МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ   
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №34

ОТЧЕТ ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, к.т.н. |  |  |  | В.А. Мыльников |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №4  **Организация разграничения доступа к объектам базы данных** |
|  |
| по курсу: БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 3843 |  |  |  | А.П.Конева |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2021

**Цель работы**

Ознакомление с основными механизмами организации доступа к объектам базы данных SQL сервера.

**Задача**

Организовать доступ к объектам базы данных.

**Механизм сетевой безопасности данных**

Рассмотрим архитектуру безопасности на примере сервера СУБД MS SQL Server. Для организации удаленного доступа к базе данных выполнили первоначальную настройку, представленную на Рис. 1.

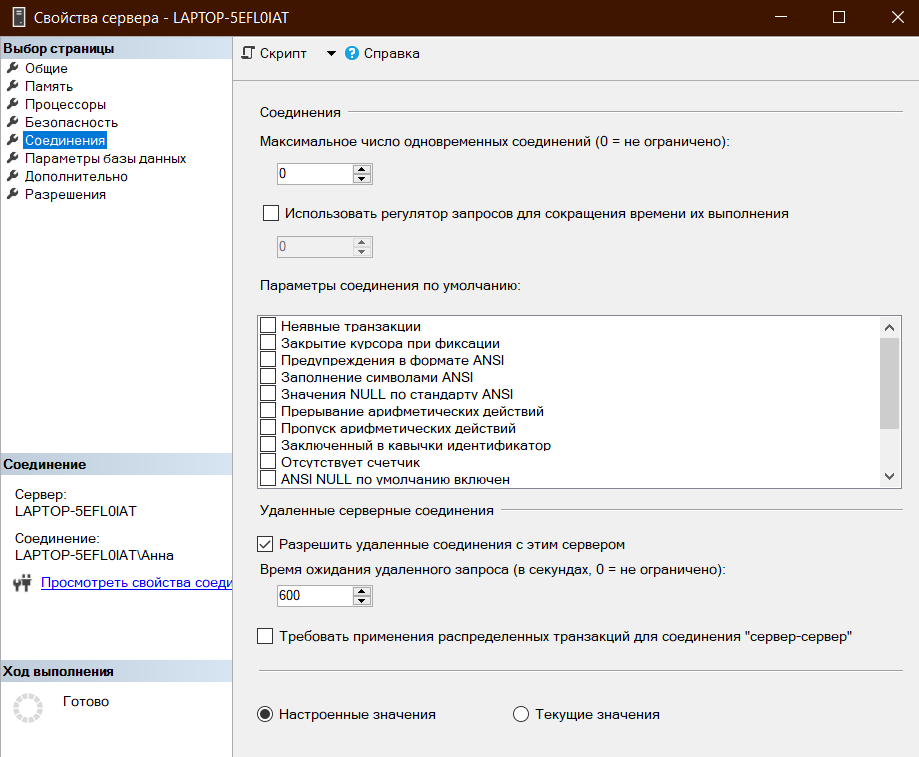


Рисунок 1 - Настройка удаленных соединений

На Рис. 2 показана настройка протоколов для установления удаленного соединения к базе данных: включенные протоколы «TCP/IP» и «Общая память».

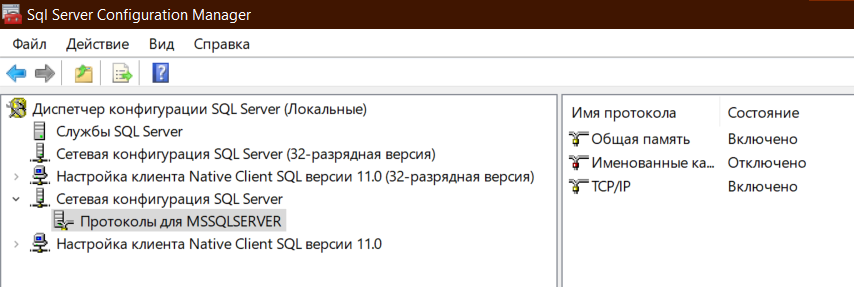


Рисунок 2 - Настройка протоколов подключения к серверу СУБД

На Рис. 3 изображена настройка аутентификации сервера.

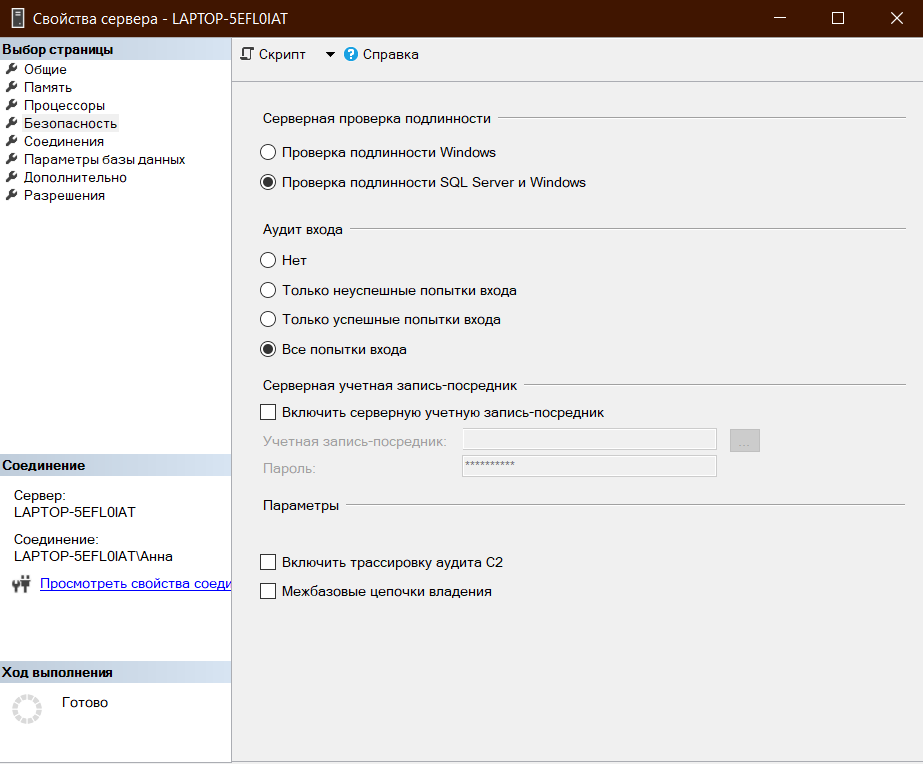


Рисунок 3 - Настройка аутентификации сервера

**Создание учетных записей**

На Рис. 4 показано создание пользователей с помощью языка Transact - SQL. Командой CREATE LOGIN создается учетная запись и пароль для работы с базой данных. Командой «CREATE USER» создается пользователь с присоединением к нему ранее созданной учетной записи. Создали следующих пользователей: Albus\_Dambldor, Severus\_Snape, Remus\_Lupin.

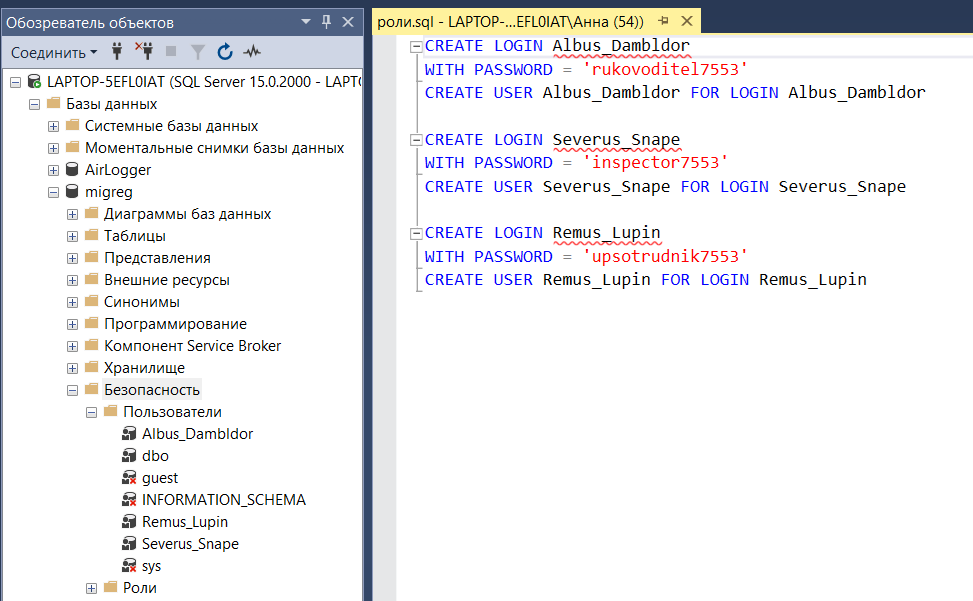
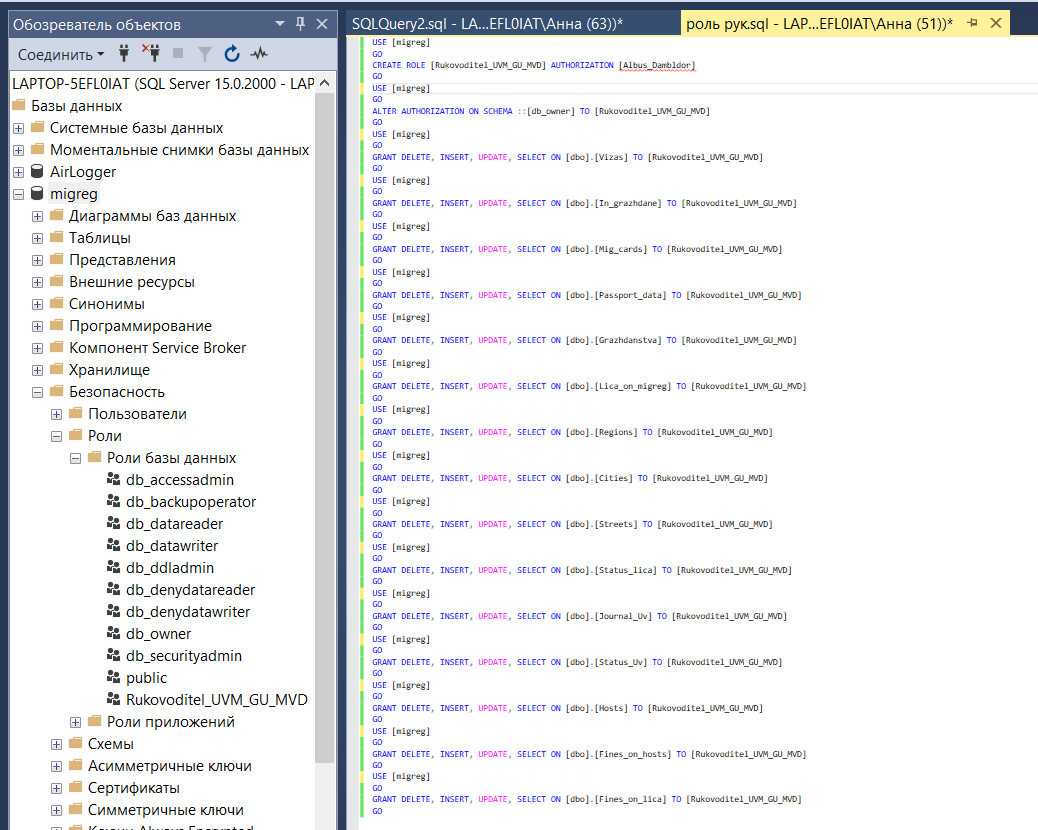
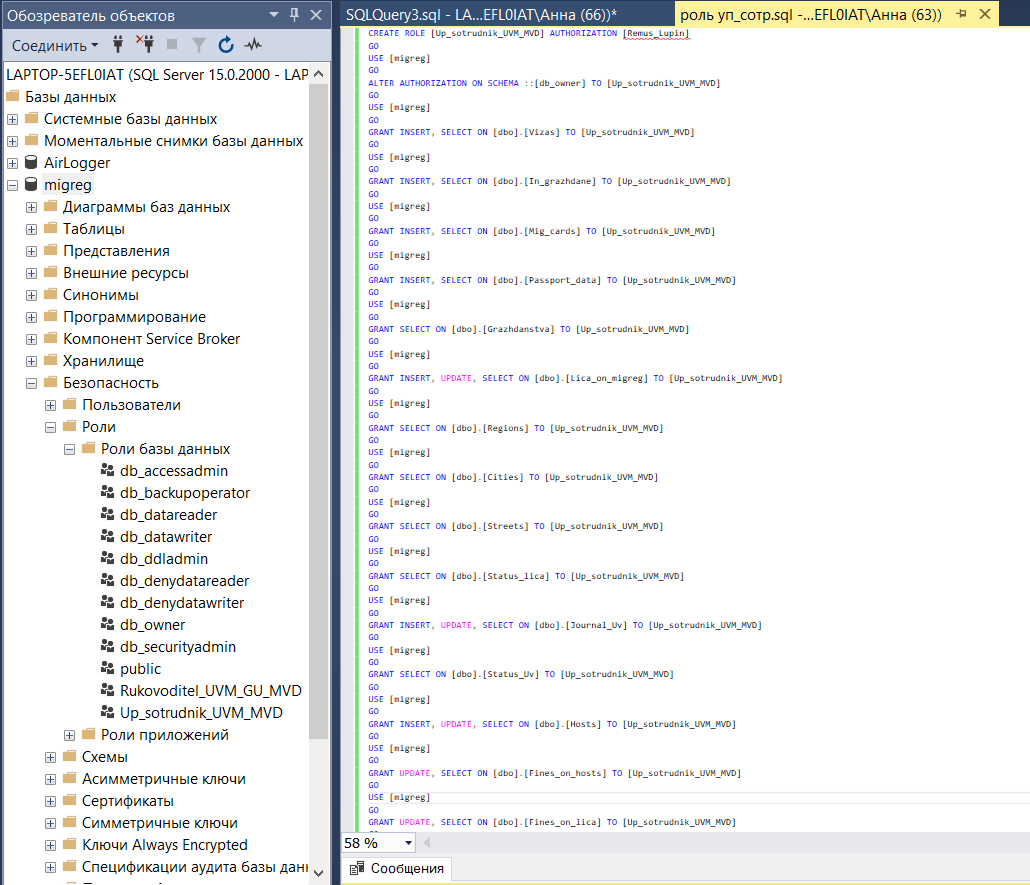
****

Рисунок 4 - Создание учетных записей

**Создание ролей**

На Рисунках 5-7 показано создание следующих ролей доступа к базе данных: Rukovoditel\_UVM\_GU\_MVD, Inspector\_UVM\_MVD, Up\_sotrudnik\_UVM\_MVD. Для каждого пользователя создается определенная роль с набором привилегий. Роли создавались в соответствии с Таблицами 1-3 из Лабораторной работы №3.

Рисунок 5 - Создание роли «Руководитель УВМ ГУ МВД»

Рисунок 6 - Создание роли «Уполномоченный сотрудник УВМ МВД»

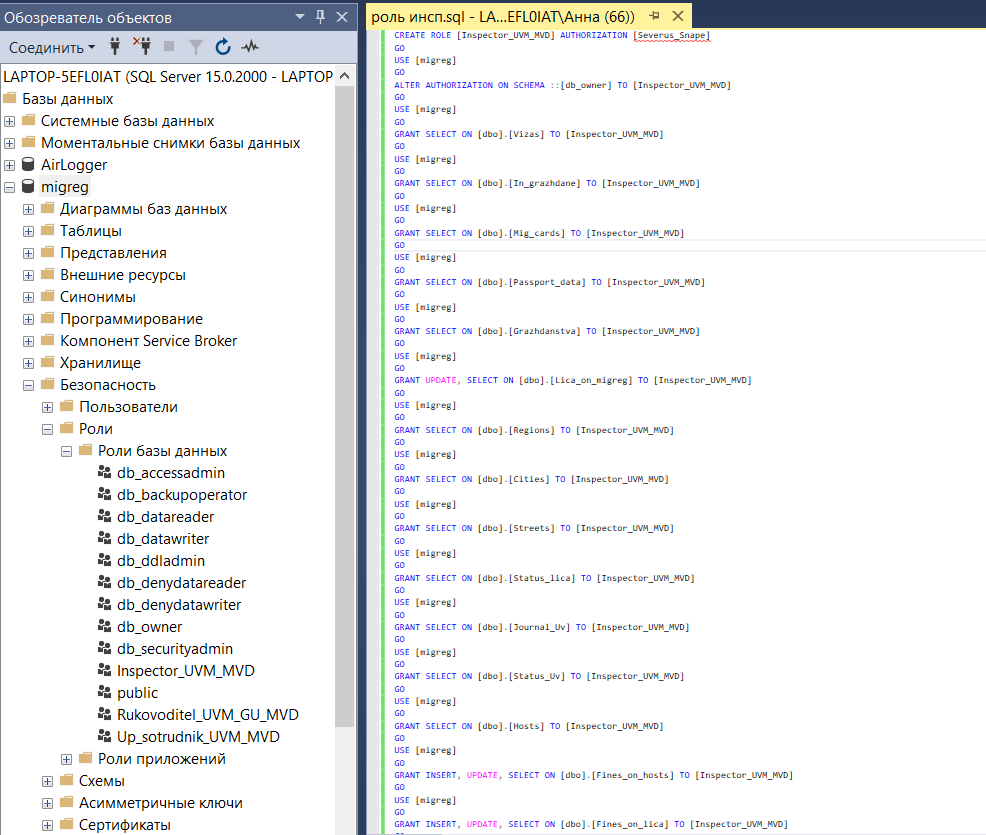


Рисунок 7 - Создание роли «Инспектор УВМ МВД»

На Рис. 8 - 10 можно увидеть результат создания необходимых ролей с определенными привилегиями.

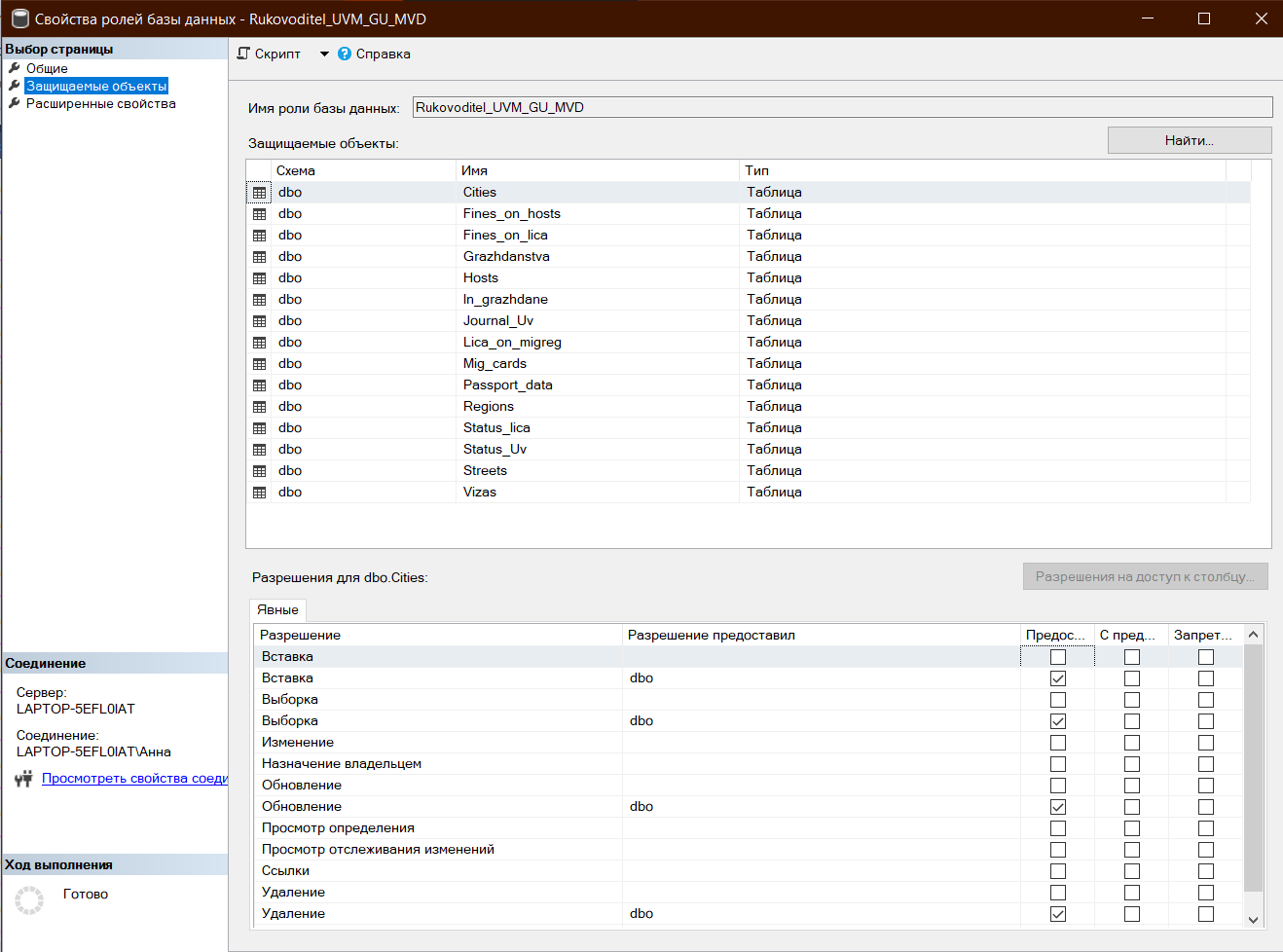
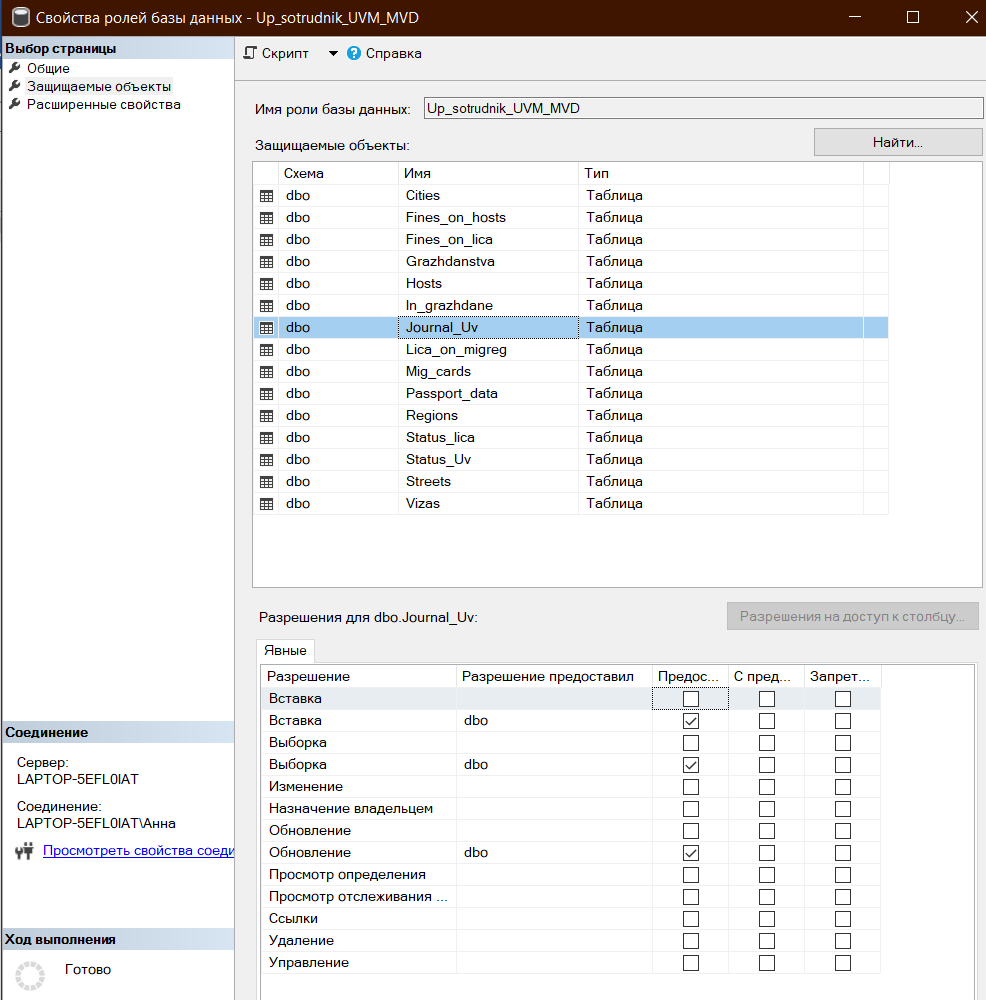
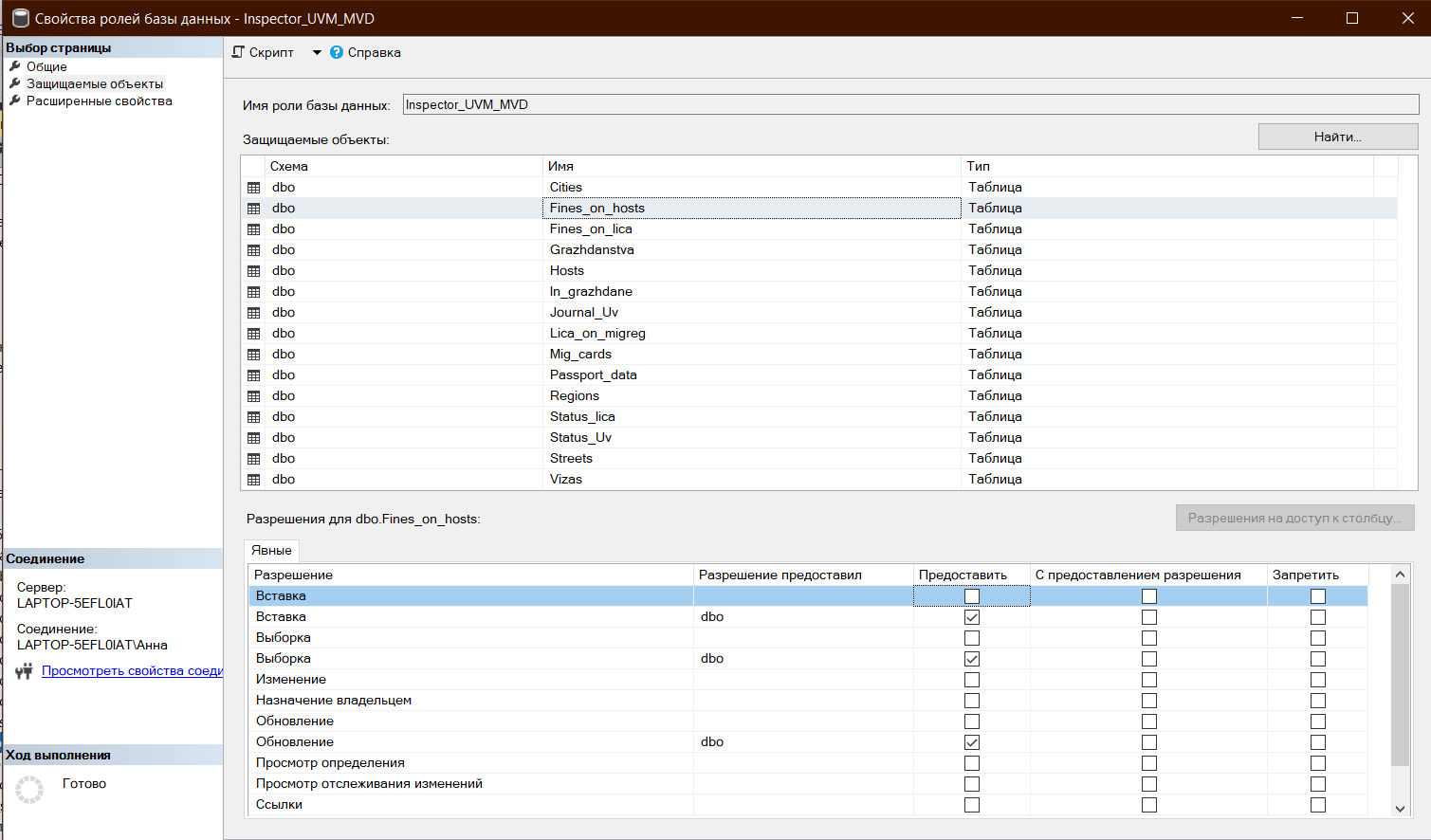
Рисунок 8 - Роль «Руководитель УВМ ГУ МВД»

Рисунок 9 - Роль «Уполномоченный сотрудник УВМ МВД»

Рисунок 10 - Роль «Инспектор УВМ МВД»

**Вывод**

Организовали доступ к объектам базы данных migreg. Спроектировали механизм сетевой безопасности базы данных (удаленный доступ, удаленные соединения, режим проверки подлинности, политику паролей) (Рис. 1-3). Создали следующих пользователей: Albus\_Dambldor, Severus\_Snape, Remus\_Lupin (Рис.4). Создали следующие роли директивного доступа (Рис. 5-7) в соответствии с Таблицами 1,2,3 из Лабораторной работы №3: Руководитель УВМ ГУ МВД, Уполномоченный сотрудник УВМ МВД, Инспектор УВМ МВД. Просмотрели результат создания необходимых ролей с определенными привилегиями (Рис. 8 - 10).