Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Новосибирский государственный технический университет»

**ПРАКТИЧЕСКАЯ РАБОТА**

по дисциплине «Основы информационной безопасности»

|  |  |
| --- | --- |
| Выполнили:  Патласов Д.А  Баталов М.В  Сурик А.В  Группа АВТ-214  Факультет АВТФ.  «18» декабря 2023 г. | Проверил:  Плеханов В.А.  (Ф. И. О.)  Балл: \_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

Новосибирск 2023

* **Введение**

В эпоху цифровизации и виртуализации мировой экономики информационная безопасность становится неотъемлемой составляющей любой успешной деятельности. Научиться эффективно обеспечивать защиту информации – значит обрести контроль и надежность в мире полный угроз. В нашем проекте мы глубоко исследуем основы информационной безопасности и предлагаем практические рекомендации для ее реализации.

Обеспечение информационной безопасности является процессом, гарантирующим конфиденциальность, целостность и доступность информации, а также связанных с ней процессов и ресурсов. Этот процесс крайне важен, поскольку информационные системы играют ключевую роль в различных сферах деятельности, включая экономику, политику, социальные и культурные аспекты. Нарушение информационной безопасности может привести к серьезным последствиям, включая финансовые убытки, нарушение работы организаций, потерю доверия к системе и даже угрозу национальной безопасности.

Модели информационной безопасности представляют различные методы обеспечения защиты информации. Они помогают определить основные принципы и направления реализации политики безопасности, а также выбрать наиболее эффективные методы и средства защиты. Реферат будет посвящён основным моделям информационной безопасности, их особенностям и преимуществам.

В данной работе будут рассмотрены следующие вопросы:

1. Понятие политики безопасности. Цель создания политики безопасности. Субъектно-объектные модели разграничения доступа. Субъект доступа. Объект доступа. Поток информации. Аксиомы политики безопасности. Монитор безопасности. Требования по сертификации защищенных систем к реализации монитора безопасности.
2. Политика и модели тематического разграничения доступа (вариант e)

* **Подлежащая защите информация**

Наша команда выбрала для защиты договор о купле-продаже автомобиля и паспорт продавца автомобиля и база данных электронных почт.

* **Цель и инструменты разработки**

Цель заключается в том, чтобы применить на практике полученные навыки изучения основ информационной безопасности на примере разработки приложения, которое реализует модель информационной безопасности.

Инструменты разработки – нами был выбран язык программирования С#, в том числе библиотеки и платформа для программирования графического интерфейса – Avalonia (графический пользовательский интерфейс), Json.NET (Библиотека для записи данных пользователей)

* **Архитектура приложения**

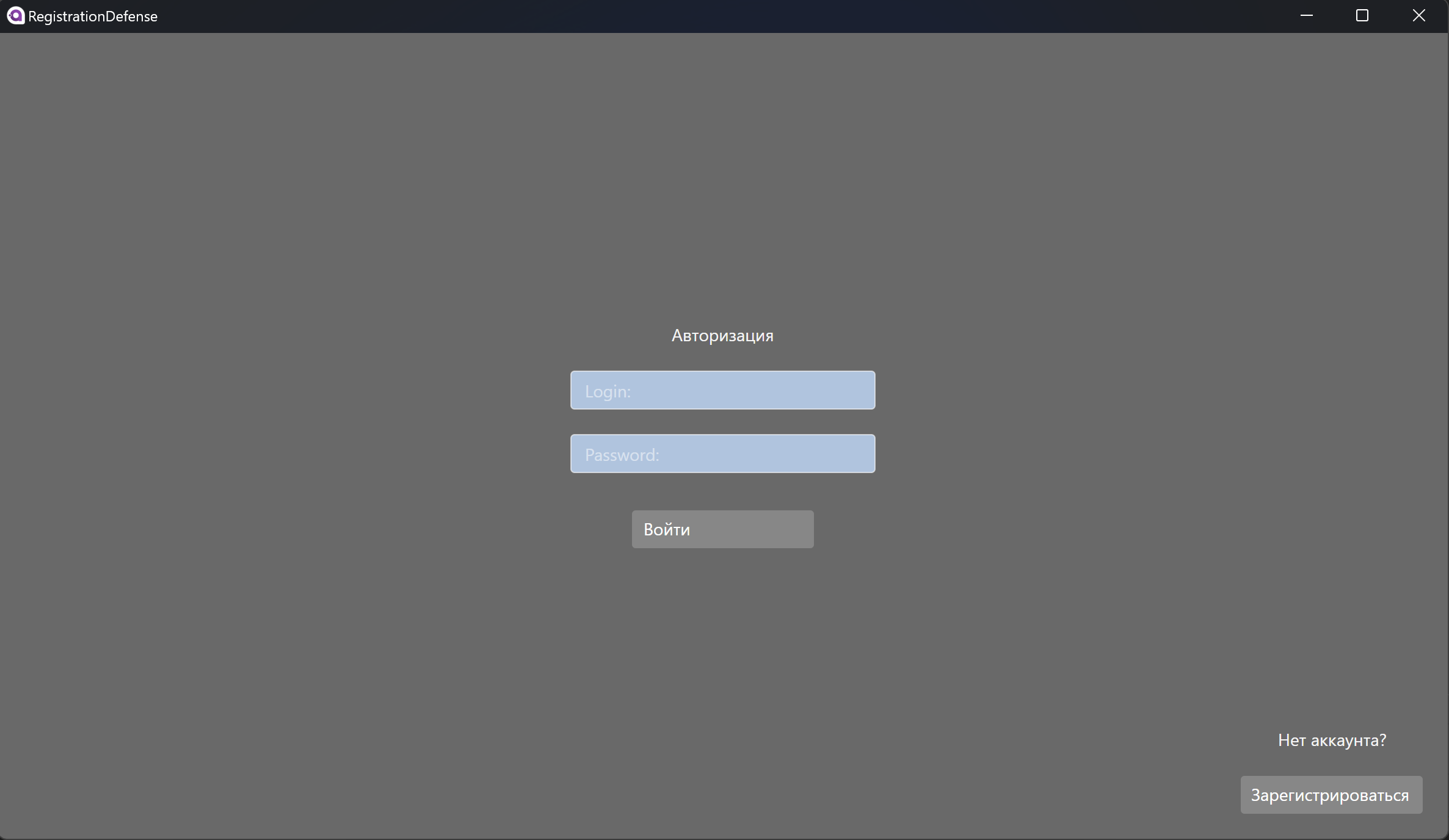
Пользователь запускает программу и открывается первое окно, где требуется пройти процесс авторизации в системе через ввод логина и пароля. Так же можно пройти регистрацию, если нажать на соответствующую кнопку в правом нижнем углу. Программа проверяет наличие логина в списке существующих, затем сверяет введённый пользователем пароль с соответствующим логину. При успешной авторизации перед пользователем открывается текстовое поле, где выводится содержимое доступного ему файла. В случае неудачной авторизации пользователь получает отказ в доступе.

* **Технология регистрации пользователей**

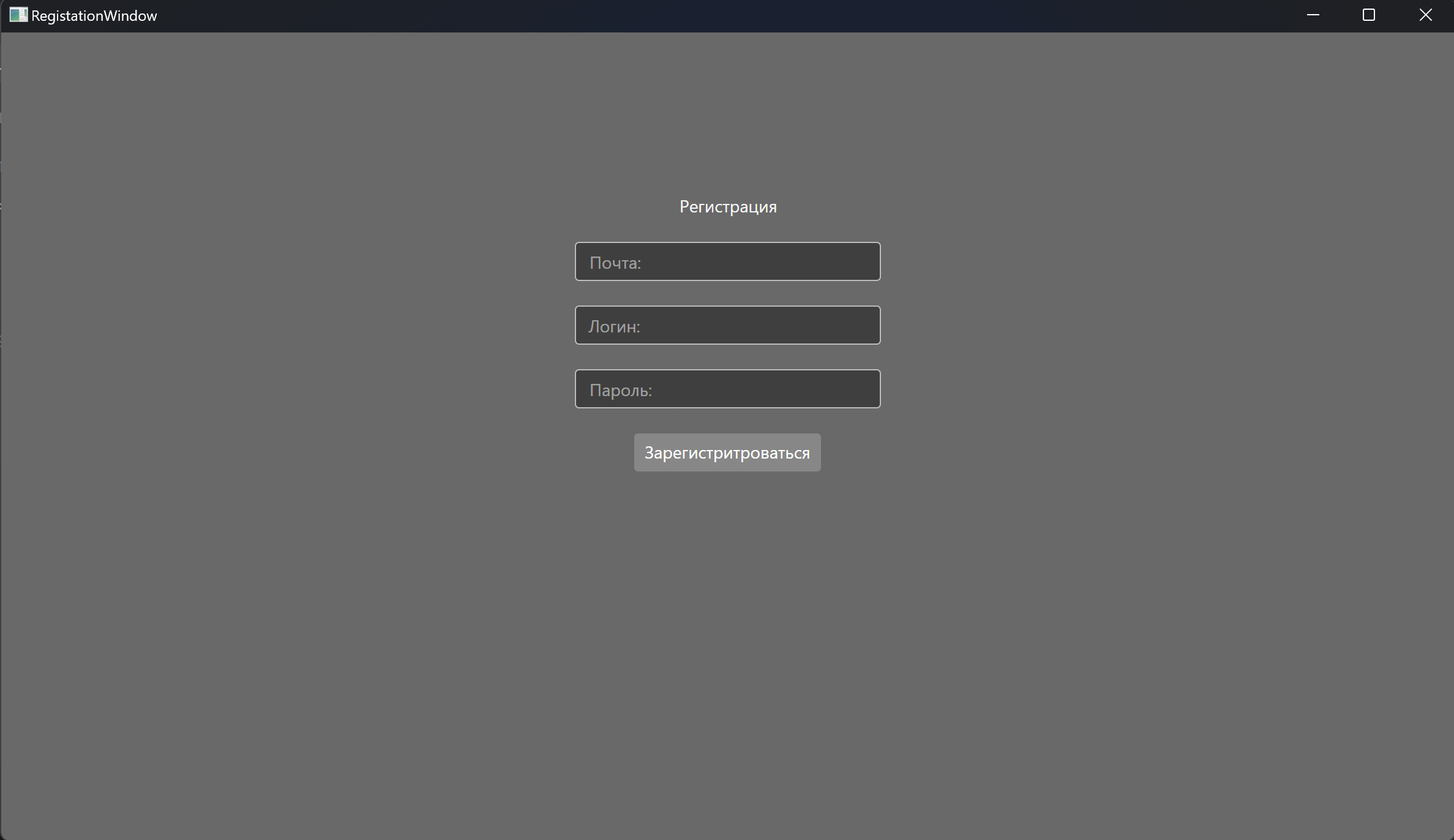
Каждый пользователь имеет логин и пароль. При вводе этих данных в окне аутентификации происходит проверка наличия логина в системе и соответствия введенного пароля указанному логину. Для этого используется структура данных, называемая "словарем", где информация хранится в виде пар ключ-значение. Если в словаре существует указанный пользователем логин и введенный пароль совпадает с паролем, связанным с этим логином в словаре, пользователь получает доступ к файлам.

* **Экранные формы**

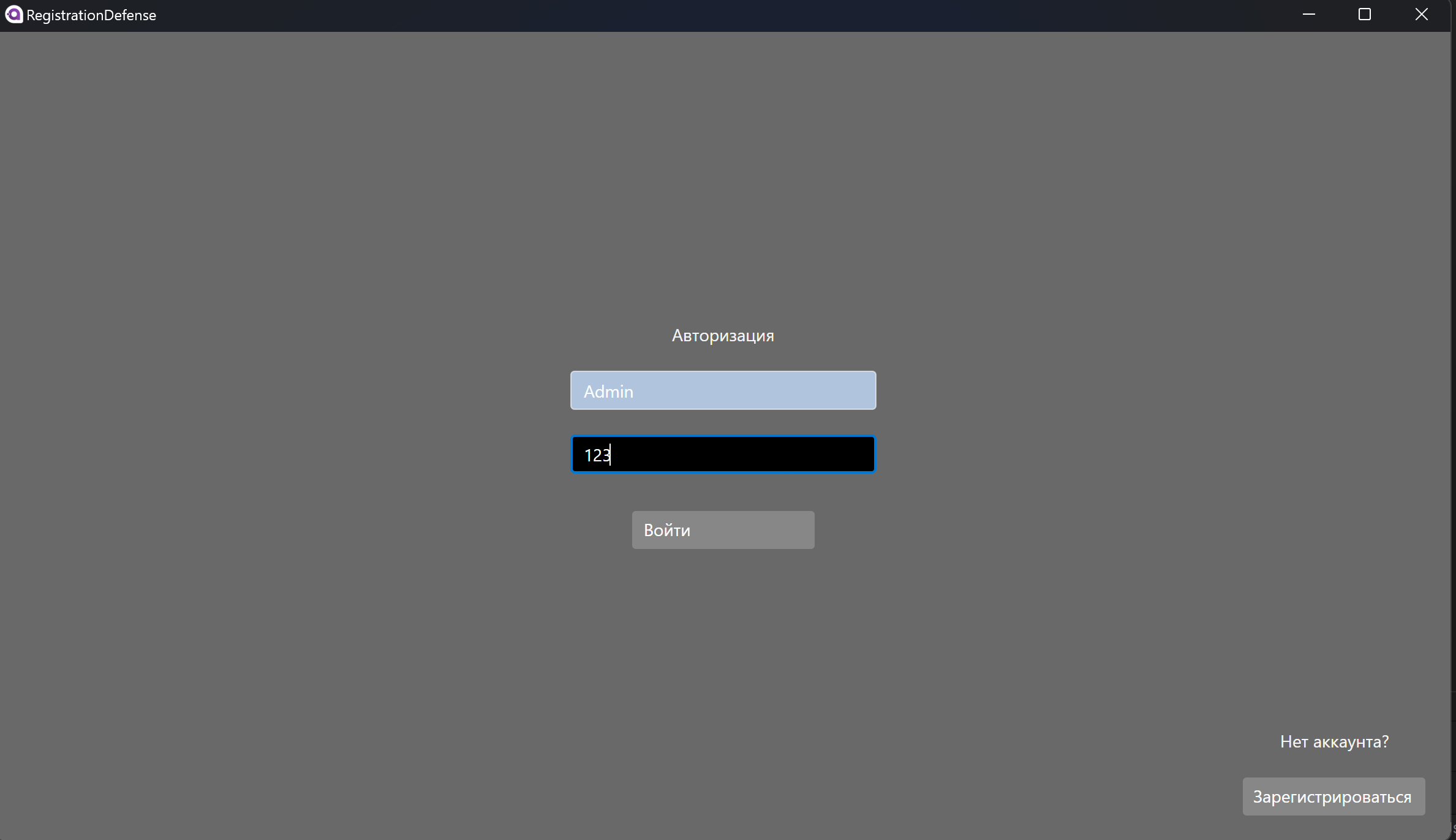
**Окно авторизации:**



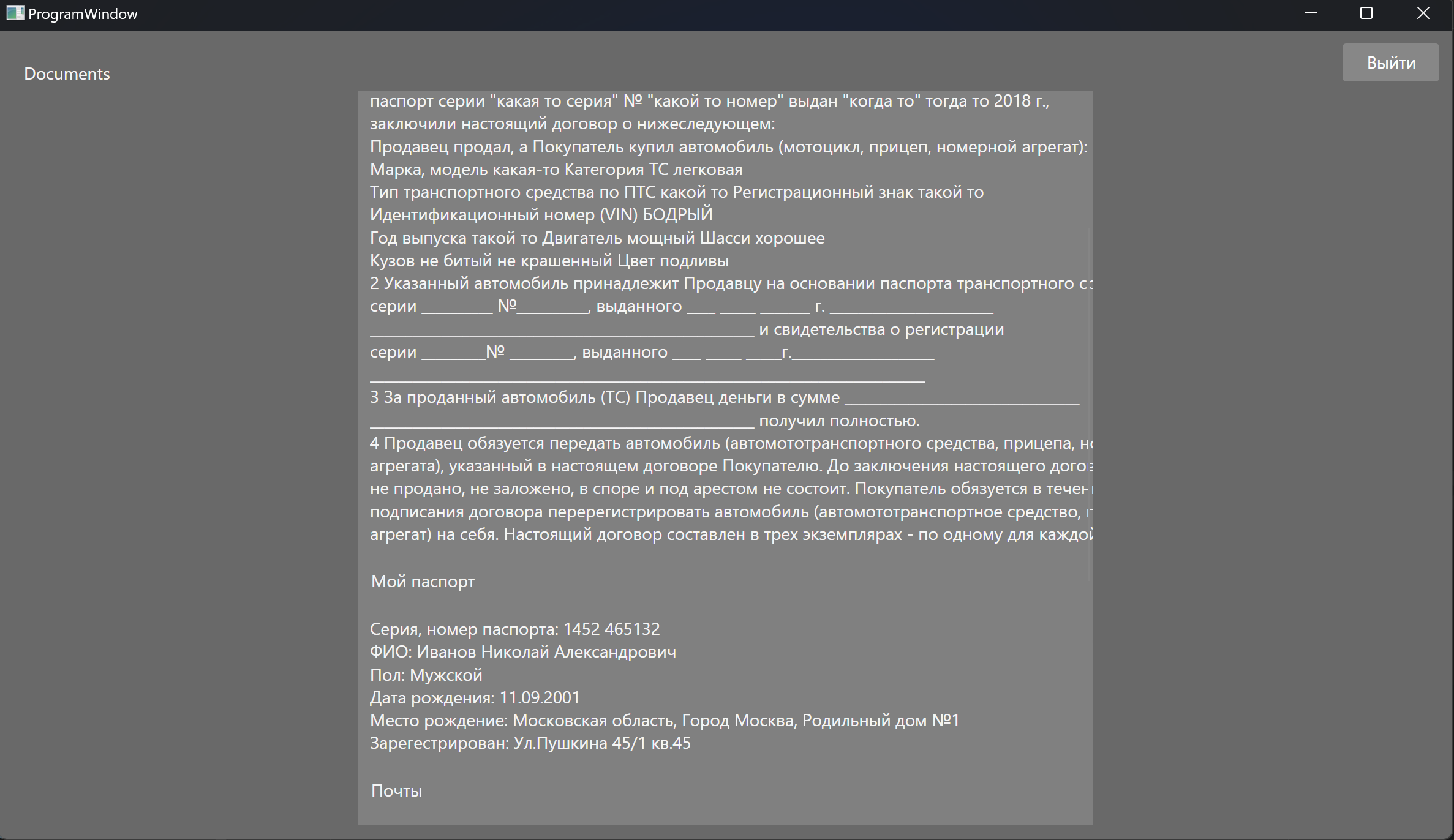
**Окно регистрации:**



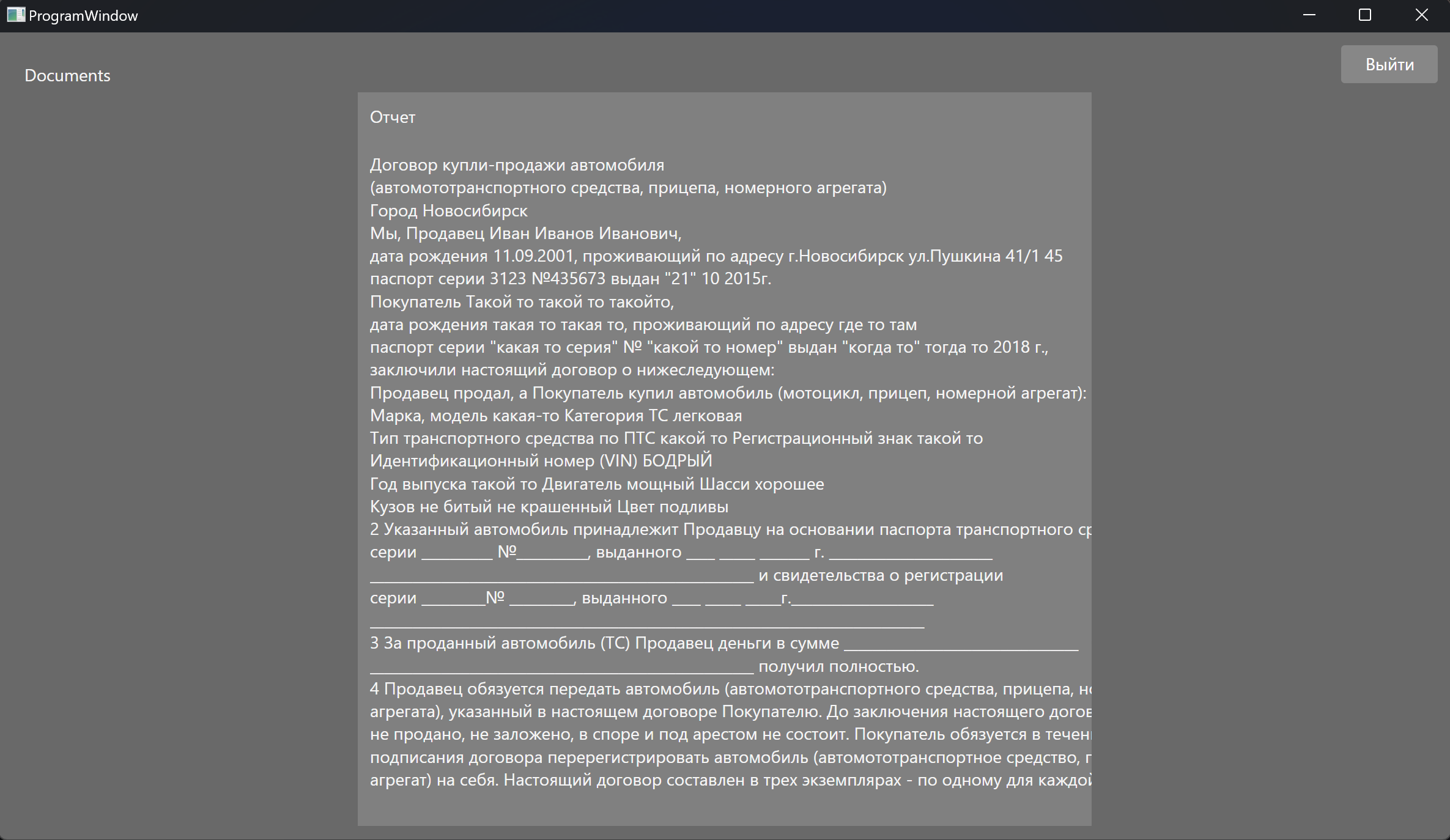
**Авторизация админа:**



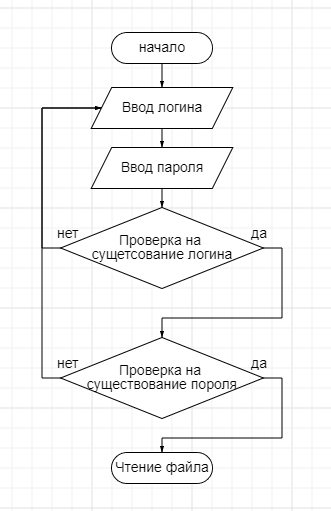
**Окно админа:**



**Окно пользователя:**



* **Блок-схемы**



**Заключение**

В заключение, следует отметить, что информационная безопасность является одним из важнейших аспектов работы любой организации. Политика информационной безопасности должна быть разработана в соответствии с требованиями законодательства, стандартов и лучших практик в области безопасности. Модели разграничения доступа, такие как субъектно-объектная и тематическая, позволяют гибко настраивать права доступа к информации и обеспечивать ее защиту от несанкционированного доступа. Важно также обеспечивать физическую безопасность информационных систем, проводить регулярное обучение и повышение осведомленности сотрудников о правилах работы с информацией и мерах безопасности. Мы провели интересную работу по применению на практике полученных знаний за семестр. Наш продукт функционировал так, как предполагалось, демонстрируя эффективное тематическое разграничение доступа к защищаемой информации.

**Список использованных ресурсов**

1. [Основы информационной безопасности — DiSpace (nstu.ru)](https://dispace.edu.nstu.ru/didesk/course/show/12142)
2. [Avalonia Tutorial: Реализация MVVM по шагам с примерами (habr.com)](https://habr.com/ru/articles/505036/)
3. [6.2. Классификация моделей безопасности (studfile.net)](https://studfile.net/preview/2880351/page:12/)