**Лабораторная работа 3. Безопасность SQL Server**

**Задание (выполняется посредством ввода команд на Transact-SQL):**

1. Измените, если это возможно, режим аутентификации SQL-сервера на смешанный режим.
2. Создайте локальную учётную запись пользователя Windows на рабочей станции с SQL-сервером.
3. Разрешите вход на SQL-сервер под учётными данными созданного пользователя в режиме Windows-аутентификации.
4. Создайте логин для входа на сервер в режиме SQL-аутентификации.
5. В тестовой базе данных создайте двух пользователей, соответствующих созданным ранее логинам.
6. Протестируйте подключение к тестовой базе данных с использованием созданных логинов. Выведите при помощи запроса название логина, который использовался при аутентификации на сервере, а также название соответствующего пользователя базы данных.
7. Разрешите доступ на чтение любой из таблиц первому пользователю, а второму пользователю – запуск любой созданной Вами хранимой процедуры. Протестируйте выданные разрешения.
8. Создайте роль «students» и включите в неё двух созданных пользователей. Выдайте разрешение этой роли вставлять записи в ранее использованную таблицу.
9. Задайте явный запрет вставки записи в ранее использованную таблицу второму пользователю.
10. Протестируйте все ранее выданные разрешения под учётными данными обоих созданных пользователей.
11. Создайте роль приложения с произвольным именем и выдайте этой роли разрешение на удаление и чтение записей в используемой таблице.
12. Продемонстрируйте технологию выполнения вышеперечисленных шагов при помощи графического интерфейса Management Studio.
13. Продемонстрируйте на простейшем примере использование созданной роли приложения. Для этого создайте простой проект с использованием технологии ADO.NET, JDBC, либо любой другой аналогичной. Можно использовать любой язык программирования. Продемонстрируйте факт того, что приложение действует в контексте созданной Вами роли приложения, а также то, что приложению разрешено выполнять операции, разрешённые для созданной Вами роли приложения и не разрешено выполнять другие операции.

**Вопросы к отчёту:**

1. Концепция трёхуровневой модели безопасности
2. Режимы аутентификации сервера
3. Преимущества и недостатки Windows-аутентификации и SQL-аутентификации
4. Концепции трёхуровневой модели безопасности SQL-Server
5. Логины на уровне сервера. Создание, поддержка, настройка
6. Серверные роли: основные концепции, предназначение
7. Пользователи на уровне базы данных. Создание, настройка, поддержка
8. Роли базы данных: основные концепции, предназначение, встроенные роли
9. Настройка прав доступа на уровне объектов базы данных. Операторы Grant, Deny, Revoke. Взаимодействие разрешений.
10. Роли приложений. Предназначение и отличия от пользовательских ролей. Порядок их использования.