Практическое занятие 2. Назначение ролей сервера и базы данных ответ.

**1. В чем разница между логином и пользователем БД?**

**2. Какие системные роли позволяют создавать новые базы данных?**

**3. Как ограничить доступ пользователя к определенным столбцам таблицы?**

**4. Что такое принцип минимальных привилегий и почему он важен?**

1. В чём разница между логином и пользователем БД?

Логин (login) представляет собой учётную запись, используемую для подключения к серверу базы данных (например, SQL Server). Логины управляются непосредственно самим сервером и предоставляют доступ к нему.

Пользователь же (database user) — это отдельная сущность внутри каждой отдельной базы данных, связанная с логином. Именно пользователям предоставляются разрешения на выполнение операций с объектами базы данных (таблицами, представлениями и прочими элементами).

Таким образом, логин даёт право подключиться к серверу, а пользователь определяет, какие именно действия возможны внутри конкретных баз данных.

2. Какие системные роли позволяют создавать новые базы данных?

Создание новых баз данных связано с правами администратора. Основные системные роли, дающие такую возможность:

sysadmin — роль сервера, позволяющая управлять всеми аспектами работы SQL Server, включая создание баз данных.

dbcreator — специальная роль, предназначенная исключительно для создания и удаления баз данных.

Эти роли имеют достаточно высокий уровень полномочий, поэтому ими наделяют только доверенных администраторов.

3. Как ограничить доступ пользователя к определенным столбцам таблицы?

Чтобы ограничить доступ пользователя к отдельным столбцам таблицы, используется механизм присвоения специальных привилегий (GRANT / DENY). Например, можно предоставить разрешение на чтение только некоторых столбцов и запретить доступ ко всем остальным.

Пример команды SQL для предоставления доступа к одному столбцу (column\_name) таблицы (table\_name) пользователю (username):GRANT SELECT ON table\_name(column\_name) TO username;

Аналогично можно добавить дополнительные разрешения или запретить доступ другим столбцам.

Также существует возможность создать специальный view (представление), содержащий только разрешенные столбцы, и предоставить пользователю доступ только к этому view.

4. Что такое принцип минимальных привилегий и почему он важен?

Принцип минимальных привилегий гласит, что каждому пользователю (или процессу) следует предоставлять ровно столько полномочий, сколько необходимо для выполнения возложенных на него задач. Этот принцип направлен на снижение риска негативных последствий от возможных компрометаций аккаунтов или внутренних ошибок.

Причина важности принципа минимальных привилегий заключается в следующем:

Уменьшается потенциальный ущерб от атаки или человеческого фактора.

Ограничиваются возможности распространения уязвимости.

Повышаются общая защищённость и управляемость инфраструктуры.

Например, рядовому сотруднику бухгалтерии совершенно необязательно давать полный административный доступ к серверам предприятия. Достаточно назначить минимальный набор необходимых привилегий для выполнения ежедневных задач.