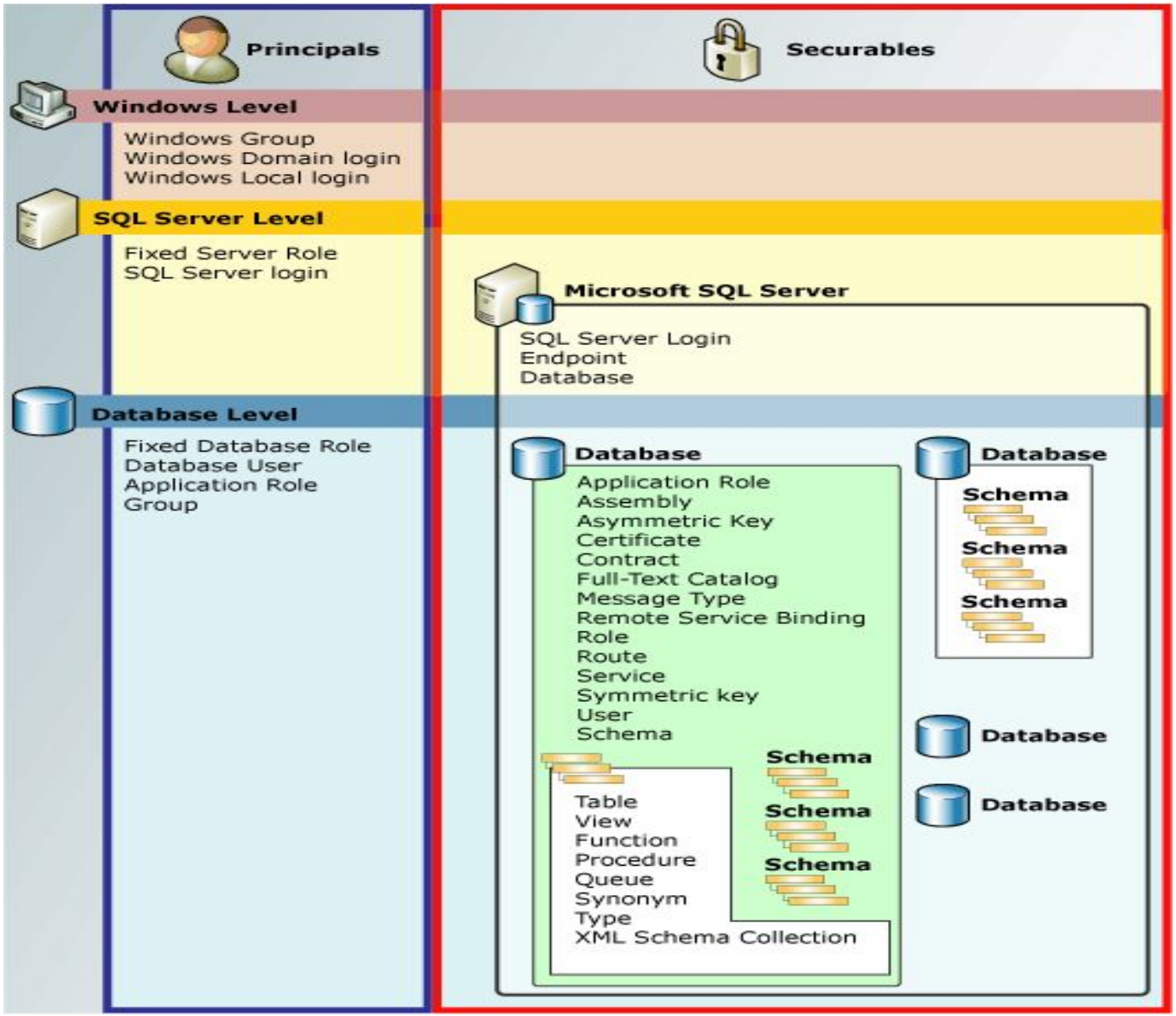
Управление базами данных

Система безопасности

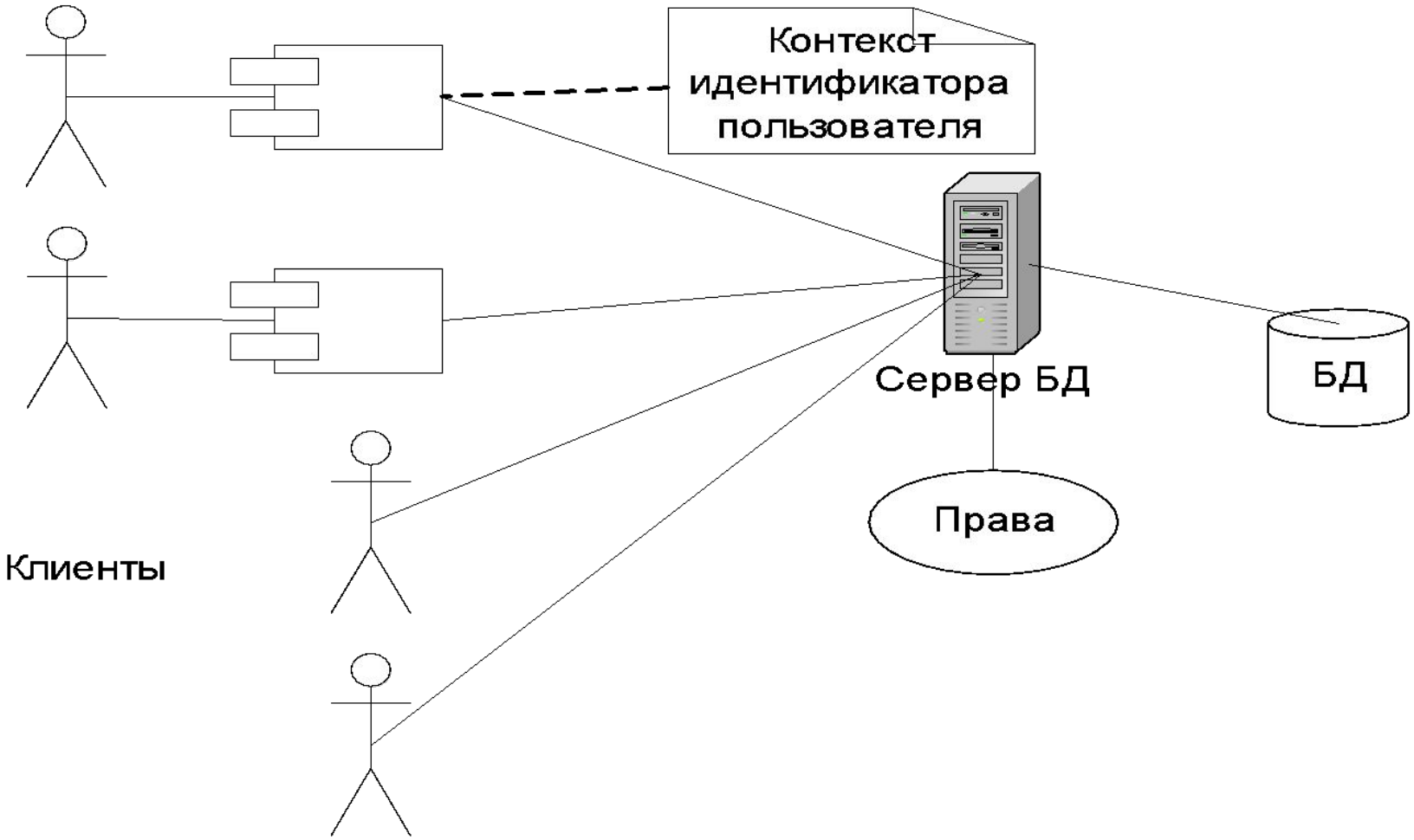

Principals
Securables
Windows Level
Windows Group
Windows Domain login
Windows Local login
SQL Server Level
Fixed Server Role
SQL Server login
Microsoft SQL Server
SQL Server Login
Endpoint
Database
Database Level
Fixed Database Role
Database User
Application Role
Group
Database
Application Role
Assembly
Asymmetric Key
Certificate
Contract
Full-Text Catalog
Message Type
Remote Service Binding
Role
Route
Service
Symmetric key
User
Schema
Table
View
Function
Procedure
Queue
Synonym
Type
XML Schema Collection
Schema
Schema
Schema
Database
Schema
Schema
Schema
Database
Database

Система безопасности сервера баз данных

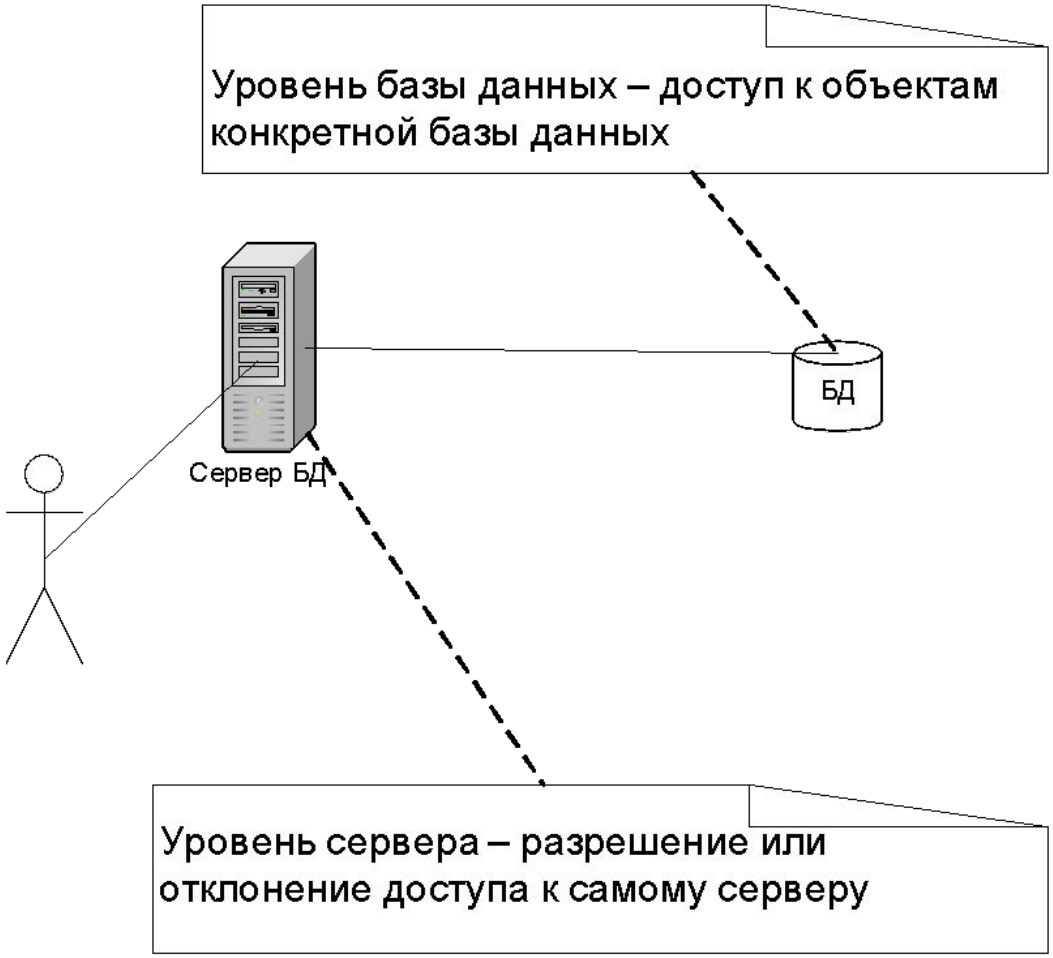
Необходимость в системе безопасности:

- Кража информации
- Злонамеренное повреждение информации
- Случайное повреждение информации

Разграничение прав пользователей СУБД



Уровни безопасности



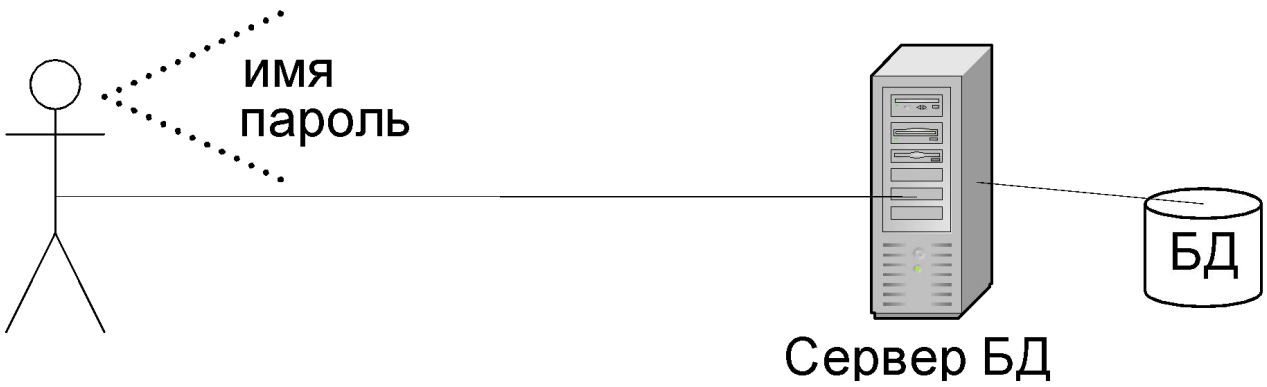
Уровень сервера

Аутентификация – проверка подлинности пользователя

- **Имя пользователя** (имя учетной записи) – пользователь СУБД называет себя
- **Пароль** – пользователь подтверждает, что он тот, за кого себя выдает

Режимы аутентификации MS SQL Server:

- Смешанный (mixed) – SQL Server и Windows
- Только Windows



Средства аутентификации Windows

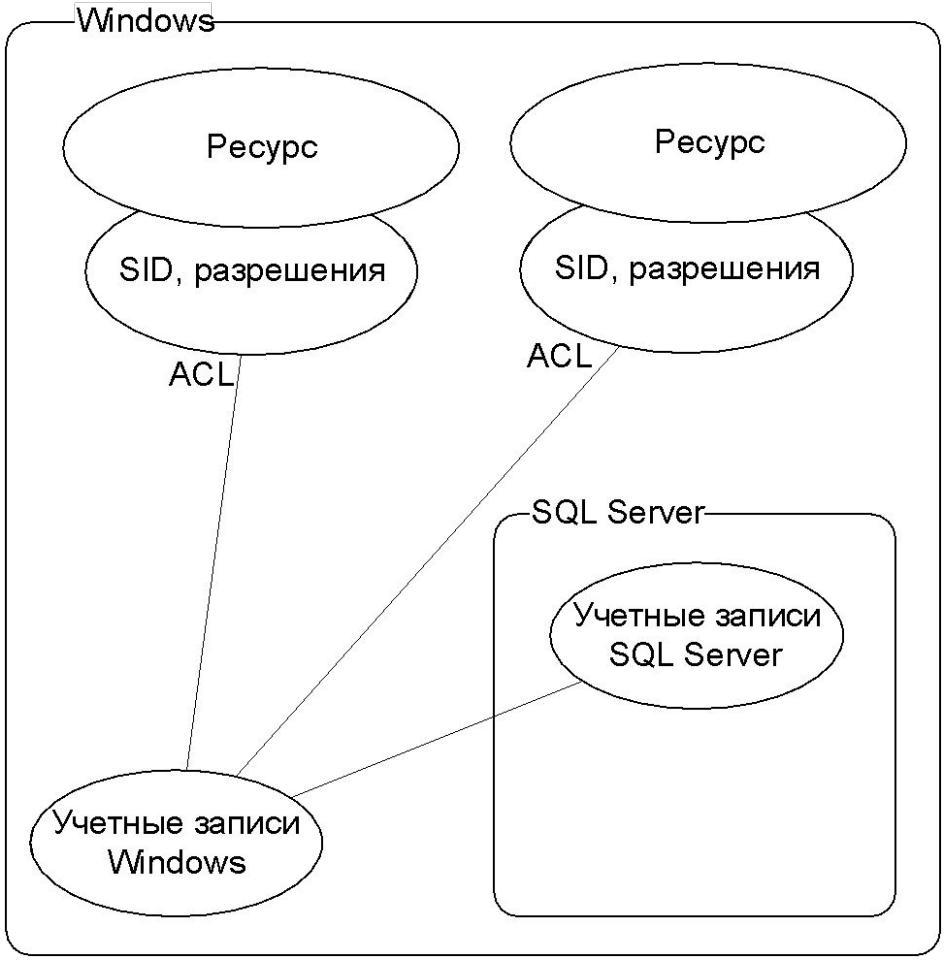
Учетная запись:

- Имя
- Пароль
- Членство в группах
- Каталог по умолчанию
- Уникальный идентификатор (генерируется)

Уникальный идентификатор = login identifier = login ID = Security Identification = SID

Список прав доступа к ресурсу = Access Control List = ACL

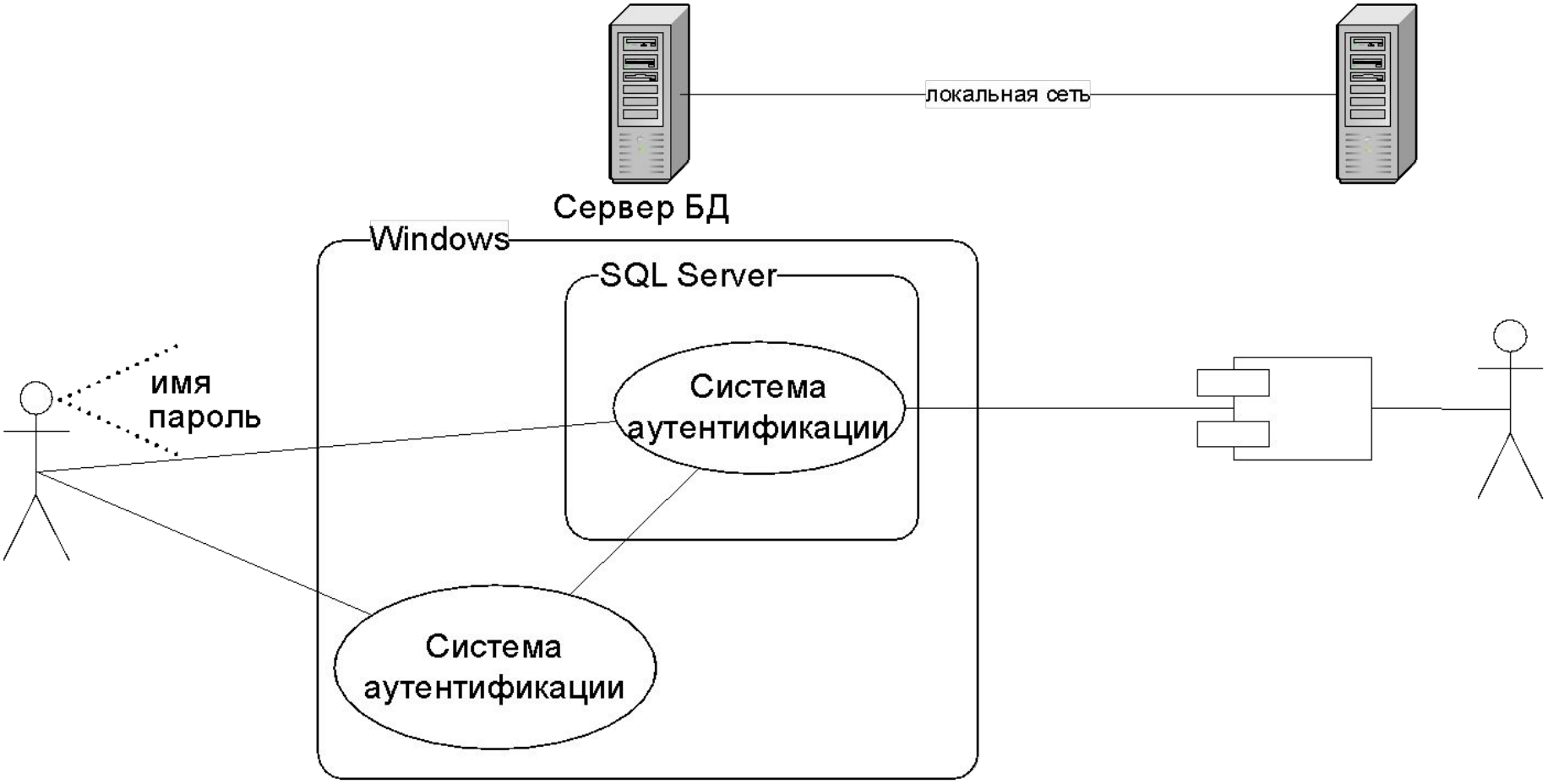
Средства аутентификации Windows



Преимущества:

- Более развитая система безопасности
- Не надо повторно проходить аутентификацию

Средства аутентификации SQL Server



Средства аутентификации SQL Server

Учетная запись в SQL Server:

- Имя / name
- Тип / type {Windows User | Windows Group | Standard}
- Доступ к серверу / Server Access
- БД по умолчанию / Default Database
- Язык по умолчанию / Default Language
- Пароль / Password

При установке: SA без пароля и BUILT IN\Administrators

Роли сервера

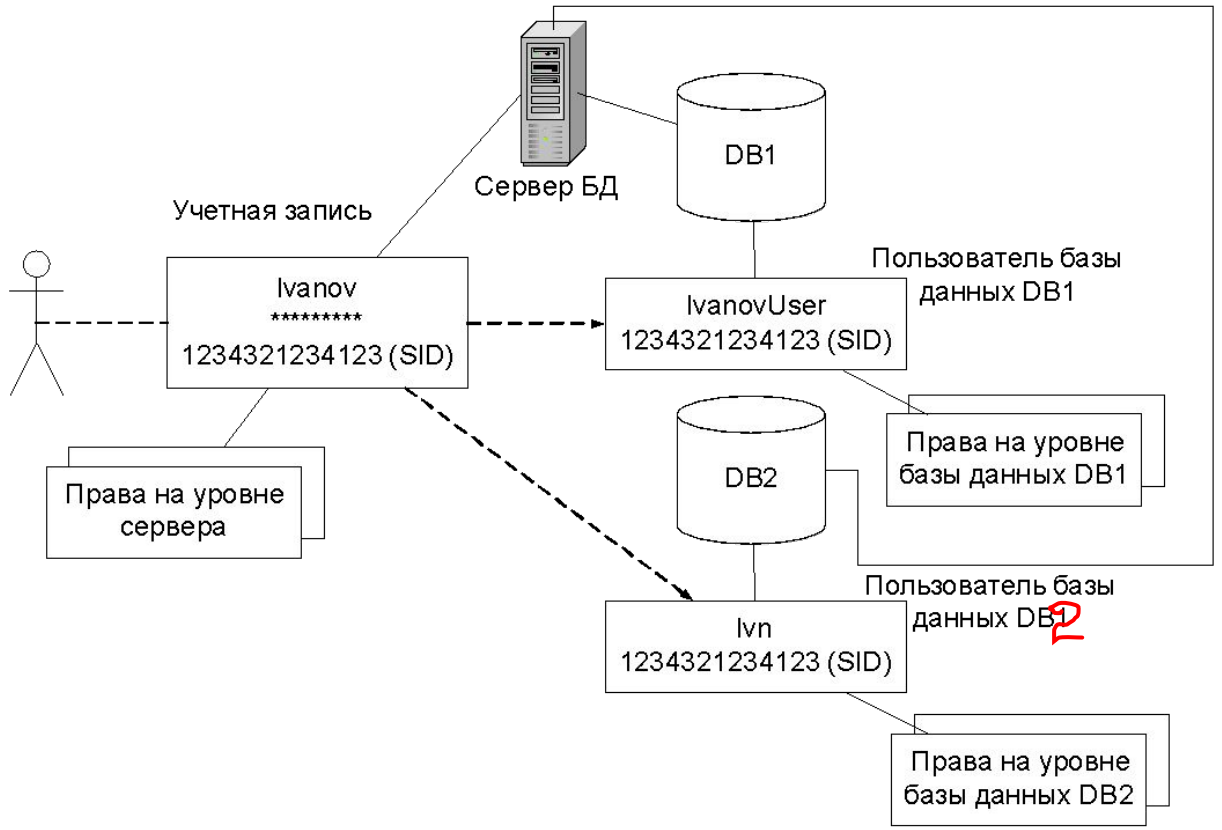
Предоставление прав по администрированию сервера БД

Фиксированные роли сервера (fixed server roles)

- sysadmin – все права
- setupadmin – конфигурирование хранимых процедур для запуска
- serveradmin – конфигурирование и выключение сервера
- securityadmin – создание и удаление учетных записей
- processadmin – управление процессами на сервере
- diskadmin – управление файлами баз данных
- dbocreator – создание новых БД

Уровень базы данных

Пользователь базы данных – административная единица системы безопасности, через которую осуществляется доступ учетной записи к объектам данных



Уровень базы данных

Пользователь БД:

- Имя / name
- Имя учетной записи / login name
- Роль в БД / role

По умолчанию создаются пользователи БД:

- Dbo – соответствует учетная запись под которой создавалась БД. Удалить невозможно
- Guest – любая учетная запись отображается в этого пользователя, если нет доступа к БД

Уровень базы данных

Типы ролей на уровне базы данных:

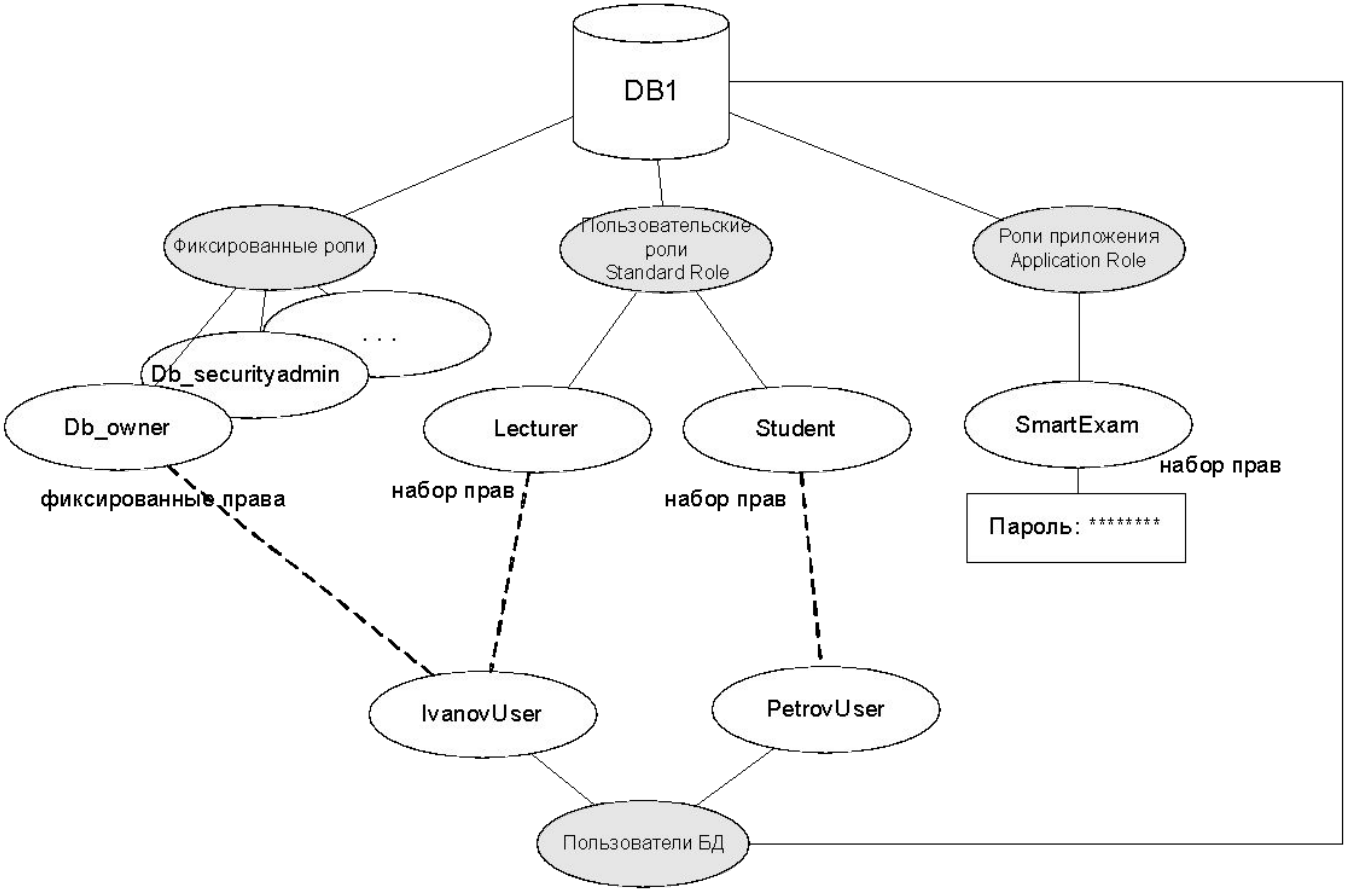
- Фиксированные роли БД / fixed database roles
- Пользовательские роли / user database roles
- Роль приложения / application role

Фиксированные роли БД

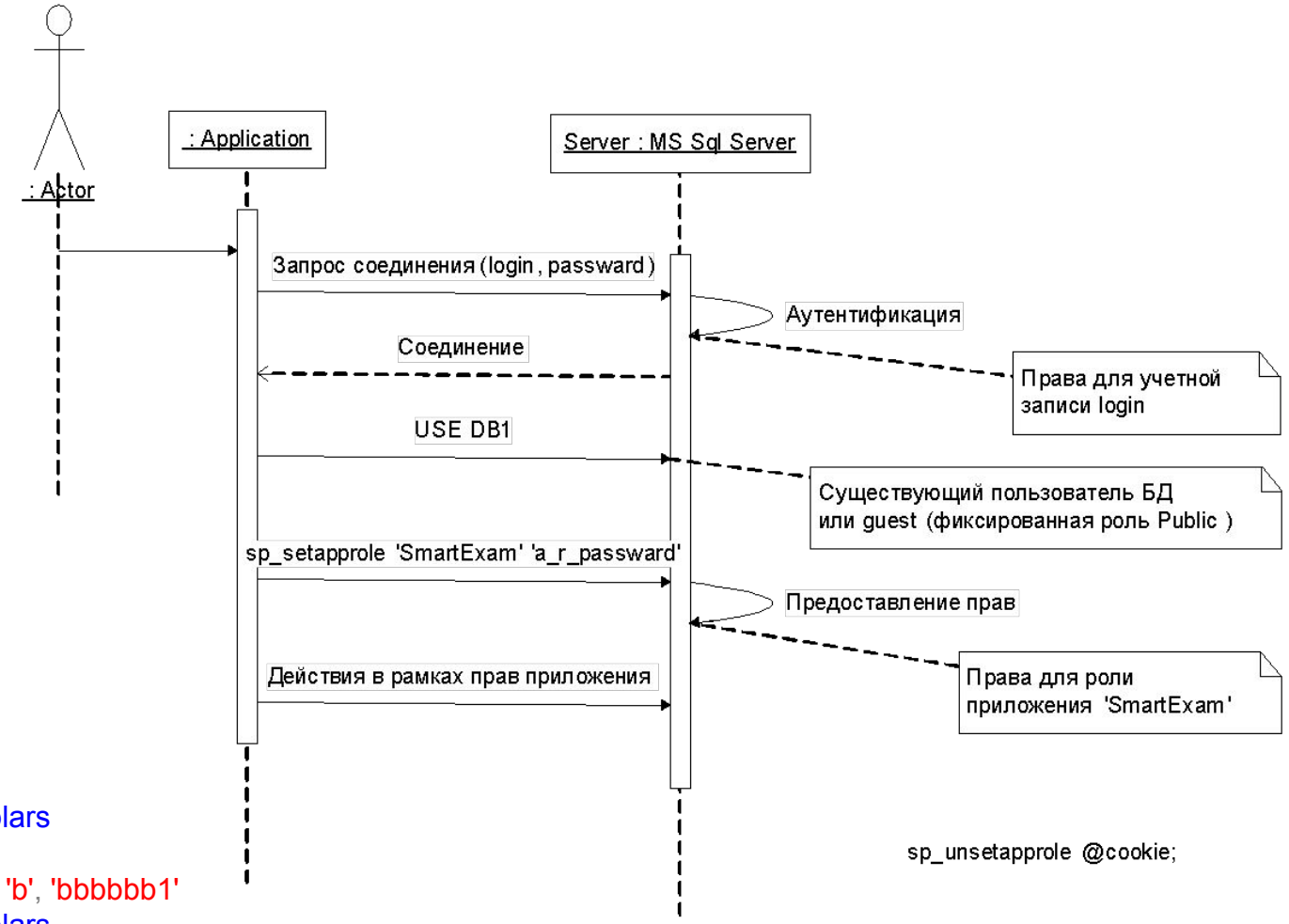
- Db_securityadmin – управление правами доступа к БД
- Db_owner – любые права, т.к. имеются права владельца
- Db_denydatawriter – запрещение изменения данных
- Db_denydatareader – запрещение чтения данных
- Db_ddladmin – создавать и управлять объектами
- Db_datawrite – может изменять данные
- Db_datareader – не может изменять данные
- Db_backupoperator – выполнение резервного копирования
- Db_accessadmin – управление пользователями БД

Роль Public – автоматически присваивается вновь созданным пользователям

Пользовательские роли и роль приложения



Порядок использования роли приложения




```
use lectures
select * from exemplars
print user
exec sp_setapprole 'b', 'bbbbbb1'
select * from exemplars
print user
```

Права

- Разрешение (предоставление) прав – команда GRANT
- Запрещение прав – команда DENY
- Отклонение прав – команда REVOKE

Минимальные права у пользователя БД после создания – Public.
Права выдаются администратором БД, владельцем БД или владельцем объектов БД.
Набор прав определяется ролями (фиксированными или пользовательскими).

Предоставление прав

Категории прав:

- Права доступа к объектам базы данных
- Права на выполнение команд Transact-SQL

Права доступа к **объектам** базы данных

GRANT
{ ALL | *permission* [,...*n*] }
{
[**(** *column* [,...*n*] **)**] ON { *table* | *view* }
| ON { *table* | *view* } [**(** *column* [,...*n*] **)**]
| ON { *stored_procedure* | *extended_procedure* }
| ON { *user_defined_function* }
}
TO *security_account* [,...*n*]
[WITH GRANT OPTION]
[AS { *group* | *role* }]

Права доступа к **объектам** базы данных

Права (permission)

- ALL – предоставляются все возможные разрения
- INSERT – вставка в таблицу или представление
- UPDATE – изменение данных таблиц и представлений, а также столбца
- DELETE – для таблицы и представления
- SELECT – выборка из таблицы, представления, столбца
- EXECUTE – разрешение запуска хранимой процедуры. Право на изменение хранимой процедуры принадлежит ее владельцу и не может быть предоставлено

Права доступа к **объектам** базы данных

- security_account – пользователь БД, пользовательская роль, пользователь Windows, группа Windows
- WITH GRANT OPTION – пользователь, которому выдаются права, тоже может предоставлять права
- AS { group | role } – группа Windows или роль БД, которой выдано разрешение предоставлять разрешения и которой принадлежит пользователь, выдающий разрешение

Права на **исполнение команд** Transact-SQL

GRANT { ALL | *statement* [**,**...*n*] }
    TO *security_account* [**,**...*n*]

Значения statement :

- ALL – все права
- CREATE DATABASE
- CREATE DEFAULT
- CREATE FUNCTION
- CREATE PROCEDURE
- CREATE RULE
- CREATE TABLE
- CREATE VIEW
- BACKUP DATABASE – резервное копирование БД
- BACKUP LOG – резервное копирование журнала транзакций

Примеры предоставления прав

```
-- Materials – таблица, Engineer – роль
-- Администратор выдает разрешение
GRANT SELECT, INSERT ON Materials TO Engineer WITH GRANT
   OPTION

-- Valentin – имеет роль Engineer,
-- Liss – не имеет роль Engineer.
-- Valentin выдает разрешение
GRANT SELECT, INSERT ON Materials TO Liss AS Engineer

-- Mary, John – пользователи БД,
-- [Corporate\BobJ] – член группы Windows
GRANT CREATE DATABASE, CREATE TABLE
TO Mary, John, [Corporate\BobJ]
```

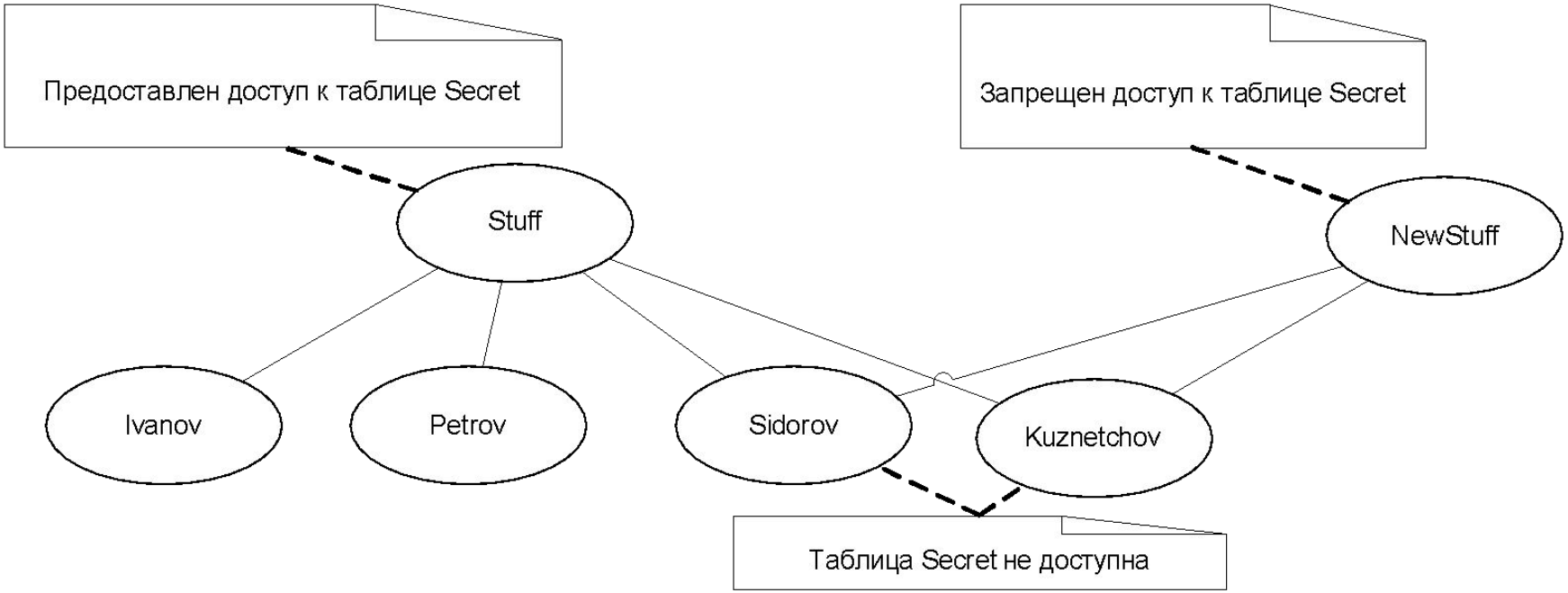
Неявные права

Неявные права не требуют явного разрешения:

- Права фиксированных ролей
- Права, переданные от других пользователей БД

Запрещение и отклонение прав

- Запрещение прав – запрещение, не зависимо от уровня, на котором выдано разрешение



Запрещение прав

Запрещение доступа к объектам базы данных

DENY
{ ALL [PRIVILEGES] | *permission* [**,**...*n*] }
{
[**(** *column* [**,**...*n*] **)**] ON { *table* | *view* }
| ON { *table* | *view* } [**(** *column* [**,**...*n*] **)**]
| ON { *stored_procedure* | *extended_procedure* }
| ON { *user_defined_function* }
}
TO *security_account* [**,**...*n*]
[CASCADE]

Запрещение права выполнения команд Transact-SQL

DENY { ALL | *statement* [**,**...*n*] }
TO *security_account* [**,**...*n*]

CASCADE – права отнимаются еще и у других пользователей, которым данный дал права

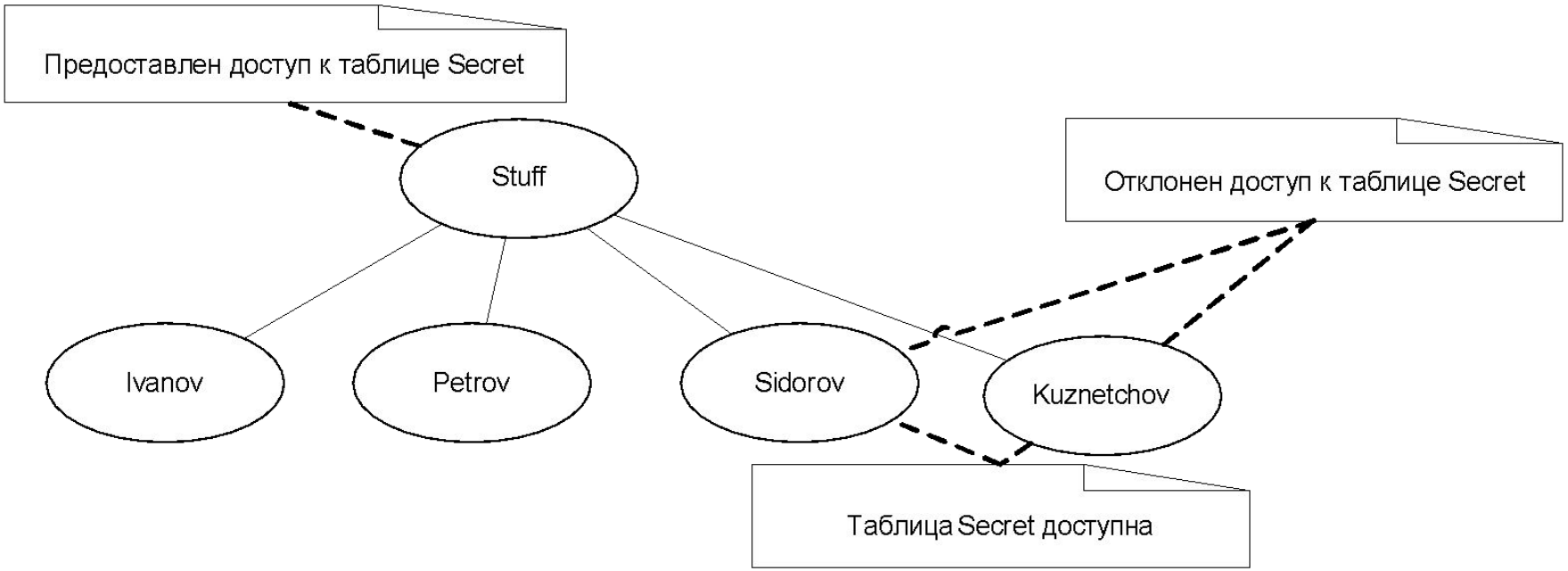
Пример запрещения

```
GRANT CREATE TABLE TO Petrov
WITH GRANT OPTION

-- Отнять разрешение у пользователя и тех пользователей,
-- которым он выдал разрешение
DENY CREATE TABLE TO Petrov
CASCADE
```

Отклонение прав

Отклонение – это запрещение, но только на том уровне, на котором оно определено.



Отклонение прав

Отклонение доступа к объектам базы данных

REVOKE [GRANT OPTION FOR]
{ ALL [PRIVILEGES] | *permission* [**,**...*n*] }
{
[**(** *column* [**,**...*n*] **)**] ON { *table* | *view* }
| ON { *table* | *view* } [**(** *column* [**,**...*n*] **)**]
| ON { *stored_procedure* | *extended_procedure* }
| ON { *user_defined_function* }
}
{ TO | FROM }
security_account [**,**...*n*]
[CASCADE]
[AS { *group* | *role* }]

Отклонение права выполнения команд Transact-SQL

REVOKE { ALL | *statement* [**,**...*n*] }
FROM *security_account* [**,**...*n*]

Отклонение прав

- GRANT OPTION FOR и CASCADE используются для того, чтобы отклонить права, выданные при помощи WITH GRANT OPTION в команде DENY
- FROM – при отклонении разрешения, TO – при отклонении запрещения

Примеры отклонения прав

```
REVOKE CREATE TABLE FROM Joe, [Corporate\BobJ]
REVOKE CREATE TABLE, CREATE DEFAULT FROM Mary, John

-- Отклонение запрещения (здесь TO, а не FROM)
REVOKE SELECT ON Budget_Data TO Mary
```

Конфликты доступа

Предоставление доступа имеет самый низкий приоритет, а запрещение – самый высокий