Администрирование БД.
Управление разрешениями

Предоставление разрешений уровня базы данных

- Система безопасности SQL Server 2000 устанавливает два уровня защиты данных – аутентификацию и авторизацию. Независимо от способа проверки подлинности, пользователь должен иметь разрешения на выполнение определенных действий в пользовательской БД.
- Для обеспечения работы с БД администратор должен установить пользователю определенные разрешения на доступ к БД.

Способы получения разрешений

- Пользователи получают разрешения доступа к БД следующими способами:
  - Членство в серверной роли sysadmin;
  - Право собственности на БД;
  - Право собственности на объект БД, полученное в результате членства в роли БД или группе Windows;
  - Членство в фиксированной роли БД;
  - Получение отдельных разрешений в результате членства в роли БД или группе Windows;
  - Наследование роли public пользователем, который обладает доступом к БД;
  - Наследование разрешений пользователя guest, пользователем не имеющим доступа к БД.

Наследуемые разрешения

- Владелец БД, а также члены серверной роли sysadmin и фиксированной роли db_owner наследуют все разрешения, необходимые для выполнения любых действий в БД.
- Владелец объекта наследует все связанные с объектом разрешения доступа, включая право предоставлять разрешения на работу с данным объектом.
- Члены роли сервера sysadmin, а также члены фиксированных ролей db_ddladmin, db_securityadmin могут менять владельца любого объекта БД и отзывать все назначенные объекту разрешения.

Действия разрешений

- Группам Windows, пользовательским ролям и отдельным пользователям можно назначать и блокировать наборы разрешений, связанные с ролями сервера и фиксированными ролями БД, а также конкретные разрешения на выполнение операторов и работу с объектами.
- Можно отзывать и блокировать разрешения отдельных ролей, групп или пользователей. Блокирование разрешений имеет более высокий приоритет по отношению ко всем другим разрешениям.

Управление разрешениями на выполнение операторов

- Разрешения на выполнение операторов (statement permissions) – это разрешения на выполнение операторов T-SQL, используемых для создания БД и их объектов.

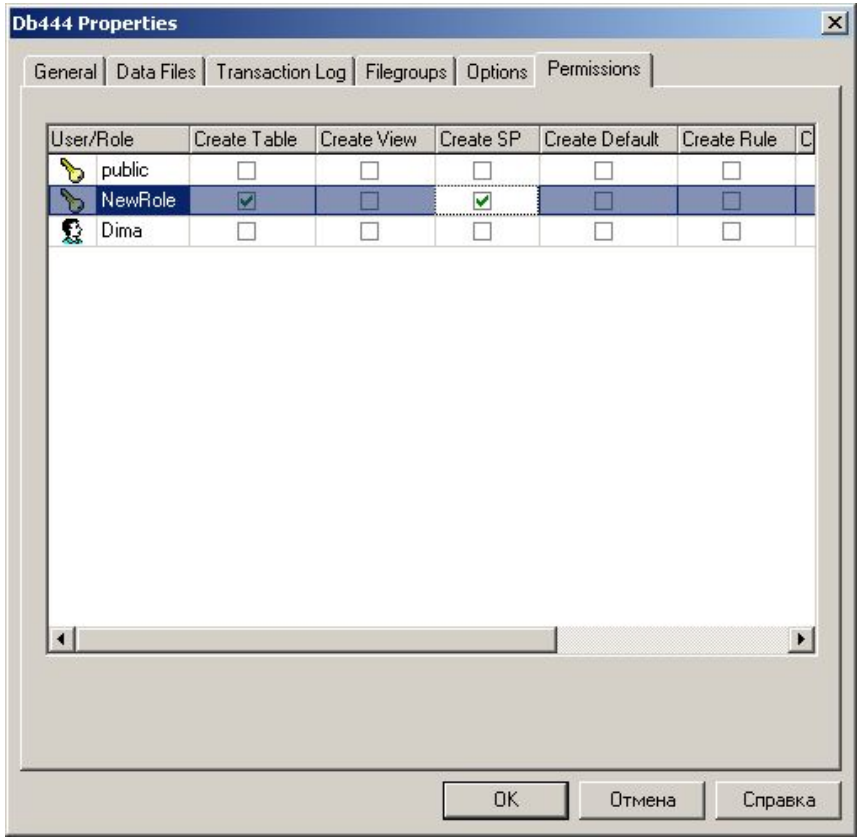
Оператор	**Разрешения на выполнение оператора**
CREATE DATABASE	Разрешение наследуется членами ролей sysadmin, dbcreator. Это разрешение доступа существует только в БД master
BACKUP DATABASE BACKUP LOG	Данные разрешения наследуются членами роли сервера sysadmin, а также фиксированными ролями db_owner и db_backupoperator
CREATE TABLE CREATE VIEW CREATE PROCEDURE CREATE RULE CREATE FUNCTION	Данные разрешения наследуются членами роли sysadmin и фиксированных ролей db_owner и db_ddladmin. По умолчанию объекты принадлежат их создателю, однако при создании можно указать владельца данного объекта.

Смена владельца объекта

- Если владельцем некоторого объекта БД является не dbo, может понадобится изменить права собственности. Члены ролей db_owner, db_ddladmin и db_securityadmin могут меня права собственности на любой объект БД.
- Системная хранимая процедура для смены владельца sp_changeobjectowner
  - sp_changeobjectowner ‘DC\Dima.Customer’, ‘dbo’

Управление разрешениями средствами Enterprise Manager

- Enterprise Manager предоставляет простой интерфейс для управления разрешениями: их просмотра предоставления, блокирования и отзыва.
- Для доступа к управлению необходимо выбрать БД и в меню Свойства выбрать закладку Permissions.



Управление разрешениями средствами Transact-SQL

- Для управления разрешениями можно использовать операторы GRANT, DENY, REVOKE.
  - GRANT CREATE TABLE TO Dima, NewRole
  - DENY CREATE VIEW TO Ivan
  - REVOKE ALL FROM Ivan

Просмотр разрешений

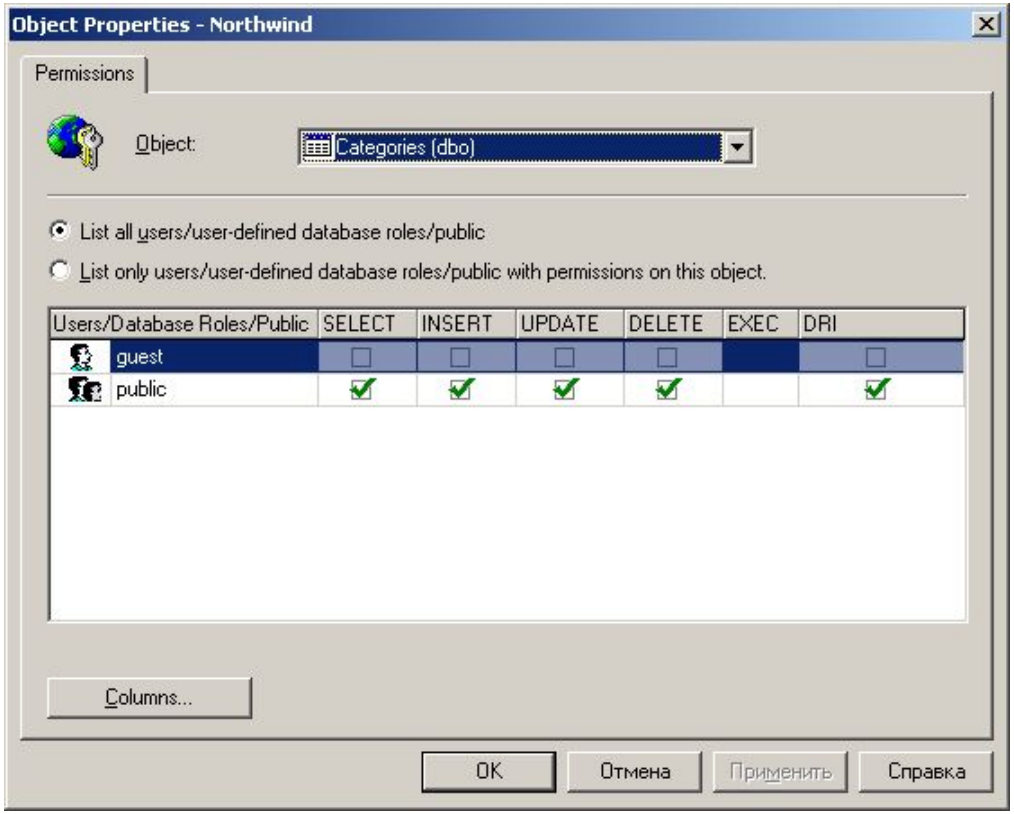
- Для просмотра разрешений на выполнение операторов можно воспользоваться хранимой процедурой sp_helprotect. Право на выполнение данной процедуры имеют все пользователи БД.
  - EXEC sp_helprotect NULL, NULL, NULL, ‘s’

Управление разрешениями доступа к объектам

- Разрешения доступа к объектам – разрешения на выполнение определенных операций с таблицами, представлениями, функциями.
- SELECT - просмотр данных в таблице, представлении, наследуется членами ролей db_owner, db_reader
- INSERT – добавление новых данных в таблицу или представление , наследуется членами ролей db_owner, db_writer
- UPDATE – обновление данных в таблице или представлении , наследуется членами ролей db_owner, db_writer
- DELETE – удаление данных из таблицы или представления , наследуется членами ролей db_owner, db_writer
- EXECUTE – выполнение хранимых процедур и пользовательских функций , наследуется членами ролей db_owner
- REFERENCES – обращение к таблице с ограничением FOREIGN KEY при отстутствии разрешений SELECT , наследуется членами ролей db_owner, db_reader

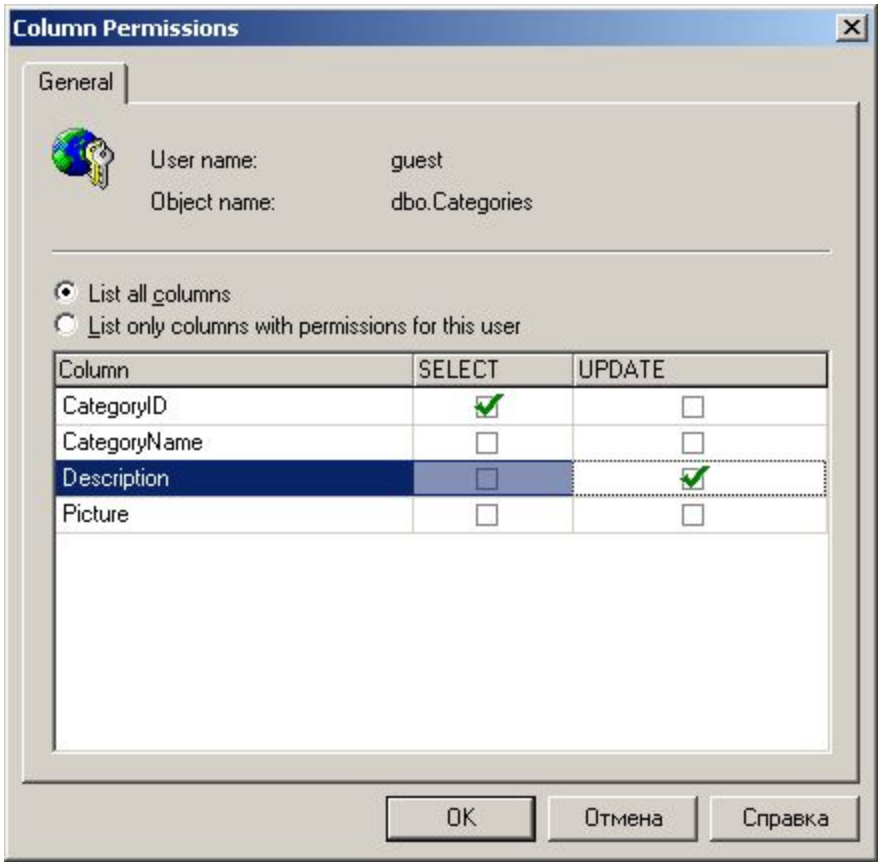
Управление доступом к объектам средствами Enterprise Manager

- Для управления разрешениями доступа к объекту используются Свойства объекта (таблицы, представления, процедуры).



Управление доступом к объектам средствами Enterprise Manager

- Можно установить дополнительные ограничения к отдельному полю.



Управление доступом к объектам средствами Transact-SQL

- Для управления доступом к объектам можно использовать операторы GRANT, DENY и REVOKE
  - GRANT SELECT ON Customer TO Ivan
  - DENY INSERT, UPDATE, DELETE TO Ivan
  - GRANT SELECT ON Customer TO NewRole WITH GRANT OPTION
  - GRANT SELECT ON Customer TO Wil AS NewRole

Просмотр разрешений

- Для просмотра предоставленных разрешений доступа к объектам БД используется системная хранимая процедура sp_helprotect
  - sp_helprotect ‘Customer’
  - sp_helprotect NULL, ‘Ivan’
  - sp_helprotect NULL, NULL, ‘NewRole’