Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Отчет

по лабораторной работе по теме: “Ролевая модель PostgreSQL”

по дисциплине «**Информационная безопасность**»

Автор: Юрпалов С. Н.

Факультет: ИТиП

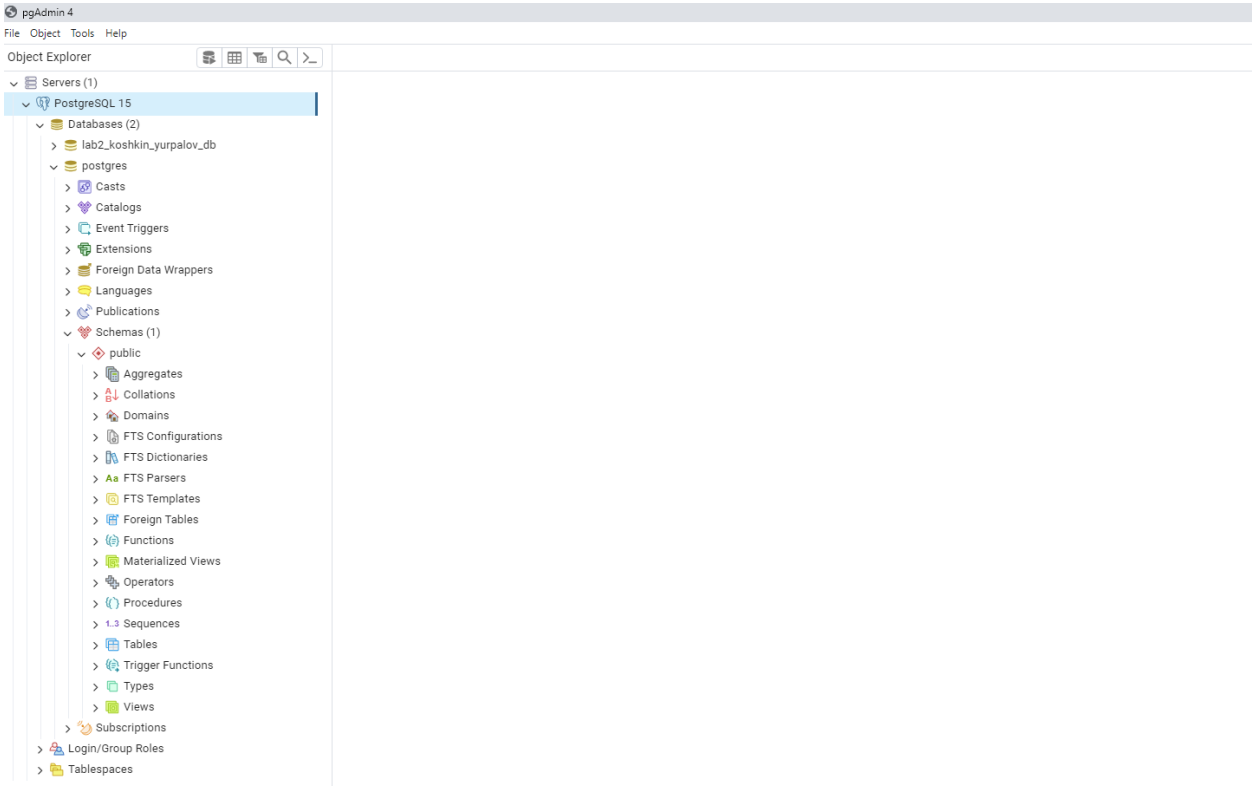
Группа: М34051

Санкт-Петербург 2023

Ход работы:

0) Настройка

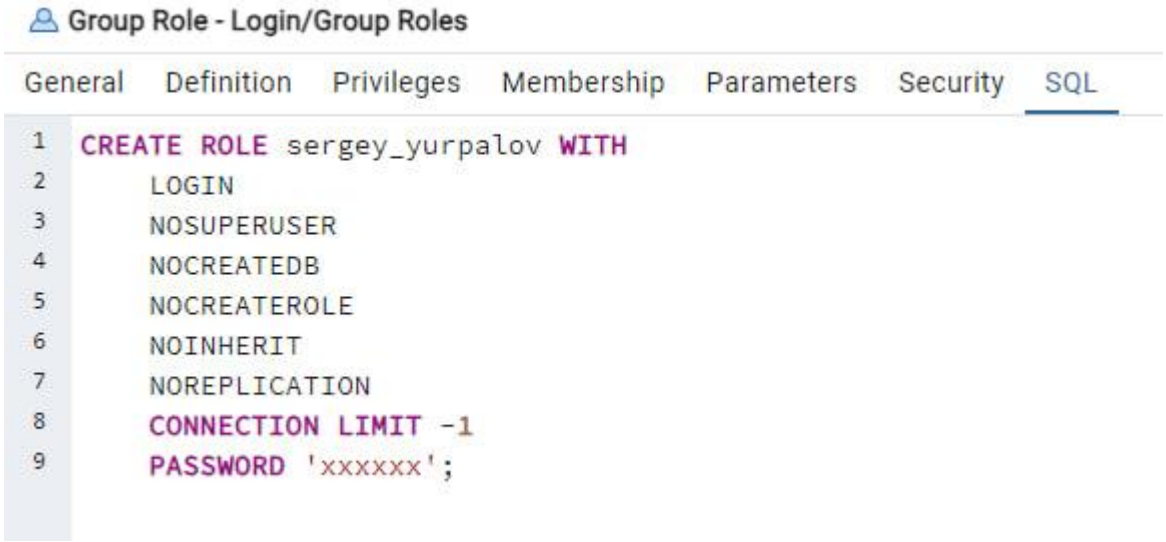
Работаем с PostgreSQL 15.6 через pgAdmin4.



1) Создание необходимых ролей

Роль, которая будет представлять Вас. В качестве имени роли укажите свои имя_фамилию, например ivan_ivanov. Роль должна иметь разрешения на вход и не должна обладать правами суперпользователя.

Включаем только опцию LOGIN.



Групповые роли с именами itmo_users и itmo_readers. Эти роли не должны обладать разрешениями: на вход, на создание баз данных, на создание других ролей.

Не включаем ни одну опцию.

Group Role - Login/Group Roles

General Definition Privileges Membership Parameters Security SQL

```
CREATE ROLE itmo_users WITH
    NOLOGIN
    NOSUPERUSER
    NOCREATEDB
    NOCREATEROLE
    NOINHERIT
    NOREPLICATION
    CONNECTION LIMIT -1;
```

Group Role - Login/Group Roles

General Definition Privileges Membership Parameters Security SQL

```
CREATE ROLE itmo_readers WITH
    NOLOGIN
    NOSUPERUSER
    NOCREATEDB
    NOCREATEROLE
    NOINHERIT
    NOREPLICATION
    CONNECTION LIMIT -1;
```

Роли с именами itmo_user_1 и itmo_reader_1. Эти роли должны обладать только разрешением на вход. Добавьте роль itmo_user_1 в групповую роль itmo_users, а itmo_reader_1 в itmo_readers. Пользовательские роли должны наследовать разрешения групповых ролей.

Включаем опции LOGIN и INHERIT, добавляем в соответствующие группы.

Group Role - Login/Group Roles

General Definition Privileges Membership Parameters Security SQL

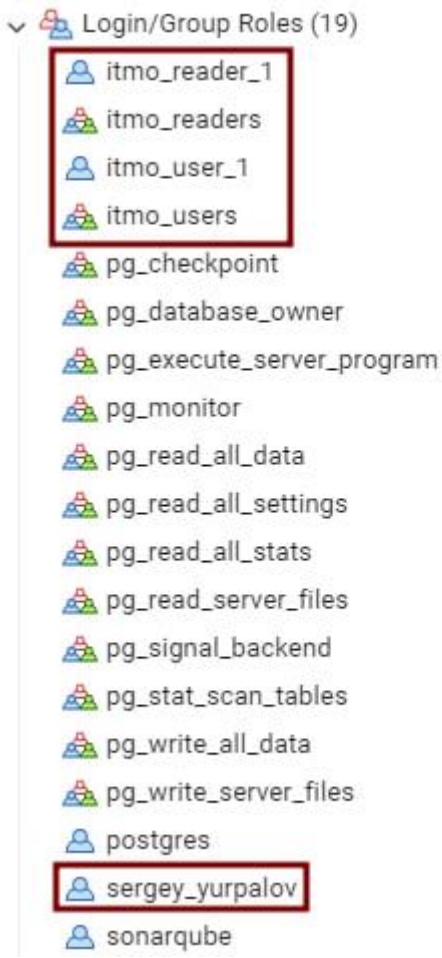
```
1  CREATE ROLE itmo_user_1 WITH
2      LOGIN
3      NOSUPERUSER
4      NOCREATEDB
5      NOCREATEROLE
6      INHERIT
7      NOREPLICATION
8      CONNECTION LIMIT -1
9      PASSWORD 'xxxxxx';
10
11 GRANT itmo_users TO itmo_user_1;
```

Group Role - Login/Group Roles

General Definition Privileges Membership Parameters Security SQL

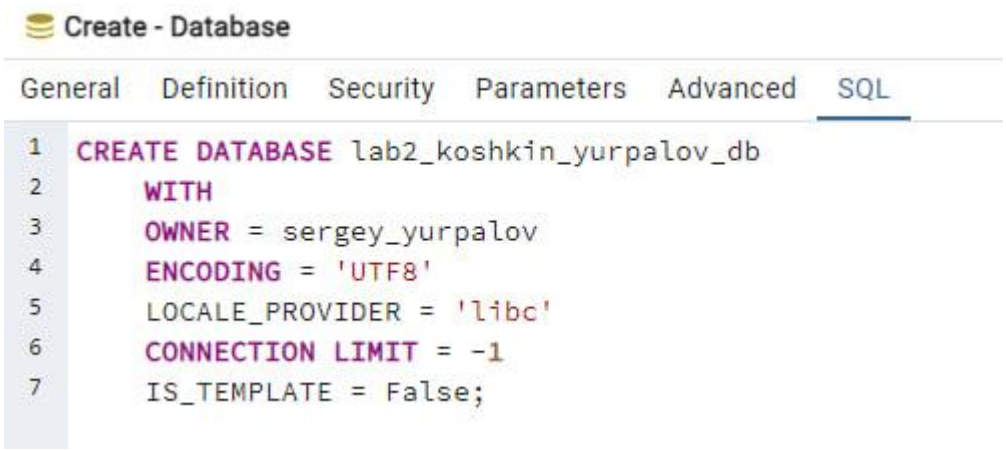
```
1  CREATE ROLE itmo_reader_1 WITH
2      LOGIN
3      NOSUPERUSER
4      NOCREATEDB
5      NOCREATEROLE
6      INHERIT
7      NOREPLICATION
8      CONNECTION LIMIT -1
9      PASSWORD 'xxxxxx';
10
11 GRANT itmo_readers TO itmo_reader_1;
```

Итого имеем:


Login/Group Roles (19)
itmo_reader_1
itmo_readers
itmo_user_1
itmo_users
pg_checkpoint
pg_database_owner
pg_execute_server_program
pg_monitor
pg_read_all_data
pg_read_all_settings
pg_read_all_stats
pg_read_server_files
pg_signal_backend
pg_stat_scan_tables
pg_write_all_data
pg_write_server_files
postgres
sergey_yurpalov
sonarqube

2) Создание Базы Данных

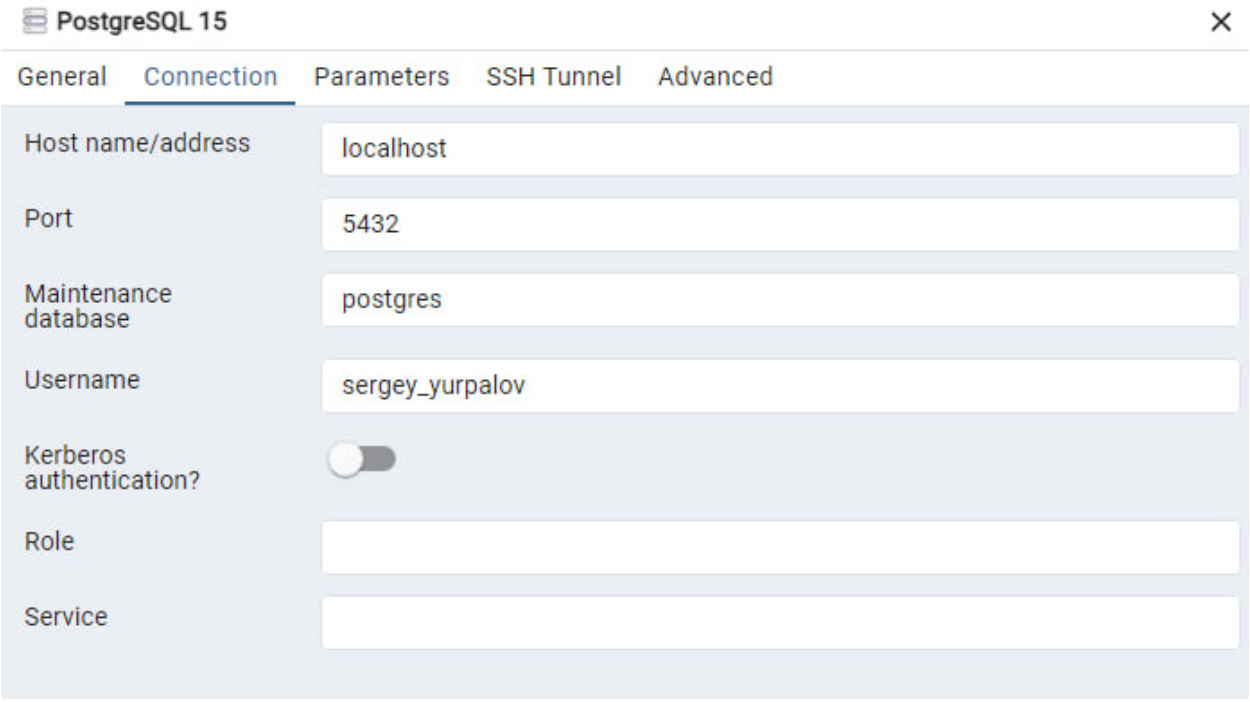
Создайте новую Базу Данных. В качестве владельца укажите Вашу роль.



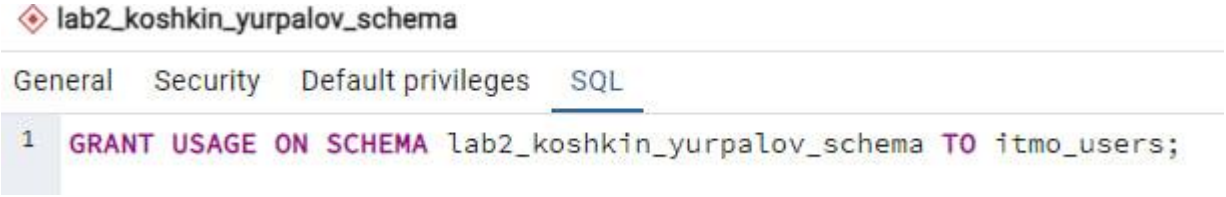
3) Создание Таблиц

Переподключитесь к новой БД под своей ролью. В этой БД создайте 2-3 таблицы. Наполните их значениями.

Используем роль sergey_yurpalov



Создадим схему, в которой будем работать. Дадим нашим ролям право на usage.



Создадим таблицы.

Create - Table

General Columns Advanced Constraints Partitions Parameters Security SQL

```sql
CREATE TABLE lab2_koshkin_yurpalov_schema.employees
(
    id serial NOT NULL,
    name character varying(100) NOT NULL,
    age integer NOT NULL,
    department character varying(100) NOT NULL,
    salary numeric(10, 2) NOT NULL,
    PRIMARY KEY (id)
);

ALTER TABLE IF EXISTS lab2_koshkin_yurpalov_schema.employees
    OWNER to sergey_yurpalov;
```

Create - Table

General Columns Advanced Constraints Partitions Parameters Security SQL

```sql
CREATE TABLE lab2_koshkin_yurpalov_schema.products
(
    id serial NOT NULL,
    name character varying(100) NOT NULL,
    category character varying(100) NOT NULL,
    price numeric(10, 2) NOT NULL,
    stock_quantity integer NOT NULL,
    PRIMARY KEY (id)
);

ALTER TABLE IF EXISTS lab2_koshkin_yurpalov_schema.products
    OWNER to sergey_yurpalov;
```

Наполним их данными из .csv

employees

```
name,age,department,salary
John Doe,30,Engineering,60000.00
Jane Smith,28,Marketing,55000.00
Michael Johnson,35,Finance,65000.00
Emily Brown,32,HR,58000.00
Chris Lee,40,Operations,70000.00
```

```
SELECT * FROM lab2_koshkin_yurpalov_schema.employees
ORDER BY id ASC
```

Data Output | Messages | Notifications

	id [PK] integer	name character varying (100)	age integer	department character varying (100)	salary numeric (10,2)
1	1	John Doe	30	Engineering	60000.00
2	2	Jane Smith	28	Marketing	55000.00
3	3	Michael Johnson	35	Finance	65000.00
4	4	Emily Brown	32	HR	58000.00
5	5	Chris Lee	40	Operations	70000.00

products

```
name,category,price,stock_quantity
Laptop,Electronics,1200.00,15
Headphones,Electronics,100.00,30
Desk,Office Furniture,250.00,10
Notebook,Stationery,5.00,100
Chair,Office Furniture,150.00,20
```

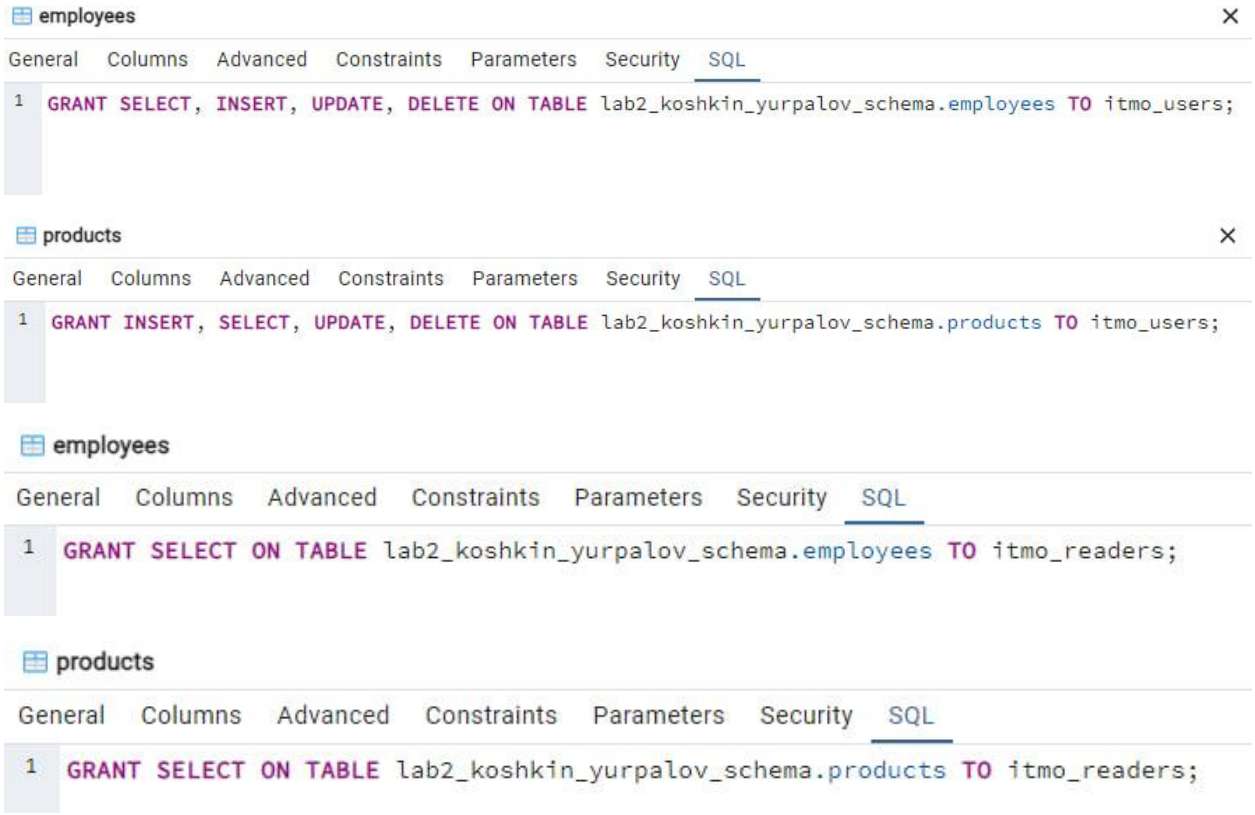
```
SELECT * FROM lab2_koshkin_yurpalov_schema.products
ORDER BY id ASC
```

Data Output | Messages | Notifications

	id [PK] integer	name character varying (100)	category character varying (100)	price numeric (10,2)	stock_quantity integer
1	1	Laptop	Electronics	1200.00	15
2	2	Headphones	Electronics	100.00	30
3	3	Desk	Office Furniture	250.00	10
4	4	Notebook	Stationery	5.00	100
5	5	Chair	Office Furniture	150.00	20

4) Установка Привилегий

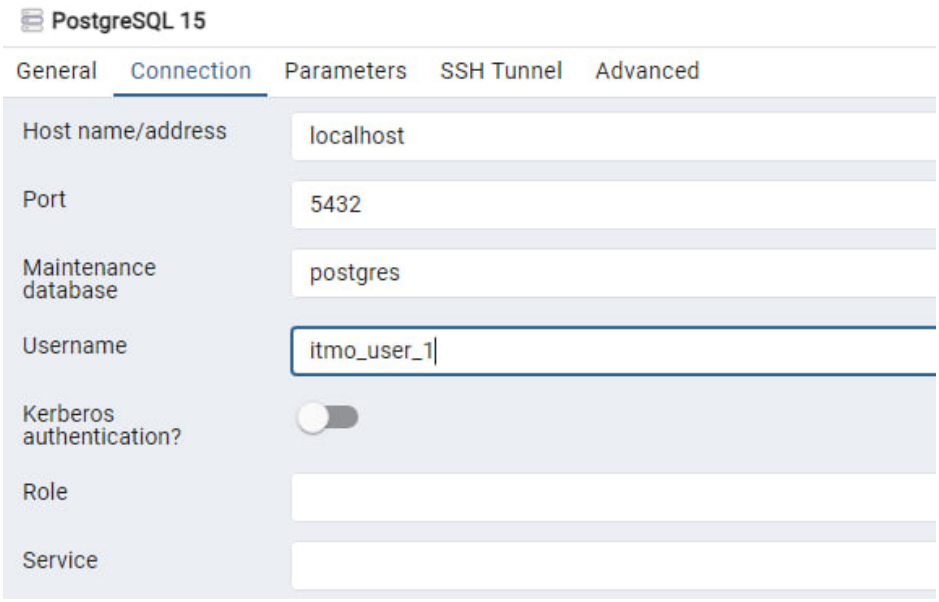
От имени своей роли выдайте разрешения роли itmo_users на чтение, вставку, обновление и удаление (SELECT, INSERT, UPDATE, DELETE) записей во всех таблицах текущей Базы Данных. От имени своей роли выдайте разрешения роли itmo_readers только на чтение (SELECT) записей во всех таблицах текущей Базы Данных



5) Проверка прав

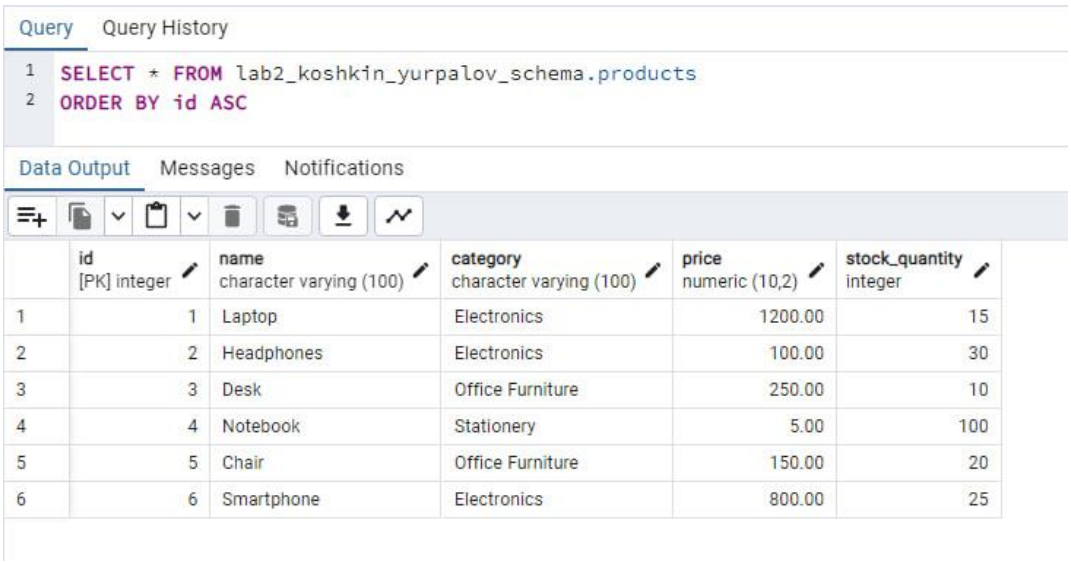
Подключитесь к БД под ролью itmo_user_1. Выполните чтение записей любой из таблиц. Выполните вставку новой записи. Попробуйте создать новую таблицу. Те же действия проделайте под ролью itmo_reader_1.

Зайдём под itmo_user_1.



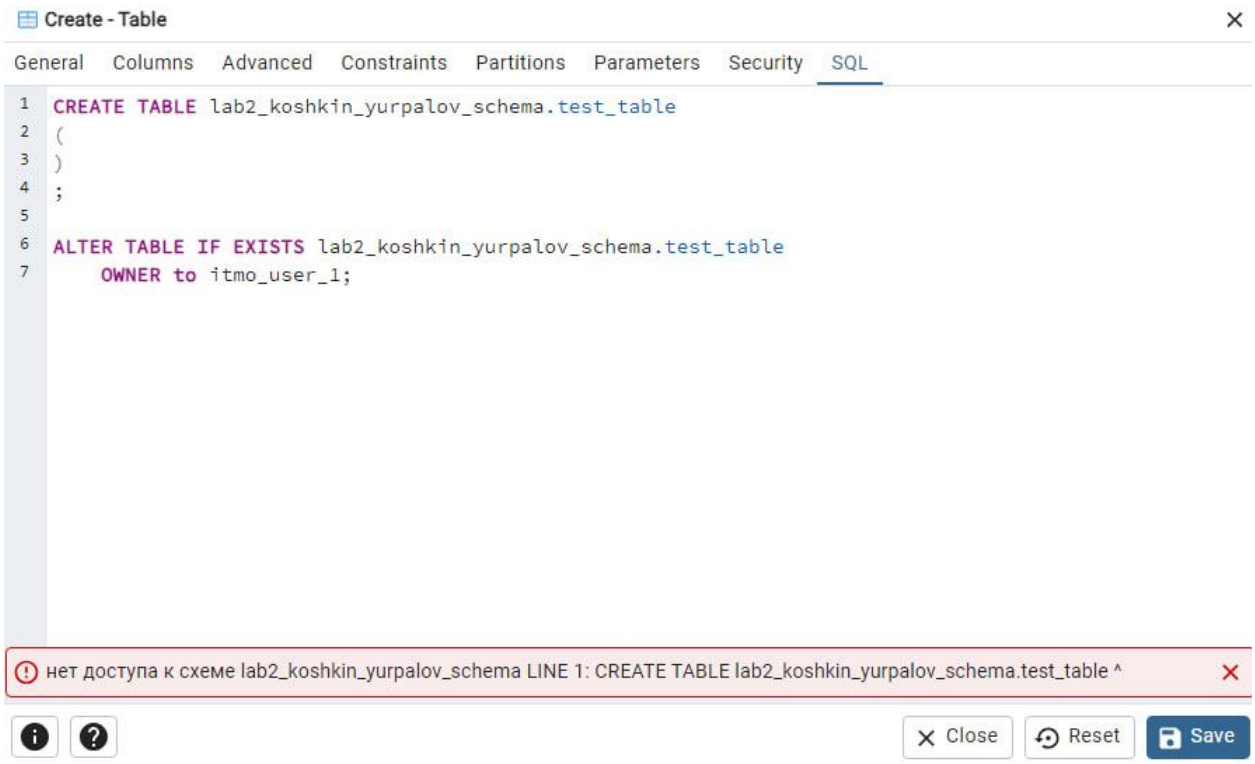
Вставим новую запись.

Прочитаем данные таблицы.



	id [PK] integer	name character varying (100)	category character varying (100)	price numeric (10,2)	stock_quantity integer
1	1	Laptop	Electronics	1200.00	15
2	2	Headphones	Electronics	100.00	30
3	3	Desk	Office Furniture	250.00	10
4	4	Notebook	Stationery	5.00	100
5	5	Chair	Office Furniture	150.00	20
6	6	Smartphone	Electronics	800.00	25

Попытаемся создать новую таблицу.



Не можем этого сделать, т.к. права роли itmo_users давались только на взаимодействие с данными в таблицах. В схеме у неё есть только право usage, которое не даёт возможности создать таблицу.

Переключимся на itmo_reader_1.

Прочитаем данные таблицы.

Query | Query History

```
1 SELECT * FROM lab2_koshkin_yurpalov_schema.products
2 ORDER BY id ASC
```

Data Output | Messages | Notifications

	id [PK] integer	name character varying (100)	category character varying (100)	price numeric (10,2)	stock_quantity integer
1	1	Laptop	Electronics	1200.00	15
2	2	Headphones	Electronics	100.00	30
3	3	Desk	Office Furniture	250.00	10
4	4	Notebook	Stationery	5.00	100
5	5	Chair	Office Furniture	150.00	20
6	6	Smartphone	Electronics	800.00	25

Попытаемся создать запись.

Query | Query History

```
1 INSERT INTO lab2_koshkin_yurpalov_schema.products (id, name, category, price, stock_quantity)
2 VALUES (7, 'Smartphone', 'Electronics', 800.00, 25);
3
```

Data Output | Messages | Notifications

```
ERROR:  нет доступа к таблице products

ОШИБКА:  нет доступа к таблице products
SQL state: 42501
```

Не можем этого сделать, т.к. права на INSERT мы не давали.

Попытаемся создать таблицу.

Create - Table

General | Columns | Advanced | Constraints | Partitions | Parameters | Security | SQL

```
1 CREATE TABLE lab2_koshkin_yurpalov_schema.test_table
2 (
3 )
4 ;
5
6 ALTER TABLE IF EXISTS lab2_koshkin_yurpalov_schema.test_table
7     OWNER to itmo_reader_1;
```

нет доступа к схеме lab2_koshkin_yurpalov_schema LINE 1: CREATE TABLE lab2_koshkin_yurpalov_schema.test_table ^

Не можем этого сделать, т.к. права роли itmo_readers давались только на взаимодействие с данными в таблицах. В схеме у неё есть только право usage, которое не даёт возможности создать таблицу.

6) Вопросы

1) Владелец базы данных — это роль, обладающая определенными привилегиями в отношении конкретной базы данных, такими как возможность создавать, изменять и удалять объекты в этой базе данных. Как правило, они имеют право собственности на созданные ими объекты. Отличие от суперпользователя заключается в том, что суперпользователь имеет полные привилегии во всей системе баз данных, включая возможность изменять системные каталоги и управлять другими пользователями и ролями.
2) Одна роль может иметь доступ к нескольким базам данных. Роли в PostgreSQL могут иметь привилегии для нескольких баз данных, что позволяет им выполнять операции в этих базах данных в соответствии с их разрешениями.
3) Роль пользователя представляет отдельного пользователя в системе баз данных, а групповая роль — это совокупность ролей пользователей. Групповые роли используются для упрощения управления разрешениями путем назначения разрешений группе, а не отдельным пользователям. При необходимости пользователей можно добавлять в групповые роли или удалять из них, что упрощает администрирование и контроль доступа.