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

Студенты гр.4237

Зиганшин Амир Маратович

Сергеев Даниил Дмитриевич

Преподаватель

Кожевников К. Д.

Казань 2024

**Цель** – Научиться реализовывать доступ пользователей к базе данных

**Задачи:**

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

**Практическая часть**

С помощью SQL Server Management Studio подключились к используемому экземпляру SQL Server. Проверили установленный на сервере режим аутентификации. На рисунке 1 показано подключение к бд.

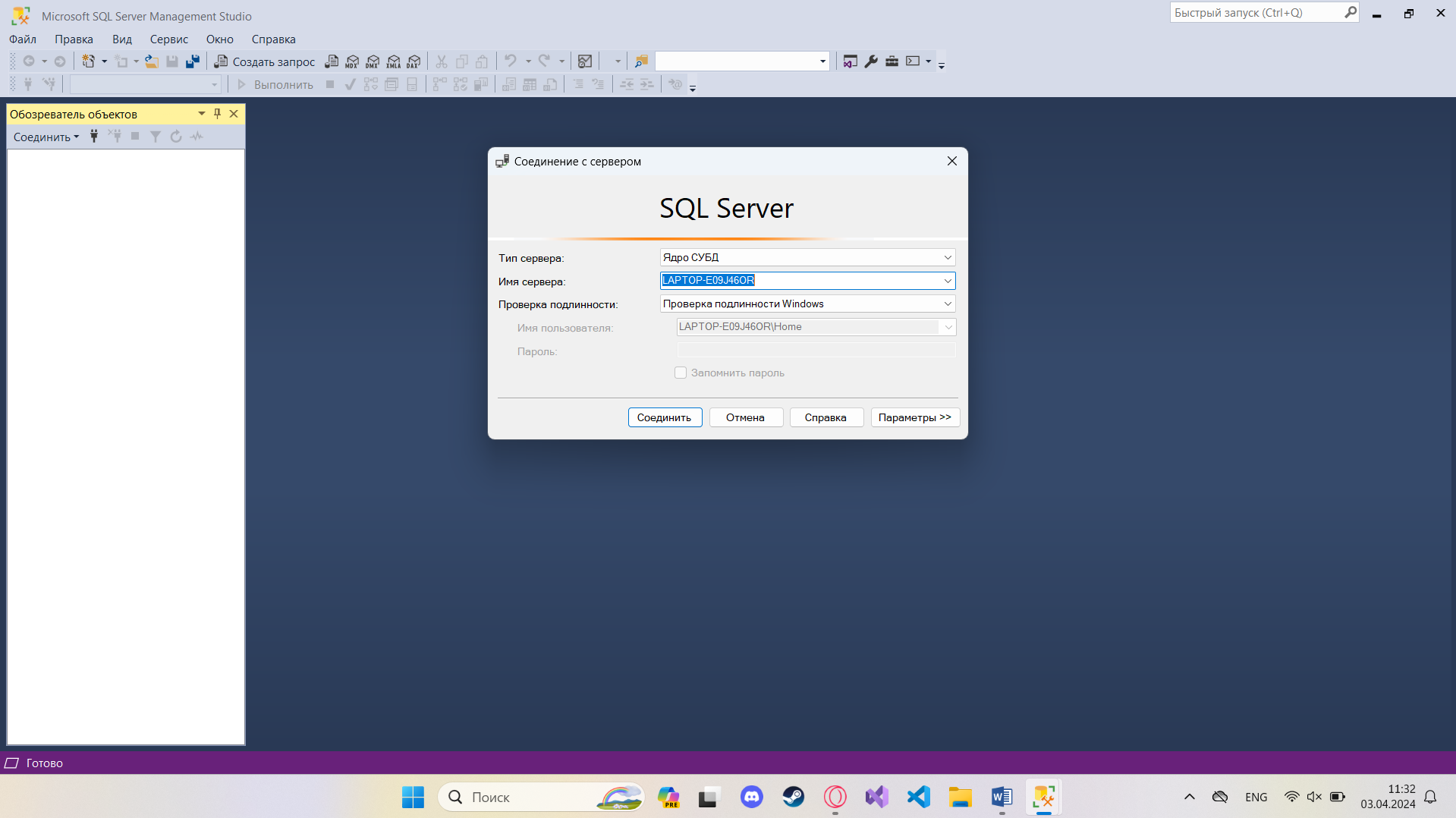


Рисунок 1 – Подключение к бд

Далее заходим в свойства. Показано на рисунке 2.

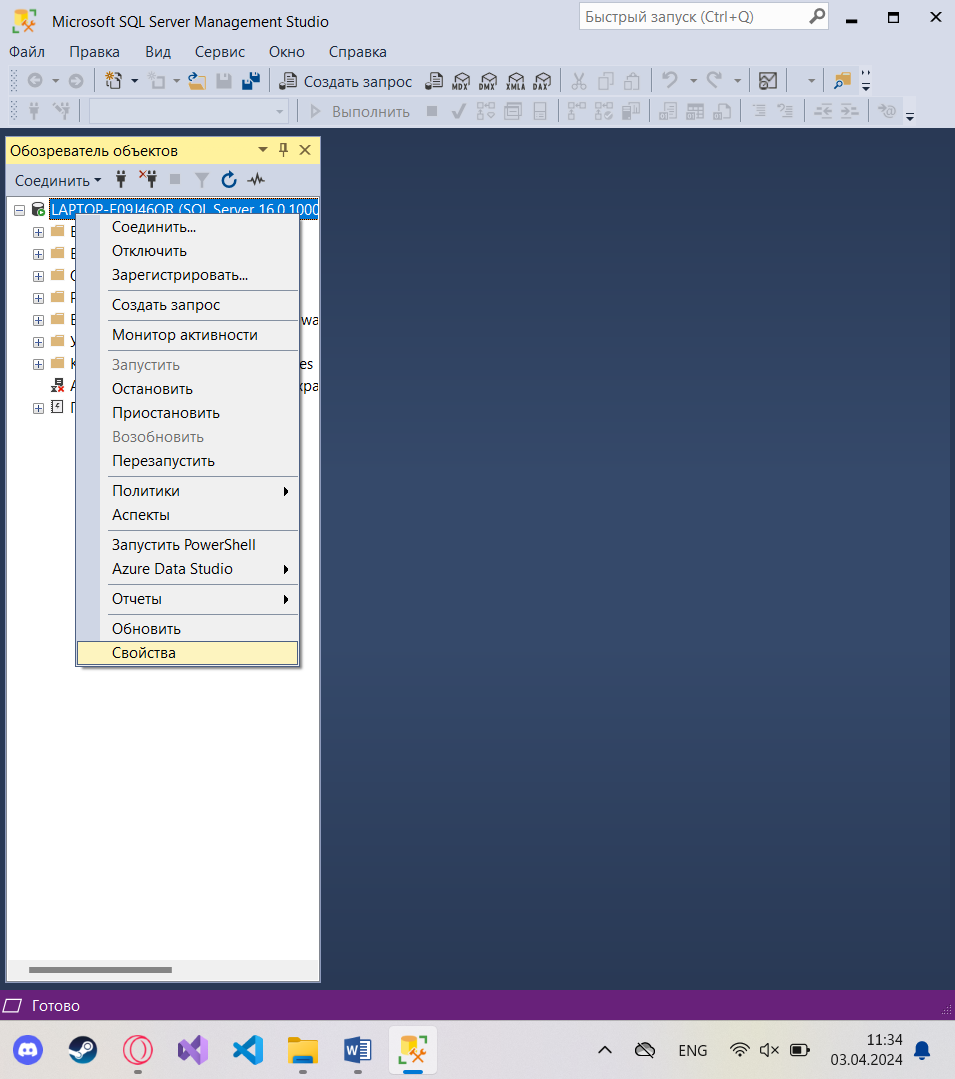


Рисунок 2 – Свойства

Проверяем какие настройки у нас установлены, в графе “Серверная проверка подлинности”. Изменяем на проверку подлинности SQL Server и Windows. Показано на рисунке 3.

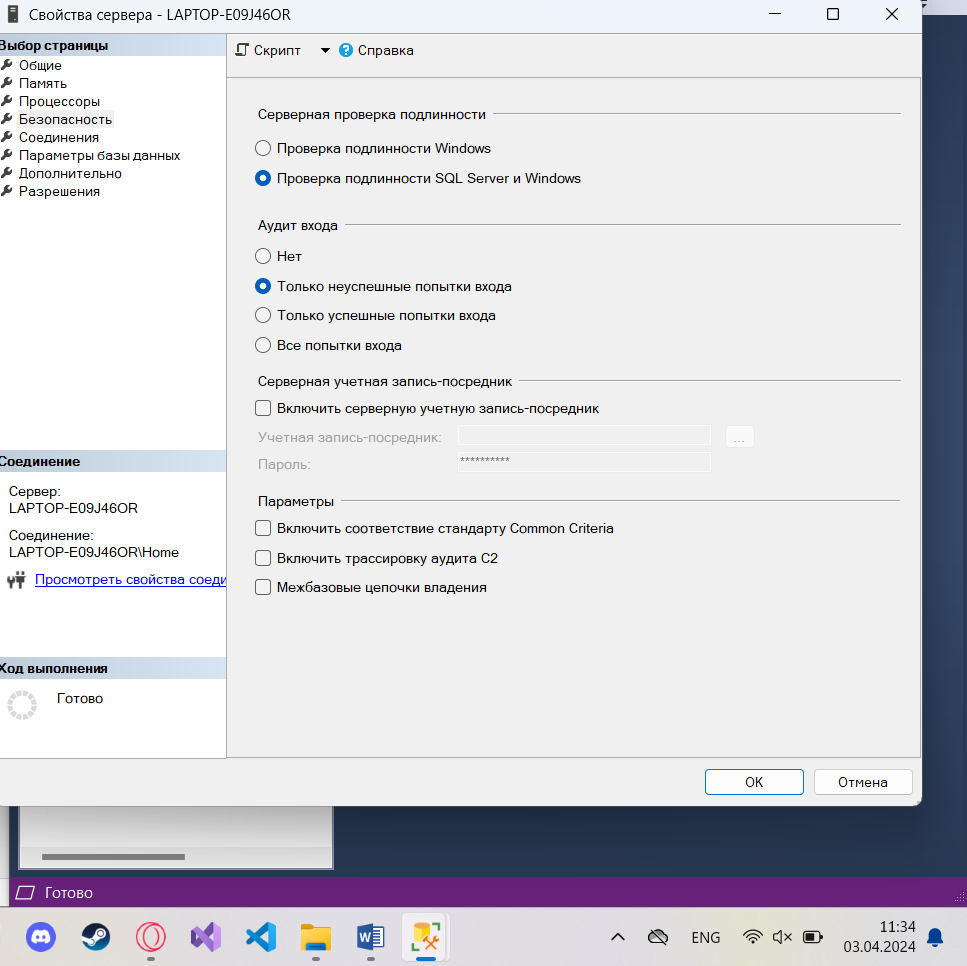


Рисунок 3 – Устанавливаем проверку подлинности Sql Server и Windows

В окне Object Explorer находим и разворачиваем дерево объектов, чтобы увидеть различные папки и объекты, связанные с нашим сервером SQL. Показано на рисунке 4.

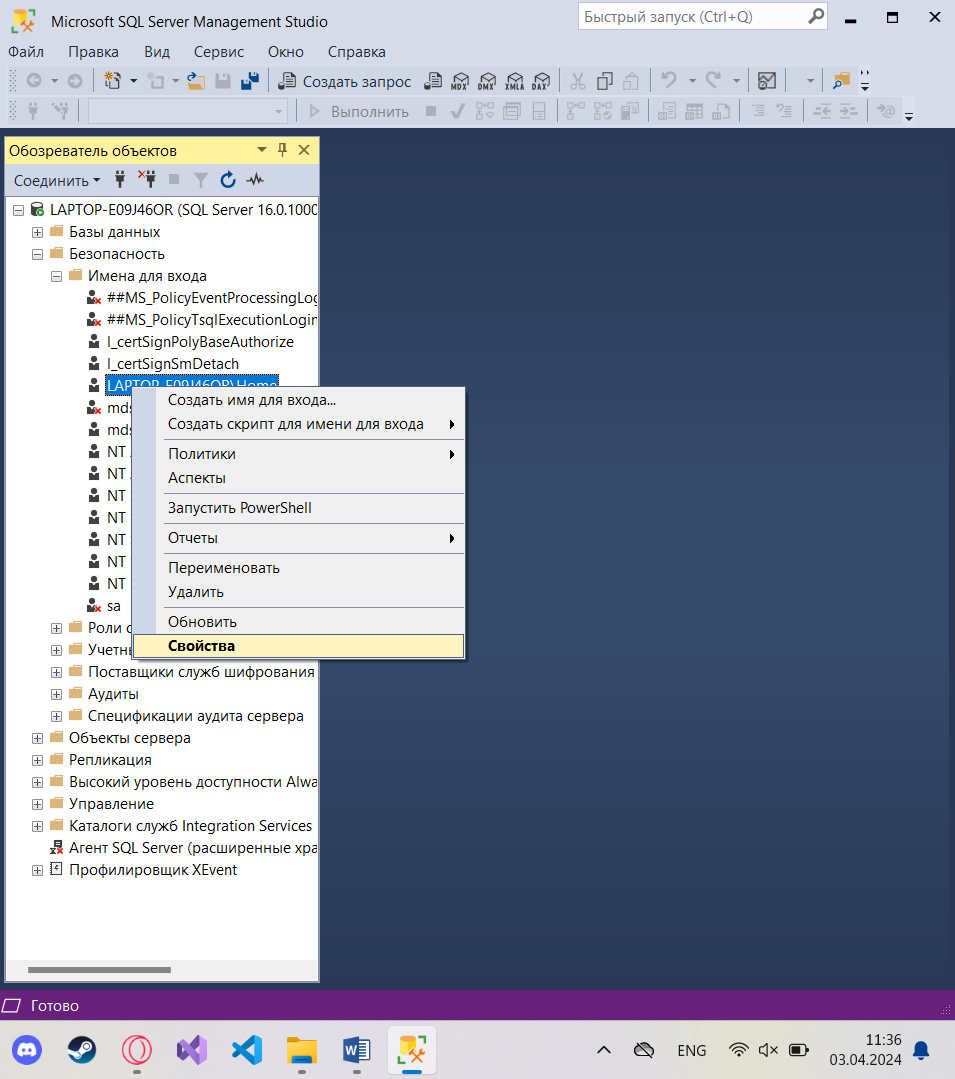


Рисунок 4 – Дерево обьектов

В открывшемся окне свойств учетной записи мы можем увидеть информацию о настройках и разрешениях нашей учетной записи.

Переходим на вкладку "Server Roles" (Роли сервера), чтобы увидеть, на выполнение каких серверных ролей авторизована наша учетная запись.

Здесь мы можем увидеть список доступных серверных ролей (например, sysadmin, dbcreator, public и т.д.) и проверить, к каким из них относится наша учетная запись. Показано на рисунке 5.

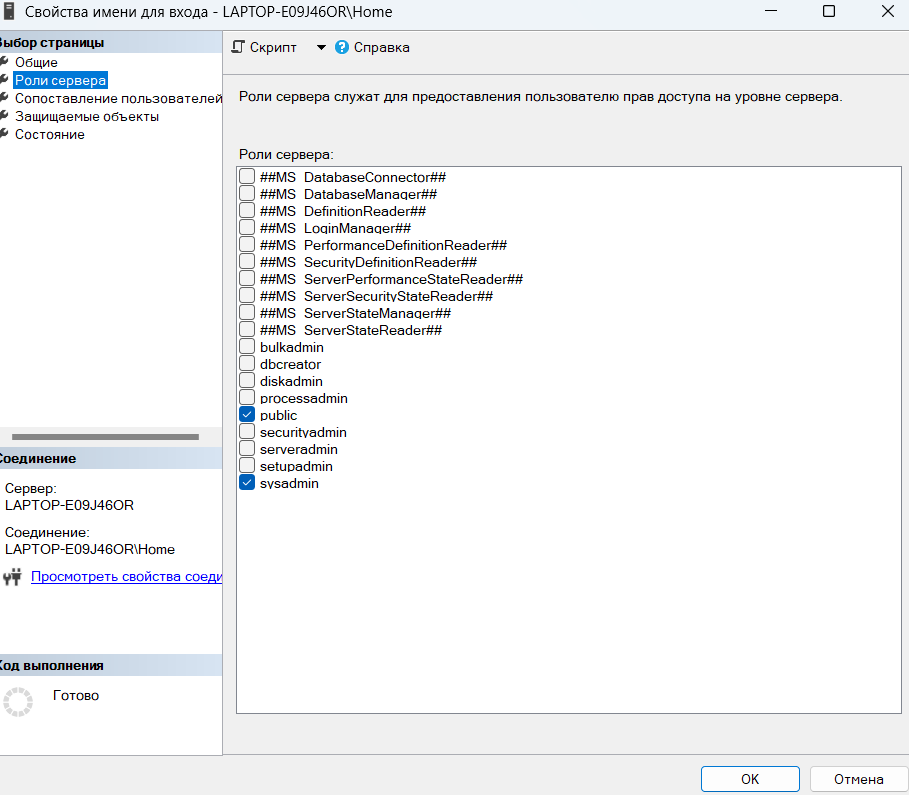


Рисунок 5 – Свойства роли сервера

Далее чтобы узнать, на выполнение каких ролей пользователь авторизован в бд мы переходим в свойства пользователей. Показано на рисунке 6.

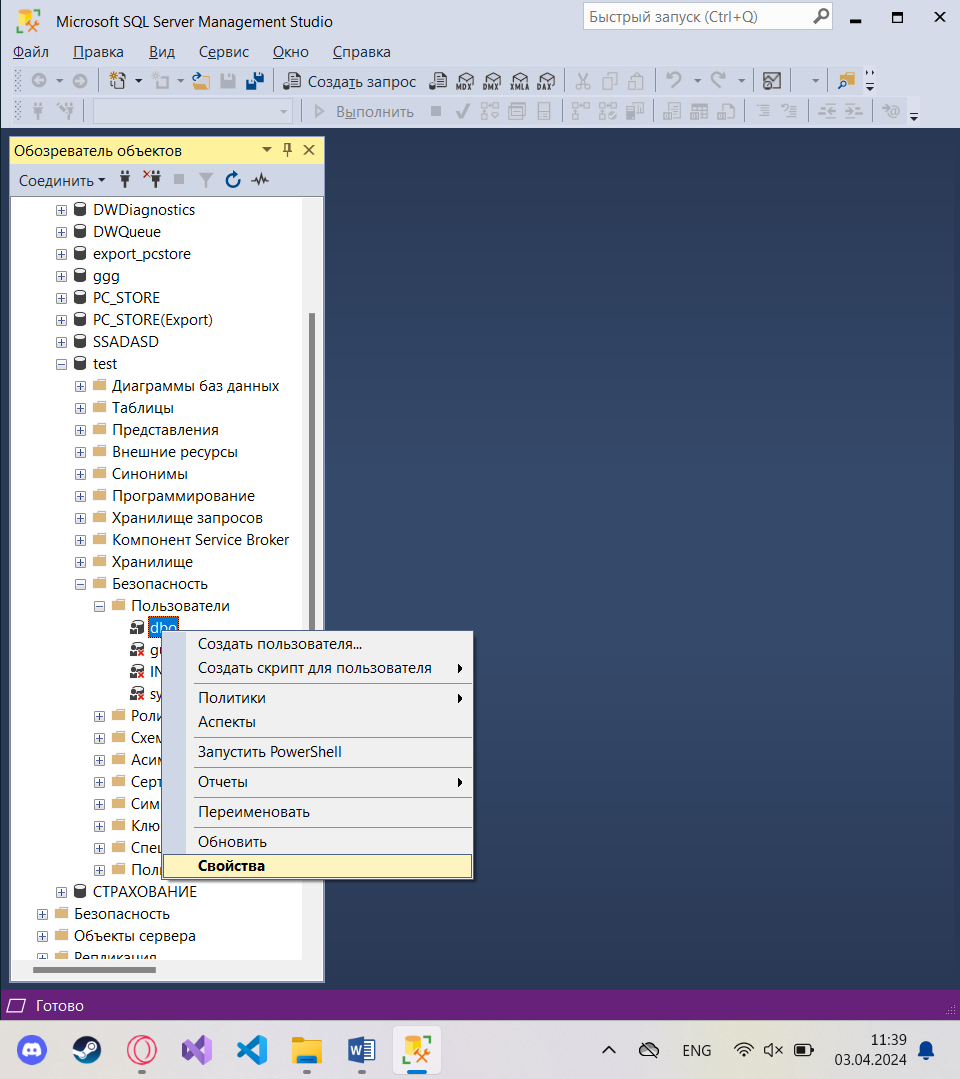


Рисунок 6 – Свойства

Переходим на вкладку "Membership" (Членство), чтобы увидеть список ролей баз данных, к которым наш пользователь относится.

Ознакамливаемся с информацией о ролях (например, db\_owner, db\_datareader, db\_datawriter и т.д.), к которым наш пользователь авторизован в данной базе данных. Показано на рисунке 7.

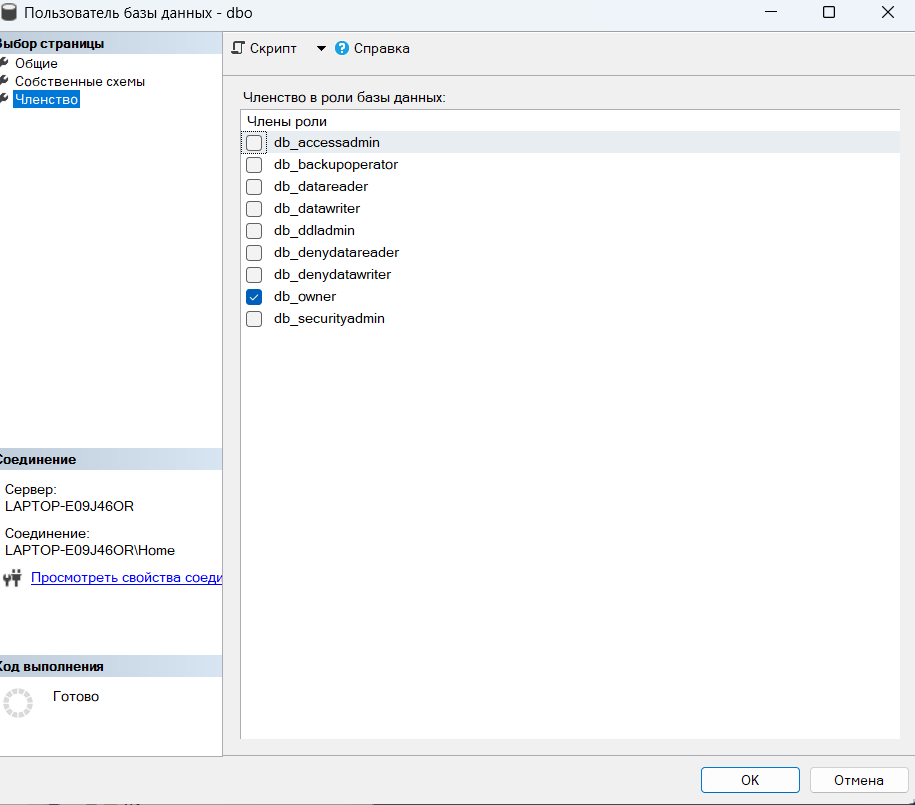


Рисунок 7 – Свойство членства ролей в бд

Далее создаем новую бд. Показано на рисунке 8, 9.

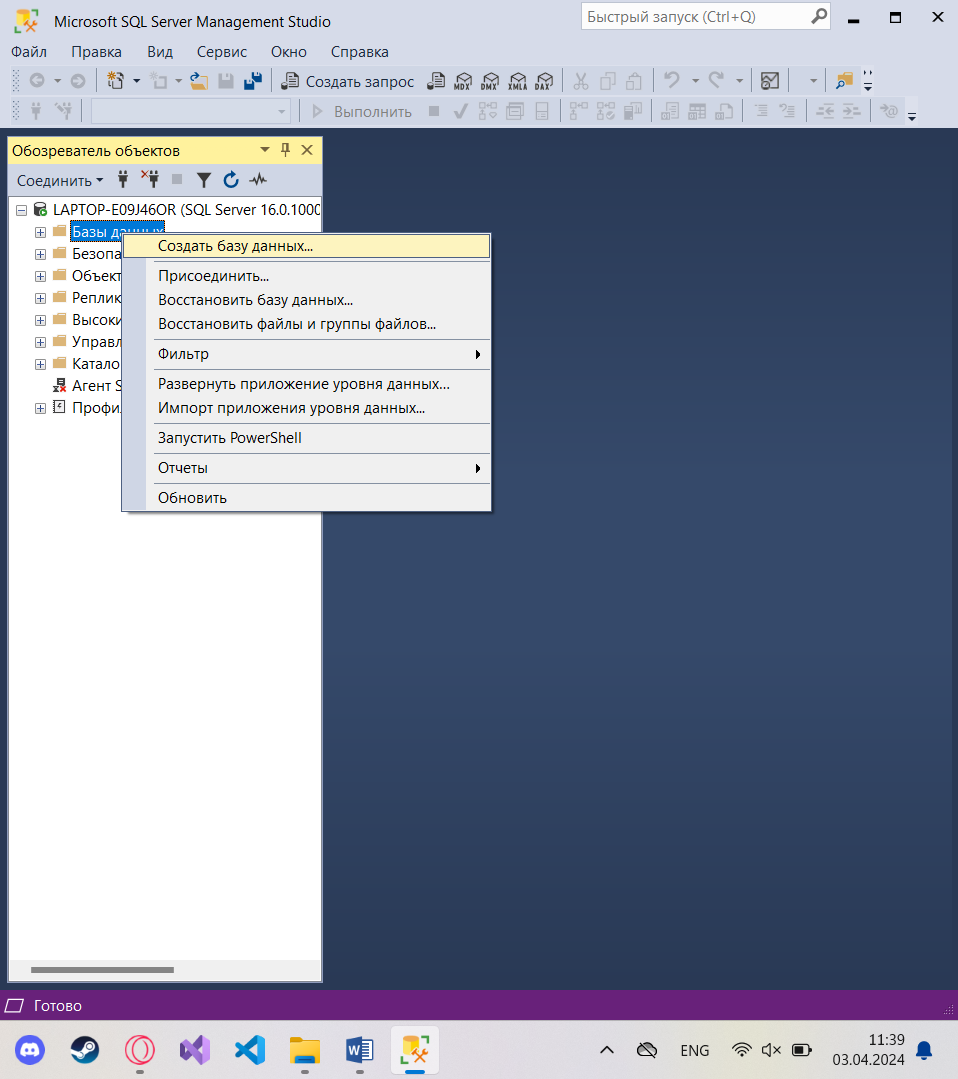


Рисунок 8 – Создание новой бд

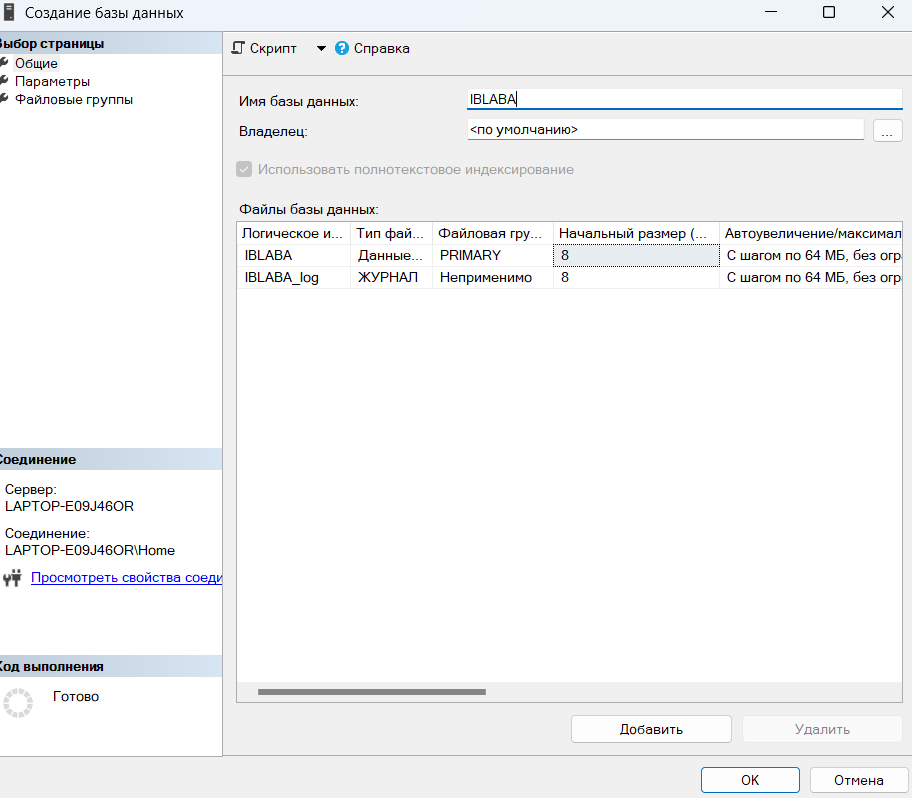


Рисунок 9 – Создание новой бд

Развернем созданную нами новую базу данных в списке баз данных.

Найдем папку "Security" внутри нашей новой базы данных и развернем ее.

Посмотрим список пользователей, сопоставленных с нашей новой базой данных. Показано на рисунке 10, 11.

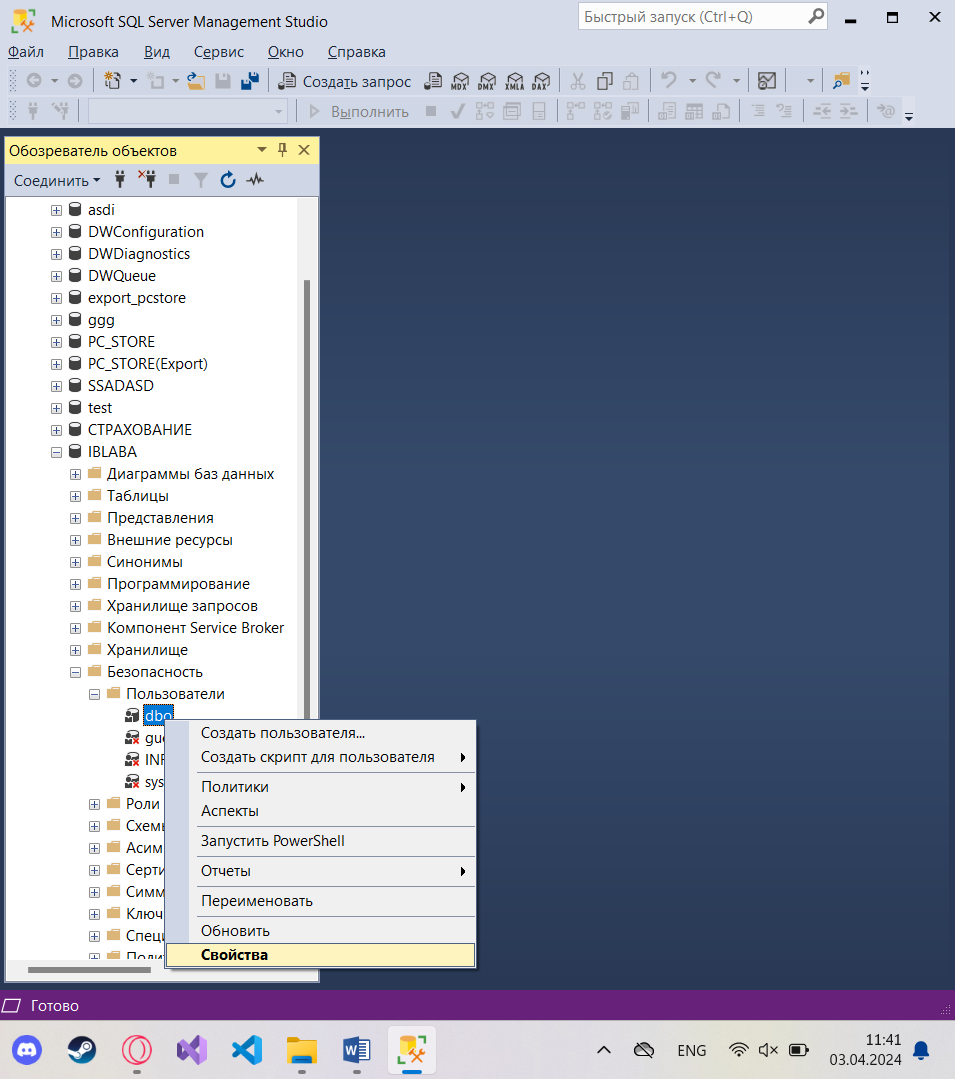


Рисунок 10 – Переход в свойства

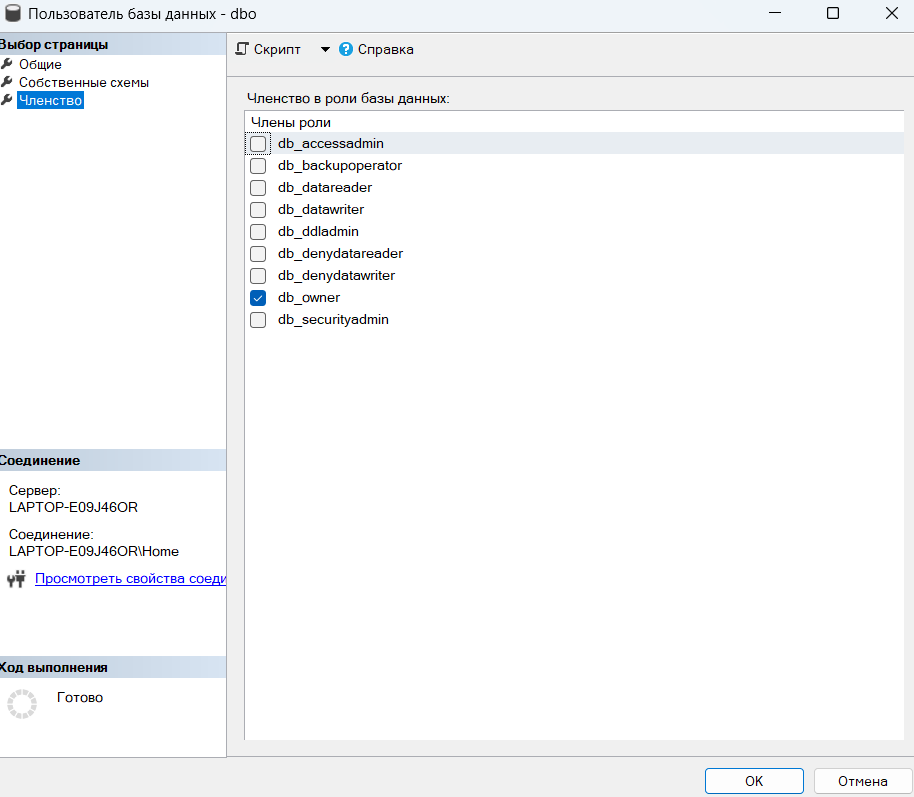


Рисунок 11 – Свойство членства ролей в бд

Используя скрипт создаем таблицы в бд. Показано на рисунке 12.

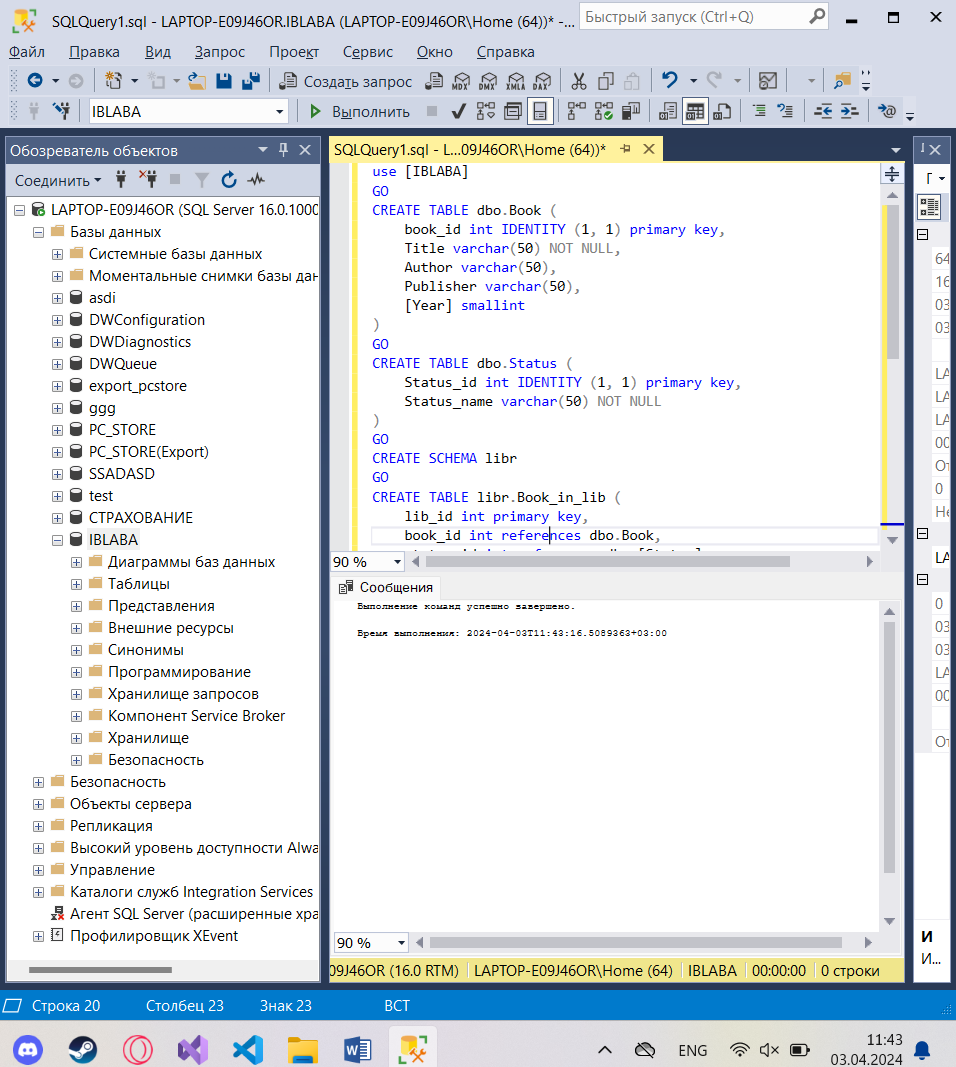


Рисунок 12 – Создание таблиц используя скрипт.

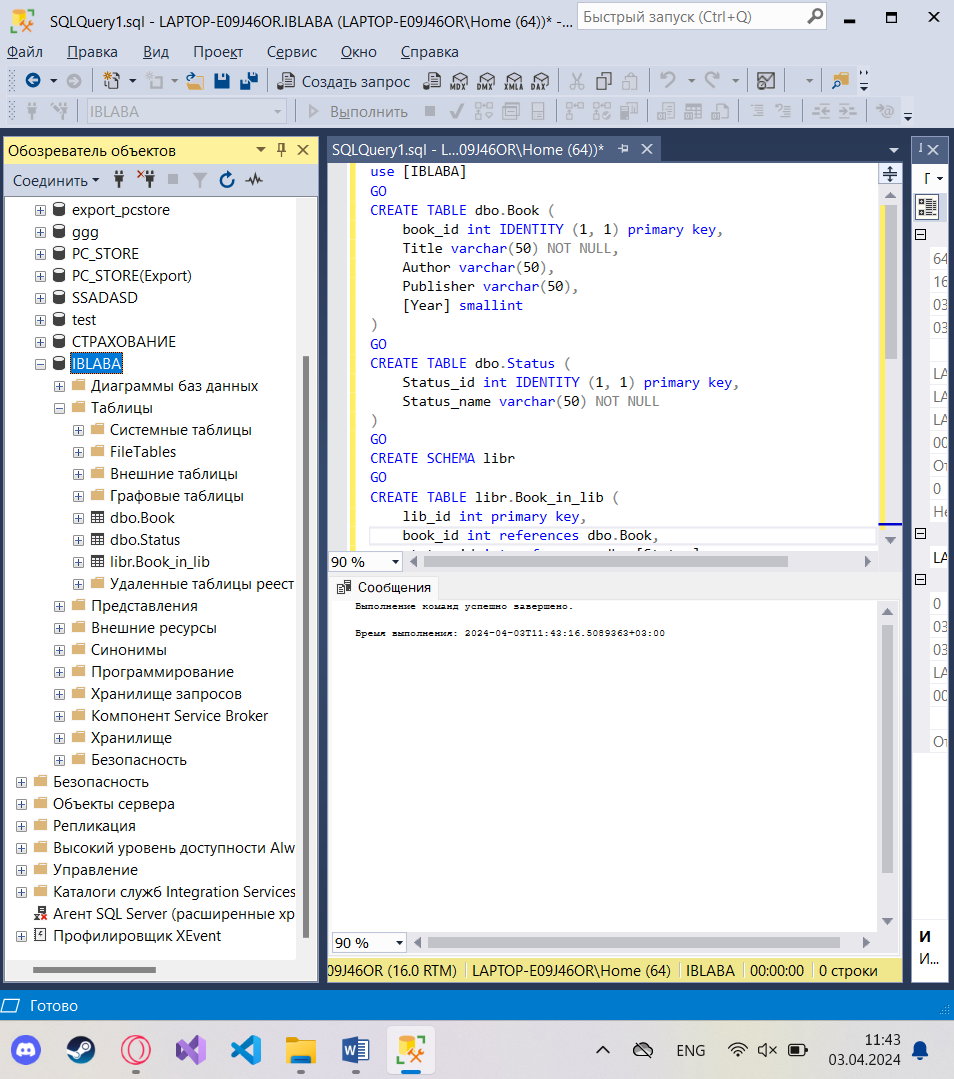


Рисунок 13 – Проверка созданных таблиц

Далее создаем пользователей и добавляем им роль. Показано на рисунке 14.

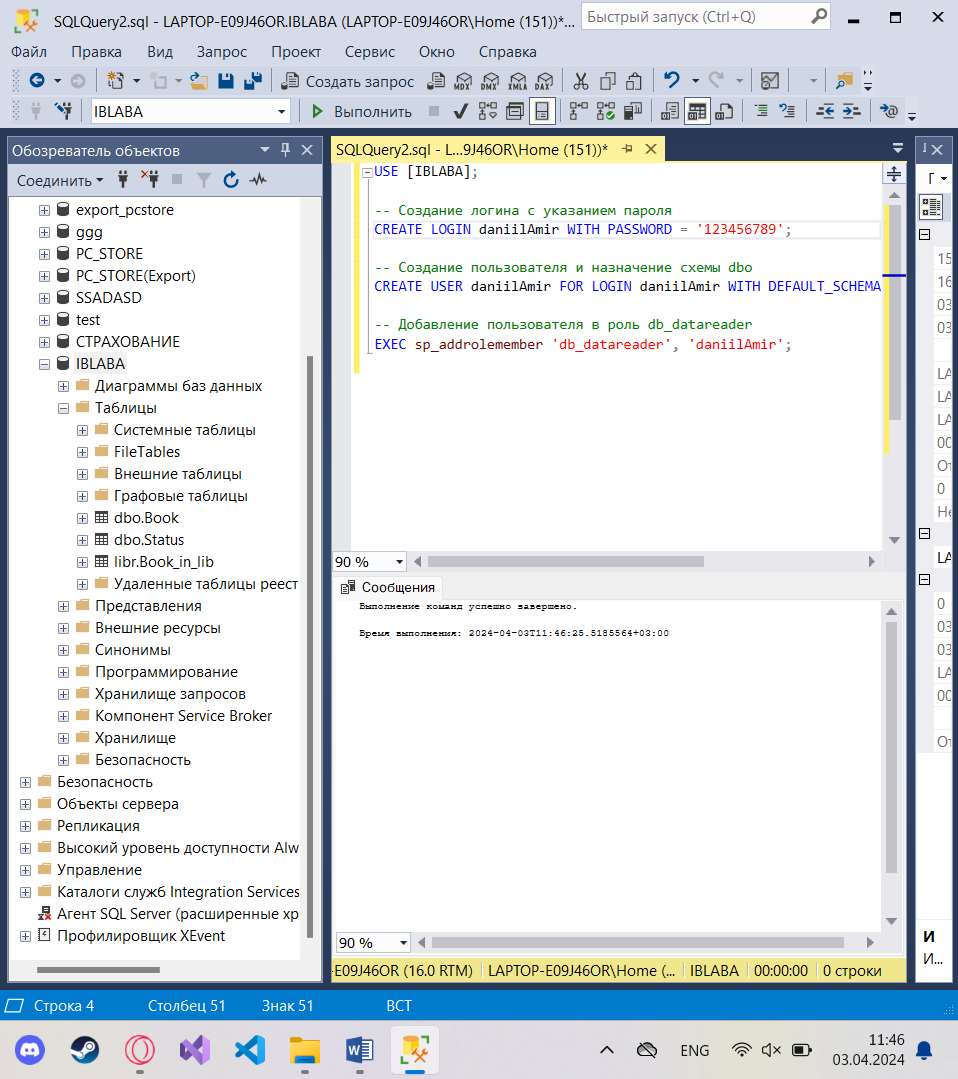


Рисунок 14 – Скрипт создание пользователей.

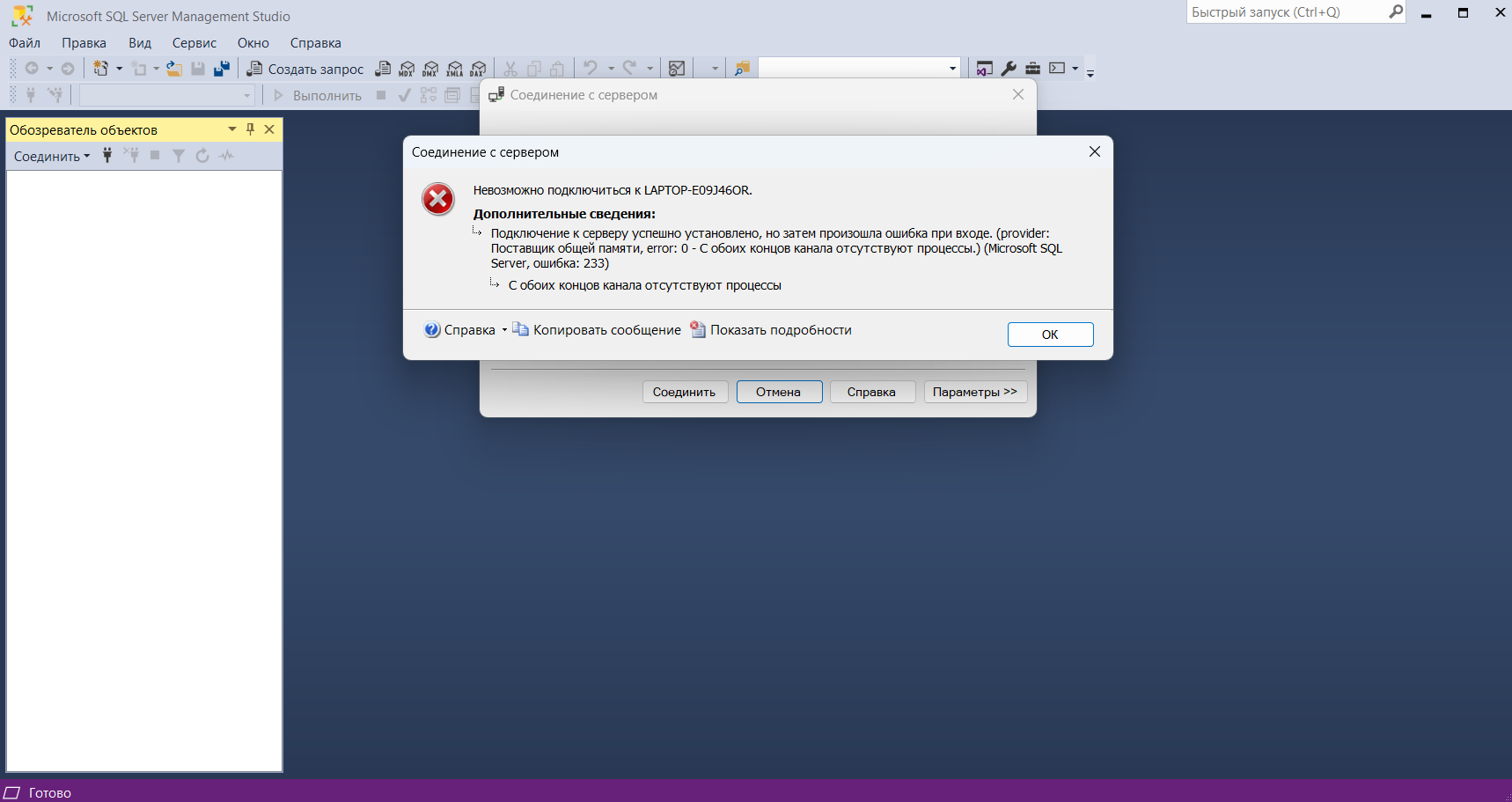


Рисунок 15 – Ошибка при входе в сервер от имени созданного пользователя.

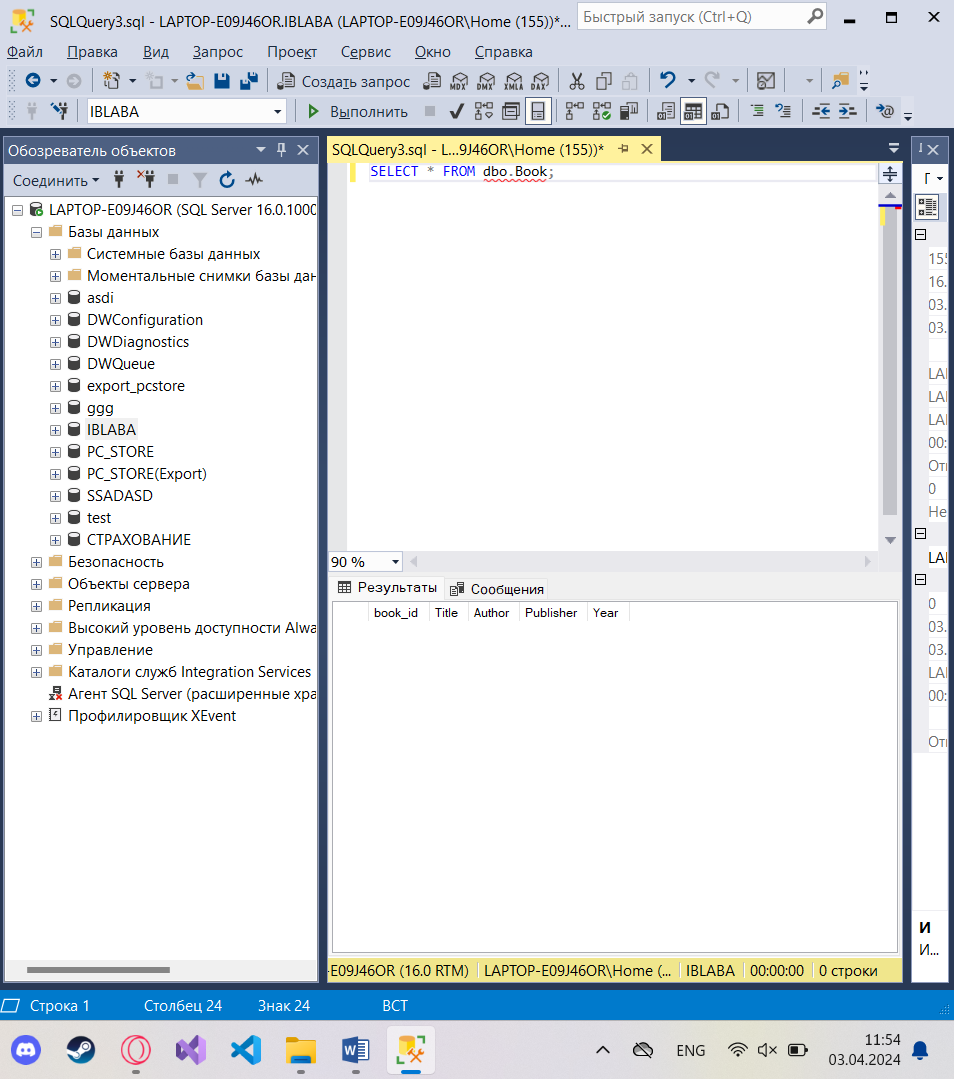


Рисунок 16 – Проверка со стороны пользователя

С помощью запроса создаем новую роль. Показано на рисунке 17.

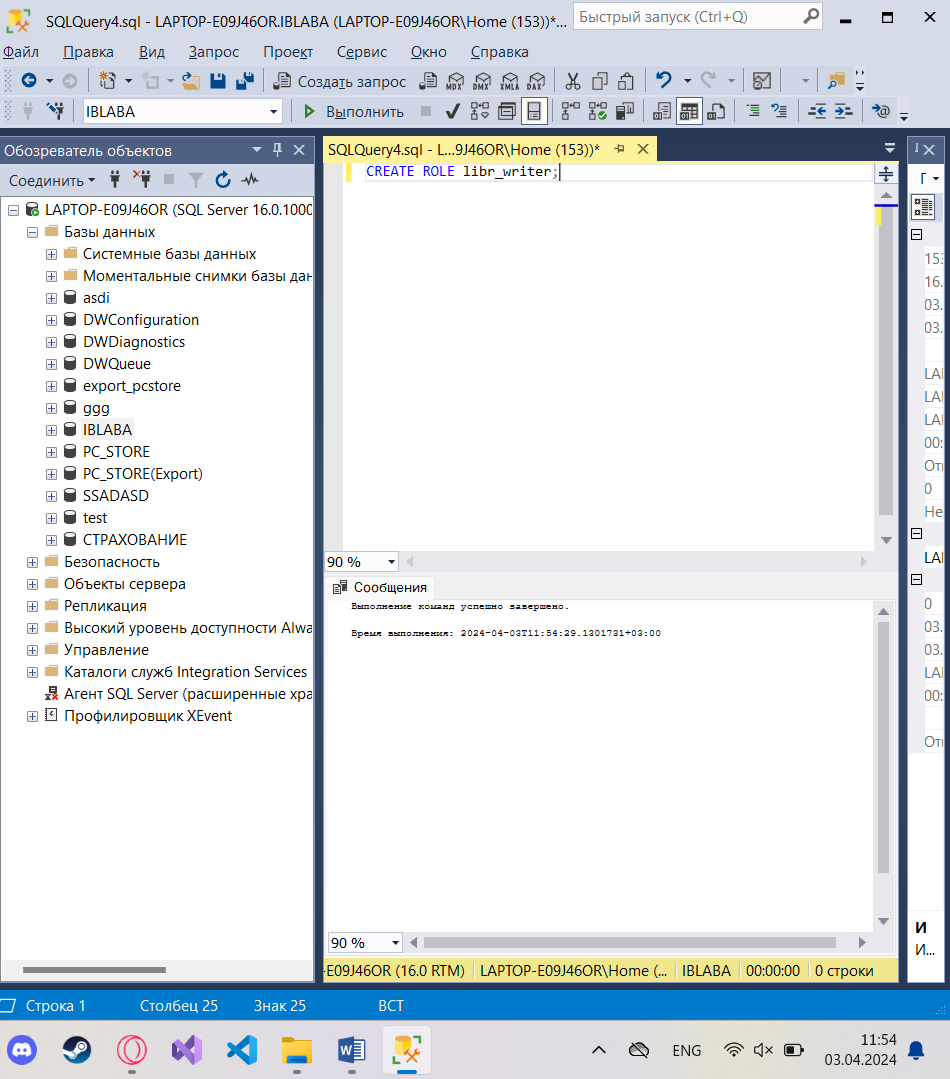


Рисунок 17 – Создание новой роли

Далее идет запрос, чтобы предоставить разрешения роли на выполнение операций INSERT, UPDATE и DELETE. Показано на рисунке 18.

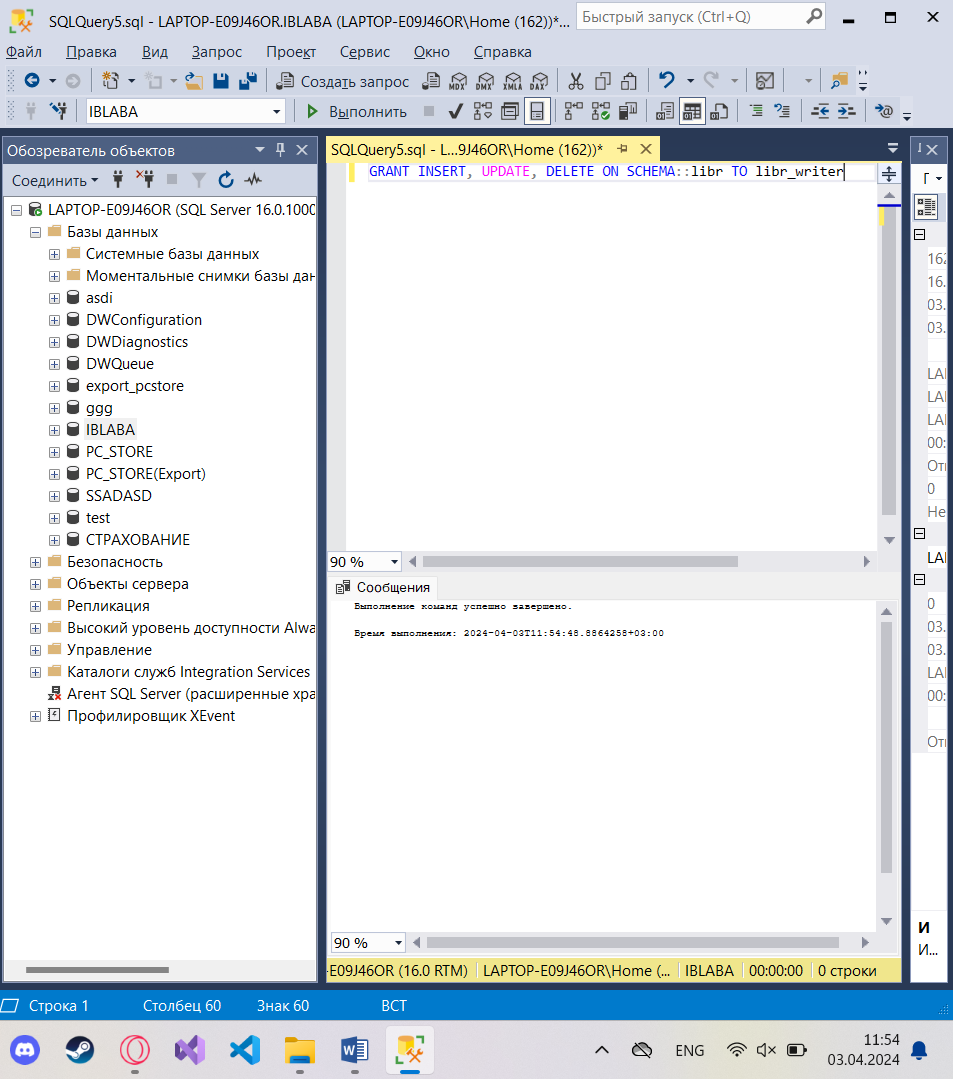


Рисунок 18 – Запрос на предоставление разрешения для роли

Далее идет запрос, который дает возможность пользователю изменять данные в обьектах схемы “libr”. Показано на рисунке 19.

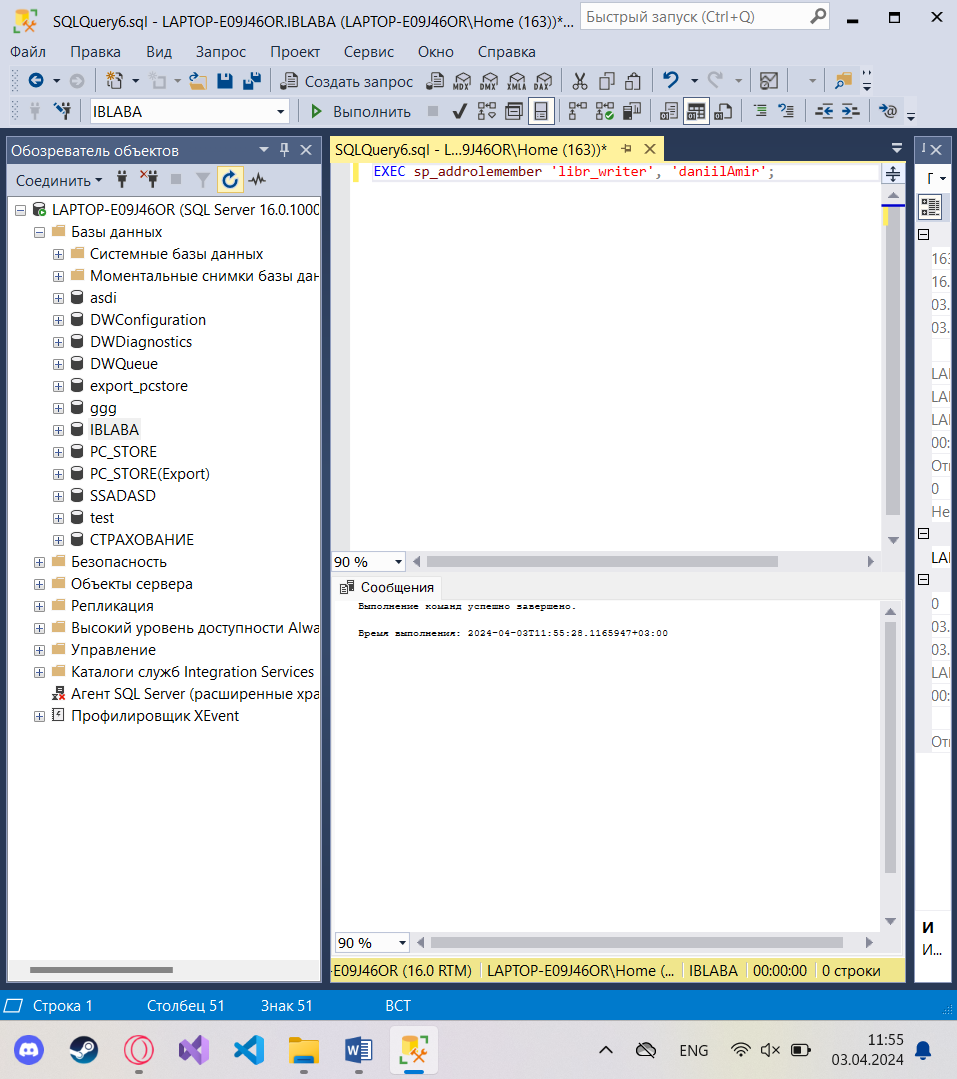


Рисунок 19 – Назначение роли

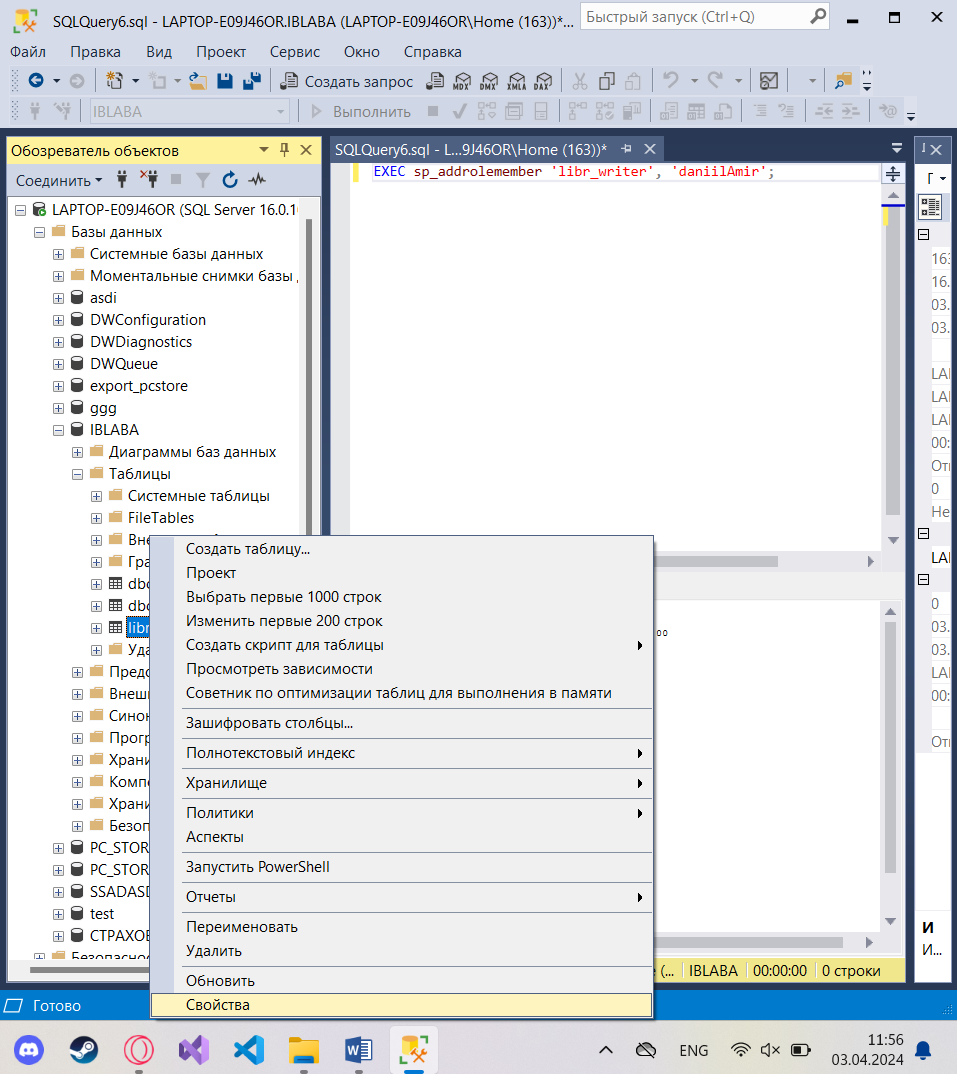


Рисунок 20 – Свойства

Назначаем разрешения для пользователя “daniilAmir”. Показано на рисунке 21.

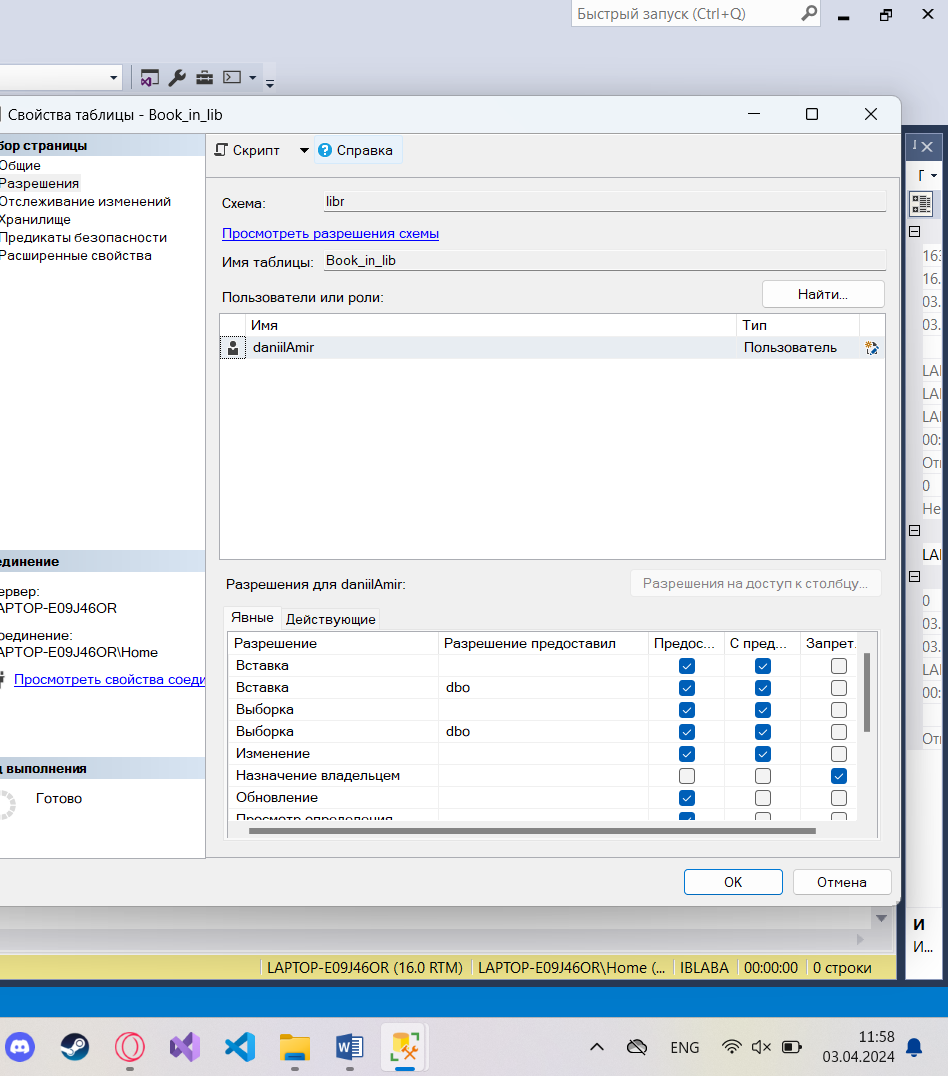


Рисунок 21 – Назначение разрешений для пользователя

Далее создаем запрос, чтобы предоставить пользователю "daniilAmir" право на обновление столбца "Title" в таблице "Book". Показано на рисунке 22.

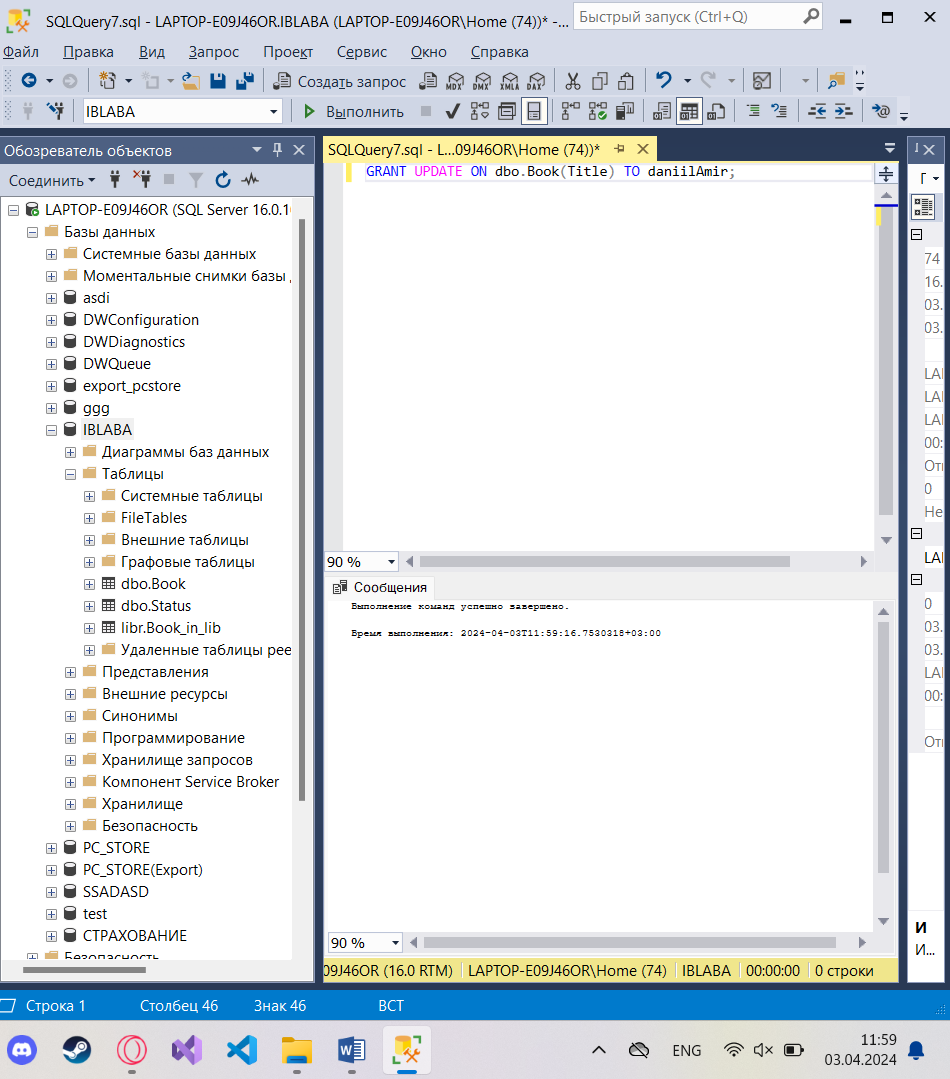


Рисунок 22 - Предоставление право.

Далее выполняется запрос на обновление столбцов. Показано на рисунке 23.

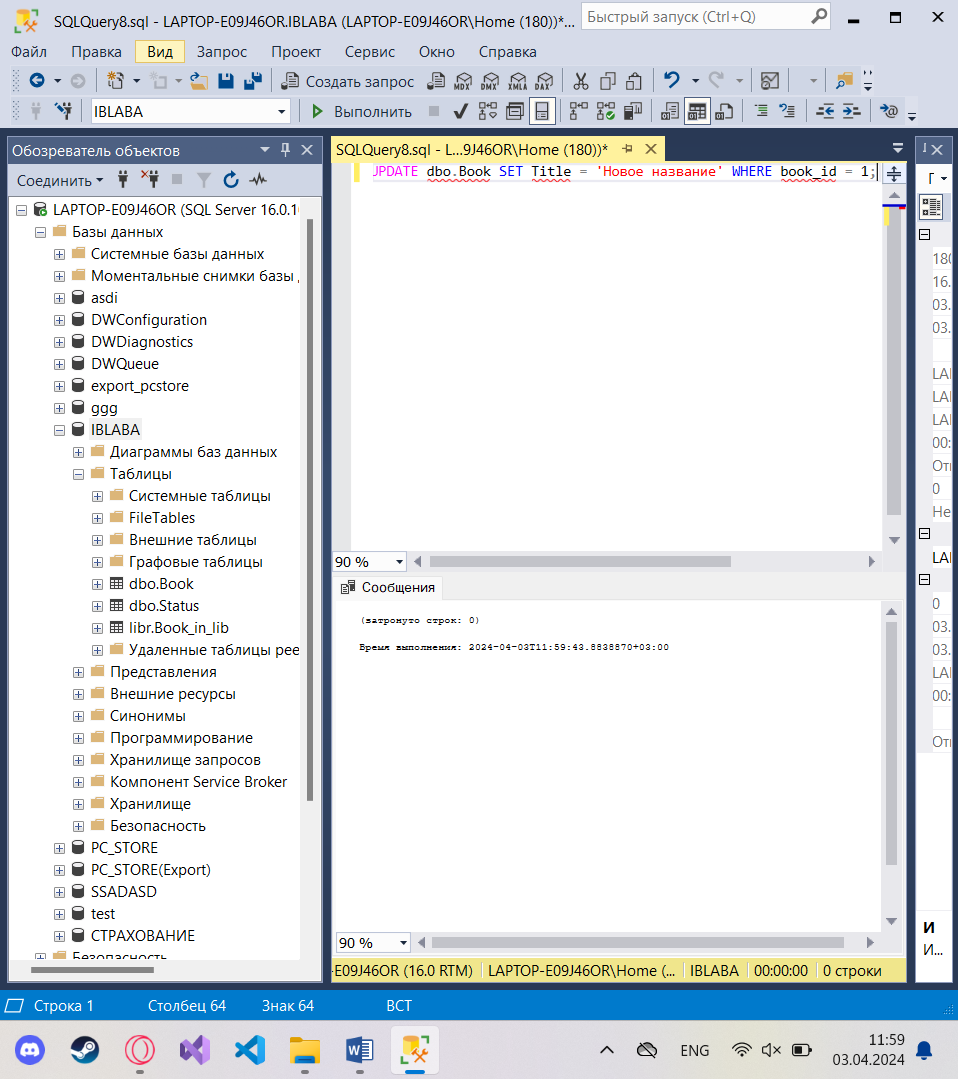


Рисунок 23 – Обновление столбцов

В запросе выполняется оператор CREATE VIEW для создания представления. Выбираем из таблицы "Book" только те книги, которые были изданы не ранее 2000 года. Показано на рисунке 24.

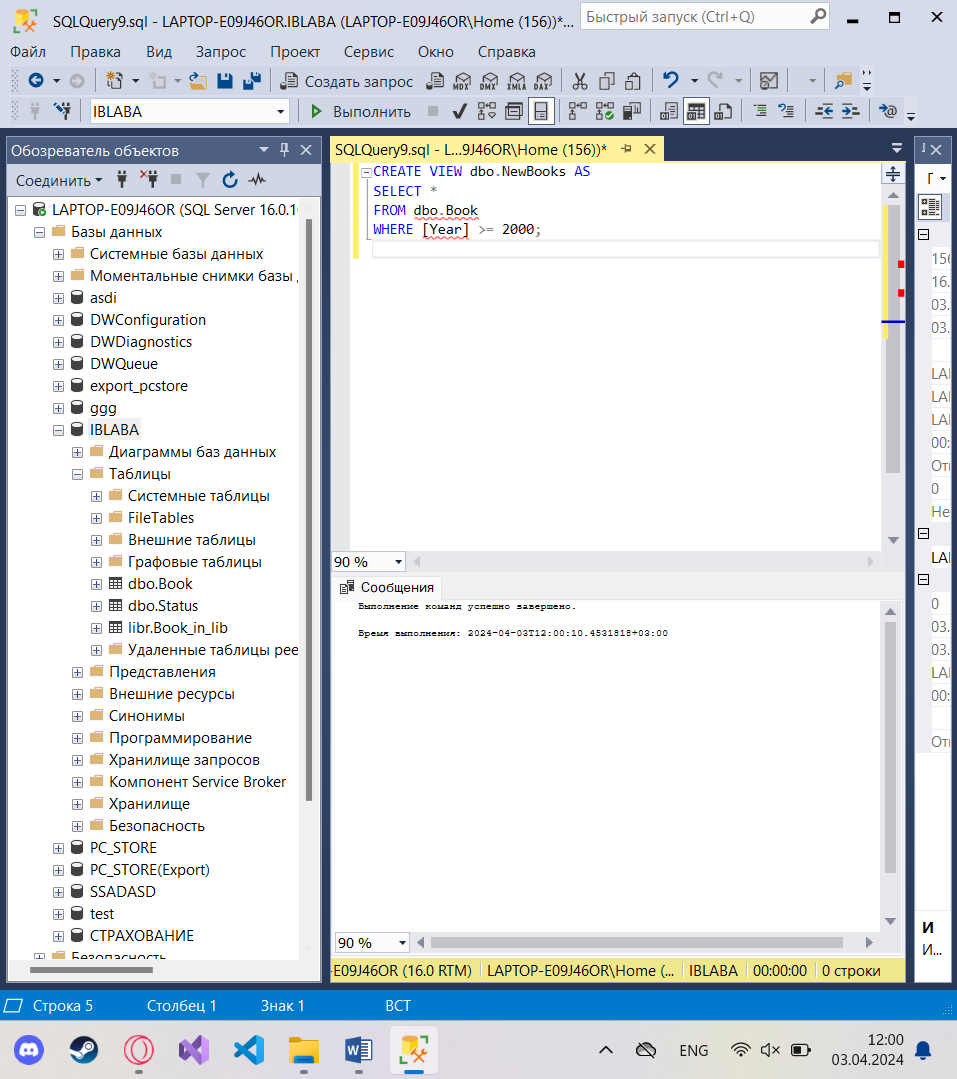


Рисунок 24 – Создание представлений

Далее представляем пользователю права на изменение и добавление записей в представление “NewBooks” на книги изданные не раньше 2000 года. Показано на рисунке 25.

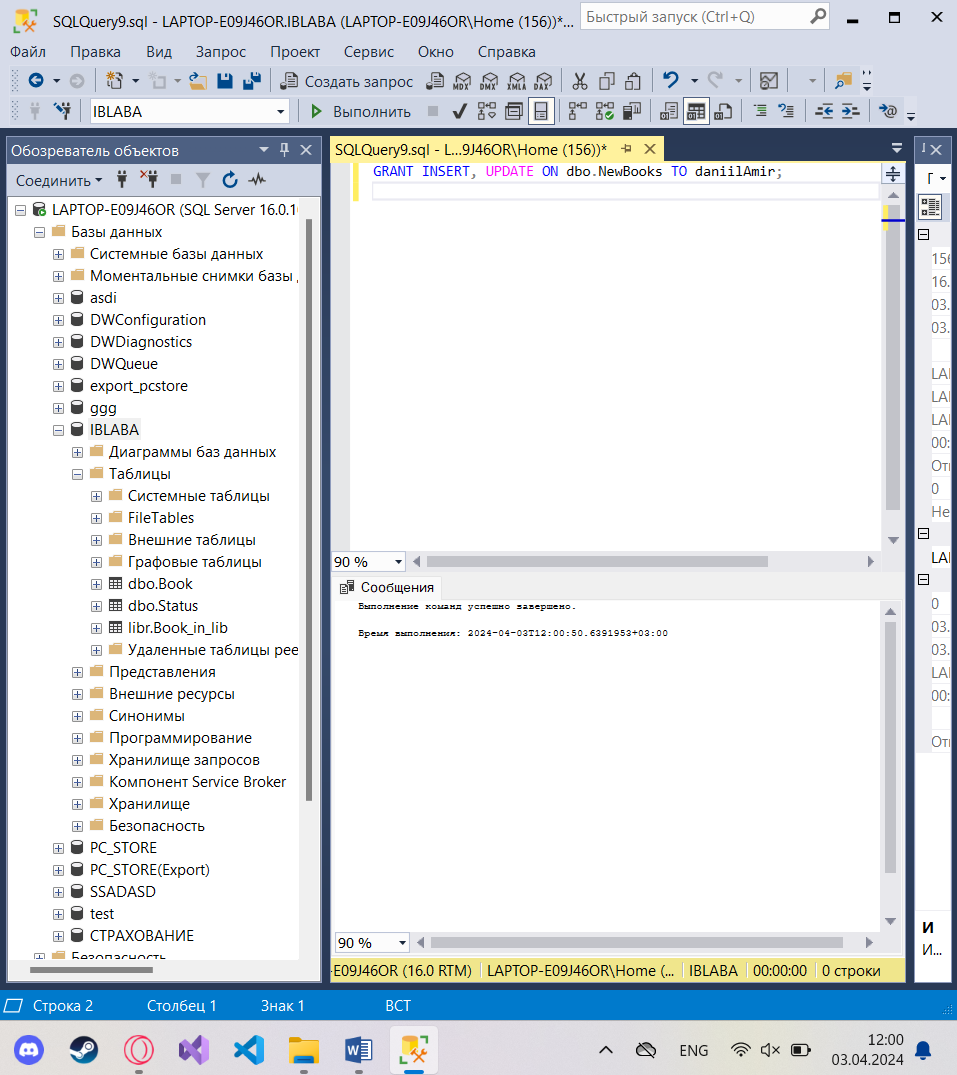


Рисунок 25 – Права на изменение записей.

Выполнив следующий запрос мы проверим права на изменение и добавление записей в представление “NewBooks”. Показано на рисунке 26.

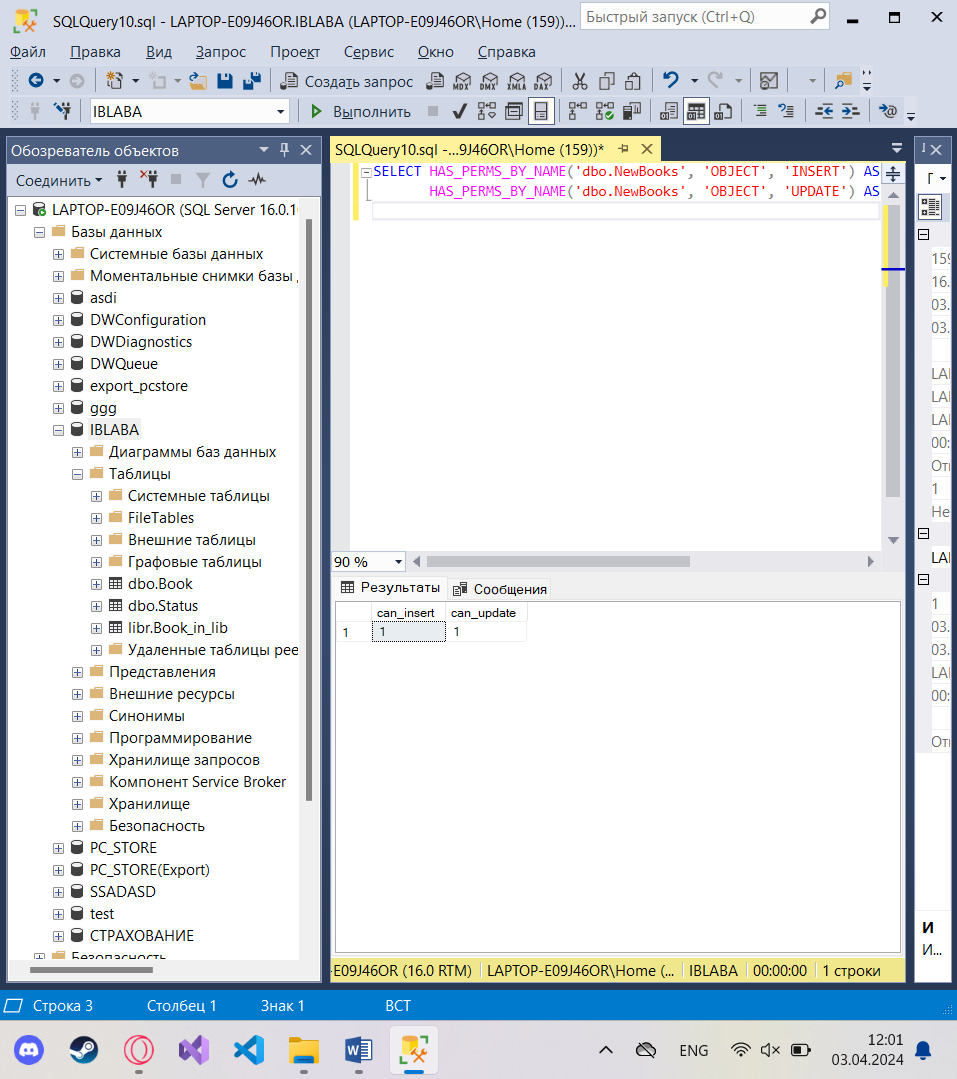


Рисунок 26 – Проверка прав пользователя.

**Вывод:** научились реализовывать доступ пользователя к бд.