МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Казанский национальный исследовательский технический университет

им. А.Н. Туполева – КАИ»

Институт компьютерных технологий и защиты информации

Отделение СПО ИКТЗИ (Колледж информационных технологий)

ЛАБОРАТОРНАЯ РАБОТА № 3

по дисциплине

Информационная безопасность

Тема: «Реализация доступа пользователей к базе данных»

Работу выполнили

Студент гр.4232

Зарипов А.Р.

Михайлова П.И.

Принял

Преподаватель Кожевников К.Д.

Казань 2024

**Цель работы**

Научиться реализовывать доступ пользователей к базе данных.

**Задание на лабораторную работу**

* изучить теоретическую часть;
* выполнить практические указания;
* составить отчет по лабораторной работе.

**Ход работы:**

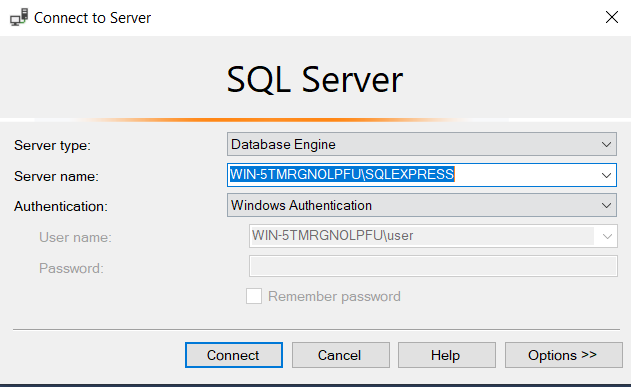
С помощью SQL Server Management Studio подключаемся к используемому экземпляру SQL Server. Проверим установленный на сервере режим аутентификации.

Рисунок 1 - соединение с сервером

Заходим в свойства сервера:

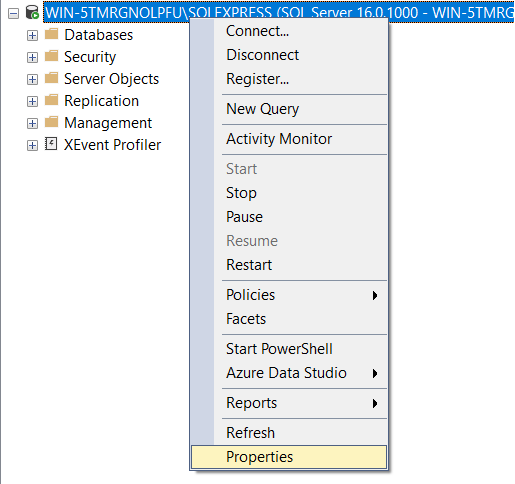


Рисунок 2 – Свойства

Проверяем какие настройки у нас установлены, в графе “Серверная проверка подлинности”. на проверку подлинности SQL Server и Windows:

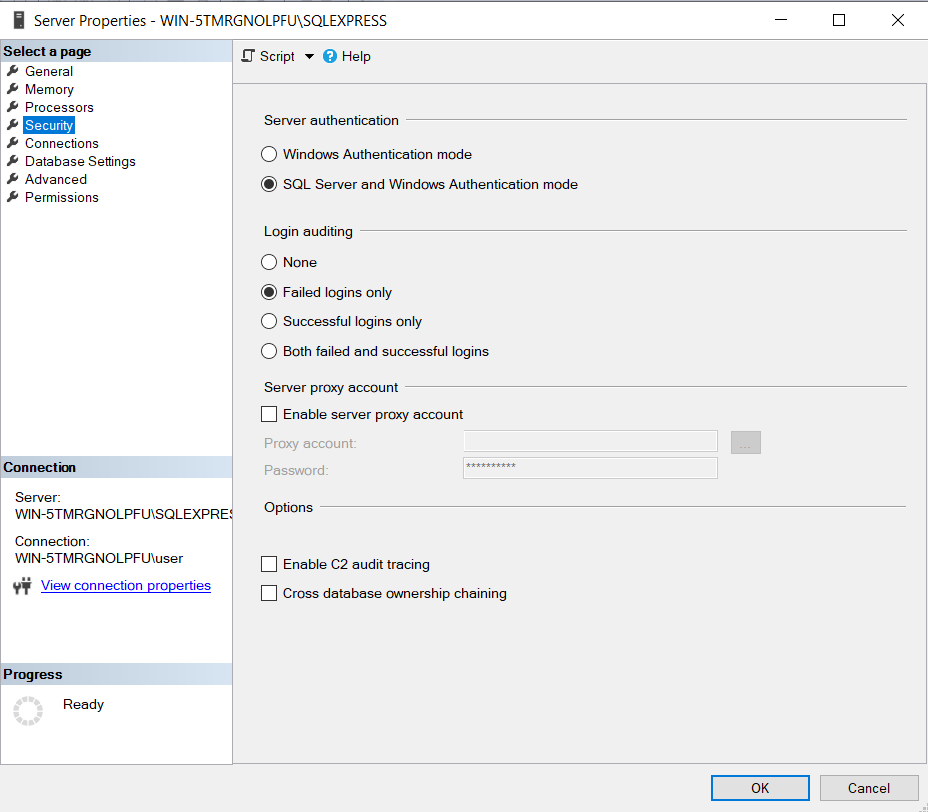


Рисунок 3 - Проверка подлинности

Заходим в свойства пользователя:

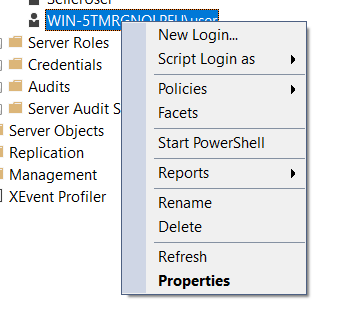


Рисунок 4 – свойства

Перешли на вкладку "Server Roles" (Роли сервера), чтобы увидеть, на выполнение каких серверных ролей авторизована ваша учетная запись:

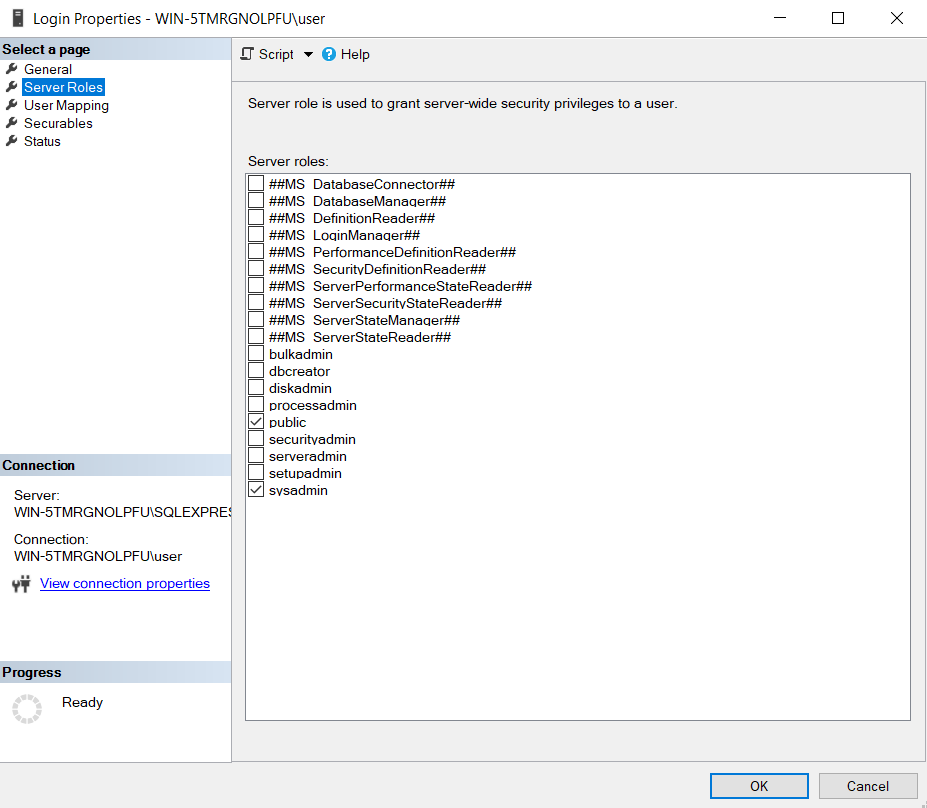


Рисунок 5 – проверка роли сервера

Открываем свойства пользователя:

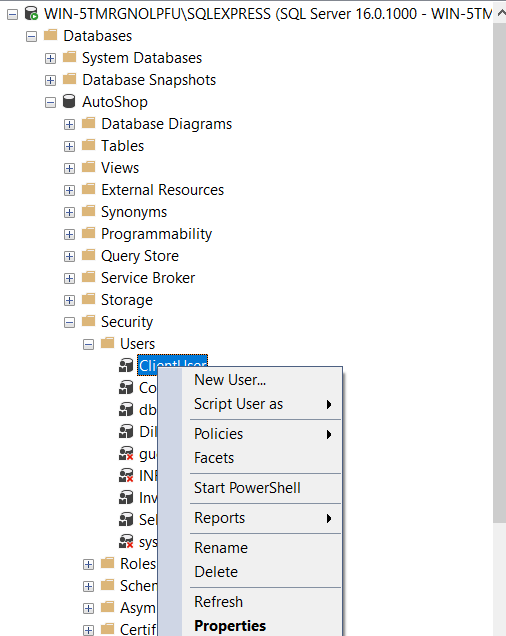


Рисунок 6 – проверка свойств

Определяем членство пользователя:

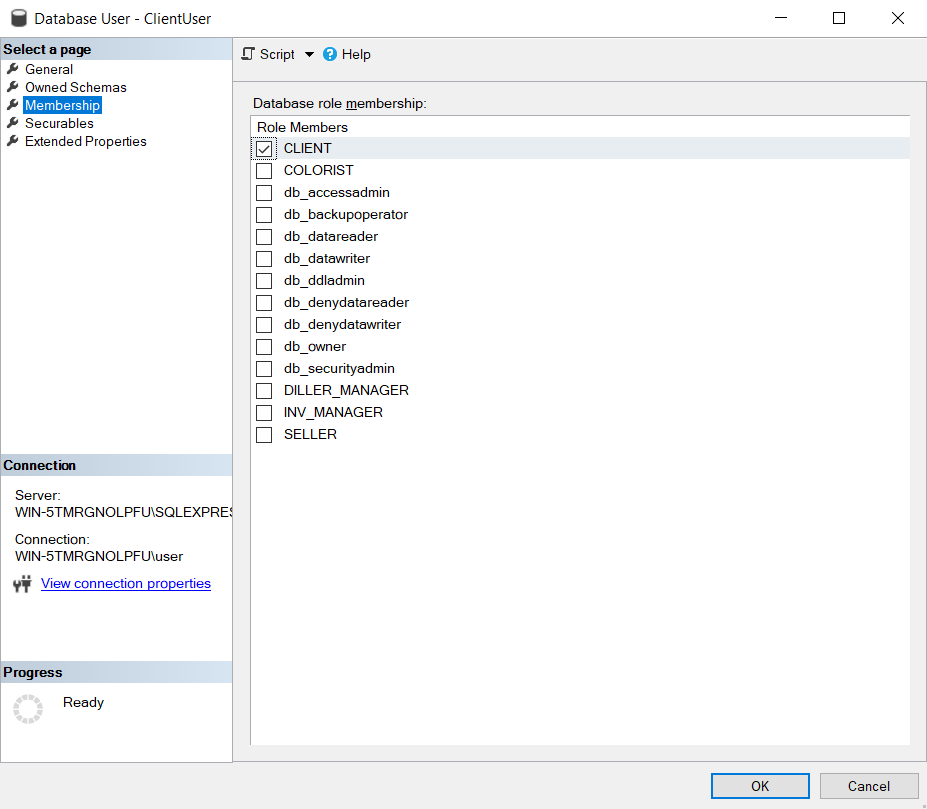


Рисунок 7 – Членство пользователя

Создание базы данных:

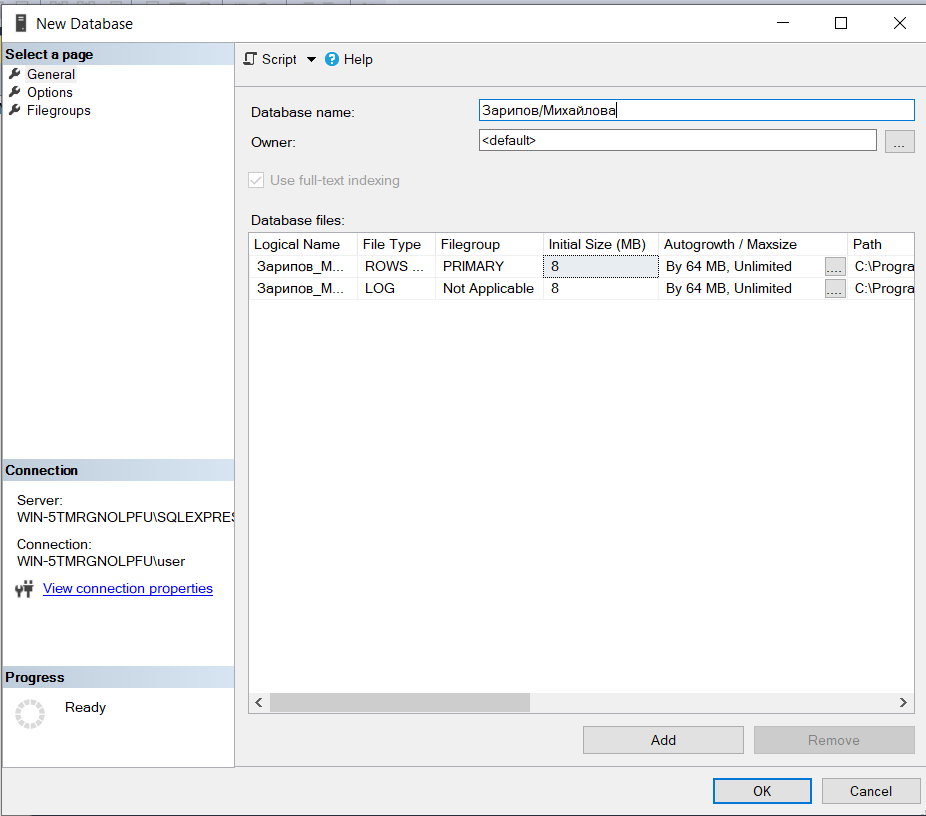


Рисунок 8 – Создание БД

Открываем свойства пользователя базы данных:

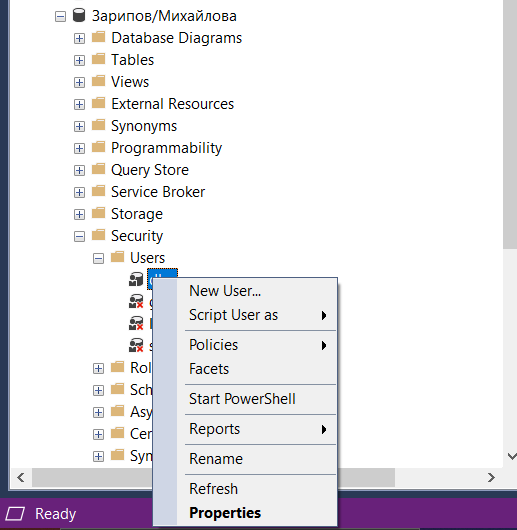


Рисунок 9 – Свойства dbo

Убедились, что роль "db\_owner" присутствует в списке ролей, к которым этот пользователь авторизован:

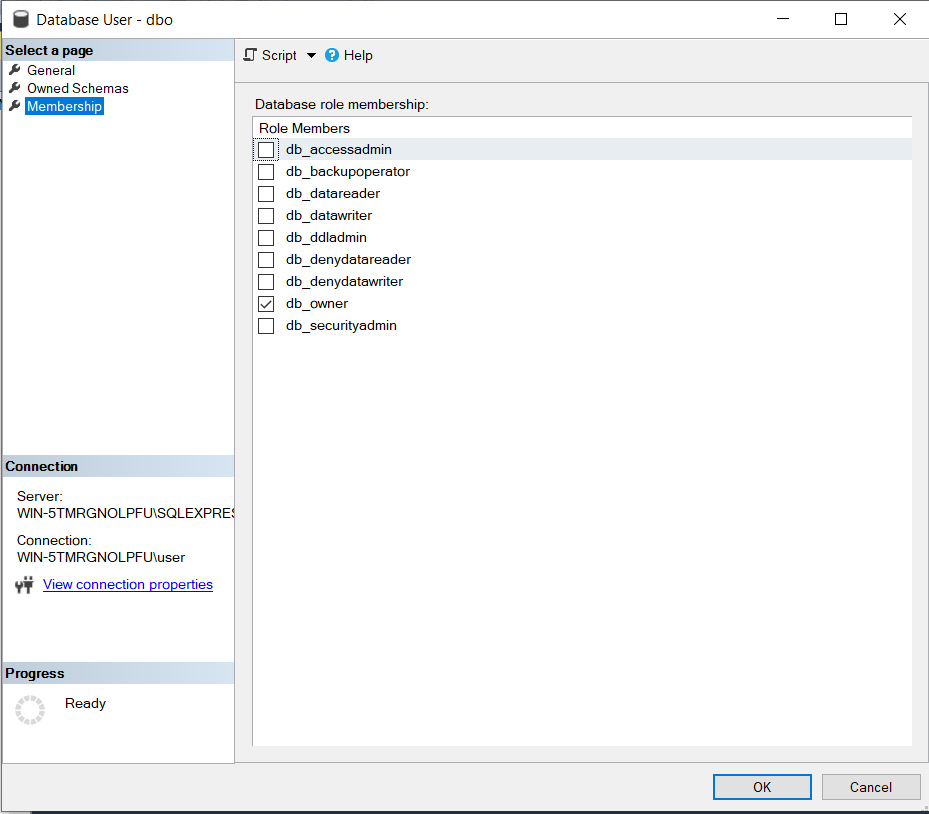


Рисунок 10 – членство

Используя приведенный ниже скрипт, создали в базе данных таблицы:

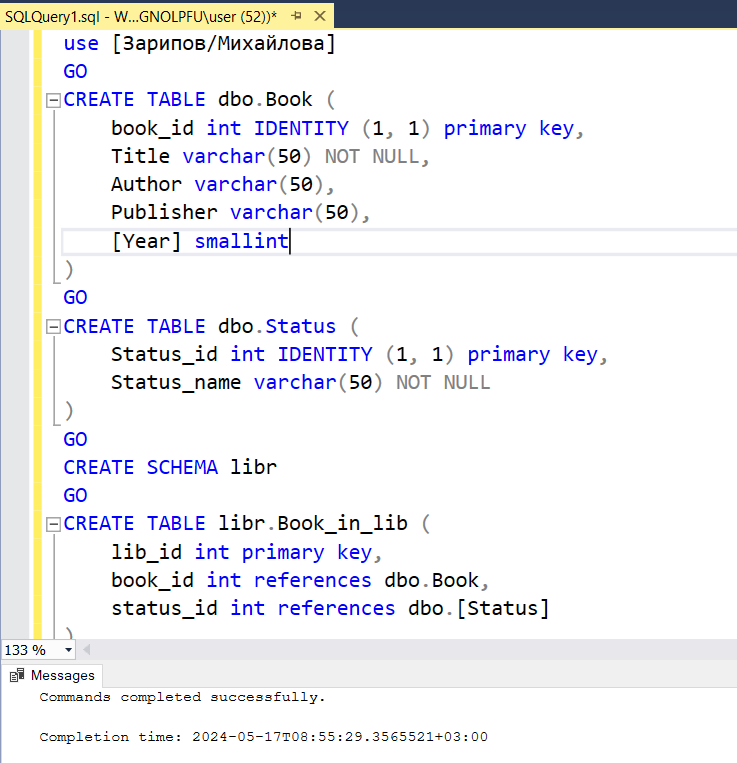


Рисунок 11 – Создание таблиц

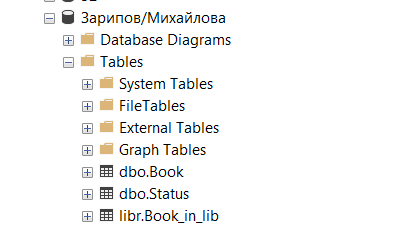


Рисунок 12 – Создание таблиц

Для создания пользователя, выбора схемы по умолчанию и добавления в роль db\_datareader, выполнили следующий скрипт:

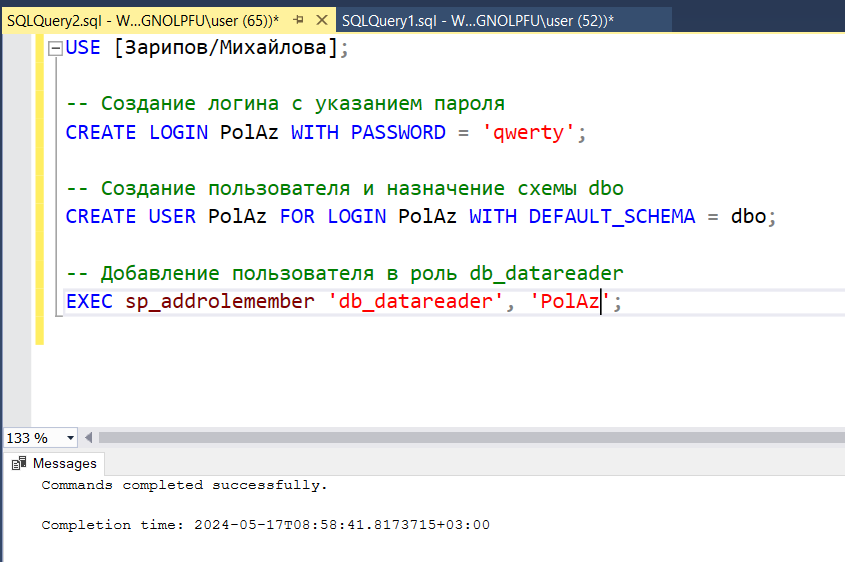


Рисунок 13 – Скрипт

Убедились, что новый пользователь имеет доступ только на чтение данных из всех таблиц базы данных:

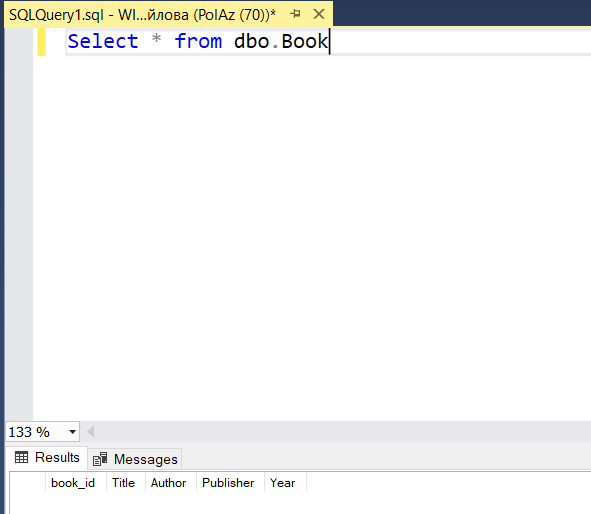


Рисунок 14 – Проверка со стороны пользователя

Создали новую роль:

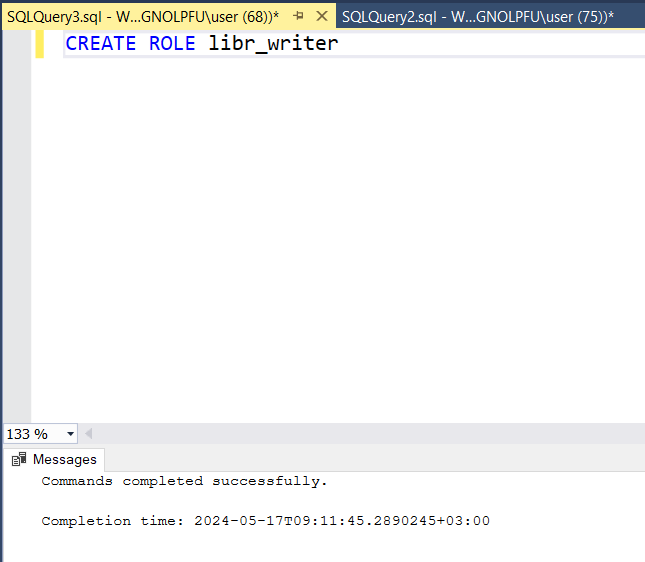


Рисунок 15 – Создание роли

Ввели следующий запрос, чтобы предоставить разрешения роли "libr\_writer" на выполнение операций INSERT, UPDATE и DELETE для объектов в схеме "libr":

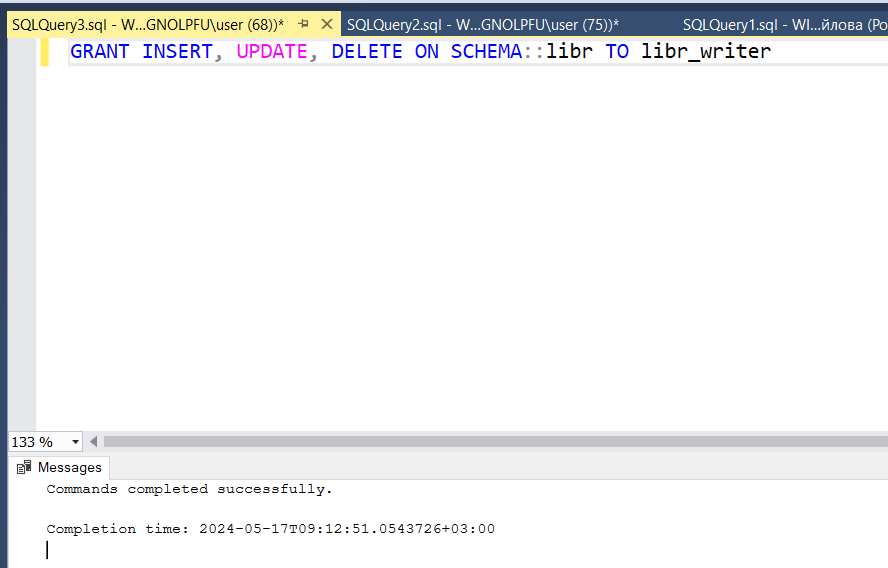


Рисунок 16 – Разращение роли

Ввели следующий запрос, чтобы добавить пользователя "kiril" в роль "libr\_writer":

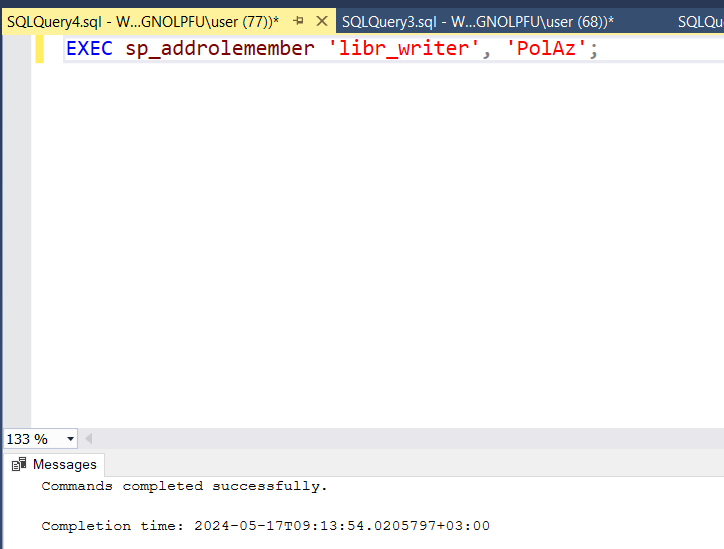


Рисунок 17 – Назначение роли

Выполнили запросы INSERT, UPDATE, DELETE:

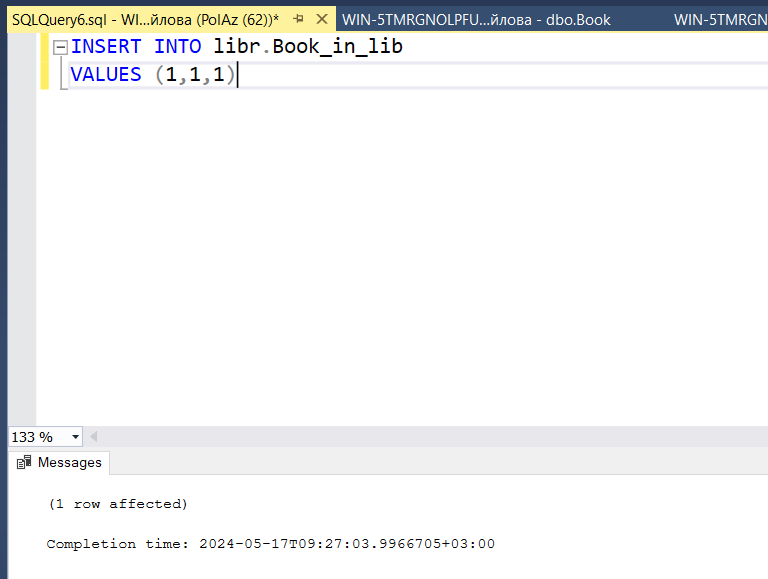


Рисунок 18 – Запрос Insert

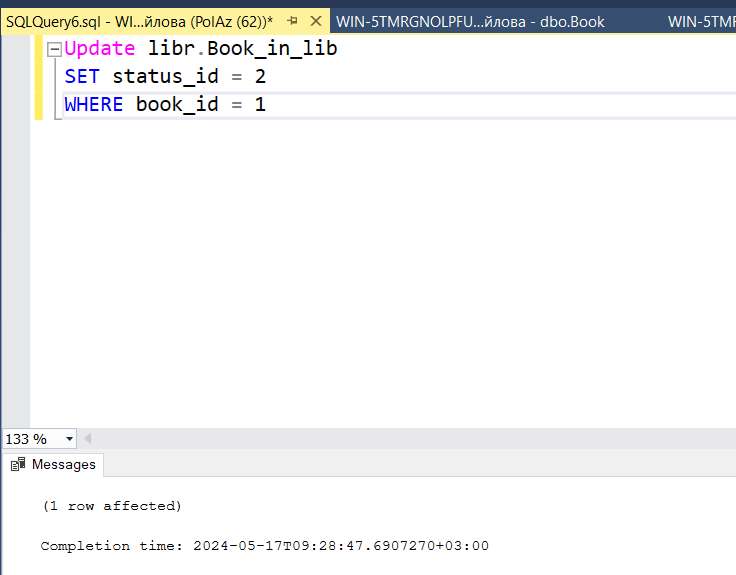


Рисунок 19 – Запрос update

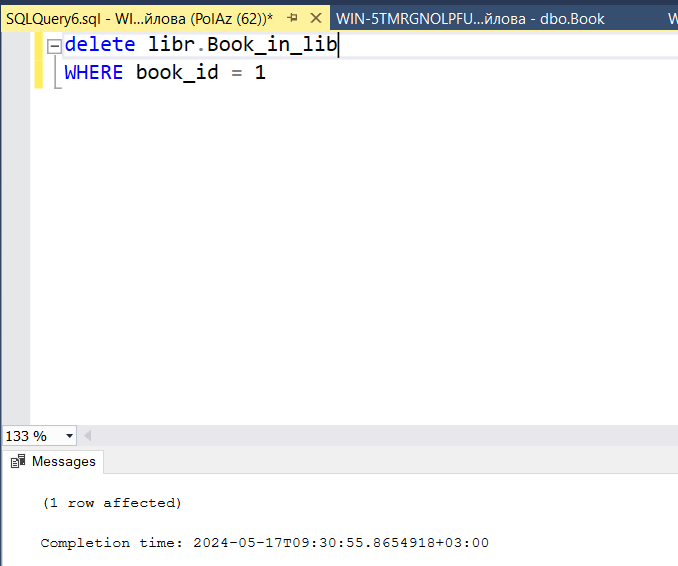


Рисунок 20 – Запрос delete

Открываем свойства таблицы libr.Book\_in\_lib:

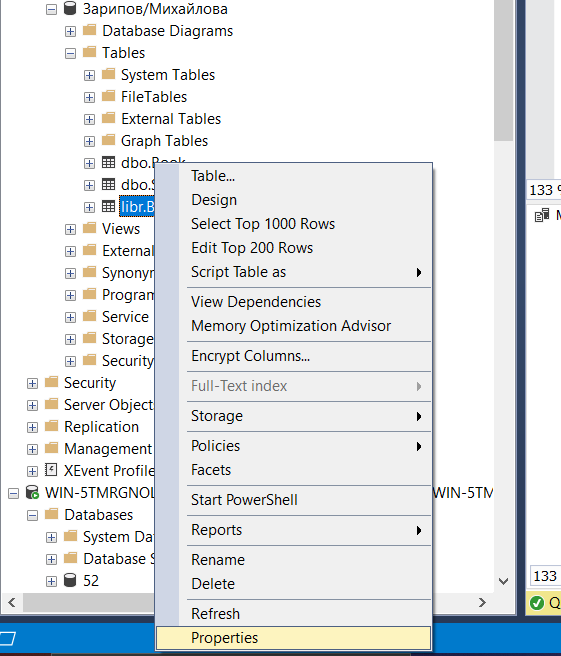


Рисунок 21 – Свойства

Назначили разрешения для пользователя AzPol:

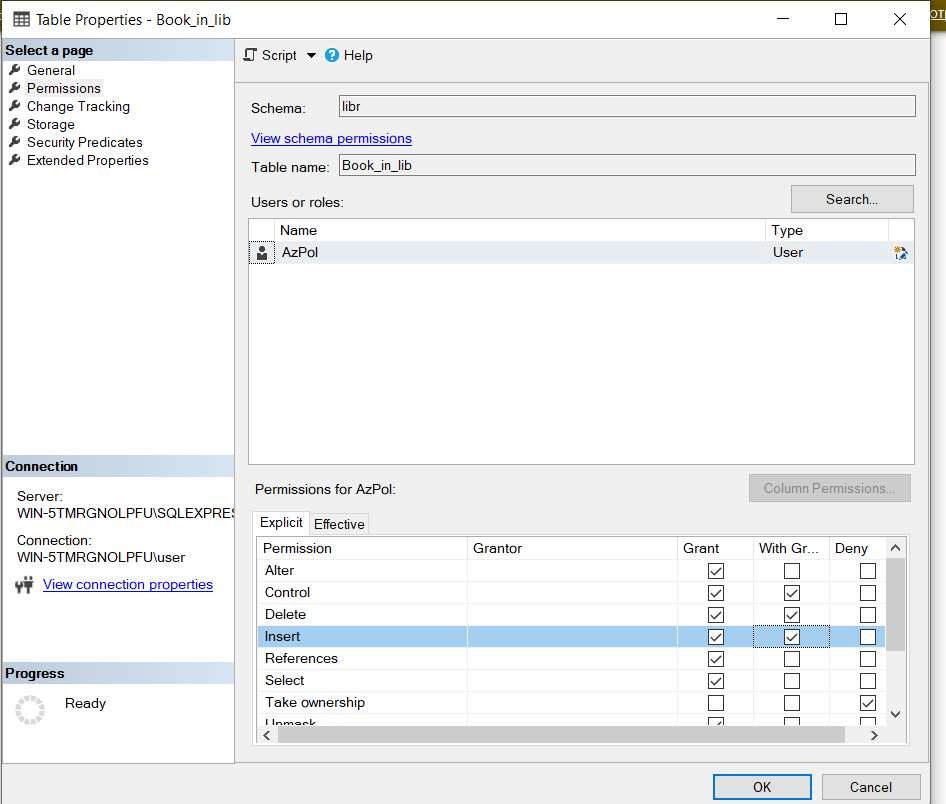


Рисунок 22 – Настройка разрешений

Выполнили запрос на предоставление прав:



Рисунок 23 – Предоставление право

Попробовали выполнить операцию обновления значения в столбце "Title" таблицы "Book":

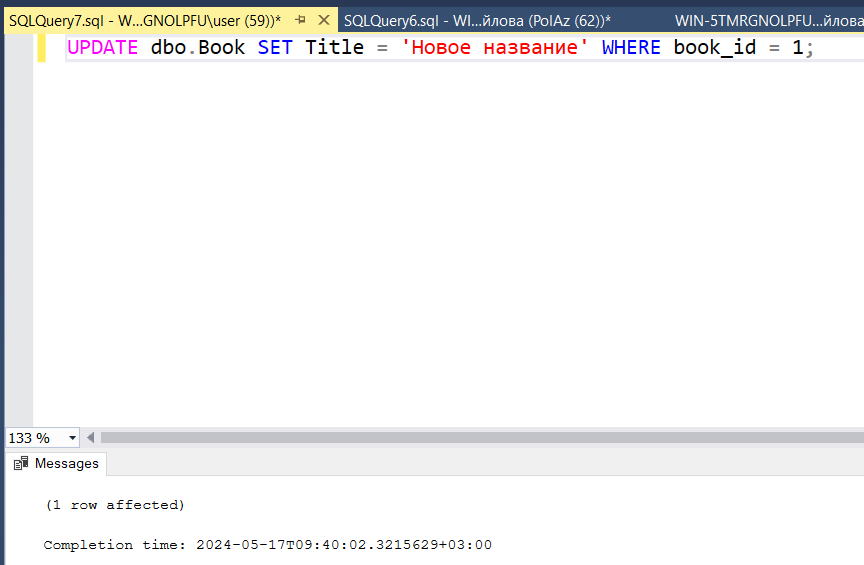


Рисунок 24 – Обновление столбцов

Создали представление:



Рисунок 25 - Создания представления

Теперь предоставили пользователю "PolAz" права на изменение и добавление записей в представление "NewBooks", но только для книг, изданных не ранее 2000 года:

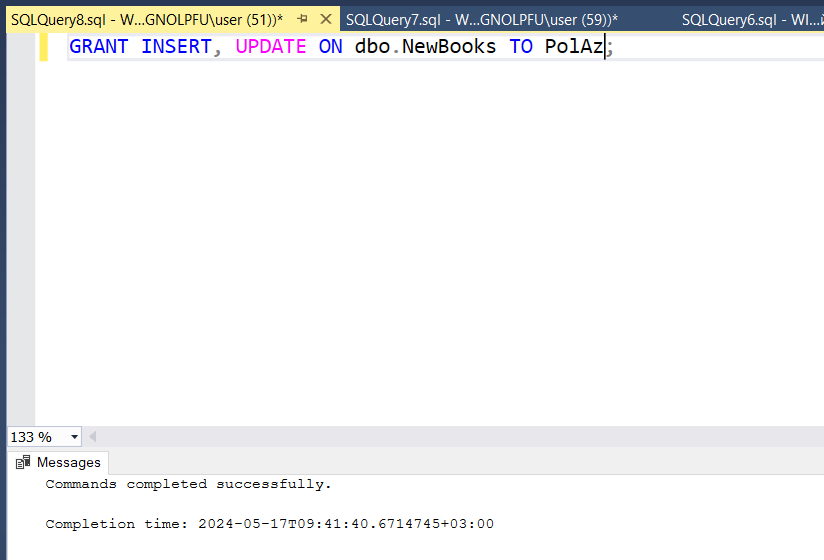


Рисунок 26 – Права на изменение записей

Убедитесь, что пользователь "PolAz" имеет права на изменение и добавление записей в представление "NewBooks":

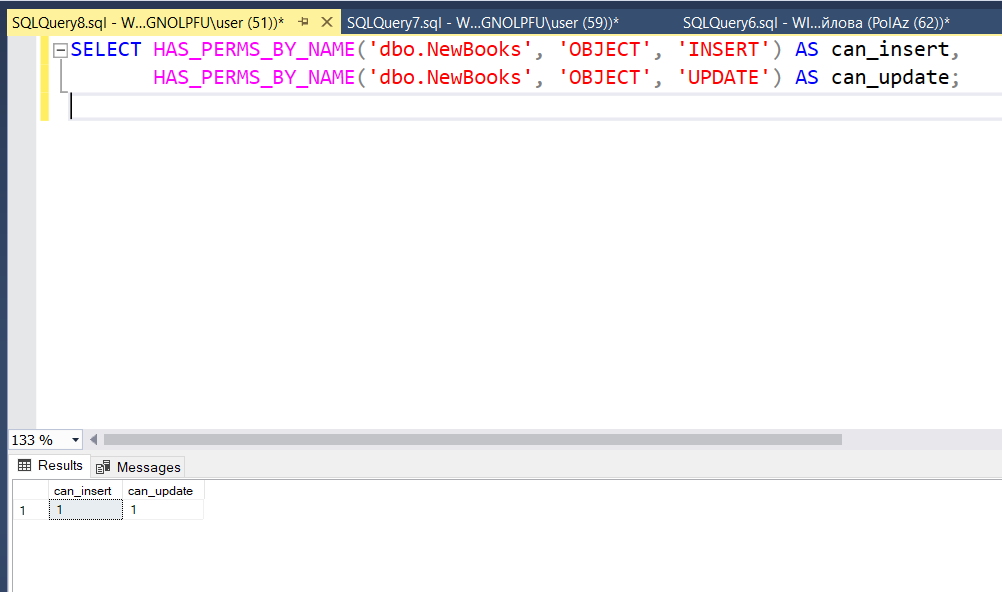


Рисунок 27 – Проверка прав пользователя

**Вывод**

Мы научились предоставлять пользователям доступ к базе данных.