

ЛАБОРАТОРНАЯ РАБОТА № 5.

Система безопасности SQL Server.

Цель: научиться разграничивать доступ к данным в среде SQL Server Management Studio Express (использовать системные хранимые процедуры для управления именами входа MS SQL Server и пользователями баз данных, а также разрешать и запрещать выполнение определенных действий некоторому пользователю).

Программное обеспечение: SQL Server Management Studio Express

Задание:

1. Создание ролей и пользователей базы данных в SQL Server Management Studio.
2. Настройка разрешений с использованием операторов GRANT и REVOKE.

Задание 1: создать пользователя базы данных.

- 1) Откройте SQL Server Management Studio и раскройте узел **Безопасность** в окне **Обозреватель объектов**.
- 2) Щелкните узел **Имена входа**. Появляется список учетных записей пользователей, имеющих доступ к серверу баз данных.
- 3) Щелкните правой кнопкой узел **Имена входа** и выберите пункт меню **Создать имя входа...**. Появится окно “Создание имени входа”.
- 4) Введите информацию об учетной записи пользователя (см. рисунок 5.1) — введите свою фамилию. Обратите внимание на то, что выбрана аутентификация пользователя средствами SQL Server.

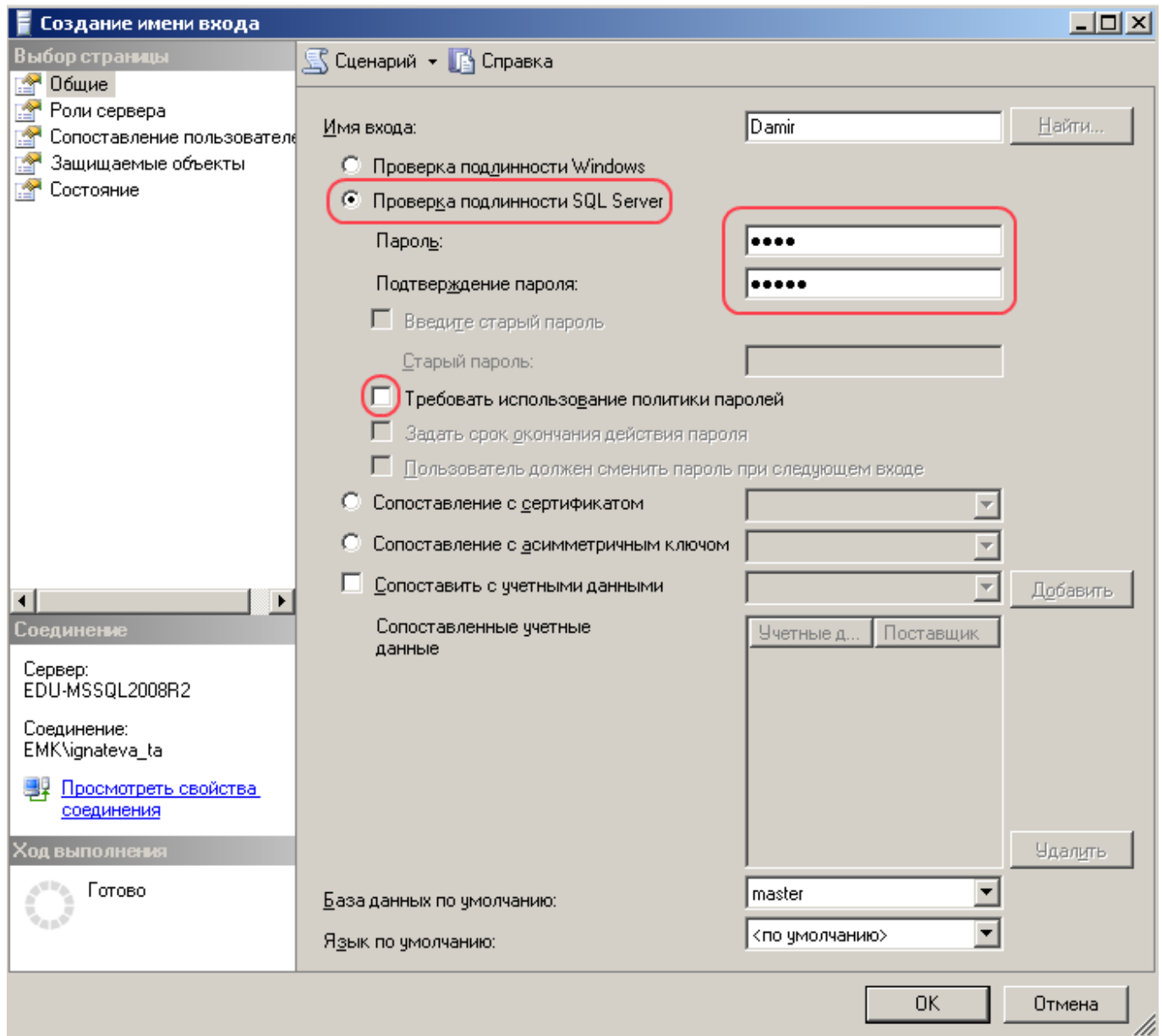


Рисунок 5.1 — Окно редактирования учетной записи пользователя

- 5) Щелкните страницу **Сопоставление пользователей** и предоставьте учетной записи доступ только к своей базе данных (см. рисунок 5.2).
- 6) Щелкните **OK**.

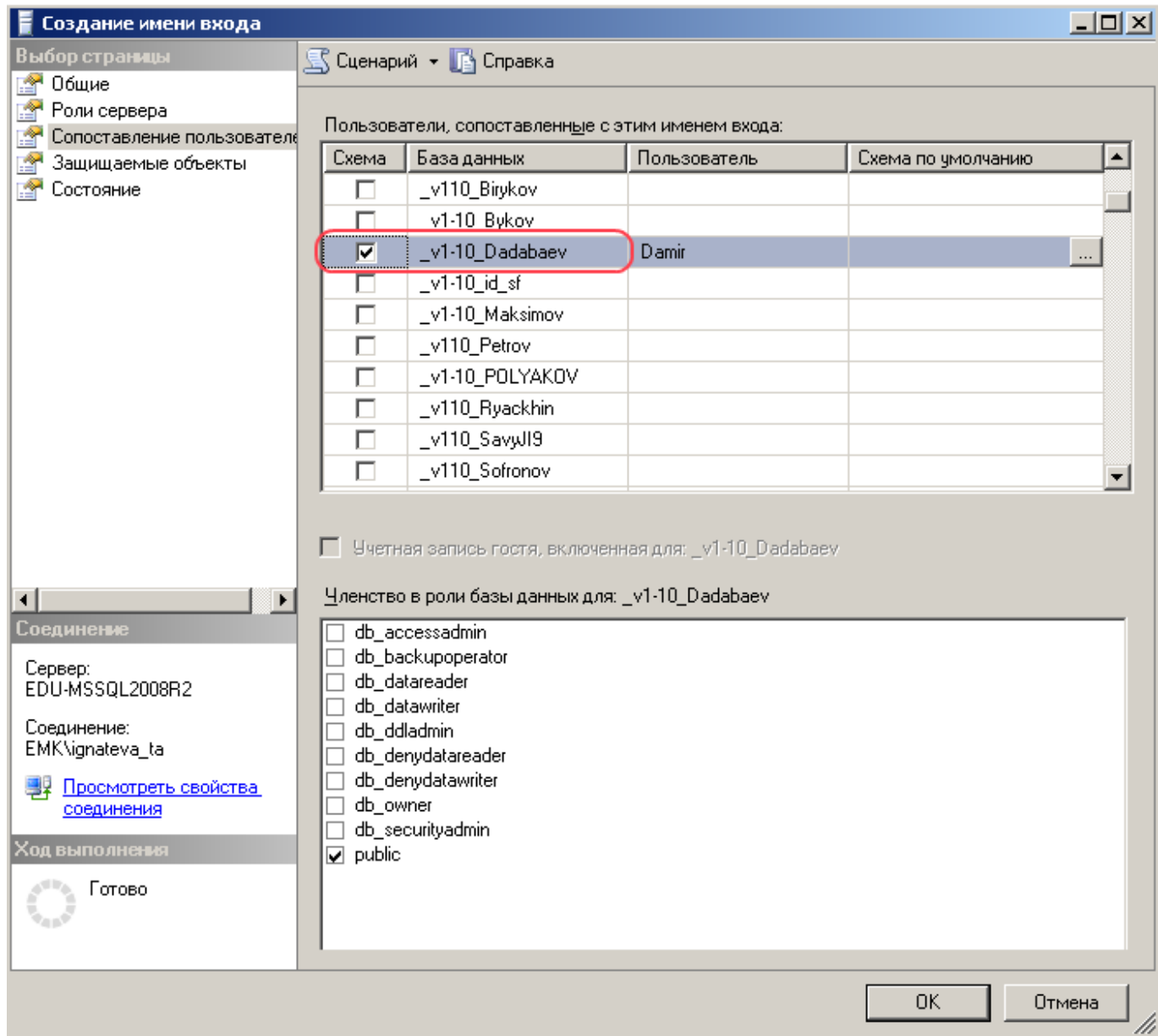


Рисунок 5.2 — Представление доступа к базе данных

- 7) Щелкните узел **Имена входа**. В список учетных записей пользователей добавлена учетная запись для пользователя с вашей фамилией.
- 8) Раскройте дерево в окне **Обозреватель объектов** до узла **Безопасность** своей базы данных.
- 9) Щелкните узел **Пользователи**. В список пользователей вашей базы данных добавлен пользователь с вашей фамилией (см. Рисунок 5.3).

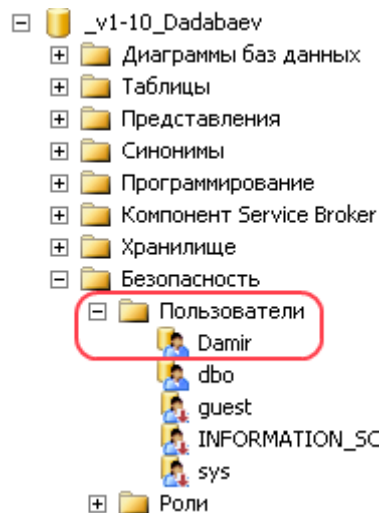


Рисунок 5.3 — Просмотр информации о пользователях базы данных

Задание 2: Создать роль “Оператор” в SQL Server Management Studio.

- 1) Раскройте дерево в окне **Обозреватель объектов** до узла **Безопасность** своей базы данных.
- 2) Щелкните узел **Роли**, затем щелкните узел **Роли базы данных**. Появится список ролей базы данных.
- 3) Щелкните правой кнопкой узел **Роли базы данных** и выберите пункт меню “Создать роль базы данных...”. Появится окно “Роль базы данных - создание”.
- 4) Наберите в текстовом поле “Имя роли” имя роли “Оператор”.
- 5) Щелкните на кнопке **Добавить...** для добавления пользователя к роли. Появится окно “Выбор пользователя или базы данных”.
- 6) Щелкните на кнопке **Обзор...** для выбора пользователя. Появится окно **Поиск объектов** со списком пользователей.
- 7) Выберите в списке своего пользователя (см. рисунок 5.4) и щелкните кнопку **ОК**.

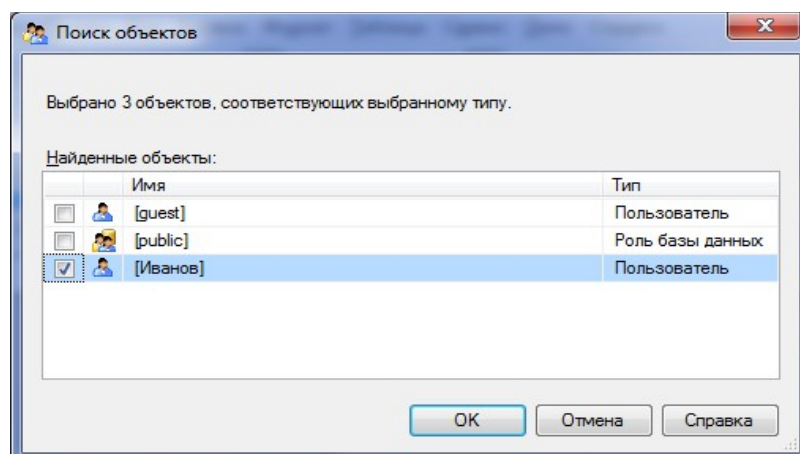


Рисунок 5.4 — Добавление пользователя к роли

- 8) Щелкните на кнопке **ОК**. К роли “Оператор” будет добавлен ваш пользователь (см. рисунок 5.5).

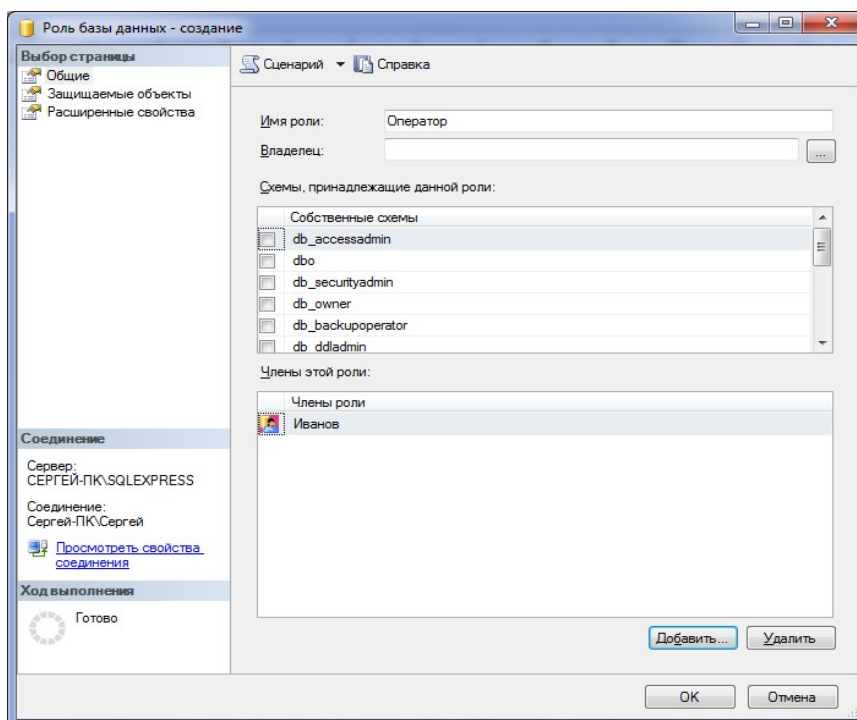


Рисунок 5.5 — Окно редактирование роли

- 10) Щелкните узел **Роли базы данных**. В список ролей базы данных добавлена роль “Оператор”.
- 11) Щелкните узел **Пользователи**. Обратите внимание на вашего пользователя в списке пользователей базы данных на правой панели.
- 12) Щелкните правой кнопкой вашего пользователя, затем щелкните пункт меню **Свойства**. Появится диалоговое окно “Пользователь базы данных - Фамилия”.
- 13) Просмотрите свойства вашего пользователя. Обратите внимание на роли, к которым принадлежит пользователь (см. рисунок 5.6).
- 14) Щелкните **ОК**.

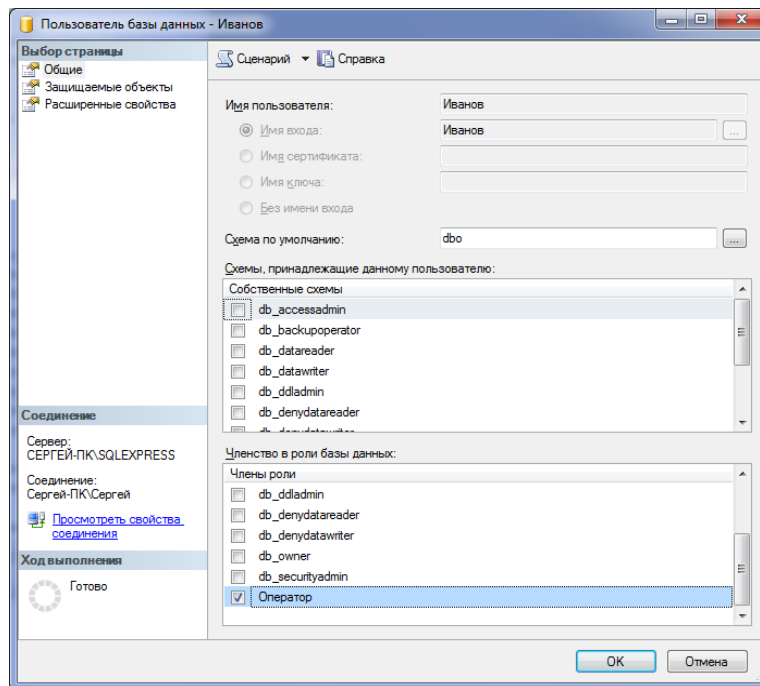




Рисунок 5.6 — Свойства пользователя Иванов

Задание 3: Настроить разрешения для роли “Оператор” с использованием оператора GRANT.

- 1) Отключитесь от сервера баз данных с помощью кнопки .
- 2) Подключитесь к серверу баз данных  под учетной записью пользователя с именем, совпадающим с Вашей фамилией.
- 3) Создайте и выполните запрос с кодом на языке SQL:

```
select * from Абитуриенты
```

- 4) На вкладке **Сообщения** выводится сообщение о запрете выполнения оператора select для таблицы Абитуриенты.
- 5) Выберите пункт меню “Файл”, затем “Отключить обозреватель объектов”.
- 6) Выберите пункт меню “Файл”, затем “Подключить обозреватель объектов ...” и подключитесь к серверу баз данных под учетной записью Windows.
- 7) На панели окна запроса введите и выполните следующий код на языке SQL:

```
grant select, insert, update
on Абитуриенты to Оператор
```

Оператор **grant** предоставляет разрешение пользователям роли “Оператор” на выполнение операторов select, insert, update на таблице Абитуриенты.

- 8) На вкладке **Сообщения** выводится сообщение об успешном завершении команды.

- 9) Выберите пункт меню “Файл”, затем “Отключить обозреватель объектов”.
- 10) Выберите пункт меню “Файл”, затем “Подключить обозреватель объектов ...” и подключитесь к серверу баз данных под учетной записью пользователя с именем, совпадающим с Вашей фамилией.
- 11) На панели окна запроса введите следующий код на языке SQL:

```
select * from Абитуриенты
```

- 12) Исполните введенный код SQL. На вкладке **Сообщения** выводится сообщение об успешном завершении команды.

Задание 4: Настроить разрешения для роли “Оператор” с помощью графического интерфейса в SQL Server Management Studio.

- 1) Откройте свойства роли “Оператор”.
- 2) В появившемся диалоговом окне "Свойства ролей базы данных — Оператор" откройте страницу **Защищаемые объекты**.
- 3) Щелкните на кнопке **Найти...** для добавления разрешений. Появится окно “Добавление объектов”. Щелкните на кнопке **ОК**.
- 4) Появится окно “Выбор объектов”. Щелкните на кнопке **Типы объектов**.
- 5) В окне “Выбор типов объектов” выберите в списке объектов **Таблицы** и щелкните кнопку **ОК** (см. рисунок 5.7).

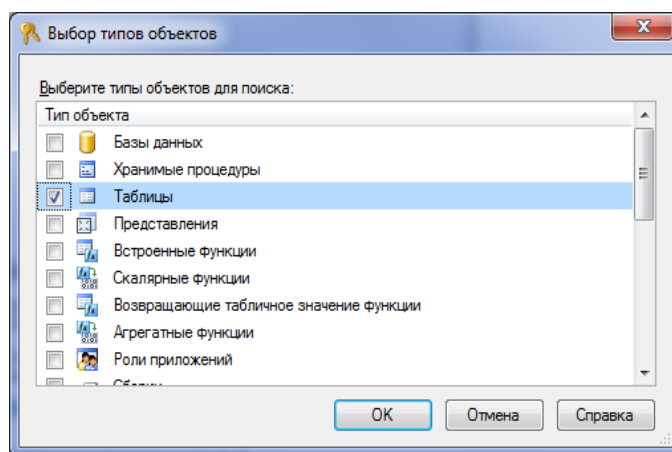


Рисунок 5.7 — Выбор типа защищаемых объектов

- 6) Щелкните на кнопке **Обзор...** для выбора таблицы. Появится окно “Поиск объектов” со списком таблиц.
- 7) Выберите в списке таблицу “Заявления” и щелкните кнопку **ОК**.

- 8) Включите разрешения на выполнения операторов select, update, insert, delete для таблицы “Заявления”.
- 9) Щелкните **ОК** и проверьте разрешения вашего пользователя, подключившись под его учетной записью.

Задание 5: Создайте роль “Методист” и предоставьте данной роли разрешение на выполнение всех действий с таблицами “Абитуриенты”, “Заявления”, “Оценки” и разрешение на выполнение оператора select на всех остальных таблицах.

Задание 6: Создайте и настройте учетную запись пользователя с помощью кода на языке SQL.

Указания к выполнению:

- 1) Создайте учетную запись пользователя с помощью хранимой процедуры **sp_addlogin**.

```
sp_addlogin 'Damir_SQL', 'Password_Damir'
```

- 2) Убедитесь, что учетная запись была добавлена при помощи хранимой процедуры **sp_helplogins**.
- 3) Попробуйте войти на сервер под созданной учетной записью.
- 4) Зайдите снова под учетной записью с аутентификацией **Windows**, т.к. для дальнейших действий снова потребуются права.
- 5) Присвойте учетной записи входа встроенной серверной роли с помощью процедуры:

```
sp_addsrvrolemember 'Damir_SQL', 'securityadmin'
```

Задание 7: Определите список ролей своей базы данных и членов роли **db_owner**.

Указания к выполнению:

- 1) Выполните хранимую процедуру **sp_helprole** для получения списка как встроенных, так и определенных пользователем ролей базы данных.
- 2) При помощи команды sp_helprolemember ‘db_owner’ определите членов роли db_owner.

Задание 8: Создайте нового пользователя базы данных для логина Damir_SQL.

Указания к выполнению:

- 1) При помощи хранимой процедуры добавьте пользователя:

```
sp_adduser 'Damir_SQL', 'Damir_user'
```

- 2) При помощи процедуры **sp_helpuser** убедитесь, что пользователь был добавлен. Какая роль ему была присвоена?
- 3) Добавьте пользователю роль **db_datareader**:

```
sp_addrolemember 'db_datareader', 'Damir_user'
```

Задание 9: Настройте права доступа пользователю Damir_User: предоставьте явным образом право только для выборки из таблицы Абитуриенты и обновления только полей *Фамилия*, *Имя* и *Отчество* этой таблицы.

Указания к выполнению:

- 1) С помощью следующей команды пользователю своей базы данных предоставляются права выборки данных таблицы Абитуриенты этой базы данных:

```
GRANT select on Абитуриенты to Damir_user
```

- 2) Следующая команда предоставляет пользователю права только изменения данных полей *Фамилия*, *Имя* и *Отчество* таблицы Абитуриенты своей базы данных:

```
GRANT update  
on Абитуриенты(Фамилия, Имя, Отчество)  
to Damir_user
```

Задание 10: Определите список всех ролей сервера и действия, разрешенные пользователям роли **dbcreator**.

Задание 11: Определите, пользователь какой роли имеет возможность создания и удаления учетных записей для входа.

Задание 12: Измените пароль учетной записи пользователя для входа с помощью процедуры **sp_password**.

Задание 13: Создайте собственную учетную запись для входа с подключением к своей базе данных, докажите правильность выполненных действий. Для созданной учетной записи присвойте права на создание и изменение баз данных, докажите правильность выполненных действий. Подключитесь к MS SQL Server, используя созданную учетную запись, и создайте еще одну учетную запись пользователя для входа, результат объясните.

Задание 14: Создайте пользователя *manager* своей базы данных на основе созданной ранее учетной записи для входа. Докажите правильность выполненных действий.

Задание 15: Пользователю *manager* присвойте роль, обладающую только возможностью просмотра содержимого своей базы данных.

Замечание. Для проверки правильности выполненных действий можно выполнить произвольный запрос к этой базе данных, например, отображающий содержимое таблицы.

Задание 16: Пользователю *manager* запретите просмотр данных своей БД, присвоив необходимую роль. Как доказать правильность внесенных изменений?

Контрольный вопрос: Какое количество пользователей базы данных может быть создано на основе одной учетной записи пользователя для входа? Ответ обоснуйте.

Контрольные задание на оценку “отлично”

- 1) Создайте учетную запись пользователя для входа на основе аутентификации SQL, подключающегося по умолчанию к вашей базе данных, имеющего права серверной роли **diskadmin**.
- 2) Определите список пользователей, входящих в роль **diskadmin** и ее разрешения.
- 3) В своей базе данных создайте пользователя на основе созданной ранее учетной записи для входа.
- 4) Для созданного ранее пользователя своей базы данных определите, членом какой роли он является и каково ее назначение. Имеет ли данный пользователь право выборки данных из таблицы *Заявления* этой базы данных? Ответ обоснуйте и проверьте, выполнив извлечение данных командой SELECT.
- 5) В своей базе данных создайте роль *managers*. Для этой роли определите право выборки данных из таблицы *Заявления* своей базы данных. Присвойте роль *managers* созданному ранее пользователю. Имеет ли теперь этот пользователь право выборки данных? Проверьте сделанный вывод. К каким еще объектам своей базы данных имеет право доступа этот пользователь? Обоснуйте и проверьте вывод.