МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«Череповецкий государственный университет»

Кафедра: Математического и программного обеспечения ЭВМ

Дисциплина: Администрирование баз данных

**Лабораторная работа № 3**

**ПРИМЕНЕНИЕ ПОЛИТИКИ ЗАЩИТЫ**

**Выполнил:**

студент гр. 1ИВТпб-01-41оп

Климов А.Г.

**Проверил:** преподаватель

Селяничев О.Л.

Отметка о зачете:

Череповец

2019 год

Указания к выполнению

В отчете отразить:

* тематику вопроса;
* придуманное задание по этой теме;
* решения (или оба).

Из общеобразовательной школы поступил заказ на написание приложения для работы с БД.

Предполагается, что пользователями его будут лица с разными правами доступа:

* директор (полные);
* учитель (успеваемость любого ученика, сведения о родителях);
* учащийся (успеваемость любого\_ученика/своя по любому предмету);
* фельдшер (медицинские данные).

Продумайте распределение прав по ширине (таблицам, полям) и по записям.

Ход работы

**Права (права)**— это возможность **выполнения конкретного типа SQL-оператора** или **доступа к объекту базы данных**, принадлежащему другому пользователю. В базе данных Oracle необходимо явно предоставить пользователю права для выполнения любых действий, включая подключение к базе данных или выборку, изменение и обновление данных в любой таблице, кроме собственной.

Существуют два основных типа прав Oracle: системные права и объектные права. Для предоставления пользователям как системных, так и объектных прав служит оператор GRANT. Оба эти типа прав Oracle подробно рассмотрены ниже.

**Системные права**

Системные права позволяют пользователю выполнить конкретное действие в базе данных либо действие с любым объектом схемы конкретного типа. Хороший пример первого типа системных полномочий — права, которые позволяют подключаться к базе данных, носящие название прав CONNECT. Другими правами этого типа являются права CREATE TABLESPACE, CREATE USER, DROP USER и ALTER USER. Второй класс системных прав предоставляет пользователям право на выполнение операций, которые влияют на объекты в любой схеме. Примерами этого типа системных прав служат ANALYZE ANY TABLE, GRANT ANY PRIVILEGE, NSERT ANY TABLE, GRANT ANY PRIVILEGE, INSERT ANY TABLE, DELETE ANY TABLE и т.п. Как видите, системные права являются очень мощным средством и выдача их не тому пользователю может оказать разрушительное влияние на базу данных. Ниже перечислены некоторые наиболее часто используемые права базы данных Oracle:

* *ADVISOR*
* *ALTER DATABASE*
* *ALTER SYSTEM*
* *AUDIT SYSTEM*
* *CREATE DATABASE LINK*
* *CREATE TABLE*
* *CREATE ANY INDEX*
* *CREATE SESSION*
* *CREATE TABLESPACE*
* *CREATE USER*
* *DROP USER*
* *INSERT ANY TABLE*

**Объектные права**

Объектные права — это полномочия по отношению к различным типам объектов базы данных. Объектные права дают пользователю возможность выполнять действия с конкретной таблицей, представлением, материализованным представлением, последовательностью, процедурой, функций или пакетом. Следовательно, всем пользователям базы данных нужны объектные права, даже если они не нуждаются в системных полномочиях. Существует ряд обычных системных прав, которые применяются ко всем объектам базы данных, и набор прав, применяемых только к определенным объектам. Для выдачи объектных прав можно использовать следующие SQL-операторы:

* *ALTER*
* *SELECT*
* *DELETE*
* *EXECUTE*
* *INSERT*
* *REFERENCES*
* *INDEX*

**Роли**

Хотя полномочиями пользователей достаточно легко управлять, непосредственно выдавая и отзывая их, эта задача может быстро стать чрезвычайно трудоемкой по мере добавления новых пользователей и увеличения количества объектов. Спустя некоторое время очень трудно отслеживать текущие полномочия каждого пользователя. Oracle решает эту проблему посредством применения ролей, представляющих собой именованные наборы прав, которые могут быть присвоены пользователям.

Роли можно считать набором прав, которые можно назначать и отзывать с помощью единственной команды *GRANT* или *REVOKE*. Роль может содержать как набор прав, так и другие роли. Роли облегчают присвоение нескольких прав пользователю. Заданная по умолчанию роль — это роль, которая автоматически вступает в действие, когда пользователь создает сеанс. Пользователю можно присваивать более одной роли по умолчанию.

Задание:

Создать базу данных школы.

Пользователи и права доступа:

* директор (полные);
* учитель (успеваемость любого ученика, сведения о родителях);
* учащийся (успеваемость любого\_ученика/своя по любому предмету);
* фельдшер (медицинские данные).

Продумать распределение прав по ширине (таблицам, полям) и по записям.

Примерная структура БД:

1. Список сотрудников Employees

Employee\_Id, Employee\_Name, Employee\_id, Employee\_Surname, Employee\_Type

2. Вид сотрудника (директор, учитель, фельдшер)

Employee\_Type\_Id, Employee\_Type\_Name, Employee\_Type\_Description

3. Список учеников (учитель) Students

Student\_Id, Student\_Name, Student\_Surname, Student\_Class\_Id, Student\_Parents\_Id

Список классов Classes

4. Class\_Id, Class\_Number, Class\_Char

5. Оценки учеников по математике (учитель) Student\_Marks\_Math

Student\_Marks\_Id, Student\_Id, Student\_Mark

6. Данные о родителях учеников (учитель) Parents

Parents\_Id, Parents\_Father\_Name, Parents\_Father\_Surname, Parents\_Mother\_Name, Parents\_Mother\_Surname, Parents\_Phone\_Number

7. Медицинские данные (фельдшер)

Medical\_Info\_Id, Medical\_Info\_Description

Выполнение

Создаём необходимые таблицы с данными.

Таблица классов школы:

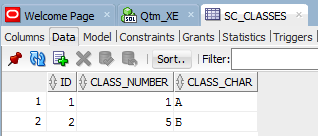


Таблица типа сотрудников школы:

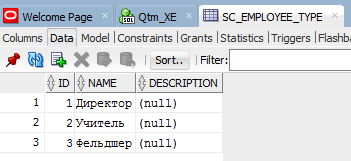


Таблица сотрудников школы:

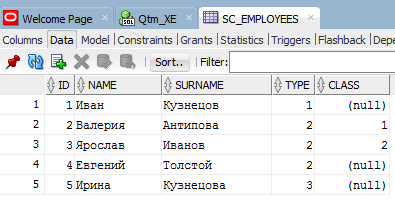


Таблица типа родителей учеников школы:

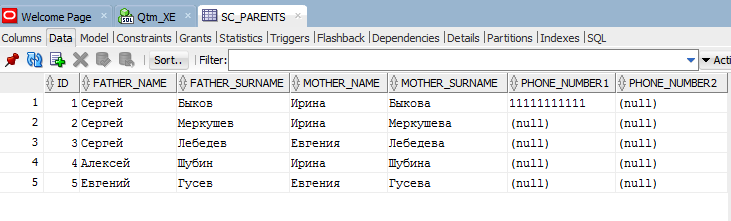


Таблица медицинской информации учеников школы:

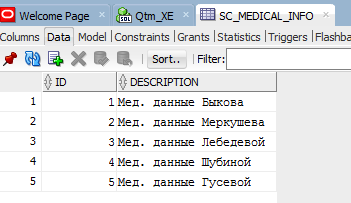


Таблица учеников школы:

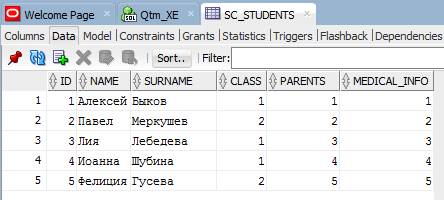
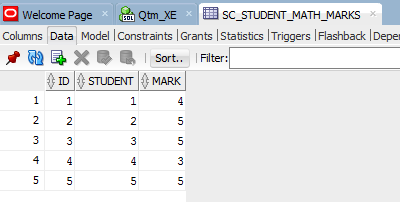


Таблица оценок по математике учеников школы:



Вывод списка пользователей БД:

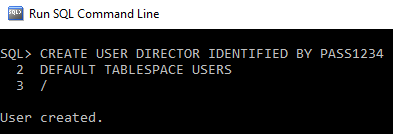
select username from dba\_users;

Создаём пользователей БД и предоставляем права.

Создание пользователя:

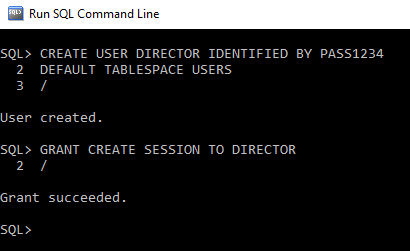
CREATE USER DIRECTOR IDENTIFIED BY PASS1234

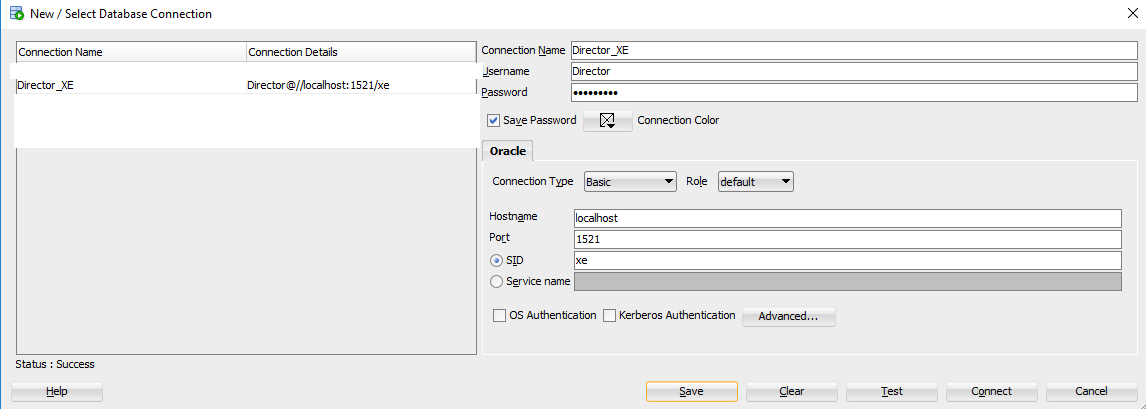
DEFAULT TABLESPACE USERS



Предоставление прав:

GRANT CREATE SESSION TO DIRECTOR





GRANT SELECT ANY TABLE TO DIRECTOR;

/

GRANT CREATE TABLE TO DIRECTOR

/

GRANT CREATE PROCEDURE TO DIRECTOR

/

GRANT CREATE TRIGGER TO DIRECTOR

/

GRANT CREATE VIEW TO DIRECTOR

/

GRANT CREATE SEQUENCE TO DIRECTOR

/

GRANT CREATE VIEW TO DIRECTOR

/

GRANT DELETE ANY TABLE TO DIRECTOR

/

GRANT DROP ANY TABLE TO DIRECTOR

/

GRANT DROP ANY PROCEDURE TO DIRECTOR

/

GRANT DROP ANY TRIGGER TO DIRECTOR

/

GRANT DROP ANY VIEW TO DIRECTOR

/

GRANT ALTER ANY TABLE TO DIRECTOR

/

GRANT ALTER ANY TABLE TO DIRECTOR

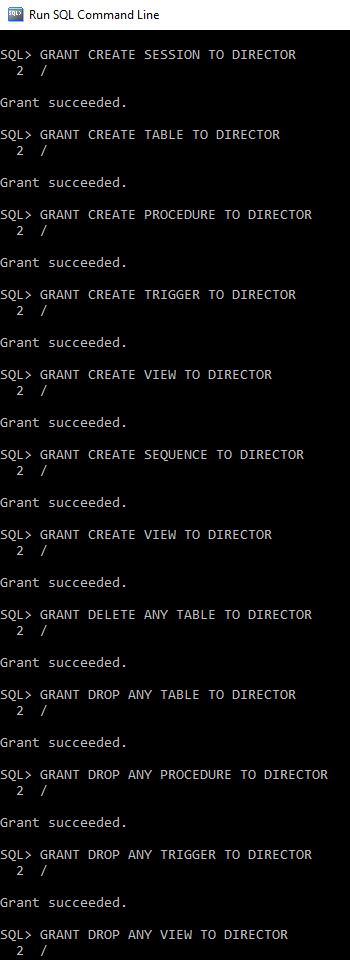
/

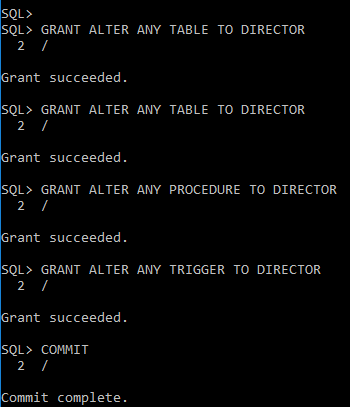
GRANT ALTER ANY PROCEDURE TO DIRECTOR

/

GRANT ALTER ANY TRIGGER TO DIRECTOR

/





GRANT SELECT ANY TABLE TO DIRECTOR;

/

GRANT SELECT on USERS to DIRECTOR;

Создание пользователя:

CREATE USER TEACHER IDENTIFIED BY PASS1234

DEFAULT TABLESPACE TEACHER

GRANT CREATE SESSION TO DIRECTOR

Предоставление прав:

GRANT SELECT ON SC\_CLASSES TO TEACHER

GRANT SELECT, INSERT, UPDATE, DELETE ON SC\_PARENTS TO TEACHER

GRANT SELECT, INSERT ON SC\_STUDENT\_MATH\_MARKS TO TEACHER

GRANT SELECT, INSERT ON SC\_STUDENTS TO TEACHER

Создание пользователя:

CREATE USER STUDENT IDENTIFIED BY PASS1234

DEFAULT TABLESPACE USERS

GRANT CREATE SESSION TO STUDENT

Предоставление прав:

GRANT SELECT ON SC\_STUDENT\_MATH\_MARKS TO STUDENT

Создание пользователя:

CREATE USER PARAMEDIC IDENTIFIED BY PASS1234

DEFAULT TABLESPACE USERS

GRANT CREATE SESSION TO PARAMEDIC

Предоставление прав:

GRANT SELECT, INSERT, UPDATE ON SC\_MEDICAL\_INFO TO PARAMEDIC

Вывод списка пользователей БД:

select username from dba\_users;



Таблицы:

SC\_STUDENTS – учитель

SC\_STUDENT\_MATH\_MARKS – учитель, студент

SC\_MEDICAL\_INFO – фельдшер

Директор может просматривать все таблицы

Права:

GRANT SELECT ANY TABLE TO DIRECTOR

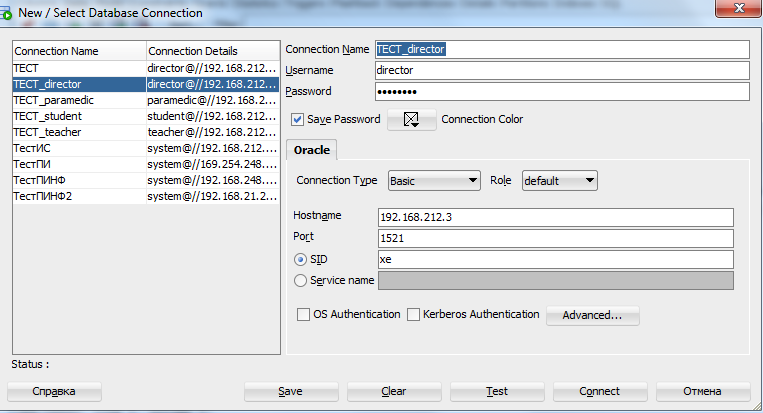
GRANT SELECT, INSERT ON SC\_STUDENTS TO TEACHER

GRANT SELECT, INSERT ON SC\_STUDENT\_MATH\_MARKS TO TEACHER

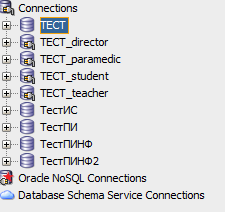
GRANT SELECT ON SC\_STUDENT\_MATH\_MARKS TO STUDENT

GRANT SELECT, INSERT, UPDATE ON SC\_MEDICAL\_INFO TO PARAMEDIC

Настройка подключения учётных записей к БД:

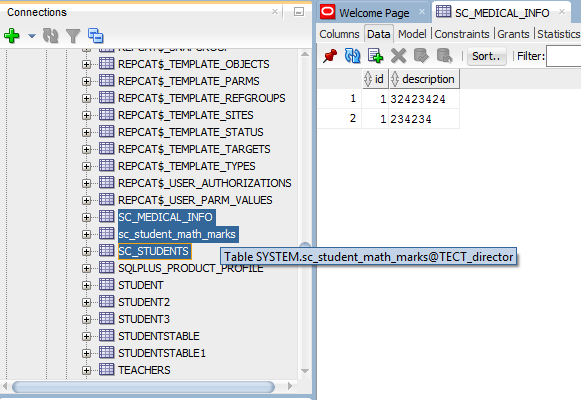


Учётные записи (DIRECTOR, TEACHER, STUDENT, PARAMEDIC) подключены к БД:

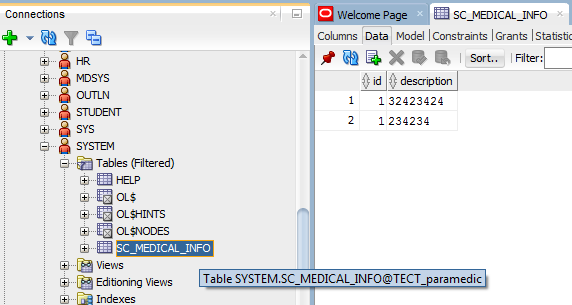


Затем производится проверка выделенных прав учётным записям.

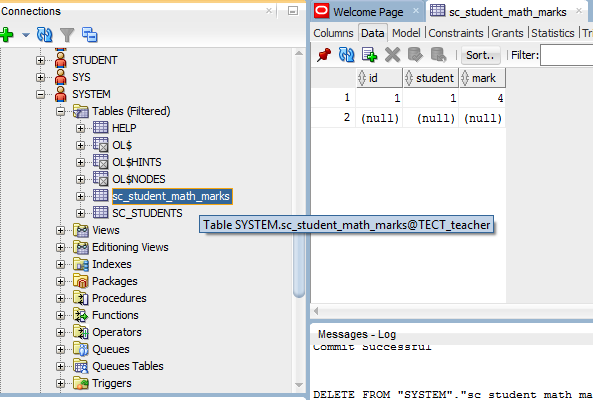
Доступ ко всем таблицам из-под учётной записи DIRECTOR:



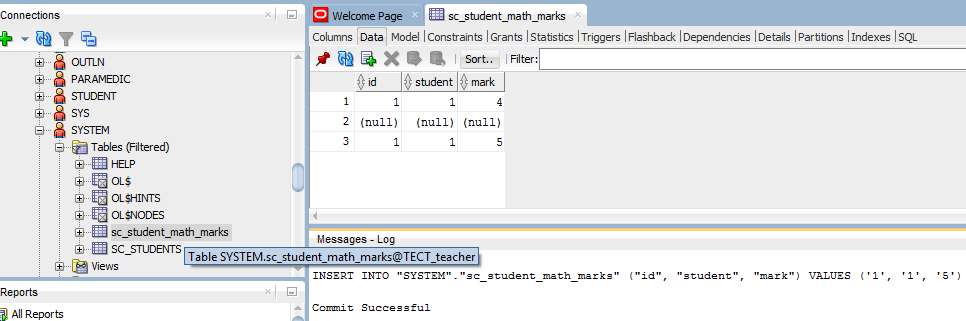
Доступ к своей таблице для PARAMEDIC:



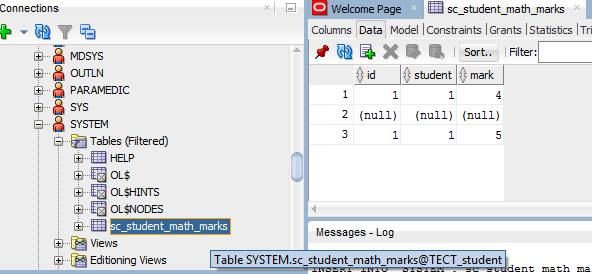
Доступ к таблицам из-под учётной записи TEACHER:



Добавление оценки из-под учётной записи TEACHER:



Доступ к таблицам из-под учётной записи STUDENT:



Добавление оценки из-под учётной записи STUDENT:

