Лабораторная работа № 9.
Контроль доступа к базе данных

Цель работы

Целью выполнения данной лабораторной работы является изучение операторов для создания представлений таблиц и получение навыков их использования.

Теоретические сведения

Привилегии пользователей назначаются им администратором базы данных и определяют,какие действия над данными и над объектами схемы являются разрешенными. При контроле привилегий используется имя пользователя базы данных, называемое иногда идентификатором авторизации (Autorization ID).

Все объекты пользователя БД входят в его схему. На практике один пользователь, как правило, ассоциируется с одной схемой, хотя стандарт подразумевает, что одному пользователю может принадлежать несколько схем, содержащих взаимосвязанные объекты.

После успешного завершения процедуры идентификации открывается сеанс пользователя и устанавливается соединение с базой данных.

Существуют привилегии двух типов:

- системные привилегии (system privileges), контролирующие общий доступ к базе данных;
- объектные привилегии (object privileges), контролирующие доступ к конкретным объектам базы данных.

Синтаксис, используемый для работы с привилегиями, на практике значительно шире стандарта, но в значительной степени зависит от архитектуры конкретной БД.

Для управления привилегиями определены следующие правила:

- объект принадлежит пользователю, его создавшему (если синтаксисом не

указано создание объекта другого пользователя, конечно, при соответствующих полномочиях);

- владелец объекта, согласно стандарту, может изменять привилегии своего объекта;
- объектная привилегия всегда соотносится с конкретным объектом, а системная — с объектами вообще.

Язык SQL поддерживает следующие привилегии:

- `ALTER` — позволяет выполнять оператор `ALTER TABLE`;
- `SELECT` — позволяет выполнять оператор запроса;
- `INSERT` — позволяет выполнять добавление строк в таблицу;
- `UPDATE` — позволяет изменять значения во всей таблице или только в некоторых столбцах;
- `DELETE` — позволяет удалять строки из таблицы;
- `REFERENCES` — позволяет устанавливать внешний ключ с использованием в качестве родительского ключа любых столбцов таблицы или только некоторых из них;
- `INDEX` — позволяет создавать индексы (не входит в стандарт SQL-92);
- `DROP` — позволяет удалять таблицу из схемы базы данных.

Предоставление и снятие привилегий

Предоставление привилегии выполняется SQL-оператором `GRANT`, который имеет в стандарте SQL-92 следующее формальное описание:

```
 ON { [TABLE] table_name
        | DOMAIN domain_name
        | COLLATION collation_name
        | CHARACTER SET set_name
        | TRANSLATION translation_name }
TO { user_name .,: } | PUBLIC
```

```
[ WITH GRANT OPTION ]
```

где `privilege` определяется как

```
{ ALL PRIVELEGES }
| SELECT
| DELETE
| INSERT [(field .,:)]
| UPDATE [(field .,:)]
| REFERENCES [(field .,:)]
| USAGE
```

После фразы `GRANT` через запятую можно перечислить список всех назначаемых привилегий.

Фраза `ON` определяет объект, для которого устанавливается привилегия.

Фраза `TO` указывает пользователя или пользователей, для которых устанавливается привилегия.

Так, оператор `GRANT SELECT ON tbl1 TO PUBLIC;` предоставляет доступ к выполнению оператора `SELECT` для таблицы `tbl1` не только всем существующим пользователям, но и тем, которые позднее будут добавлены в базу данных.

Оператор `GRANT UPDATE ON tbl1 TO user1;` предоставляет пользователю `user1` привилегию `UPDATE` на всю таблицу, а оператор `GRANT UPDATE (f1,f2) ON tbl1 TO user1` предоставляет привилегию `UPDATE` для изменения только столбцов `f1` и `f2`.

Фраза `WITH GRANT OPTION` предоставляет получающему привилегию пользователю дополнительную привилегию `GRANT OPTION`,позволяющую выполнять передачу полученных привилегий.

Отмена привилегии выполняется SQL-оператором `REVOKE`, который имеет в стандарте SQL-92 следующее формальное описание:

```
REVOKE [ GRANT OPTION FOR ]
```

```
{ ALL PRIVILEGES } | privilege
ON { [TABLE] table_name
     | DOMAIN domain_name
     | COLLATION collation_name
     | CHARACTER SET set_name
     | TRANSLATION translation_name }
FROM { PUBLIC | user_name .,: }
[ CASCADE | RESTRICT ]
```

После фразы `REVOKE` через запятую можно перечислить список всех отменяемых привилегий.

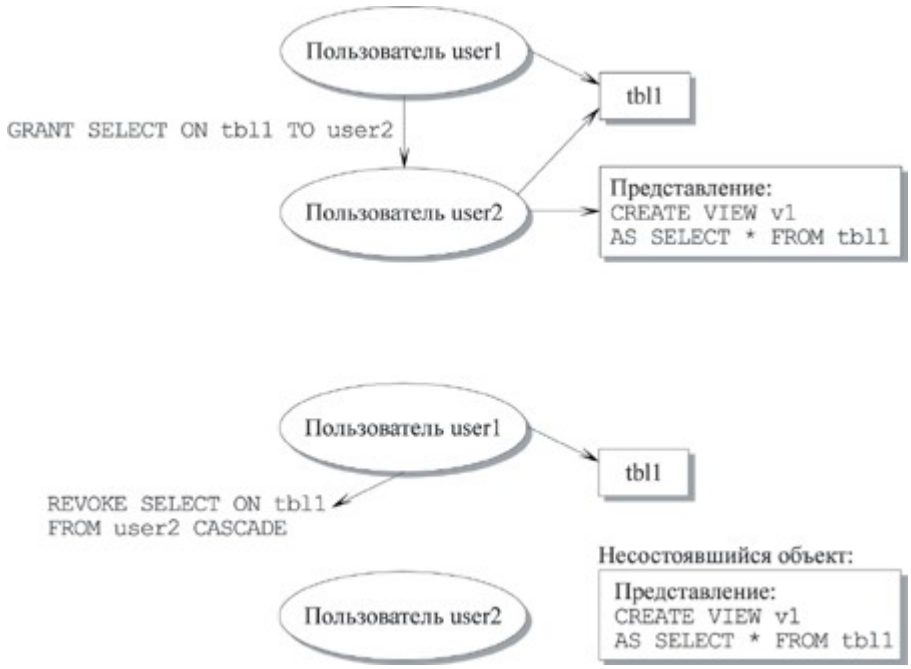
Фраза `ON` определяет объект, для которого отменяется привилегия.

Фраза `FROM` указывает пользователя или пользователей, для которых отменяется привилегия.

Фраза `GRANT OPTION FOR` определяет отмену не самих привилегий, а только права их передачи другим пользователям.

Если одна привилегия вместе с опцией `WITH GRANT OPTION` была последовательно передана от одного пользователя другому несколько раз, то образуется цепочка зависимых привилегий. Фразы `CASCADE` и `RESTRICT` определяют, что будет происходить с этими привилегиями при отмене одного из звеньев этой цепочки.

Если при отмене зависимой привилегии для объекта не остается ни одной существующей привилегии, то такой объект называется несостоявшимся. Например, подобное может произойти с представлением, созданным как запрос к таблице, привилегия на которую была утрачена. Эта ситуация показана на рисунке.



Если при отмене привилегии появляется несостоявшийся объект, то фраза RESTRICT предотвратит выполнение оператора REVOKE, и никакие привилегии отменены не будут.

Если указана фраза CASCADE и при отмене привилегии появляется несостоявшийся объект, то все несостоявшиеся объекты (представления) удаляются, а при наличии несостоявшихся ограничений в таблицах они отменяются автоматически выполнением оператора ALTER TABLE несостоявшиеся ограничения в доменах отменяются автоматически выполнением оператора ALTER DOMAIN.

Ролью называется именованный набор привилегий. Объединение привилегий в роли значительно упрощает процесс назначения и снятия привилегий. Если СУБД поддерживает управление ролями, то в SQL-операторах GRANT и REVOKE вместо имени пользователя можно указывать имя роли.

Ход выполнения работы

1. Изучить теоретические сведения.
2. По указанию преподавателя создать нескольких пользователей для разра-

ботанной ранее базы данных, назначить им различные привелегии.

3. Составить отчет о выполнении лабораторной работы.
4. Подготовить ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое привелегии пользователей?
2. Какие типы привелегий поддерживает язык SQL?
3. Приведите синтаксис оператора предоставления привелегий.
4. Приведите синтаксис оператора отмены привелегий.