Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Лекция №4

каф. КИБЭВС
И.В. Горбунов

Управление доступом

Каждая СУБД должна поддерживать механизм, гарантирующий, что *доступ* к базе данных смогут получить только те *пользователи*, которые имеют соответствующее разрешение.

В языке SQL предусмотрен набор операторов, предназначенный для организации защиты таблиц в базе данных:

GRANT

REVOKE

Механизм защиты построен на использовании:

- идентификаторов пользователей;
- предоставляемых прав;
- привилегии.

Идентификатором пользователя называется обычный идентификатор языка SQL, применяемый для обозначения некоторого *пользователя* базы данных.

Каждому *пользователю* назначается собственный **(уникальный)** *идентификатор*, присваиваемый администратором базы данных.

Идентификатор пользователя **связывается с *паролем*.**

Каждый выполняемый СУБД SQL-оператор выполняется **от имени какого-либо *пользователя***.

Идентификатор пользователя определяет, на какие объекты базы данных *пользователь* может ссылаться и какие операции с этими объектами он имеет *право* выполнять.

Каждый созданный SQL-объект имеет своего *владельца*, который **изначально** является единственной персоной, знающей о существовании данного объекта и имеет *право* выполнять с ним **любые операции**.

Привилегиями, или ***правами***, называются действия, которые *пользователь* имеет *право* выполнять в отношении **данной таблицы** базы данных или представления.

В стандарте SQL определяется следующий набор *привилегий*:

SELECT – *право* выбирать данные из таблицы;

INSERT – *право* вставлять в таблицу новые строки;

UPDATE – *право* изменять данные в таблице;

DELETE – *право* удалять строки из таблицы;

REFERENCES – *право* ссылаться на столбцы указанной таблицы в описаниях требований поддержки целостности данных;

USAGE – *право* использовать домены, проверки и

Привилегии **INSERT** и **UPDATE** могут ограничиваться лишь отдельными столбцами таблицы, в этом случае *пользователю* разрешается модифицировать значения только указанных столбцов.

Привилегия **REFERENCES** распространяется исключительно на отдельные столбцы таблицы, что позволяет использовать их имена в формулировках требований защиты целостности данных (например для CHECK и FOREIGN KEY при определении в других таблицах).

Когда *пользователь* с помощью оператора **CREATE TABLE** создает новую таблицу, он автоматически становится ее *владельцем* и получает по отношению к ней полный набор *привилегий.*

Для обеспечения *доступа* пользователям, *владелец* должен явным образом предоставить необходимые *права*, для чего используется оператор GRANT.

Предоставление привилегий пользователям

Оператор GRANT применяется для ***предоставления привилегий*** в отношении поименованных объектов базы данных указанным *пользователям*. Обычно его использует *владелец* таблицы с целью *предоставления доступа* к ней другим *пользователям* .

Предоставление привилегий пользователям

Оператор GRANT имеет следующий формат:

<предоставление_привилегий>::=

GRANT {<привилегия>[,...n] | ALL PRIVILEGES}

ON имя_объекта TO {<идентификатор_пользователя> [,...n]| PUBLIC}

[WITH GRANT OPTION]

ALL PRIVILEGES – все привилегии для указанного пользователя

PUBLIC – всем пользователям, существующим и создаваемым заново

WITH GRANT OPTION – право передачи привилегий другим пользователям, указанных в операторе GRANT

Предоставление привилегий пользователям

Параметр <привилегия> представляет собой:

<привилегия>::=

{SELECT | DELETE | INSERT [(имя_столбца[,...n])] | UPDATE [(имя_столбца[,...n])]} |

REFERENCES [(имя_столбца[,...n])] |

USAGE }

Отмена предоставленных пользователям привилегий

Оператор REVOKE имеет следующий формат:<отмена_привилегий>::=

REVOKE [GRANT OPTION FOR] {<привилегия>[,...n] | ALL PRIVILEGES}

ON имя_объекта

FROM {<идентификатор_пользователя> [,...n]|PUBLIC}

[RESTRICT | CASCADE]

ALL PRIVILEGES – отмена всех привилегий предоставленных ранее

GRANT OPTION FOR – отменяет возможность передачи привилегий

RESTRICT – успешно выполняется команда REVOKE если привилегии не образуют у других пользователей «оставленных» привилегий.

CASCADE – удаляет все привилегии, которые остались у других пользователей

Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Спасибо за внимание!!!