**Отчёт по практической работе 5**

**Аутентификация пользователей.**

**Ответить на контрольные вопросы:**

1. Сделать конспект теоретической части в электронном формате.
2. Создать учётную запись на сервере SQL Server, а также пользователей и пользовательских ролей в БД.
3. Назначить права доступа к объектам БД для каждой пользовательской роли.

Оформить отчёт.

**Конспект теория.**

В СУБД Microsoft SQL Server имеется подсистема защиты от несанкционированного доступа (НСД), называемая также в терминах компании-разработчика ***системой безопасности SQL Server***. Является совокупностью механизмов идентификации, аутентификации и авторизации пользователей в системе. Особенность её в том, что защита от НСД происходит а ней на двух уровнях:

1. Уровень сервера.

На этом уровне конечный пользователь или клиентское приложение проходит идентификацию и аутентификацию, получая право на доступ к ресурсам *сервера СУБД.*

1. Уровень БД.

Для каждой БД определяются дополнительные системные настройки. В них отражается информация о пользователях БД, о разделении их на группы и предоставленных каждой из групп правах на выполнение различного рода действий с объектами – таблицами, представлениями, хранимыми подпрограммами и т. д.

**Защита от НСД на уровне сервера СУБД. Идентификация и аутентификация. Учётной записи**

Идентификация и аутентификация пользователей в СУБД SQL Server выполняются по общепринятой схеме: с использованием имени и пароля соответственно. Имя, пароль, а также связанная с ними дополнительная информация, образуют ***учетную запись***.

При прохождении идентификации и аутентификации стандартными средствами SQL Server система получает имя и пароль текущего пользователя, преобразует пароль в хешированное значение и ищет запись в таблице syslogins (таблице, где хранятся учётные записи), где поля name и password совпадают с текущим именем и хешированным паролем соответственно.

Помимо указанного способа, SQL Server поддерживает аутентификацию *с использованием учетной записи домена Windows NT*.

Учетные записи Windows NT находятся в специальном хранилище системы безопасности домена, существующей отдельно от SQL Server.

Перечисленные способы аутентификации не следует путать с ***режимами аутентификации***, которых в СУБД SQL Server тоже два.

1. Режим смешанной аутентификации.

Работая в этом режиме, SQL Server поддерживает оба метода аутентификации. Если пользователь не имеет учетной записи в Windows NT, он не получит доступа к серверу автоматически, но у него есть возможность зайти под учетной записью SQL Server.

2. Режим аутентификации Windows.

В этом режиме доступ предоставляется только пользователям, зарегистрированным в домене. Этот режим не удобен для пользователей операционных систем, несовместимых с Windows NT, однако он более защищен по сравнению с предыдущим.

**Серверные роли. *Серверной ролью*** называется механизм, позволяющий группировать учетные записи и предоставлять группе определенный набор административных прав.

Список учетных записей содержится в папке **\Security\Logins**. При ее открытии в окне **Summary** отображается список имеющихся учетных записей.

Создание новой учетной записи предполагает следующую последовательность действий со стороны пользователя.

1. Выбирается опция **New Login** контекстного меню папки **Logins**. В результате на экране появляется окно **Login – New**. Автоматически активизируется вкладка **General**.

2. Указывается имя учетной записи в поле **Login** **Name**.

3. Указывается тип аутентификации. Для внутренних учетных записей SQL Server требуется дважды прописывается пароль.

4. Если SQL Server работает под управлением Windows 2003 Server, можно определить следующие требования к паролю:

* использование парольной политики Windows, применяемой к локальным учетным записям на данном компьютере (флажок **Enforce password policy**);
* включение «устаревания» пароля (флажок **Enforce password expiration**); означает, что на создаваемую учетную запись распространяются требования по смене пароля по прошествии промежутка времени, определяемого локальной политикой безопасности Windows; данная опция может быть настроена только при установленном флажке **Enforce password policy**;
* установка требования смены пароля при каждом входе (флажок **User must change password at next logon**); настройка этого параметра возможна только в том случае, если установлены два предыдущих флажка.

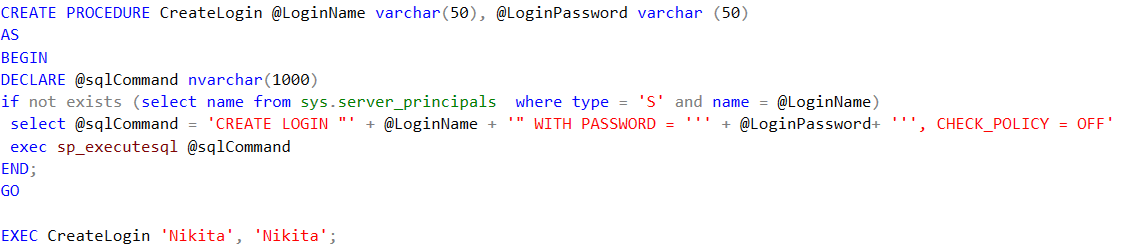
5. В списке **Default database** для создаваемой учетной записи выбирается «БД по умолчанию» - та БД, к которой пользователь будет автоматически подключаться при входе в СУБД. *Важное замечание:* без крайней необходимости не следует указывать в этом пункте системную БД!

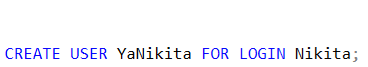
6. Если требуется включить учетную запись в одну или несколько фиксированных ролей сервера, следует перейти на вкладку **Server Roles** и установить соответствующие флажки.

7. Возможна ситуация, когда создаваемой учетной записи необходимо назначить отдельные административные права, но ни одна роль сервера для этого не подходит. В этом случае можно, не включая учетную запись ни в одну из ролей, перейти на вкладку **Securables**, выбрать объект доступа (сервер или учетную запись), после чего установить конкретное разрешение. Например, можно наделить создаваемую учетную запись правом изменять пароли других учетных записей; можно разрешить учетной записи выполнение команды **create database**, но не дать разрешения на использование команд **drop database** и **alter database** и т. п.

Система безопасности SQL Server допускает изменение свойств большинства учетных записей. Изменить имя учетной записи можно только средствами Transact-SQL, используя опцию **name** оператора **alter login**. Все прочие параметры учетных записей настраиваются как языковыми средствами, так и при помощи GUI.

Использовать аутентификацию в коде можно следующим образом:





**Защита от НСД на уровне БД. Пользователи и роли БД**

***Пользователь БД*** – это административная единица системы безопасности, через которую учетной записи предоставляется доступ к объектам БД. Для любой БД существует свой набор пользователей. Каждый пользователь связывается с одной из имеющихся учетных записей и наделяется правами доступа к объектам БД: таблицам, представлениям, процедурам, функциям. Во многих случаях целой группе пользователей предоставляются одинаковые права. При этом в качестве механизма группирования используются ***роли БД***, которые классифицируются следующим образом:

* фиксированные роли БД;
* пользовательские роли БД;
* роли приложений.

***Фиксированные роли БД*** стандартны, не могут быть удалены или добавлены, невозможно повлиять на права доступа фиксированных ролей к объектам БД.

Реализовать роли в коде можно следующим образом:



