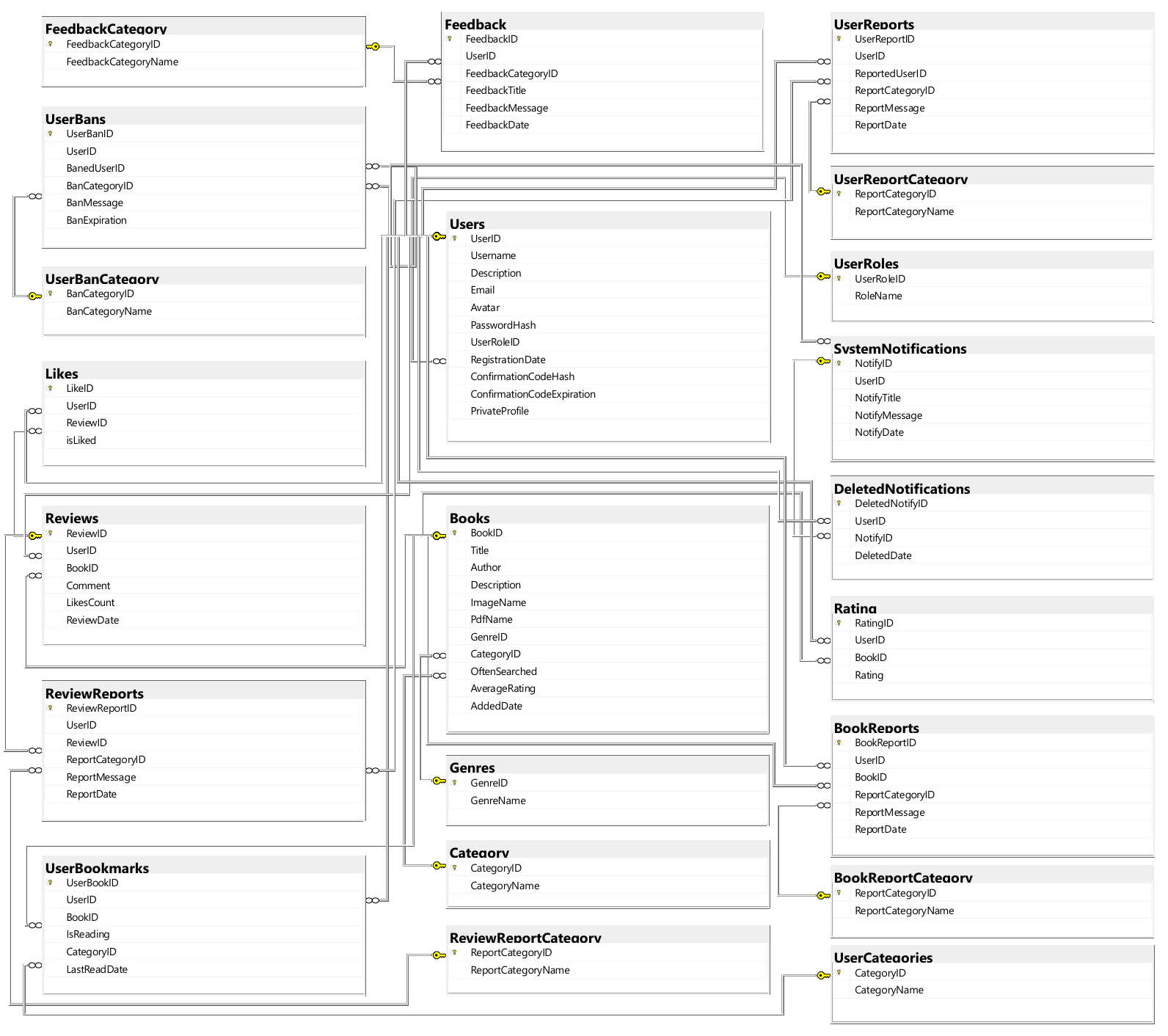
### 2.2.1 Основные таблицы и их назначение

Ниже приведено описание ключевых сущностей базы данных.

|  |  |
| --- | --- |
| **Таблица** | **Назначение** |
| **Users** | Хранит информацию о пользователях: UserID (PK), Username, Email, PasswordHash, Avatar (в формате Base64), UserRoleID (FK), RegistrationDate, PrivateProfile (флаг приватности). |
| **UserRoles** | Справочник ролей: UserRoleID (PK), RoleName (User, Admin, SuperAdmin). |
| **Books** | Основная таблица книг: BookID (PK), Title, Author, Description, ImagePath (имя файла обложки), PdfName (имя PDF-файла), AddedDate, AverageRating, OftenSearched (флаг популярности). |
| **Genres** | Справочник жанров: GenreID (PK), GenreName. |
| **BookGenres** | Связующая таблица «многие-ко-многим» между книгами и жанрами. |
| **Reviews** | Отзывы пользователей: ReviewID (PK), UserID (FK), BookID (FK), Comment, LikesCount, ReviewDate. |
| **Rating** | Оценки книг: RatingID (PK), UserID (FK), BookID (FK), Rating (целое число от 1 до 10). |
| **Likes** | Фиксирует лайки к отзывам: LikeID (PK), UserID (FK), ReviewID (FK), isLiked (флаг). |
| **UserBookmarks** | Закладки пользователя: UserBookmarkID (PK), UserID (FK), BookID (FK), CategoryID (FK), LastReadDate. |
| **UserCategories** | Категории закладок: CategoryID (PK), CategoryName (читаю, буду читать, прочитано, брошено, отложено). |
| **SystemNotifications** | Системные уведомления от администрации: NotifyID (PK), UserID (FK), NotifyTitle, NotifyMessage, NotifyDate. |
| **UserReports** | Жалобы пользователей: UserReportID (PK), UserID (FK — отправитель), ReportedUserID (FK — нарушитель) или BookID (FK — книга), ReportCategoryID (FK), ReportMessage, ReportDate. |
| **ReportCategory** | Категории жалоб: ReportCategoryID (PK), ReportCategoryName (дубль, несоответствие жанра, другое, мне нравится, мне не нравится, нашёл баг, есть предложение). |
| **UserBans** | Информация о банах: UserBanID (PK), UserID (FK — забаненный), BanCategoryID (FK), BanMessage, BanExpiration. |
| **BanCategory** | Справочник категорий банов. |
| **Feedback** | Обратная связь по приложению: FeedbackID (PK), UserID (FK), FeedbackCategoryID (FK), FeedbackTitle, FeedbackMessage, FeedbackDate. |
| **FeedbackCategory** | Категории обратной связи. |

Примечание:

* **PDF-файлы** книг и **обложки** хранятся в **локальной папке** на диске. В базе данных сохраняются **только имена файлов** (PdfName, ImagePath).
* **Аватары пользователей** хранятся **в базе данных в формате Base64**, что исключает необходимость хранения файлов на диске и упрощает резервное копирование.

*Рисунок 3 - Диаграмма базы данных*

### 2.2.2 Взаимосвязи и целостность данных

Модель базы данных обеспечивает целостность данных за счёт:

* **Внешних ключей (FK)** между связанными таблицами.
* **Каскадного удаления** (например, при удалении книги автоматически удаляются её отзывы, оценки и жалобы).
* **Уникальных ограничений** (например, пользователь не может оставить более одного отзыва на одну книгу).

Ключевые связи:

* Books → BookGenres → Genres (многие-ко-многим).
* Users → Reviews → Books (оценка и отзыв).
* Users → UserBookmarks → Books + UserCategories (закладки с категориями).
* Users → UserReports → Books (жалобы на книги).

### 2.2.3 Триггеры и автоматизация

Для обеспечения актуальности данных используются **SQL-триггеры**:

* **trg\_UpdateAverageRating**
* Автоматически пересчитывает средний рейтинг книги (Books.AverageRating) при добавлении, обновлении или удалении оценки в таблице Rating.
* **trg\_ValidateUserRole** (реализован на уровне приложения)
* Запрещает назначение роли SuperAdmin через интерфейс — только прямое редактирование в БД.

**Примечание**: в отличие от аналогов, **BiblioLand не хранит прогресс чтения (номер страницы)**, так как эта функция реализована на уровне операционной системы: PDF-файлы открываются в стандартном просмотрщике, который **сам запоминает позицию чтения**. В БД сохраняется только дата последнего открытия (LastReadDate) для сортировки в разделе «Продолжить чтение».

## 2.3 Проектирование интерфейсов

Пользовательский интерфейс приложения BiblioLand разработан с учётом современных принципов UX/UI-дизайна для десктопных приложений: минимализм, читаемость, визуальная иерархия и мгновенная обратная связь. Все элементы интерфейса объединены единой цветовой палитрой, типографикой и системой отступов, что создаёт целостное и профессиональное впечатление.

### 2.3.1 Используемые технологии и подходы

Для создания интерфейса использованы следующие библиотеки:

* **Guna UI2** — для реализации кнопок, текстовых полей, панелей с анимациями, тенями и плавными переходами.
* **MaterialSkin** — для соблюдения принципов Material Design (акцентные цвета, карточки, возвышение элементов).
* **Собственные кастомные контролы** — 13 переиспользуемых компонентов (например, MainBookControl, UserCommentsControl, NavigationControl), что обеспечивает единообразие и упрощает поддержку.

Особое внимание уделено **динамическому фону**: на формах отдельных книг используется библиотека **SixLabors.ImageSharp** для создания **размытого** (по Гауссу) фона на основе обложки книги. Это создаёт эффект **глубины и визуального погружения** без нагрузки на производительность.

### 2.3.2 Основные формы приложения

Приложение состоит из 28 форм: 19 пользовательских и 9 административных. Все они спроектированы в соответствии с принципом единая навигационная модель — через кастомный NavigationControl.

Ниже приведено описание ключевых форм (визуальные прототипы см. в Приложении B).

* **Форма авторизации и регистрации**
* Единая модальная форма с переключением между вкладками «Вход» и «Регистрация».
* Валидация полей в реальном времени (проверка email, длины пароля).
* Защита от брутфорса: блокировка на 5 минут после 5 неудачных попыток.
* Восстановление пароля через отправку кода на email (требуется интернет).
* **Главная форма (MainForm)**
* Отображает книги по категориям:
* **Популярное** — книги с наибольшим количеством оценок.
* **Последние обновления** — недавно добавленные книги.
* **Продолжить чтение** — книги из категории читаю, отсортированные по LastReadDate (новые — первыми).
* Использует кастомный контрол MainBookControl для отображения каждой книги.
* **Каталог книг (CatalogForm)**
* Полноэкранный каталог с панелью фильтров слева:
* Поиск по названию или автору.
* Фильтрация по жанру.
* Сортировка: по новизне, популярности, количеству оценок, среднему рейтингу (с возможностью смены порядка через стрелку).
* Каждая книга отображается через MainBookControl.
* **Форма книги (BookInfoForm)**
* Детальная карточка книги с:
* Обложкой и размытым фоном (реализовано через SixLabors.ImageSharp).
* Названием, автором, жанром, описанием.
* Статистикой: средний рейтинг (10-балльная шкала), количество закладок.
* Кнопкой «Читать», которая:
  + - * Автоматически добавляет книгу в категорию *читаю* (если не добавлена).
      * Открывает PDF-файл в стандартном просмотрщике ОС (позиция чтения сохраняется браузером).
* Отзывы других пользователей (через UserCommentsControl).
* Возможность:
* Оценить книгу (1–10).
* Написать отзыв (50–1000 символов).
* Добавить в закладки с выбором категории (читаю, буду читать, прочитано, брошено, отложено).
* Пожаловаться на книгу (дубль, несоответствие жанра, другое).
* Поставить лайк комментарию.
* **Форма профиля (ProfileForm)**
* Верхняя панель: аватар, никнейм, кнопки для администраторов (забанить/разбанить, сменить роль, скопировать email).
* Левая панель: статистика (количество лайков, отзывов, дата регистрации, описание).
* Правая панель: закладки по категориям.
* Приватность: если включена — закладки заменяются заглушкой «Профиль приватный».
* **Админ-панель (AdminPanelForm)**
* Управление пользователями: поиск, сортировка, фильтрация (забанен/не забанен, с описанием/без).
* Управление книгами: добавление/редактирование/удаление с загрузкой обложки и PDF.
* Модерация: просмотр и удаление жалоб, отправка системных уведомлений.

### 2.3.3 Кастомные контролы

Для обеспечения единообразия и повторного использования созданы 13 кастомных контролов, рассмотрим самые основные:

|  |  |
| --- | --- |
| **Контрол** | **Назначение** |
| MainBookControl | Отображение книги в каталоге: обложка, название, автор, жанр |
| UserCommentsControl | Отзыв одного пользователя: аватар, ник, оценка, текст, лайк |
| UserBookmarksControl | Элемент закладки с категорией (*читаю*, *прочитано* и др.) |
| StatisticsControl | Статистика книги: оценки и закладки по категориям |
| NavigationControl | Панель навигации с поиском, уведомлениями, профилем |
| QuickSearchControl | Контрол быстрого поиска (по названию/автору) |
| AdminUserControl | Карточка пользователя в админ-панели: аватар, роль, дата регистрации, статус (забанен/нет) |

Каждый контрол инкапсулирует свою логику отображения и взаимодействия, что упрощает модификацию и тестирование.

### 2.3.4 Адаптивность и поддержка разрешений

Интерфейс адаптируется под два состояния окна:

* **Оконный режим**: компактное отображение панелей.
* **Полноэкранный режим**: расширенные панели, увеличенные отступы.

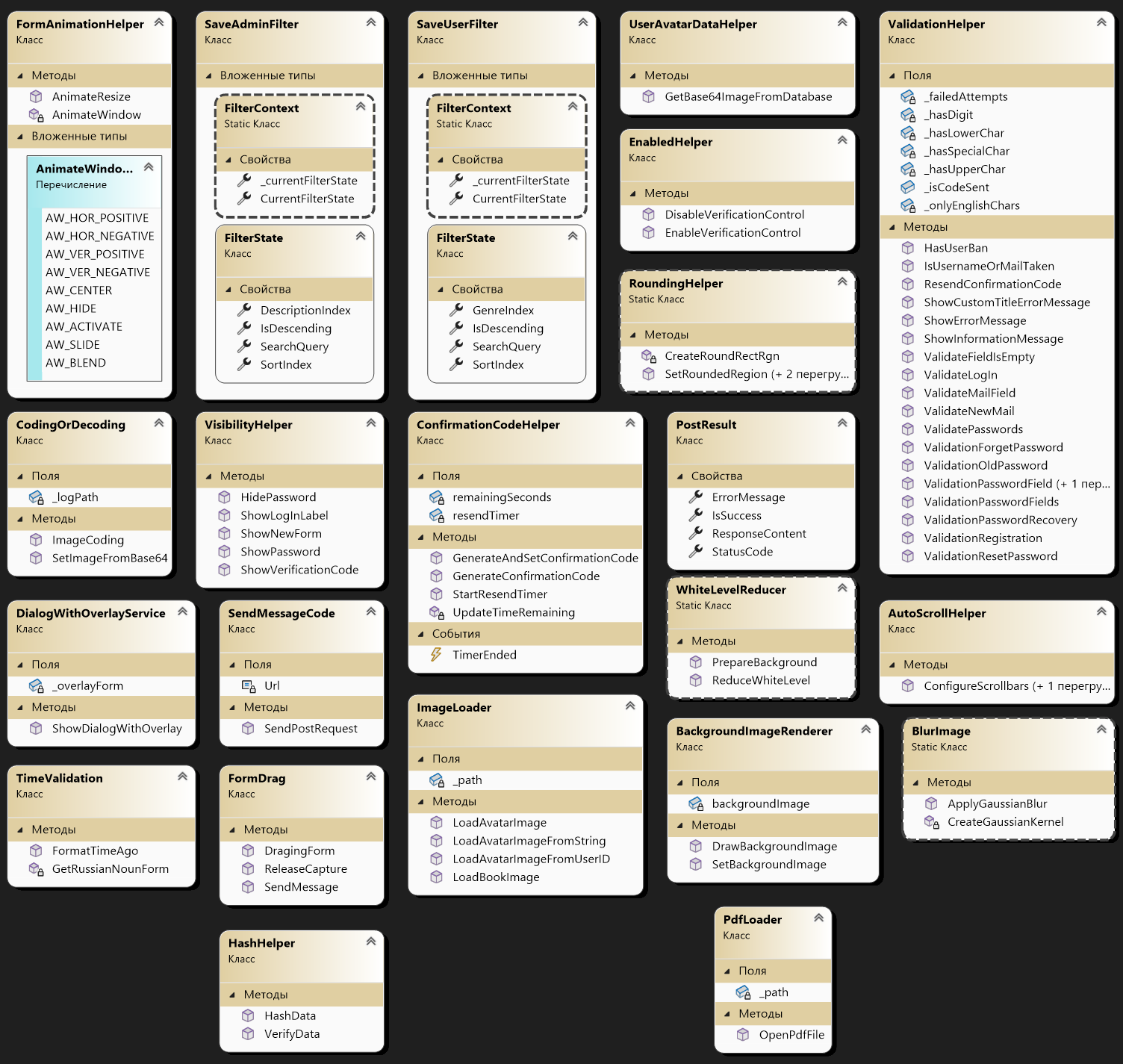
Поддерживаемые разрешения: от **1280×720** и выше. Все формы корректно перестраиваются при изменении размера окна через обработчики SizeChanged и Resize.

### 2.3.5 Визуальная обратная связь

* Анимации при наведении и нажатии на кнопки.
* Красная рамка у полей с ошибками валидации (email, пароль).
* Уведомления об успешных действиях: «Данные обновлены», «Книга добавлена».
* Курсор Hand над кликабельными элементами.

## Реализация

## 3.1 Реализация основных функций

*Рисунок 4 - Диаграмма классов*

Разработка приложения BiblioLand выполнена с применением архитектурных паттернов MVC (Model–View–Controller) и Repository, что обеспечивает чёткое разделение ответственности между уровнями приложения:

* **Model — сущности Entity Framework (Books, Users, Reviews, Rating и др.), отражающие структуру данных;**
* **View — формы и кастомные контролы на основе WinForms;**
* **Controller/Service — классы, реализующие бизнес-логику без привязки к UI.**

Такой подход упрощает сопровождение, расширение и отладку кода.

#### **Работа с данными: Entity Framework + Repository**

Подключение к локальной базе данных MS SQL Server осуществляется через Entity Framework Core. Для изоляции логики работы с БД от интерфейса созданы репозитории, например:

public interface IBookRepository  
{  
 List<Books> GetAll();  
 Books GetById(int id);  
 void Add(Books book);  
 void Update(Books book);  
 void Delete(int id);  
}

Аналогичные интерфейсы реализованы для IUserRepository, IReviewRepository и других сущностей.

#### **Авторизация и безопасность**

Регистрация и вход реализованы с проверкой учётных данных через хеширование:

var storedHash = user.PasswordHash;  
if (BCrypt.Net.BCrypt.Verify(inputPassword, storedHash))  
{  
 // Авторизация успешна  
}

* **Пароли и коды восстановления** хешируются с помощью библиотеки **BCrypt.Net-Next** — даже при компрометации БД восстановить исходные значения вычислительно невозможно.
* **Восстановление пароля:**
* Пользователь вводит email;
* Система генерирует одноразовый код, хеширует его и сохраняет в БД;
* Код отправляется на почту (требуется интернет);
* После ввода кода разрешается смена пароля.

**Важно**: основной функционал (поиск, чтение, отзывы, закладки) **работает полностью офлайн**. Интернет требуется **только для восстановления пароля**.

#### **Управление книгами и файлами**

* **Хранение файлов:**
* **PDF-файлы книг** и обложки сохраняются в локальной папке на диске;
* В базе данных хранятся **только имена файлов** (PdfName, ImagePath);
* **Аватары** пользователей хранятся в БД в формате **Base64**, что исключает необходимость хранения файлов на диске.
* **Загрузка файлов:**
* При добавлении книги администратор выбирает обложку и PDF через OpenFileDialog с фильтром: openFileDialog.Filter = "Image Files|\*.jpg;\*.jpeg;\*.png|PDF Files|\*.pdf";
* Файлы копируются в системные папки (bookImg, bookPdf), а их имена сохраняются в БД.
* **Чтение книг:**
* Книга открывается через стандартный PDF-просмотрщик ОС;
* **Прогресс чтения не отслеживается приложением** — он сохраняется **браузером или системным просмотрщиком**;
* При повторном открытии PDF-файл автоматически проматывается до последней просмотренной страницы.

#### **Закладки и категории**

* При первом нажатии «**Читать**» книга автоматически добавляется в категорию «**читаю**» (если не добавлена ранее).
* Пользователь может изменить категорию на: буду читать, прочитано, брошено, отложено.
* Дата последнего открытия (LastReadDate) сохраняется в таблице UserBookmarks и используется для сортировки в разделе «**Продолжить чтение**».

#### **Отзывы, оценки и жалобы**

* **Оценка** — целое число от **1 до 10**.
* **Отзыв** — текст длиной от **50 до 1000** **символов**.
* **Лайки** — пользователь может ставить лайки комментариям других.
* **Жалобы** подаются по категориям:
* на книгу: дубль, несоответствие жанра, другое;
* на комментарий: оскорбление, спам и т.д.;
* общая обратная связь: мне нравится, мне не нравится, нашёл баг, есть предложение.

#### **Роли пользователей**

* **Обычный пользователь** — чтение, закладки, отзывы.
* **Администратор** — управление книгами, пользователями, жалобами, уведомлениями, бан-система.
* **Суперадминистратор** — назначение роли администратора другим пользователям.

**Замечание**: роль суперадминистратора назначается только вручную в БД для защиты от несанкционированного повышения привилегий.

#### **Бан-система**

* Администратор может забанить пользователя с указанием:
* срока (через календарь);
* причины бана.
* После входа забаненного пользователя вместо главной формы отображается **форма с информацией о бане**.
* По истечении срока бан **автоматически снимается** (проверка выполняется при входе).

#### **Приватность профиля**

* Пользователь может включить **режим приватности**.
* В этом режиме другие пользователи **видят только аватар**, **никнейм**, **статистику и дату регистрации**.
* **Закладки скрываются** и заменяются заглушкой: «Профиль приватный».

#### **Уведомления**

* Администратор может отправлять **системные уведомления** всем пользователям (например, о технических работах).
* Обычные пользователи видят уведомления и могут удалять их после прочтения.

## 3.2 Реализация интерфейсов

Интерфейс приложения **BiblioLand** разработан с применением современных UI-библиотек и принципов проектирования, обеспечивающих **единый стиль**, **визуальную целостность** и **интуитивную навигацию**.

Для улучшения пользовательского опыта были использованы следующие библиотеки:

* **Guna UI2**

Используется для реализации всех кнопок, текстовых полей, панелей и других элементов управления. Обеспечивает:

* Плавные анимации при наведении и нажатии.
* Поддержку скруглённых углов, теней и прозрачности.
* Тонкую настройку цветов при отображении, нажатии и наведении на элементы.
* **MaterialSkin**

Применяется для соблюдения принципов **Material Design**:

* Чёткая визуальная иерархия.
* Использование карточек для отображения книг и отзывов.
* Единая типографика (шрифт **Segoe UI**, размер 9–12 pt).
* **SixLabors.ImageSharp**

Ключевая особенность интерфейса — **динамический размытый фон** на формах отдельных книг. При открытии карточки книги:

* Обложка автоматически **обрезается под размеры формы**.
* Применяется **гауссово размытие** с радиусом 15 пикселей.
* Результат устанавливается как фон, создавая эффект глубины и визуального погружения без нагрузки на производительность.

Пример кода:

using (var image = Image.Load(inputStream))  
{  
 image.Mutate(x => x.Resize(formWidth, formHeight).Blur(15));  
 pictureBox.BackgroundImage = image.ToBitmap();  
}

## 3.3 Тестирование

В рамках разработки приложения BiblioLand было проведено ручное функциональное тестирование всех ключевых сценариев использования. Поскольку проект реализован в рамках дипломной работы и не предполагает автоматизированного тестирования (unit-тестов, интеграционных тестов), основной акцент сделан на сквозные пользовательские сценарии для каждой роли.

### 3.3.1 Методика тестирования

Тестирование выполнялось по следующему принципу:

* Для каждой формы и функции составлен **тест-кейс** с предусловием, шагами и ожидаемым результатом.
* Тестирование проводилось в двух режимах:
* **Оконный режим** (разрешение 1280×720).
* **Полноэкранный режим** (разрешение 1920×1080).
* Проверялась корректность работы **без интернета** (все функции, кроме восстановления пароля).
* Проверялась устойчивость к **некорректному вводу** (валидация email, длины пароля, формата файлов).

### 3.3.2 Основные тест-кейсы

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Сценарий** | **Ожидаемый результат** | **Статус** |
| TC-01 | Регистрация нового пользователя | Учётная запись создана, хеш пароля сохранён в БД | ✅ Пройден |
| TC-02 | Авторизация под обычным пользователем | Открывается главная форма с доступом к каталогу, закладкам, профилю | ✅ Пройден |
| TC-03 | Авторизация под администратором | Доступна админ-панель, кнопки управления книгами и пользователями | ✅ Пройден |
| TC-04 | Блокировка после 5 неудачных попыток входа | Форма входа недоступна в течение 5 минут | ✅ Пройден |
| TC-06 | Добавление книги в закладки с выбором категории | Книга появляется в указанной категории (читаю, прочитано и др.) | ✅ Пройден |
| TC-07 | Оценка книги по 10-балльной шкале и отзыв (50–1000 символов) | Оценка и отзыв отображаются на форме книги, средний рейтинг пересчитан триггером | ✅ Пройден |
| TC-08 | Открытие PDF-файла книги | Файл открывается в стандартном просмотрщике ОС, позиция чтения сохраняется браузером | ✅ Пройден |
| TC-09 | Отправка жалобы на книгу (дубль, несоответствие жанра) | Жалоба сохраняется в БД, администратор может её просмотреть и удалить | ✅ Пройден |
| TC-10 | Включение приватности профиля | Закладки скрываются для других пользователей, остальная статистика видна | ✅ Пройден |
| TC-11 | Бан пользователя с указанием срока и причины | После входа отображается форма с информацией о бане, доступ к функционалу закрыт | ✅ Пройден |
| TC-12 | Добавление книги администратором с обложкой и PDF | Книга отображается в каталоге, файлы сохранены в системных папках, имена записаны в БД | ✅ Пройден |
| TC-13 | Восстановление пароля (с интернетом) | Код приходит на почту, пароль успешно меняется | ✅ Пройден |
| TC-14 | Работа без интернета | Все функции (поиск, чтение, отзывы, закладки) работают без ошибок | ✅ Пройден |
| TC-15 | Назначение роли администратора суперадмином | Пользователь получает права администратора, кнопка «админка» становится активной | ✅ Пройден |

### 3.3.3 Обработка ошибок

Все выявленные в процессе тестирования ошибки были устранены:

* **Дублирование книг в закладках** → исправлено через проверку UserBookmarks.Any(...).
* **Ошибка при удалении жалобы** → добавлена проверка на null.
* **Некорректное отображение закладок** **у забаненного пользователя** → добавлена проверка статуса бана при загрузке профиля.
* **Ошибка валидации email при смене почты** → реализована проверка уникальности email в БД.

### 3.3.4 Итоги тестирования

Тестирование подтвердило:

* **Корректность работы всех 28 форм** и **13 кастомных контролов**.
* **Стабильность приложения** без аварийного завершения.
* **Полную автономность** основного функционала.
* **Соответствие требованиям** к безопасности и пользовательскому опыту.

Приложение готово к эксплуатации в образовательных, библиотечных и частных средах.

## Руководство администратора/пользователя

## 4.1 Руководство для администратора

Администратор обладает расширенными правами и отвечает за наполнение каталога, модерацию контента и взаимодействие с пользователями через системные уведомления.

Администратор обладает расширенными правами и отвечает за наполнение каталога, управление контентом и взаимодействие с пользователями через системные уведомления.

#### **Авторизация:**

* + Запустите приложение **BiblioLand**.
  + На форме авторизации введите логин/email и пароль учётной записи с ролью «Администратор» или «**Суперадминистратор**».
  + Нажмите кнопку «**Войти**».
  + После успешной авторизации откроется главная форма с доступом к админ-панели (кнопка «**Админ панель**» в профиле).

#### **Управление книгами**

##### **Добавление новой книги**

* + - В профиле нажмите «**Добавить контент**» → «**Добавить книгу**».
    - Заполните поля:
    - **Название** — полное название книги.
    - **Автор** — ФИО автора.
    - **Жанр** — выберите из списка (поддерживаются множественные жанры).
    - **Описание** — краткое содержание (до 3000 символов).
    - Нажмите «**Выбрать обложку**» — выберите изображение (только JPG/PNG, до 5 МБ).
    - Нажмите «**Выбрать PDF-файл**» — выберите файл книги (только PDF, до 100 МБ).
    - Нажмите «**Сохранить**».

Книга отобразится в каталоге, а файлы будут скопированы в системные папки (bookImg, bookPdf).

##### **Редактирование и удаление книги**

* Откройте карточку книги.
* Нажмите «**Изменить**» — внесите правки и сохраните.
* Для удаления нажмите «**Удалить книгу**» → подтвердите действие.

Книга и все связанные данные (отзывы, жалобы) удалятся автоматически (каскадное удаление).

#### **Управление пользователями**

* Чтобы профиль определенного пользователя:
* В профиле нажмите «Админ панель».
* Откроется панель с фильтрами и сортировкой:
  + - * **По нику**, **дате регистрации**, **роли**, **наличию описания**.
      * **Фильтры**: забанен/не забанен, с описанием/без.
* Нажмите на карточку пользователя → откроется его профиль.

##### **Бан пользователя**

* В профиле пользователя нажмите «**Забанить**».
* Укажите:
  + - **Причину бана** (выпадающий список: оскорбление, спам, нарушение правил и др.).
    - **Сообщение** (до 500 символов).
    - **Срок бана** — выберите дату окончания через календарь.
* Нажмите «**Подтвердить**».

Пользователь увидит форму с информацией о бане при следующем входе.

##### **Разбан**

* В профиле забаненного пользователя нажмите «Разбанить».
* Бан снимается немедленно.

#### **Примечание для суперадминистратора:**

В профиле любого пользователя доступна кнопка «**Сменить роль**» → можно назначить роль «**Администратор**» или «**Пользователь**».

**Роль суперадминистратора назначается только вручную в БД.**

#### **Модерация жалоб и уведомления**

##### **Просмотр жалоб**

* В админ-панели перейдите в раздел «**Уведомления**».
* Отобразится список всех жалоб с фильтрами:
* **Тип жалобы**: на книгу, на комментарий, на пользователя.
* **Категория**: дубль, несоответствие жанра, оскорбление и др.
* Нажмите на жалобу → откроется модальное окно с деталями (отправитель, сообщение, дата).
* Нажмите «**Удалить**» → жалоба исчезнет из списка (сохранится в архиве БД).

##### **Отправка системных уведомлений**

* На форме уведомлений нажмите «**+** (**Новое уведомление)**».
* Укажите:
* **Заголовок** (например, «Технические работы»).
* **Текст** (до 500 символов).
* Нажмите «**Отправить**».

**Все пользователи увидят уведомление при следующем запуске приложения.**

#### **Безопасность и обслуживание**

* + **Резервное копирование БД**: выполняйте через **SQL Server Management Studio**.
  + **Обновление приложения**: замените .exe и папку bookImg/bookPdf при обновлении.
  + **Смена пароля админа**: в настройках профиля → вкладка **«Смена пароля»**.

## 4.2 Руководство для пользователя

**Обычный пользователь может использовать BiblioLand для поиска, чтения и управления электронными книгами в полностью офлайн-режиме. Ниже приведена пошаговая инструкция по основным действиям.**

#### **Регистрация и авторизация**

##### **Регистрация:**

* На стартовой форме нажмите «**Регистрация**».
* Заполните поля:
* **Никнейм** (уникальный, от 3 до 30 символов).
* **Email** (для восстановления пароля).
* **Пароль** (минимум 8 символов, с цифрами и заглавными буквами).
* **Подтверждение пароля**.
* Нажмите «**Зарегистрироваться**».
* После успешной регистрации откроется форма авторизации.

##### **Авторизация:**

* Введите **никнейм/email** и пароль.
* Нажмите «**Войти**».
* При 5 неудачных попытках вход заблокируется на **5 минут**.

##### **Восстановление пароля:**

* Нажмите «**Забыли пароль?**».
* Введите email → на почту придёт **6-значный код**.
* Введите код и новый пароль → авторизуйтесь.

**Важно**: восстановление пароля требует интернета. Все остальные функции работают **без подключения**.

#### **Поиск и фильтрация книг**

* На **главной форме** или в каталоге используйте:
* **Поле поиска** — введите название книги или имя автора.
* **Фильтр по жанру** — выберите из списка (Ужасы, Философия, Научная литература и др.).
* **Сортировку**:
* По новизне добавления.
* По популярности (количеству оценок).
* По среднему рейтингу (1–10).
* По алфавиту.
* Стрелка рядом с названием сортировки меняет порядок (возрастание/убывание).

#### **Чтение книги**

* Кликните на книгу в каталоге → откроется **форма книги**.
* Нажмите «**Читать**»:
* Книга **автоматически добавится** в категорию «**читаю**» (если не добавлена).
* PDF-файл откроется в стандартном просмотрщике ОС (браузер, Adobe Reader и др.).
* **Позиция чтения сохраняется автоматически** — при повторном открытии файл промотается к последней странице.

**Примечание**: BiblioLand **не отслеживает номер страницы** — эту функцию выполняет сам просмотрщик.

#### **Управление закладками**

* На форме книги нажмите «**В закладки**» → выберите категорию:
* **Читаю** — активное чтение.
* **Буду читать** — планируемые книги.
* **Прочитано** — завершённые книги.
* **Брошено** — незавершённые книги.
* **Отложено** — книги на потом.
* Все закладки отображаются в разделе «**Закладки**» (в профиле).

#### **Отзывы и оценки**

* На форме книги:
* Выберите **оценку от** **1 до 10** (нажмите на звезду).
* Напишите **отзыв** (от 50 до 1000 символов).
* Нажмите «**Отправить**».
* **Лайки**:
* Кликните по иконке ❤ под отзывом другого пользователя.
* Лайк можно отменить повторным нажатием.

#### **Настройка профиля**

* В профиле нажмите «**Настройки**» → выберите вкладку:
* **Профиль**:
* Измените никнейм.
* Загрузите аватар (JPG/PNG до 5 МБ).
* Укажите описание (до 200 символов).
* **Смена пароля** — введите текущий и новый пароль.
* **Смена email** — укажите новый адрес.
* **Приватность**:
* Включите переключатель → закладки будут скрыты от других пользователей.
* Другие пользователи увидят только статистику и описание.

#### **Жалобы и обратная связь**

##### **Жалоба на книгу:**

* На форме книги нажмите «**Пожаловаться**».
* Выберите категорию: дубль, несоответствие жанра, другое.
* Напишите сообщение → отправьте.

##### **Обратная связь:**

* В меню профиля выберите «**Обратная связь**».
* Категории: мне нравится, мне не нравится, нашёл баг, есть предложение.

#### **Уведомления**

* Системные уведомления от администратора (например, «Технические работы») отображаются в разделе «Уведомления».
* Прочитанные уведомления можно удалить кнопкой 🗑️.

#### **Просмотр профилей других пользователей**

* Кликните на аватар или никнейм в отзыве → откроется профиль.
* Если у пользователя включена приватность — вы увидите только статистику и заглушку «Профиль приватный».

## Мероприятия по информационной безопасности

## 5.1 Определение угроз при эксплуатации приложения «GameEnergy»

Несмотря на то, что приложение BiblioLand является локальным десктопным решением и не использует веб-интерфейс, оно подвержено ряду потенциальных угроз информационной безопасности:

#### **SQL-инъекции**

Возможны при некорректной обработке пользовательского ввода (поиск по названию/автору, форма регистрации). Злоумышленник может попытаться внедрить вредоносные SQL-запросы для получения несанкционированного доступа к данным.

#### **Кража учётных данных**

При физическом доступе к файлу базы данных (\*.mdf) возможна попытка восстановления паролей пользователей или извлечение персональной информации (email, аватары в Base64).

#### **Неавторизованный доступ к профилям**

Если система не проверяет права доступа при просмотре профилей, пользователи могут получить доступ к закладкам других лиц, несмотря на включённую приватность.

#### **Загрузка вредоносных файлов**

Администратор может (намеренно или по ошибке) загрузить вредоносный файл под видом обложки книги (JPG/PNG) или PDF-документа, что теоретически может привести к RCE (Remote Code Execution) при открытии.

#### **Брутфорс-атака на форму входа**

Автоматизированный перебор паролей при многократных неудачных попытках авторизации.

#### **Утечка персональных данных**

Email, никнеймы, статистика (отзывы, лайки) хранятся в БД и могут быть извлечены при компрометации системы.

#### **Несанкционированное повышение привилегий**

Попытка назначить себе роль администратора или суперадминистратора через манипуляции с БД или интерфейсом.

## 5.2 Реализованные меры защиты

Для обеспечения безопасности пользовательских данных и стабильной работы приложения BiblioLand реализован комплекс мер защиты на уровне кода, базы данных и пользовательского интерфейса.

#### **Защита от SQL-инъекций**

Весь доступ к базе данных осуществляется через **Entity Framework Core**, который автоматически использует **параметризованные запросы**.

Пользовательский ввод (поиск по названию/автору, регистрация, авторизация) обрабатывается через LINQ-выражения, что исключает прямую конкатенацию строк и делает SQL-инъекции невозможными.

Пример:

var books = Program.context.Books.Where(b => b.Title.Contains(searchTerm));

#### **Безопасное хранение паролей и кодов восстановления**

* **Пароли** и **коды восстановления** хешируются с использованием библиотеки **BCrypt.Net-Next** — современного адаптивного алгоритма с автоматической «солью».
* Даже при компрометации базы данных **восстановить исходные значения вычислительно невозможно**.

Пример:

string hash = BCrypt.Net.BCrypt.HashPassword(password);  
bool isValid = BCrypt.Net.BCrypt.Verify(input, storedHash);

#### **Контроль доступа на уровне приложения**

* Все действия, требующие повышенных прав (удаление книги, бан пользователя, назначение администратора), **проверяют роль текущего пользователя**:

if (Program.CurrentUser.UserRoleID != 2 && Program.CurrentUser.UserRoleID != 3)  
{  
 MessageBox.Show("Доступ запрещён");  
 return;  
}

* **Ключи активации** и **личные данные** отображаются **только владельцу профиля**.
* При включённой **приватности профиля** закладки скрываются от других пользователей.

#### **Безопасная загрузка файлов**

* При добавлении книги администратор может загрузить **только разрешённые форматы**:
* **Обложка**: JPG, PNG (до 5 МБ)
* **PDF-файл книги**: только PDF (до 100 МБ)
* Файлы **не сохраняются на диск в исполняемом виде**, а копируются в защищённые системные папки (bookImg, bookPdf).
* **Аватары пользователей** хранятся в БД в формате **Base64**, что исключает выполнение вредоносного кода.

Пример валидации:

openFileDialog.Filter = "Image Files|\*.jpg;\*.jpeg;\*.png|PDF Files|\*.pdf"

#### **Защита от брутфорс-атак**

* После **5 неудачных попыток** **входа** пользователь **блокируется на 5 минут**.
* Блокировка реализована через **таймер в памяти** и проверку даты последней попытки.

#### **Минимизация утечки данных**

* Все данные — книги, пользователи, отзывы, закладки — хранятся **локально в MS SQL Server**.
* Приложение **не отправляет данные в сеть**, за исключением **восстановления пароля** (отправка кода на email).
* **PDF-файлы и обложки** хранятся **вне базы данных**, в изолированных папках, что снижает риск повреждения БД при компрометации файлов.

#### **Целостность данных**

* В БД настроены **внешние ключи (FK)** и **ограничения (UNIQUE, CHECK)**.
* **Каскадное удаление** автоматически удаляет связанные данные (отзывы, оценки, жалобы) при удалении книги или пользователя.
* **Триггеры** автоматически обновляют средний рейтинг книги при изменении оценок:

CREATE TRIGGER trg\_UpdateAverageRatingAfterInsert ON Rating ...

#### **Защита восстановления пароля**

* Код восстановления **одноразовый**, **хешируется** и имеет **срок действия** **5 минут**.
* Код отправляется **только на email**, указанный при регистрации.
* Даже при перехвате **хеша кода** злоумышленник не сможет его использовать.

## 5.3 Рекомендации пользователям по безопасной работе

Для обеспечения максимальной безопасности при использовании приложения BiblioLand рекомендуется соблюдать следующие правила:

#### **Общие рекомендации для всех пользователей**

* **Используйте надёжный пароль**
* Пароль должен содержать **не менее 8 символов**, включать **заглавные и строчные буквы**, **цифры и** **специальные символы**.
* Не используйте один и тот же пароль для нескольких приложений.
* **Регулярно обновляйте пароль**

Особенно если компьютер используется в общем доступе (библиотека, учебное заведение).

* **Не передавайте файл базы данных третьим лицам**

Файл базы данных (\*.mdf) **содержит персональные данные** (email, аватары в Base64) и **не должен передаваться** без необходимости.

* **Включайте приватность профиля**

Если вы не хотите, чтобы другие пользователи видели ваши закладки, активируйте переключатель «**Приватность**» в настройках профиля.

#### **Рекомендации для администраторов и суперадминистраторов**

* **Назначайте администраторов ответственно**

Роль администратора даёт доступ к управлению книгами, пользователями и жалобами. Назначайте её только **доверенным лицам**.

* **Баньте нарушителей с указанием срока**

При модерации используйте **временные баны** (а не бессрочные), чтобы дать пользователям возможность исправиться.

* **Не оставляйте учётную запись администратора без пароля**

Убедитесь, что пароль администратора соответствует требованиям надёжности.

* **Ограничьте физический доступ к компьютеру с БД**

Поскольку приложение локальное, основная угроза — **прямой доступ к файлу базы данных**. Храните его в защищённой папке.

* **Выполняйте резервное копирование**

Регулярно создавайте резервные копии базы данных через **SQL Server Management Studio**, чтобы избежать потери данных при сбое.

#### **В случае компрометации аккаунта**

* **Немедленно смените пароль**

Используйте функцию «**Восстановить пароль**», если у вас есть доступ к email.

* **Обратитесь к администратору**

Если email утерян, **администратор** может сбросить пароль вручную через базу данных (требуется физический доступ к серверу).

* **Проверьте свои закладки и отзывы**

После восстановления доступа убедитесь, что ваши данные не были изменены.

#### **Безопасность при работе с PDF-файлами**

* Приложение **не проверяет содержимое PDF-файлов.**
* Убедитесь, что загружаемые книги поступают из **надёжных источников**, чтобы избежать открытия вредоносных документов.

## Заключение

В ходе выполнения дипломного проекта было успешно разработано локальное десктопное приложение «BiblioLand», предназначенное для удобного, безопасного и многофункционального управления электронной библиотекой без зависимости от онлайн-сервисов. Приложение полностью соответствует поставленной цели — демонстрации навыков проектирования и реализации сложного программного продукта на платформе C# WinForms в рамках подготовки к демонстрационному экзамену.

#### **Основные задачи проекта выполнены в полном объёме:**

* Реализован **расширенный каталог книг** с возможностями поиска по названию/автору, фильтрации по жанру и сортировки по новизне, популярности, количеству оценок и среднему рейтингу.
* Обеспечена **трёхуровневая система ролей**: обычный пользователь, администратор и суперадминистратор, что позволяет гибко адаптировать приложение под различные сценарии использования — от личного до корпоративного.
* Разработаны ключевые модули:
* **Закладки** с пятью категориями (читаю, буду читать, прочитано, брошено, отложено),
* **Отзывы и оценки** по 10-балльной шкале,
* **Модерация** через систему жалоб и банов с указанием срока,
* **Обратная связь** по категориям (мне нравится, мне не нравится, баг, идея).
* Реализована система **уведомлений** для информирования пользователей о технических работах или важных событиях.
* Пользователи могут **настраивать приватность профиля**, скрывая свои закладки от других.
* Обеспечена **безопасная регистрация**, **авторизация и восстановление пароля** с использованием хеширования **BCrypt.Net-Next**.
* Все данные — профили, книги, отзывы, уведомления — хранятся локально в **MS SQL Server**, а PDF-файлы и обложки — в защищённых системных папках, что гарантирует полную **автономность и защиту от внешних угроз**.
* Архитектура приложения построена на принципах **MVC** и **паттерна Repository**, что обеспечивает читаемость, расширяемость и сопровождаемость кода.
* Интерфейс реализован с использованием современных UI-библиотек **Guna UI2**, **MaterialSkin** и **SixLabors.ImageSharp**, обеспечивающих **единый**, **визуально привлекательный и интуитивно понятный пользовательский опыт**, включая динамический размытый фон на основе обложек книг.

Приложение **работает полностью офлайн**: основной функционал — поиск, чтение, управление закладками, отзывы — доступен без подключения к интернету. Единственное исключение — восстановление пароля, требующее отправки кода на email, что не критично для повседневного использования.

Проведённое **ручное функциональное тестирование** подтвердило корректную работу всех 28 форм и 13 кастомных контролов. Выявленные ошибки (дублирование закладок, некорректное отображение профилей) были своевременно устранены.

**Практическая значимость** проекта заключается в демонстрации возможности создания **полноценной**, **защищённой и гибкой библиотечной платформы** без использования веб-технологий. BiblioLand может быть успешно развёрнут:

* в **образовательных учреждениях** — как цифровая библиотека учебной литературы,
* в **библиотеках** — для удалённого доступа к фондам,
* в **корпоративной среде** — для внутреннего документооборота,
* в **личном пользовании** — как удобный менеджер PDF-книг с закладками и статистикой.

#### **Перспективы дальнейшего развития:**

* Добавление **оффлайн-режима восстановления пароля** (через секретные вопросы).
* Реализация **статистики чтения** (количество прочитанных книг, страниц в день).
* Поддержка **мультиязычного интерфейса** (русский/английский).
* Внедрение **резервного копирования и восстановления** библиотеки в один клик.
* Экспорт/импорт каталога книг в формате **JSON** для переноса между устройствами.

Таким образом, **BiblioLand** представляет собой **завершённое, функционально насыщенное и технически грамотно реализованное решение**, выходящее далеко за рамки простой «читалки». Оно демонстрирует высокий уровень владения стеком **C# + WinForms + Entity Framework + MS SQL**, а также понимание принципов проектирования, безопасности и пользовательского опыта.

## Список источников

#### **Нормативная документация**

1. ГОСТ 34.602–2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. [Электронный ресурс] - <https://protect.gost.ru/document1.aspx?control=31&id=241754>
2. ГОСТ 19.106–78. Единая система программной документации. Требования к программным документам, выполненным печатным способом. [Электронный ресурс] - <https://protect.gost.ru/document1.aspx?control=31&id=241756>
3. ГОСТ Р 2.105–2019. Единая система конструкторской документации. Общие требования к текстовым документам. [Электронный ресурс] - <https://protect.gost.ru/document1.aspx?control=31&id=217667>

#### **Официальная документация и технические ресурсы**

1. Microsoft. .NET Documentation [Электронный ресурс]. — Режим доступа: <https://learn.microsoft.com/ru-ru/dotnet/>, свободный. — (дата обращения: 05.07.2025).
2. Microsoft. Entity Framework Core Documentation [Электронный ресурс]. — Режим доступа: <https://learn.microsoft.com/ru-ru/ef/core/>, свободный. — (дата обращения: 03.08.2025).
3. Microsoft. Windows Forms Documentation [Электронный ресурс]. — Режим доступа: <https://learn.microsoft.com/ru-ru/dotnet/desktop/winforms/>, свободный. — (дата обращения: 09.28.2025).
4. Microsoft. SQL Server Documentation [Электронный ресурс]. — Режим доступа: <https://learn.microsoft.com/ru-ru/sql/>, свободный. — (дата обращения: 24.07.2025).

#### **Библиотеки и инструменты**

1. Guna UI2 Framework. Official GitHub Repository [Электронный ресурс]. — Режим доступа: <https://github.com/sunnyvalley/Guna.UI2>, свободный. — (дата обращения: 15.07.2025).
2. MaterialSkin for .NET. Official GitHub Repository [Электронный ресурс]. — Режим доступа: <https://github.com/IgnaceMaes/MaterialSkin>, свободный. — (дата обращения: 12.10.2025).
3. BCrypt.Net-Next. NuGet Package Documentation [Электронный ресурс]. — Режим доступа: <https://www.nuget.org/packages/BCrypt.Net-Next>, свободный. — (дата обращения: 19.09.2025).
4. SixLabors.ImageSharp .NET. Official GitHub Repository [Электронный ресурс]. — Режим доступа: <https://github.com/SixLabors/ImageSharp>, свободный. — (дата обращения: 03.11.2025).

#### **Учебные и научные издания**

1. Троелсен Э., Джепикс Ф. Язык программирования C# 10 и платформа .NET 6. — 9-е изд. — СПб.: Питер, 2022. — 1296 с.
2. Либерти Дж., Харди Д. Освой самостоятельно C# за 21 день. — М.: Вильямс, 2021. — 672 с.
3. Макконнелл С. Совершенный код. — 2-е изд. — М.: Русская редакция, 2020. — 950 с.
4. Фаулер М. Рефакторинг. Улучшение существующего кода. — М.: Вильямс, 2021. — 432 с.
5. Васюков В.Т., Симбирцев А.В. Информационная безопасность: учебник для вузов. — 2-е изд., испр. и доп. — М.: Юрайт, 2023. — 379 с.

#### **Интернет-ресурсы**

1. OWASP Foundation. Top 10 Web Application Security Risks [Электронный ресурс]. — Режим доступа: <https://owasp.org/www-project-top-ten/>, свободный. — (дата обращения: 06.09.2025).
2. YouTube Data API — Embedding Videos [Электронный ресурс]. — Режим доступа: <https://developers.google.com/youtube/player_parameters>, свободный. — (дата обращения: 29.10.2025).

## Приложение А

### Метод авторизации пользователя:

public static bool ValidationRegistration(MaterialSingleLineTextField LoginField, MaterialSingleLineTextField MailField, MaterialSingleLineTextField PasswordField, MaterialSingleLineTextField ConfirmPasswordField)

{

string originalUsername = LoginField.Text;

string newUsername = originalUsername?.Replace(" ", "");

string originalMail = MailField.Text;

string newMail = originalMail?.Replace(" ", "");

string originalPassword = PasswordField.Text;

string newPassword = originalPassword?.Replace(" ", "");

bool hadSpaces = originalUsername.Contains(" ") || originalMail.Contains(" ") || originalPassword.Contains(" ");

if (\_onlyEnglishChars.IsMatch(newUsername))

{

if (!IsUsernameOrMailTaken(newUsername, newMail))

{

string passwordHash = HashHelper.HashData(newPassword);

string base64Avatar = CodingOrDecoding.ImageCoding(null);

Users newUser = new Users

{

Username = newUsername,

Email = newMail,

PasswordHash = passwordHash,

UserRoleID = 1,

RegistrationDate = DateTime.Now,

Avatar = base64Avatar

};

LoginField.Clear();

MailField.Clear();

PasswordField.Clear();

ConfirmPasswordField.Clear();

Program.context.Users.Add(newUser);

Program.context.SaveChanges();

string registrationMessage = hadSpaces

? "Пробелы в полях были удалены.\n\nПриветствуем в наших рядах читателей!"

: "Приветствуем в наших рядах читателей!";

ShowInformationMessage(registrationMessage, "Регистрация прошла успешно");

return true;

}

ShowErrorMessage("Имя пользователя или почта уже существуют.");

return false;

}

ShowErrorMessage("Имя пользователя должно содержать только английские буквы, символы или цифры.");

return false;

}

### Метод для валидации пароля:

public static bool ValidatePasswords(string password, string confirmPassword)

{

if (!\_onlyEnglishChars.IsMatch(password))

{

ShowErrorMessage("Пароль должен содержать только английские буквы.");

return false;

}

if (password.Contains(" "))

{

ShowErrorMessage("Пароль не должен содержать пробелов.");

return false;

}

if (!\_hasUpperChar.IsMatch(password))

{

ShowErrorMessage("Пароль должен содержать хотя бы одну заглавную букву.");

return false;

}

if (!\_hasLowerChar.IsMatch(password))

{

ShowErrorMessage("Пароль должен содержать хотя бы одну строчную букву.");

return false;

}

if (!\_hasDigit.IsMatch(password))

{

ShowErrorMessage("Пароль должен содержать хотя бы одну цифру.");

return false;

}

if (!\_hasSpecialChar.IsMatch(password))

{

ShowErrorMessage("Пароль должен содержать хотя бы один специальный символ.");

return false;

}

if (password.Length < 8)

{

ShowErrorMessage("Пароль должен содержать минимум 8 символов.");

return false;

}

if (password.Length > 32)

{

ShowErrorMessage("Пароль не должен превышать 32 символа.");

return false;

}

if (password != confirmPassword)

{

ShowErrorMessage("Пароли не совпадают.");

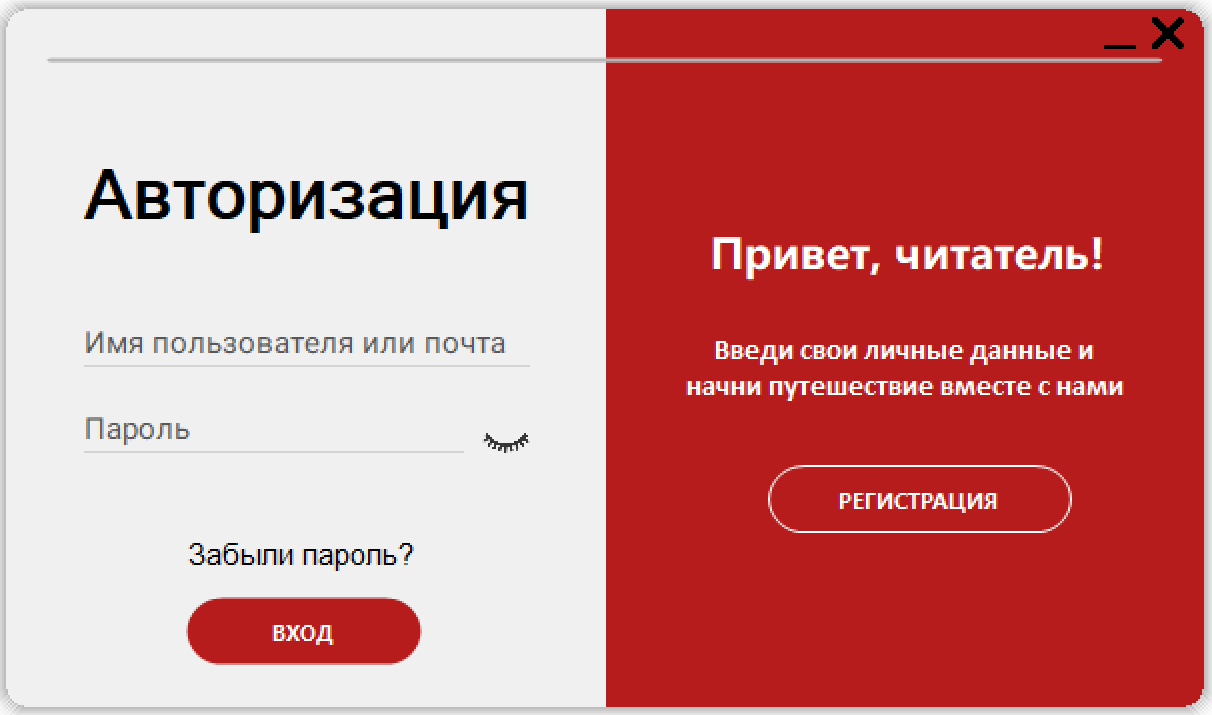
return false;

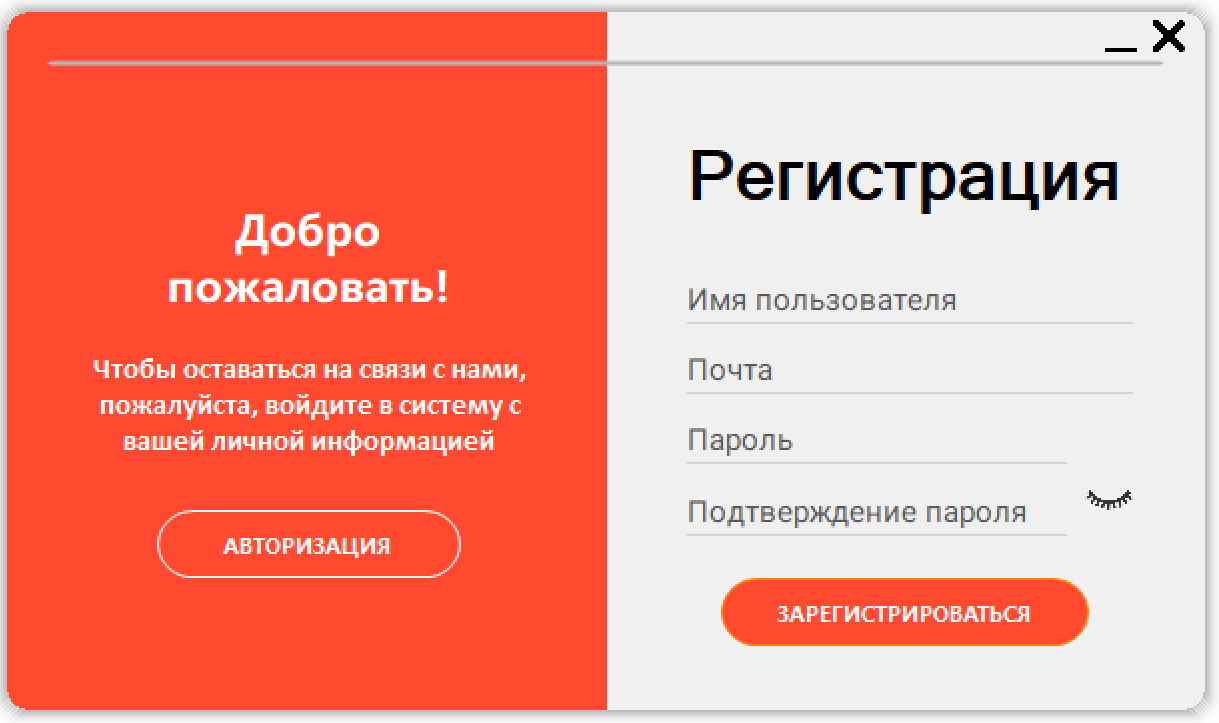
}

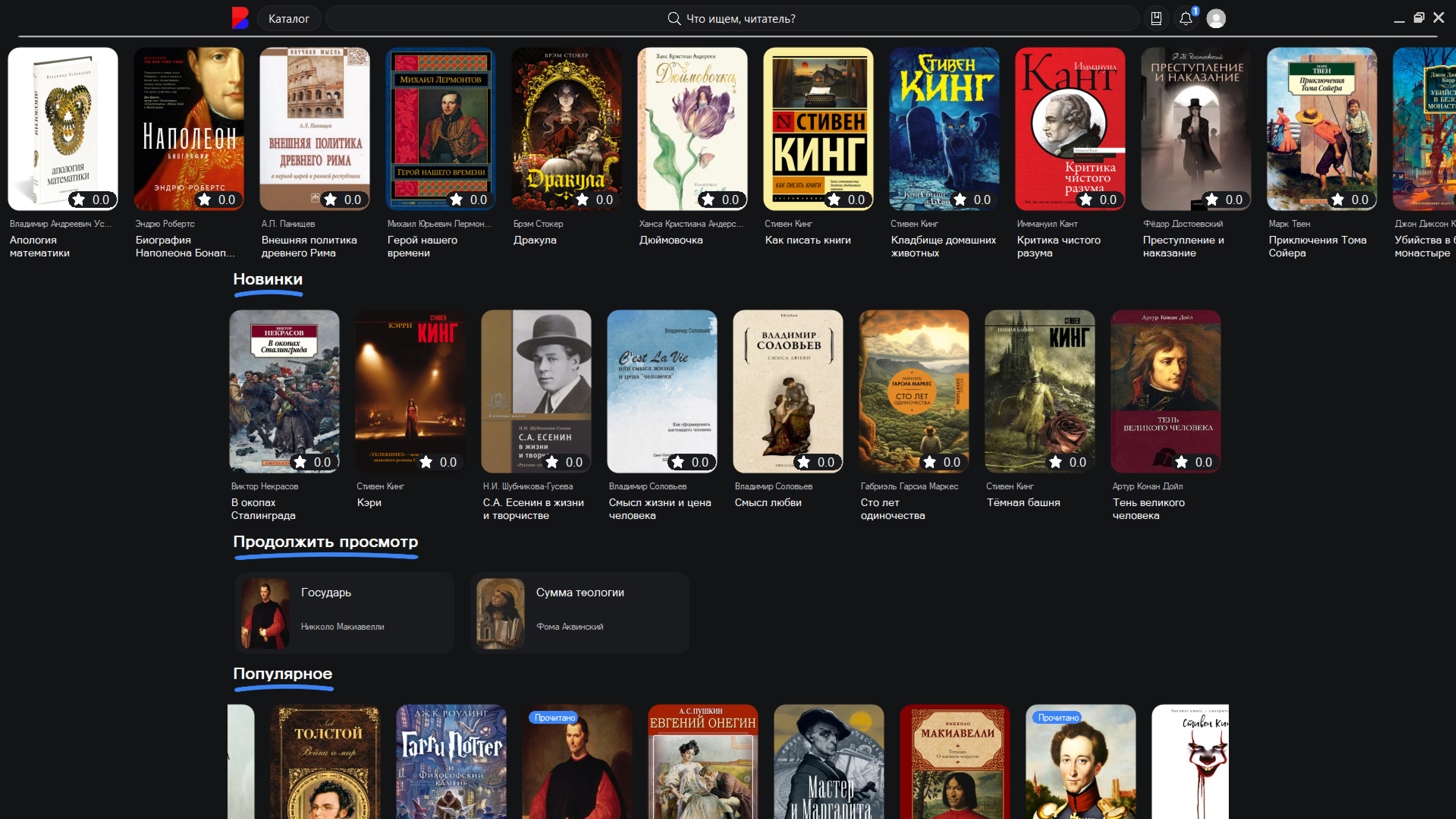
return true;

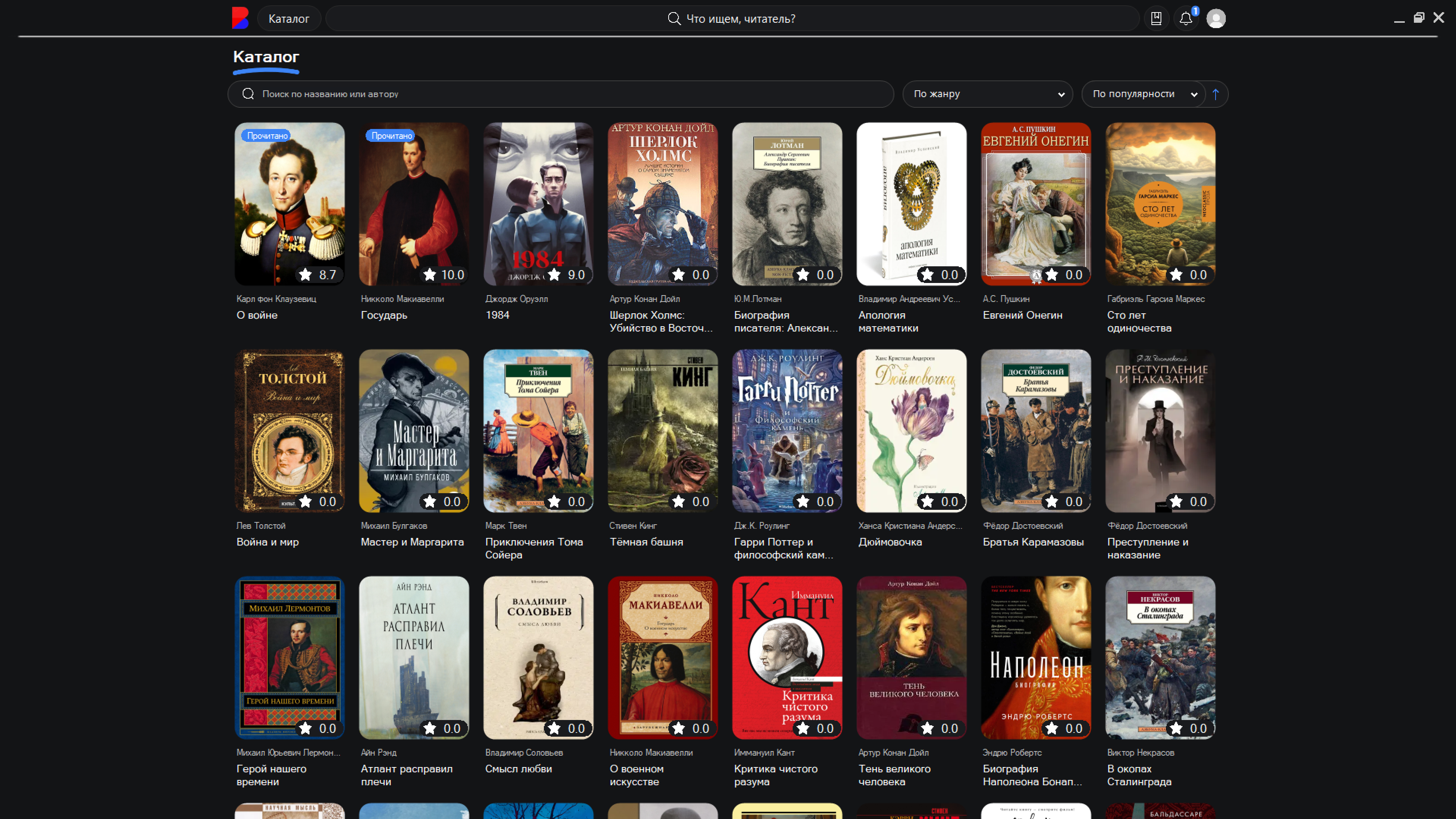
}

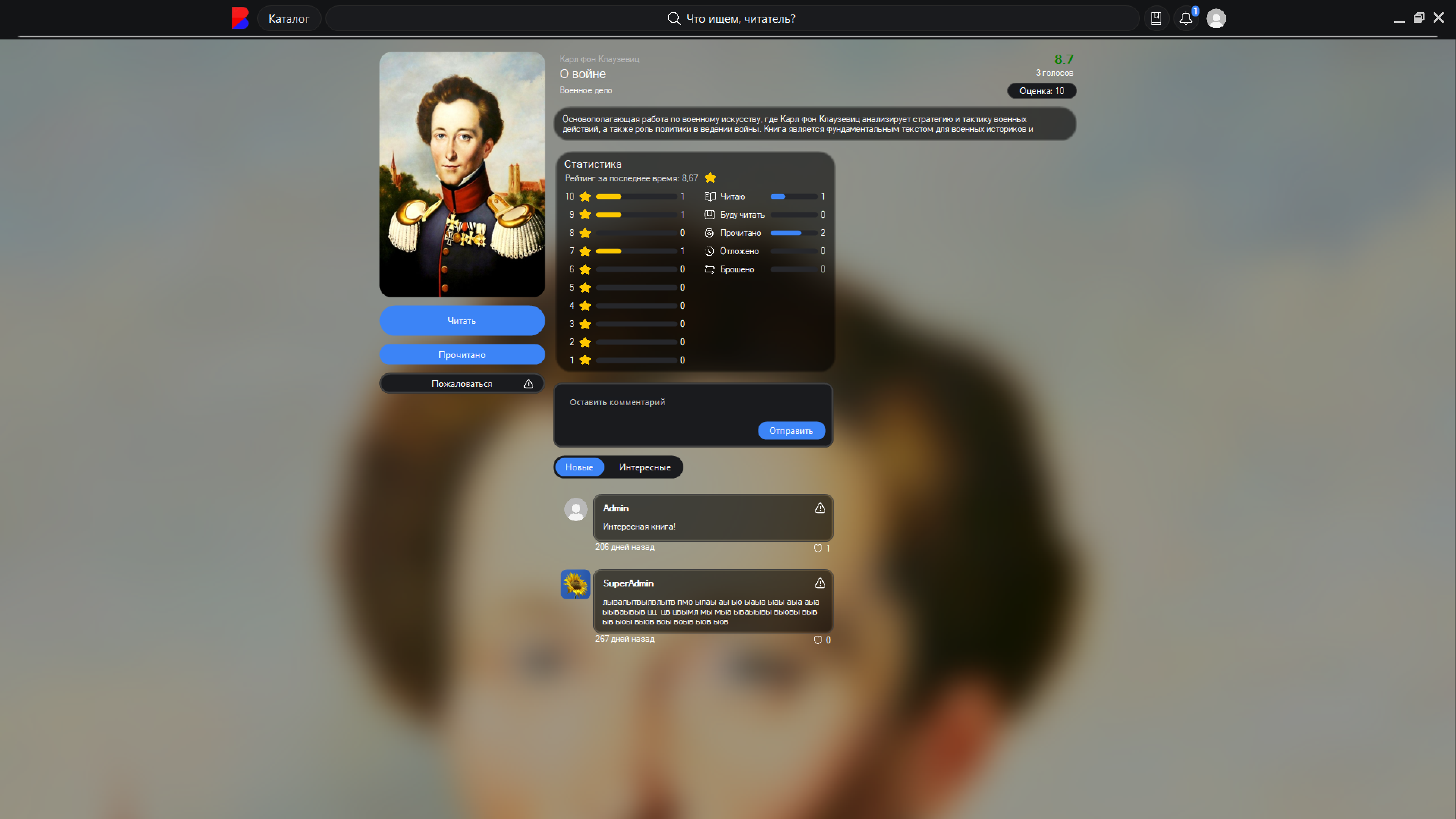
## Приложение Б

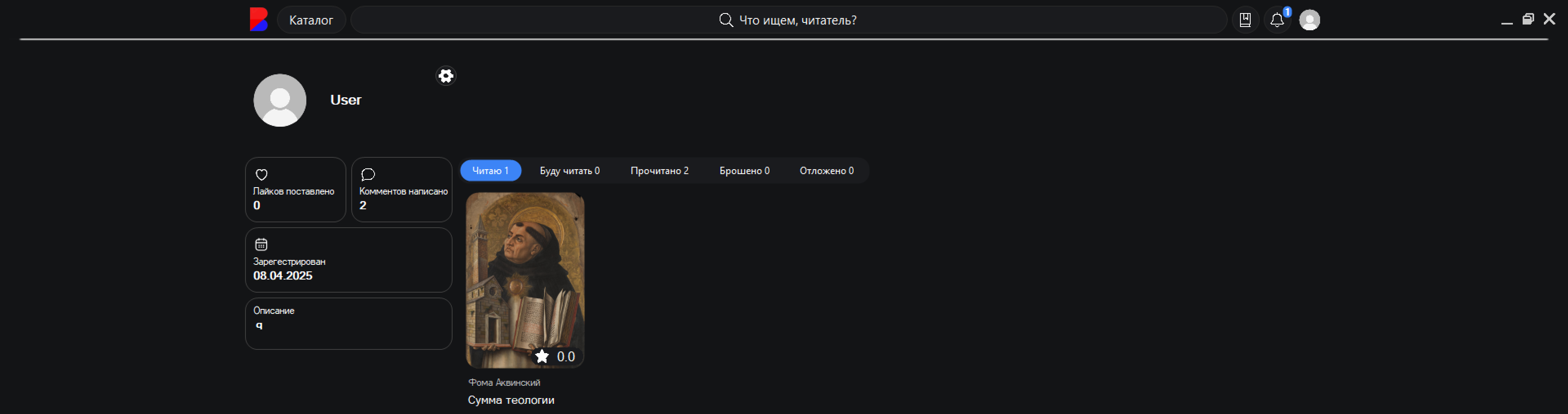
*Рисунок 5 – Авторизация*

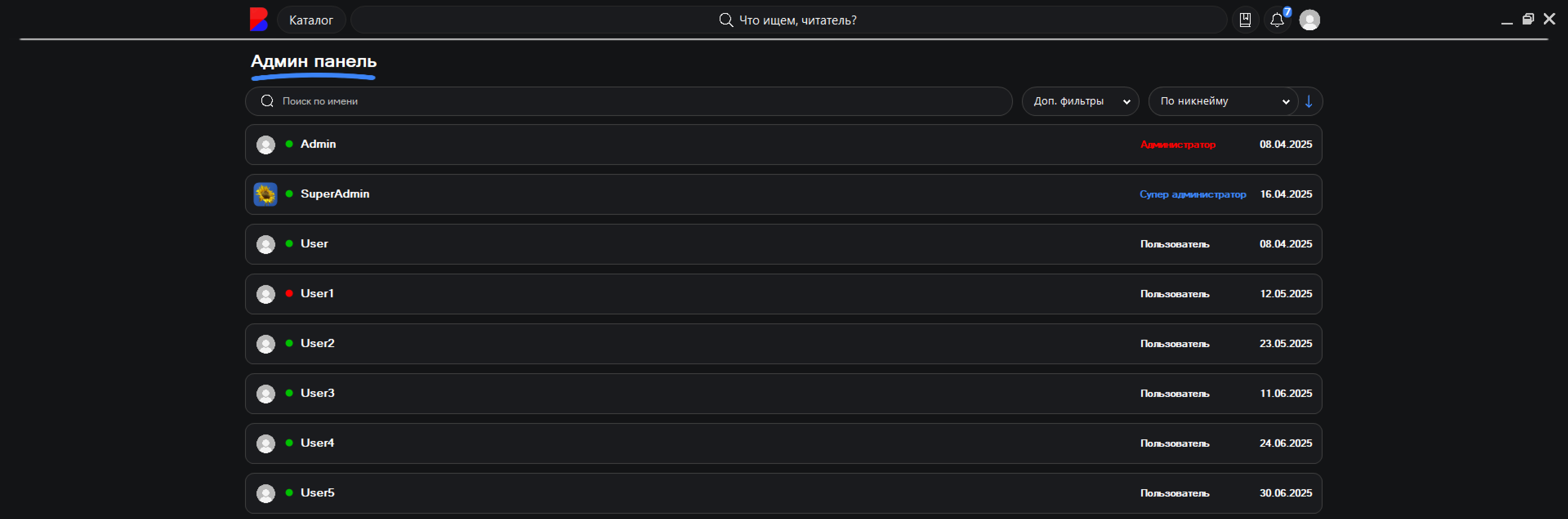
*Рисунок 6 – Регистрация*

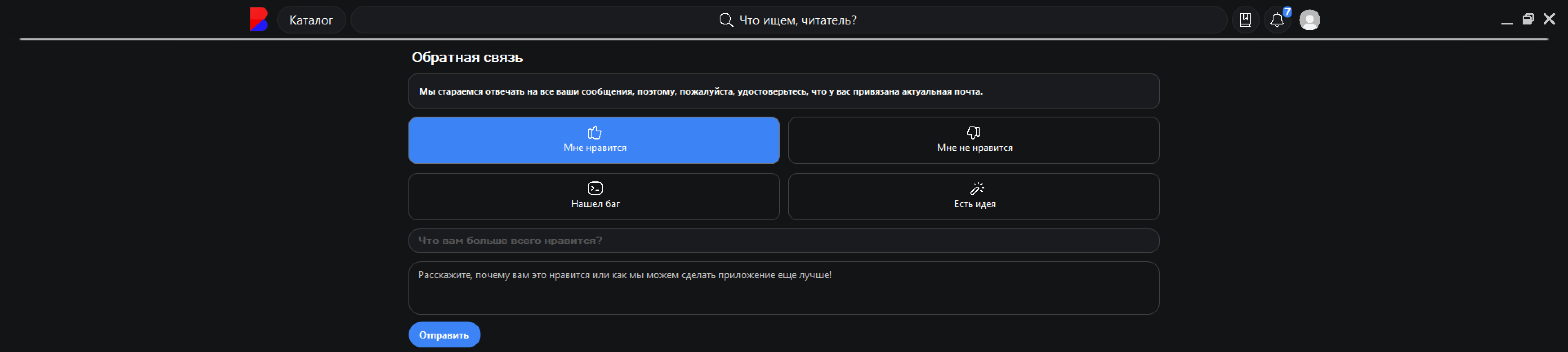
*Рисунок 7 – Главная форма*

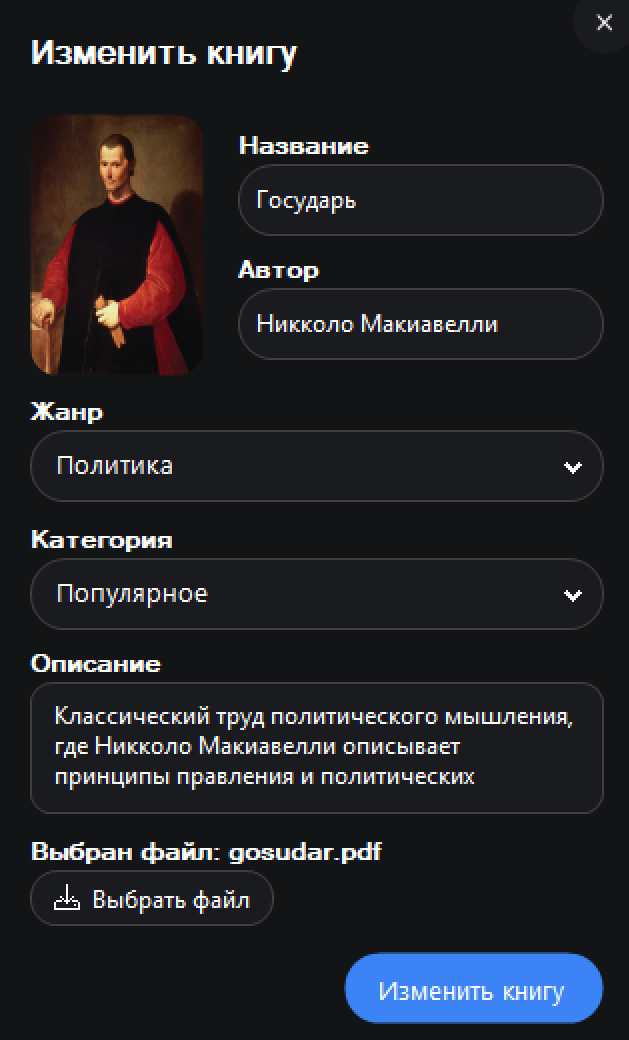
*Рисунок 8 – Каталог*

*Рисунок 9– Форма книги*

*Рисунок 10– Профиль пользователя*

*Рисунок 11– Админ панель*

*Рисунок 12– Обратная связь*



*Рисунок 13– Изменение книги*