Запросы SQL, используемые для управления безопасностью

Лекция 10

Цель

обеспечения безопасности доступа к базе данных – защитить информацию от неавторизованного использования. В процессе ее осуществления администратор БД должен решить, какие пользователи и с какими объектами БД могут совершать определенные действия.

Эти права доступа, предоставленные пользователям, называются **привилегиями** БД.

Требования к безопасности БД

- данные в любой таблице должны быть доступны не всем пользователям, а лишь некоторым из них;
- некоторым пользователям разрешено обновлять данные в таблицах, в то время как другие допускаются лишь к выборке данных из этих же таблиц;
- для некоторых таблиц необходимо обеспечить выборочный доступ к ряду ее столбцов;
- некоторым пользователям должен быть запрещен непосредственный (через запросы) доступ к таблицам, но разрешен доступ к этим же таблицам в диалоге с прикладной программой.

Пользователи

- *Прикладные программисты;*
- *Конечные пользователи,* получающие доступ к базе данных с помощью одного из интерактивных приложений или же интерфейса, интегрированного в ПО самой СУБД;
- *Администраторы баз данных,* работа которых заключается в создании самих баз данных и организации технического контроля, необходимого для обеспечения решений, принятых при проектировании базы данных. Они (он) несут также ответственность за обеспечение необходимого быстродействия системы, ее техническое обслуживание и защиту данных

Привилегии в СУБД

1. *Системные привилегии* позволяют пользователям выполнять определенное действие на уровне системы или над конкретным типом объектов.
2. *Объектные привилегии* позволяют пользователям выполнять определенные действия с конкретным объектом. Объектные привилегии назначаются конечным пользователям для того, чтобы они могли работать с приложениями к базе данных для решения конкретных задач.

Предложение GRANT

Это предложение назначает пользователям и ролям привилегии, которые позволяют им обращаться к объектам базы данных и использовать их (т. е. объектные привилегии).

Синтаксис предложения GRANT

GRANT { {объектная_привилегия [,...]| роль [,...]} }

[ON имя_объекта_базы]

[TO получающий_привилегию [,...]]

[WITH GRANT OPTION | WITH ADMIN OPTION];

Стандартные привилегии

- ALL PRIVILEGES — краткое обозначение всех привилегий, которое не рекомендуется использовать, поскольку это способствует неаккуратному назначению прав доступа;
- EXECUTE — предоставляется право запускать хранимую процедуру, пользовательскую функцию или пакет (см. главу 18);
- { SELECT | INSERT | UPDATE | DELETE } — предоставляется право выполнять соответствующие операции применительно к указанному объекту базы данных (таблице, представлению и пр.);
- REFERENCES — предоставляется право определять ограничения, обеспечивающие ссылочную целостность.

указание WITH GRANT OPTION или WITH ADMIN OPTION предоставляет получателям права передавать привилегии другим пользователям.

Роль

— это именованный набор привилегий, которые можно присваивать пользователям и другим ролям базы данных.

Если роль назначается пользователю, этот пользователь получает все привилегии и допуски, содержащиеся в данной роли.

Роли повсеместно используются как один из лучших способов обеспечения безопасности и управления привилегиями в базе данных.

Роль должна быть заранее создана с помощью предложения CREATE ROLE.

ON *имя_объекта_базы*

Привилегии присваиваются для доступа к конкретному существующему объекту базы данных (имя_объекта_базы).

К объектам базы данных относятся: таблицы, представления, последовательности, хранимые процедуры и т. д.

ТО *получатель_привилегии*

Привилегия присваивается указанному в получатель_привилегии пользователю или роли.

Можно присваивать привилегии нескольким пользователям и (или) ролям, для чего их разделяют запятыми.

В качестве альтернативы можно присвоить привилегии с ключевым словом *PUBLIC*, это означает, что все пользователи (в том числе и те, которые появятся в будущем) будут иметь указанные привилегии.

Предложение REVOKE

служит для отмены назначенных привилегий и ролей.

Синтаксис предложения REVOKE

REVOKE { {привилегия [,...]| роль [,...]} }
[ON имя_объекта_базы]
[FROM имя_получателя [,...]];