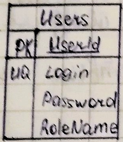
**Защита данных**

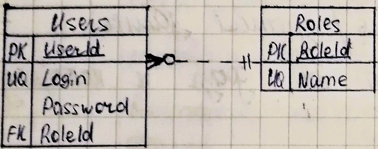
**Защита данных на уровне клиентского приложения** – требует создания в БД таблицу с пользователями

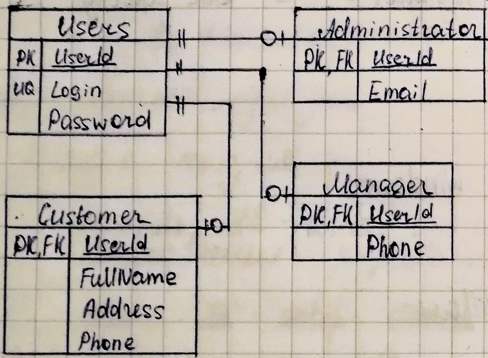
**Защита данных на уровне сервера** – требует создания пользователей сервера и БД и назначения им прав доступа

**Проектирование таблицы пользователей:**

* Всё в одной таблице



* Разделение таблиц
* Хранение информации о роли с указанием дополнительных атрибутов роли



Пароли в таблицах пользователей можно зашифровать, используя хеширование  
UPDATE Users

SET [Password] = HASHBYTES('SHA\_256', [Password])

WHERE UserId = ...

SELECT LolGame,

[Name],

HASHBYTES('SHA\_256',[Platform])

FROM [GamesN]

**Система безопасности MsSQL**

* Этапы предоставления доступа к данным

1. Аутентификация пользователя и предоставление доступа к серверу
2. Предоставление доступа к БД
3. Определение ролей, к которым принадлежит пользователь и авторизация доступа пользователя к логическим объектам БД на основе прав доступа логина и полей пользователя

* Получение доступа к серверу

Логин – учетная запись для подключения к SQL-серверу пример: ispp2101

Типы проверки подлинности:

- Windows использует логин Windows

* Защищенный
* Не требует ввода пароля
* Подключение только к ПК, на котором установлена СУБД

- SQL Server

Проверить состояние имени входа: Безопасность – Имя – Параметры – Свойства

Создание логина:

1. CREATE LOGIN ИмяВхода

WITH PASSWORD = 'пароль'

Дополнительные настройки:

CHECK\_EXPIRATION = ON – применение политики истечения срока действия

CHECK\_POLICY = ON – требования к паролю

MUST\_CHANGE – смена пароля после авторизации

1. Процедура: sp\_addlogin ‘ИмяВхода’, ‘пароль’
2. Сервер – Безопасность – Имена для входа – создать

Если имени входа нужны права доступа на уровне сервера, ему назначаются серверные роли, их нельзя создать, выбираются из списка доступных:

* public – нет прав, у каждого по умолчанию
* abcreator – создание / изменение / удаление / восстановление БД
* securityadmin – управление логинами и разрешениями
* sysadmin – все права доступа на сервере
* bulkadmin – команды BULK INSERT – вставка данных из файлов
* sp\_addsrvrolemember ‘ИмяВхода’ ‘РольСервера’
* sp\_dropsrvrolemember ‘Логин’ ‘Роль’
* Предоставление доступа на уровне БД

1. Создание пользователя

Пользователь БД – объект, создается на уровне БД и используется для предоставления разрешений к объектам БД

Схема БД – набор объектов БД, объединённым общим пространством имен

dbo – схема по умолчанию (database owner)

Пользователь: БД – Безопасность – Пользователи

Встроенные пользователи БД:

* dbo – владелец БД
* guest – используется для логина, которому нужно разрешить чтение данных

1. CREATE USER ИмяПользователяБД

FOR LOGIN ИмяВхода

1. sp\_adduser ‘ИмяВхода’, ‘ИмяПользователяБД’
2. Через оконный интерфейс
3. Назначение ролей доступа

Стандартные роли:

db\_owner – владелец БД

db\_datareader – разрешение чтения данных

db\_datawriter – DML-команды

db\_denydatareader – запрет чтения

db\_denydatawriter – запрет изменения

db\_ddladmin – DDL-команды

db\_accessadmin – добавления / удаление прав доступа к БД

db\_backupoperator – создание резервной копии БД

DCL – Data Control Language – GRANT, DENY, REVOKE

GRANT список команд

ON объект БД

TO пользователь БД

GRANT CREATE TABLE

TO guest

GRANT SELECT, UPDATE

ON Games

TO Guest

GRANT команды

ON Таблица(столбец1,столбец2, ...)

TO пользователь

DENY EXECUTE

ON Proct

TO guest

DENY VIEW

ANY DATABASE --запрет просмотра списка БД

TO ИмяВхода

Создание скриптов для автоматизации действий по настройке прав доступа

DECLARE @userCount INT = 15

DECLARE @currentUser INT = 1

DECLARE @abName VARCHAR (10)

DECLARE @password VARCHAR (20)

WHILE (@currentUser <= @userCount)

BEGIN

SET @abName = 'test' + CAST(@currentUser AS VARCHAR)

SET @password = 'pwd' + @abName

PRINT @abName

EXEC('CREATE LOGIN ['+@abName+'] WITH PASSWORD = N'''

+@password+''', CHECK\_POLICY = OFF')

EXEC('CREATE DATABASE ['+@abName+']')

EXEC('ALTER LOGIN ['+@abName+'] WITH DEFAULT\_DATABASE =

['+@abName+']')

EXEC('DENY VIEW ANY DATABASE TO ['+@abName+']')

--запрет просмотра баз данных

EXEC('USE ['+@abName+']')

EXEC (dbo.sp\_changedowner @loginame = '+@abName')

SET @currentUser +=1

END