Министерство образования и науки Российской Федерации

Санкт-Петербургский государственный политехнический университет

Институт Компьютерных наук и кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 1**

по дисциплине «Безопасность баз данных»

Выполнил

студент гр. 5141001/30301 Б.Ю. Фитьо

<*подпись*>

Преподаватель

доцент, к.т.н. М.А. Полтавцева

<*подпись*>

Санкт-Петербург

2023

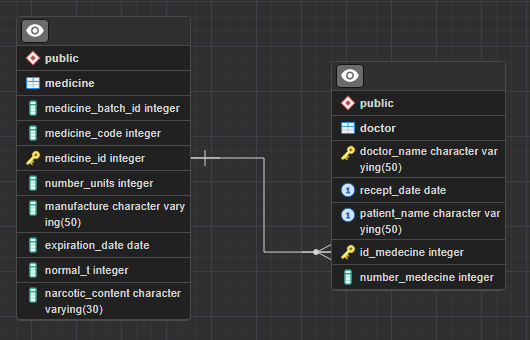
2. Цель работы

Получение навыков создания схемы данных и базового разграничения доступа при работе с СУБД.

3. Задание на работу (Вар. 3)

Создание схемы данных и реализации над ней набора прав доступа, как минимум — указанных в варианте выполнения лабораторной работы.

4. Логическая схема данных в виде рисунка



5. Код реализации схемы данных

DROP TABLE IF EXISTS Medicine CASCADE;

CREATE TABLE Medicine

( Medicine\_batch\_id int not null,

Medicine\_code int not null,

Medicine\_id serial primary key,

Number\_units int not null,

Manufacture varchar(50) not null,

Expiration\_date date not null,

Normal\_t int,

Narcotic\_content varchar(30) not null default 'No');

DROP TABLE IF EXISTS Visits CASCADE;

CREATE TABLE Doctor

( Doctor\_name varchar(50) not null default current\_user,

Recept\_date date not null default now(),

Patient\_name varchar(50) not null,

Id\_medecine int not null,

Number\_medecine int not null default 1,

primary key (Doctor\_name, Id\_medecine),

foreign key (Id\_medecine) references Medicine(Medicine\_id)

on delete cascade on update cascade,

CONSTRAINT AK1 UNIQUE

(Recept\_date, Id\_medecine),

CONSTRAINT AK2 UNIQUE

(Patient\_name, Id\_medecine)

);

6. Разработанная матрица доступа со всеми условиями и дополнениями

|  |  |  |
| --- | --- | --- |
|  | Врач (истекший срок годности лекарств) | Врач (свежие лекарства) |
| Medicine.Medicine\_batch\_id | - | - |
| Medicine.Medicine\_code | - | R |
| Medicine.Medicine\_id | - | - |
| Medicine.Number\_units | - | R |
| Medicine.Manufacture | - | R |
| Medicine.Expiration\_date | - | R |
| Medicine.Normal\_t | - | R |
| Medicine.Narcotic\_content | - | R |

|  |  |  |
| --- | --- | --- |
|  | Врач (чужие пациенты) | Врач (свои пациенты) |
| Doctor. Doctor\_name | R | R |
| Doctor. Recept\_date | R | R |
| Doctor. Patient\_name | - | RUC |
| Doctor. Id\_medecine | R | RC |
| Doctor. Number\_medecine | R | RUC |

7. Код реализации учетных записей

DROP ROLE IF EXISTS Doctor;

CREATE ROLE Doctor;

ALTER TABLE medicine ENABLE ROW LEVEL SECURITY;

GRANT SELECT

(Medicine\_code, Number\_units, Manufacture, Expiration\_date, Normal\_t, Narcotic\_content)

ON table medicine TO Doctor;

CREATE POLICY Doctor\_select\_policy ON Medicine

FOR SELECT TO Doctor

USING (medicine.Expiration\_date > now())

GRANT SELECT

(Doctor\_name, Recept\_date, Patient\_name, Id\_medecine, Number\_medecine)

ON table doctor TO Doctor;

GRANT INSERT

(Patient\_name, Id\_medecine, Number\_medecine)

ON table doctor TO Doctor;

GRANT update

(Patient\_name, Number\_medecine)

ON table doctor TO Doctor;

CREATE POLICY Doctor\_insert\_policy ON doctor

FOR Insert TO Doctor

with check (doctor.doctor\_name = current\_user)

CREATE POLICY Doctor\_upd\_policy ON doctor

FOR Update TO Doctor

using (doctor.doctor\_name = current\_user)

8. Выводы

Реализовать часть разграничения доступа не получилось, так как предикатов и политики недостаточно. В данном случае информация для создания булевых условий для ролей хранится в разных таблицах. В предикатах невозможно использовать сложные условия, а в политиках невозможно сравнивать значения из разных таблиц, SQL не предоставляет такой возможности ни USING, ни в WITH CHECK.

9. Список литературы

1. Практикум по построению защищенных баз данных — М.А. Полтавцева, Е.А. Зубков, Д.А. Москвин, Т.Д. Овасапян, И.А. Сикарев — ПолитехПресс 2023

2. Официальная документация PostgreSQL – www.postgresql.org/docs/