Лабораторна робота №8
Тема: Безпека бази даних. Користувачі, ролі, права.

Теоретичні відомості:

Серед усіх користувачів бази даних головним є системний адміністратор, який зареєстрований під іменем SYSDBA з паролем „masterkey”. Ім’я SYSDBA не може змінюватись. В цілях безпеки бази даних пароль необхідно зразу ж поміняти.

По замовчуванню системний адміністратор самостійно може створювати бази даних, володіє всіма правами над будь-яким об’єктом бази даних, реєструє користувачів і надає їм права доступу. При реєстрації користувача вказується його ім’я і пароль.

У програмі *IB Expert* для реєстрації нових користувачів використовується *User Manager*  , для надання прав – *Grant Manager*  .

1. Надання прав

GRANT *права* **ON [TABLE]** *ім’я_таблиці* [(*поля*)]
TO {*користувачі*| **PUBLIC}**
[WITH GRANT OPTION];

де *привілеї* – список з одного або декількох прав, розділених комами. Права можуть бути наступні:

- **ALL [PRIVILEGES]** – повний дозвіл;
- **SELECT** – дозвіл на виконання запитів до таблиці;
- **INSERT** – дозвіл на додавання записів в таблицю;
- **UPDATE [(***ім’я_поля***[,** *ім’я_поля***...])]** – дозвіл на коригування даних таблиці;
- **DELETE** – дозвіл на видалення даних з таблиці.
- **REFERENCES [(***ім’я_поля***[,** *ім’я_поля***...])]** – дозвіл на встановлення зовнішніх ключів.

При наданні дозволу на коригування даних таблиці **UPDATE** чи встановлення зовнішніх ключів **REFERENCES** можна додатково вказувати імена полів, які можна коригувати чи визначати як зовнішній ключ.

користувачі – список, який включає одне або декілька імен користувачів, розділених комами.

поля – список полів таблиці, для яких встановлюється доступ.

PUBLIC означає передачу прав усім зареєстрованим користувачам.

WITH GRANT OPTION означає, що вказані користувачі можуть надавати вказані права іншим користувачам.

Права можна встановлювати відносно не тільки таблиці, а й представлення і збережених процедур.

Для представлень синтаксис команди подібний, тільки замість імені таблиці вказується ім’я представлення.

Права на виконання збережених процедур надаються командою

GRANT EXECUTE ON PROCEDURE *ім’я_процедури*
TO {*користувачі*| **PUBLIC}**
[WITH GRANT OPTION];

2. Відміна прав

REVOKE [GRANT OPTION FOR] *права*
ON [TABLE] *ім'я_таблиці*
FROM {*користувачі***| PUBLIC};**

GRANT OPTION FOR – використовується для відміни уповноважень, наданих раніше користувачу за допомогою опції **WITH GRANT OPTION.**

Приклад:

Надати користувачу STUD права на виконання запитів до таблиці STUDENTS і модифікацію полів SFAM і SIMA цієї таблиці .

GRANT SELECT, UPDATE (SFAM, SIMA**)**
ON STUDENTS
TO STUD**;**

Приклад:

Надати користувачам STUD і USER права на виконання запитів до таблиці STUDENTS і модифікацію полів SFAM і SIMA цієї таблиці з можливістю передачі вказаних прав іншим користувачам .

GRANT SELECT, UPDATE (SFAM, SIMA**)**
ON STUDENTS
TO STUD, USER
WITH GRANT OPTION;

Якщо декілька користувачів виконують одну і ту ж роботу і мають однакові права, то їх об'єднують в групи. Для цього використовується механізм ролей. Ролі дозволяють задавати певні права доступу до об'єктів бази абстрактно, незалежно від імені користувача, а потім конкретному користувачу при реєстрації присвоювати вибрану роль.

Спрощено порядок дії ролі можна записати таким чином:

1. **Створення ролі**

CREATE ROLE *ім'я_ролі*;

2. **Надання прав ролі**

GRANT *права* **ON [TABLE]** *ім'я_таблиці* [(*поля*)]
TO *ім'я_ролі*
[WITH GRANT OPTION];

3. **Призначення конкретним користувачам даної ролі**

GRANT *ім'я_ролі* **TO** *ім'я_користувачів*;

При приєднанні до певної бази даних користувач, крім імені і пароля, повинен вказувати надану йому роль.

Знищення ролі

DROP *ім'я_ролі*;

Завдання до виконання:

1) Завантажте програму *IBExpert.*
2) Відкрийте базу даних **Univer**.
3) Використовуючи *User Manager*, створити користувача *ST* з паролем *ST.*
4) Надати йому права на модифікацію полів **SEMESTR**, **GOD** таблиці **PREDMET**.
5) Закрийте базу даних **Univer**. Відкрийте її заново як користувач ST. Перевірте, чи можна коригувати поля **SEMESTR**, **GOD** таблиці **PREDMET**, інші поля даної таблиці.
6) Відкрийте базу даних **Univer** як користувач SYSDBA.
7) Створіть роль READER, що дозволяє виконувати запити до таблиці **STUDENTS**.
8) Відкрийте базу даних **Univer** заново як користувач ST з роллю READER. Переконайтесь у дії даної ролі, створивши простий запит до таблиці **STUDENTS.**
9) Самостійно створіть користувачів і ролі, надавши їм певні права. Переконайтесь у правильній роботі даних користувачів по відношенню до різних об’єктів бази даних. Результати запишіть у зошит.
10) Завершіть роботу.

Контрольні запитання:

1) Яку інформацію містить зареєстрований запис про користувача?
2) Який користувач має повний доступ до бази даних?
3) Як реєструються користувачі у програмі *IB Expert*?
4) Які права мають користувачі?
5) Яка команда використовується для надання прав користувачам?
6) Що таке ролі?
7) Для чого створюються ролі?
8) Який механізм дії ролі?
9) Як відмінити права, надані користувачу?
10) Як знищити роль?