**АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ**

**ИМ. Б.Л. РОЗИНГА (ФИЛИАЛ) СПбГУТ**

**(АКТ (ф) СПбГУТ)**

**Отчеты по лабораторным и практическим работам**

**МДК 11.01**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Студент | ИСПП-35 | |  |  | *Пожидаев Г.С.* |
|  | (Группа) | | (Подпись) | (Дата) | (И.О. Фамилия) |
| Преподаватель | | |  |  | *Маломан Ю. С.* |
|  | |  | (Подпись) | (Дата) | (И.О. Фамилия) |

Архангельск 2024

# **Лабораторная работа №10**

**Реализация доступа пользователей к базе данных**

1. **Цель работы** 
   1. Научиться использовать системные хранимые процедуры и DDL-команды для управления именами входа и пользователями БД в СУБД;
   2. Научиться назначать привилегии пользователю БД;
   3. Закрепить навык создания объектов БД.
2. **Контрольные вопросы**

Вопрос: В чем отличие между именами входа и пользователями БД?

Отличия между именами входа и пользователями базы данных в MS SQL Server:

1. Имя входа:

- Это имя, которое используется для аутентификации при подключении к серверу.

- Оно не связано напрямую с конкретной базой данных.

2. Пользователь БД:

- Это отдельный объект внутри конкретной базы данных.

- Может иметь свои права доступа и разрешения на уровне базы данных.

Основные различия:

- Имя входа применяется на уровне сервера, пользователь БД - на уровне базы данных.

- Имя входа может быть использовано для доступа ко всем базам данных на сервере, пользователь БД ограничен одной базой данных.

- Права доступа могут быть назначены отдельно для имени входа и пользователя БД.

Вопрос: 8.2 Как идентифицируются пользователи в MS SQL Server?

В MS SQL Server пользователи могут быть идентифицированы следующими способами:

1. Имя входа (Login):

- Это уникальное имя пользователя, которое используется для аутентификации.

- Пример: 'john\_doe'

2. Пароль:

- Секретный код, который пользователь должен знать для аутентификации.

3. Учетная запись Windows:

- Возможность использования учетных данных из Active Directory.

- Пользователи могут аутентифицироваться с помощью имени пользователя и пароля Windows.

4. Сертификаты:

- Возможность использования цифровых сертификатов для шифрования паролей.

5. Azure AD:

- Поддержка аутентификации через Azure Active Directory.

Вопрос: 8.3 На какие уровни разделяется система безопасности MS SQL Server?

Система безопасности в MS SQL Server разделена на несколько уровней:

1. Сетевой уровень:

- Определяет, может ли клиент подключиться к серверу.

- Контролируется через сетевые протоколы и файрволы.

2. Серверный уровень:

- Управление правами доступа к серверу.

- Контролируется через SQL Server Configuration Manager.

3. Базовый уровень:

- Управление правами доступа в конкретных базах данных.

- Контролируется через объекты базы данных (пользователи, роли).

4. Объектный уровень:

- Права доступа к отдельным объектам в базе данных (таблицы, процедуры и т.д.).

5. Программный уровень:

- Безопасность приложений, использующих SQL Server.

Вопрос: 8.4 Каково назначение ролей сервера?

Роли сервера в MS SQL Server используются для:

1. Управления правами доступа к серверу.

2. Контроля над ресурсами сервера.

3. Определения уровня привилегий пользователей.

4. Управления доступом к системным объектам и функциям.

5. Контроля над выполнением определенных операций на сервере.

Примеры ролей сервера:

- sysadmin: полные права управления сервером

- serveradmin: управление конфигурацией сервера

- setupadmin: управление установкой и настройкой сервера

- securityadmin: управление правами безопасности

- processadmin: управление процессами SQL Server

Вопрос: Каково назначение ролей БД?

Роли базы данных в MS SQL Server используются для:

1. Управления правами доступа к объектам базы данных.

2. Контроля над выполнением определенных операций в рамках базы данных.

3. Определения уровня привилегий пользователей.

4. Группировки пользователей с схожими потребностями в правах доступа.

5. Упрощения управления правами доступа на уровне базы данных.

Примеры ролей базы данных:

- db\_owner: полные права доступа ко всем объектам базы данных

- db\_datareader: чтение данных во всех таблицах

- db\_datawriter: запись данных во все таблицы

- db\_ddladmin: выполнение DDL-запросов

- db\_securityadmin: управление правами безопасности

1. **Вывод**
   1. В ходе лабораторной работы мы научились использовать системные хранимые процедуры и DDL-команды для управления именами входа и пользователями БД в СУБД;
   2. Научились назначать привилегии пользователю БД;
   3. Закрепили навык создания объектов БД.