НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Практична робота № 6

з дисципліни

“Основи захисту інформації”

Варіант 4

Виконала:

студентка групи ІС-71

Вознюк О. В.

Перевірив:

аспірант

Ільїн К. І.

Київ-2020

**Хід виконання роботи**

1. Напишіть команди Transact SQL для наступних дій:

1 Створити новий обліковий запис;



2. Назначити користувачу роль БД (будь-яку);



3. Надати користувачу Bill повноваження на доступ к збереженої

процедури (будь-якої);



4. Відкликати всі надані користувачу John привілегії.



2. Поясніть призначення наступних команд Transact SQL:

1. GRANT SELECT, INSERT ON SUPPLIES TO J\_Smith WITH

GRANT OPTION AS Economists

Надати можливість зчитувати та додавати дані в таблицю SUPPLIES користувачу J\_Smith та надати користувачу J\_Smith можливість надавати дозволи на зчитування та додавання даних в таблицю SUPPLIES іншим користувачам. Цей запит викликається користувачем зі вказанням членства в групі Economists.

2. EXEC[UTE] sp\_addlogin ‘king\_of\_the\_db', ‘a2h7d0f7dg84mdf94',

‘PROJECTS', ‘Ukrainian', ‘master', ‘NULL'

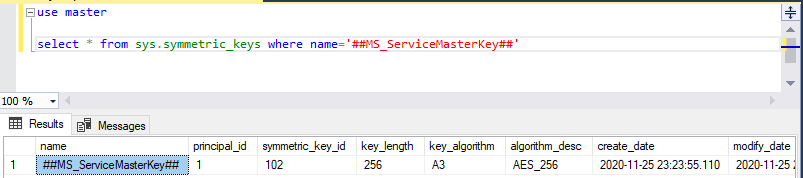
Створити обліковий запис для користувача king\_of\_the\_db з паролем - a2h7d0f7dg84mdf94, базою даних за замовчуванням PROJECTS, мовою за замовчуванням - Ukrainian, SID – master, без шифрування пароля.

3. REVOKE ALL TO ‘M\_Ivanenko' CASCADE

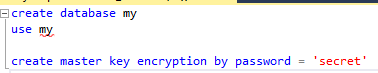
Відкликати всі надані користувачу John дозволи, а також відкликати всі дозволи користувачів, яким вони були надані користувачем John.

3. Напишіть послідовність команд, яка шифрує вміст однієї з колонок таблиці в створеній БД.

1. Впевнитися, що для екземпляра SQL Server створено мастер-ключ.



2. Створити мастер-ключ бази даних my\_db



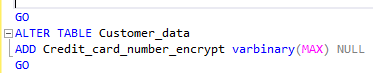
3. Створити сертификат.



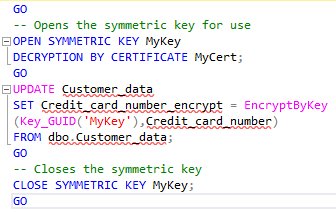
4. Створення симетричного ключа:



5. Зміна схеми даних. Для зберігання зашифрованої інформації даних тип колонки має бути varbinary, тому в таблицю додається колонка такого типу з іменем Credit\_card\_number\_encrypt:



6. Шифрування колонки таблиці. Для шифрування використовується команда EncryptByKey. Перед шифруванням необхідно відкрит симетричный ключ, а по закінченню закрити.



**Відповіді на теоретичні питання**

1. Які етапи автентифікації проходять користувачі для роботи з MS SQL Server?

Спочатку перевіряється, чи співставлене дане ім’я користувацькому

запису, яка має дозвіл на підключення до екземпляра SQL Server. Далі ядро бази перевіряє, чи має даний обліковий запис дозвіл на доступ до тієї бази, до якої намагається він підключитися.

2. Як можна встановити довірче з’єднання?

При підключення до SQL Server необхідно використати ім’я входу

Windows.

3. Коли варто використовувати змішаний режим аутентифікації?

Деякі сторонні програми підтримують лише змішану автентифікацію, а деякі мови програмування, такі як Java, не підтримують автентифікацію Windows для з'єднань SQL Server. В інших випадках архітектори програм можуть визначити, що змішана автентифікація забезпечує найшвидший і найпростіший шлях для розробки, або вам може знадобитися працювати з існуючими програмами, які використовують змішану автентифікацію, поки у вас не буде часу або персоналу переписати їх для використання автентифікації Windows.

4. Який термін використовується фактично при доступі об’єкта до БД?

(login чи user)

User

5. Яке призначення ролі сервера і ролі БД?

SQL Server надає ролі на рівні сервера, щоб допомогти вам керувати

дозволами на сервері. Ці ролі є основами безпеки, які групують інших принципи безпеки. Ролі сервера є загальносерверними за обсягом дозволів. Ролі бази даних можна використовувати для призначення дозволів бази даних в групі користувачів.

6. Що значить параметр CASCADE?

Виконання зазначеної операції або запиту відносно записів або об’єктів, що пов’язані з тим, над яким виконується операція або запит.

7. Коли виникає конфлікт доступу?

Два користувачі зчитують одні й ті самі дані. Користувач 1 оновлює дані та записує ці зміни назад у базу даних, перш ніж користувач 2 зробить те саме. Тепер у вас виник конфлікт, оскільки користувач 1 прочитав дані, перш ніж користувач 2 записав їх назад до бази даних.

8. Яким є призначення сертифікату в системі криптографічного захисту MS SQL Server?

Сертифікат забезпечує безпеку шифрування та доступу до зашифрованих даних. Користувач, який намагається отримати доступ до зашифрованих даних має вказати сертифікат, який був використаний при їх шифруванні.

**Висновок**

В цій роботі були набуті навички налаштування системи безпеки в SQL (створення користувача, розмежування прав доступу) на прикладі MS SQL Server.