«Национальный исследовательский ядерный университет «МИФИ»

Институт интеллектуальных кибернетических систем

Кафедра №42 «Криптология и кибербезопасность»

Отчёт по лабораторной работе № 2\_2

"Безопасность базы данных"

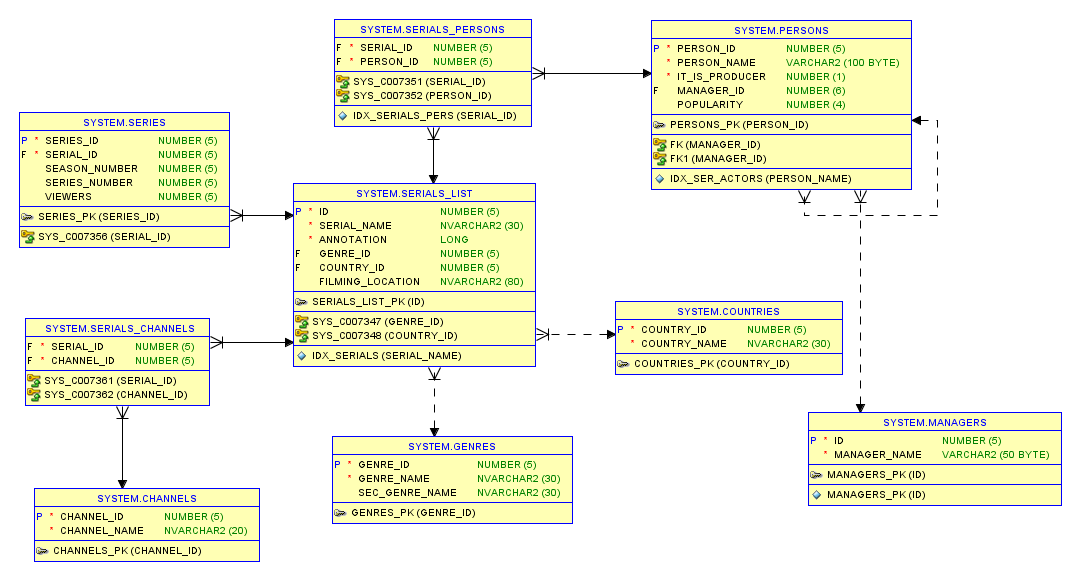
Студент: Нурматов С.Р.

Группа: Б17-565

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2020

**Диаграмма сущностей**

****

|  |  |  |
| --- | --- | --- |
| Пользователи | Роль | Полномочия |
| Admin | Администратор Базы Данных | Человек, который отвечает, создание, проектирование, корректировку, а также разграничение доступа в БД. |
| Manager  Manager\_assistant | Менеджер и его ассистент | Человек и группа людей, имеющие объектные привилегии и дополнительные, соответствующие его должности. |
| User1, User2, Trainee | Рядовые пользователи и стажер (потенциальный рядовой пользователь) | Люди, имеющие доступ к данным не конфиденциального характера и к данным, которые требуются для работы, но при неправильной корректировки не понесут серьезных последствий. |

1. От лица главного пользователя создан пользователь “admin” который будет обладать всеми привилегиями.

CREATE user c##admin identified by password;

GRANT ALL PRIVILEGES TO c##admin;

1. Для проверки корректной работы базы данных от лица пользователя “admin” были созданы пользователи manager(менеджер) и manager\_assistant (Ассистент менеджера). Чтобы не выдавать одинаковые привилегии каждому пользователю была создана роль, которой были выданы объектные привилегии.

CREATE ROLE c##manager\_role;

GRANT CREATE TABLE TO C##manafer\_role;

GRANT SELECT ANY TABLE TO c##manager\_role;

GRANT DELETE ANY TABLE TO c##manager\_role;

GRANT INSERT ANY TABLE TO c##manager\_role;

GRANT UPDATE ANY TABLE TO C##manager\_role;

GRANT CREATE SESSION TO c##manager\_role;

CREATE user C##MANAGER identified by manager;

Кроме того, менеджеру были выданы ряд следующих привилегий которые должны соответствовать должности менеджера.

GRANT CREATE ANY MATERIALIZED VIEW TO c##manager;

GRANT CREATE ANY VIEW TO c##manager;

GRANT CREATE ANY TRIGGER TO c##manager;

GRANT ALTER ANY TABLE TO c##manager;

GRANT CREATE USER TO c##manager;

GRANT DROP USER TO c##manager;

GRANT DROP ANY MATERIALIZED VIEW TO c##manager;

GRANT DROP ANY VIEW TO c##manager;

GRANT DROP ANY TRIGGER TO c##manager;

GRANT CREATE CLUSTER TO c##manager;

GRANT DROP ANY CLUSTER TO c##manager;

CREATE user c##manager\_assistant identified by manager\_assistant

Роль, которой были выданы основные привилегии присваивается менеджеру и его ассистенту.

GRANT c##manager\_role TO c##manager;

GRANT c##manager\_role to c##manager\_assistant;

1. Так же были созданы обычные пользователи “user1”, ‘user2”. Для них была создана роль user\_role, которая будет иметь пакет привилегий, соответствующий их должностям. Так как есть открытые вакансии, на работу могут устроиться еще несколько таких же пользователей, которым потребуются такие же привилегии. С готовым пакетом привилегий не потребуется лишних усилий для выдачи GRANTов.

CREATE ROLE c##user\_role;

REVOKE CREATE SESSION FROM c##user1;

REVOKE CREATE SESSION FROM c##user2;

GRANT CREATE SESSION TO c##user\_role;

GRANT CREATE ANY MATERIALIZED VIEW TO c##user\_role;

GRANT UPDATE ANY TABLE TO c##user\_role;

GRANT CREATE ANY VIEW TO c##user\_role;

REVOKE CREATE ANY VIEW FROM C##user\_role;

GRANT CREATE VIEW TO c##user\_role;

GRANT SELECT ON serials\_list TO c##user\_role;

GRANT SELECT ON countries TO c##user\_role;

GRANT SELECT ON genres TO c##user\_role;

REVOKE UPDATE ANY TABLE FROM c##user\_role;

GRANT UPDATE ON countries TO c##user\_role;

GRANT UPDATE ON genres TO c##user\_role;

CREATE VIEW serial\_persons\_view AS

SELECT serials\_persons.serial\_id, persons.person\_name, persons.it\_is\_producer

FROM serials\_persons

JOIN persons

ON serials\_persons.person\_id = persons.person\_id;

GRANT SELECT ON serial\_persons\_view TO c##user\_role;

GRANT c##user\_role to c##user1;

GRANT c##user\_role to c##user2;

1. Кроме того, каждому пользователю выдаются дополнительные привилегии для дальнейшей работы, так как у каждого сотрудника могут быть свои индивидуальные, постоянные задания

CREATE user C##USER1 identified by user1;

GRANT SELECT ON serials\_actors TO c##user1;

GRANT INSERT ON serials\_actors to c##user1;

GRANT UPDATE ON serials\_actors to c##user1;

GRANT INSERT ON serials\_list TO c##user1;

GRANT UPDATE ON serials\_list to C##user1;

CREATE user C##USER2 identified by user2;

GRANT SELECT ON serial\_stat TO c##user2;

GRANT UPDATE ON serial\_stat TO c##user2;

GRANT INSERT ON serial\_stat TO c##user2;

GRANT INSERT ON countries TO c##user2;

GRANT INSERT ON genres TO c##user2;

GRANT INSERT ON series TO c##user2;

1. С целью проверки корректной работы базы данных, был создан пользователь “Trainee” (Стажер), которому было выдано ограниченное количество привилегий, с целью получения той или иной практики. Так как всегда есть данные, в которые не только нельзя вносить корректировки, но и даже просматривать обычным пользователям. Так же стоит учесть, что стажеру выданы привилегии просмотра столбцов таблицы “serials\_list”, чтобы опираюсь на нее можно было вносить те или иные корректировки в остальные таблицы, к которым предоставлен доступ.

CREATE user c##trainee identified by trainee;

GRANT CREATE SESSION TO c##trainee;

GRANT CREATE VIEW TO c##trainee;

GRANT CREATE TRIGGER TO c##trainee;

GRANT SELECT ON serial\_name TO c##trainee;

GRANT SELECT ON serial\_id TO c##trainee;

GRANT SELECT ON countries TO c##trainee;

GRANT SELECT ON genres TO c##trainee;

GRANT UPDATE ON countries TO c##trainee;

GRANT UPDATE ON genres TO c##trainee;

1. От имени главного пользователя были созданы публичные синонимы для таблиц.

CREATE PUBLIC SYNONYM starring FOR serials\_actors;

CREATE PUBLIC SYNONYM statistics FOR serials\_stat;

CREATE PUBLIC SYNONYM TV\_series FOR serials\_list;

1. От имени каждого пользователя приведены примеры запросов, для проверки их работы
2. **От лица пользователя Manadger**

SELECT person\_name

FROM system.persons

where it\_is\_producer = 1;

PERSON\_NAME

----------------------------------------------------------------------------------------------------

Вячеслав Муругов

Эдуард Илоян

Виталий Шляппо

Антон Щукин

Антон Зайцев

Артем Логинов

Александр Цекало

Руслан Сорокин

Иван Самохвалов

Марк Гейтисс

Стивен Моффат

PERSON\_NAME

----------------------------------------------------------------------------------------------------

Берил Верту

Дэвид Бениофф

Д.Б. Уайсс

Джордж Р.Р. Мартин

Кэрин Мэндабах

Джэми Глазенбрук

Джули Бринкман

18 rows selected.

1. **От лица пользователя Manadger\_assistant**

SELECT manager\_name

FROM system.managers;

MANAGER\_NAME

--------------------------------------------------

Рамин Джавади

Стивен Моффат

Павел Данилов

Киллиан Мёрфи

Александр Цекало

Константин Галдаев

6 rows selected.

1. **От лица пользователя user1**

CREATE INDEX idx\_serials

ON serials\_list(serial\_name);

SELECT serial\_name, country\_name, genre\_name, annotation

FROM countries

JOIN serials\_list

ON countries.country\_id = serials\_list.country\_id

JOIN genres

ON serials\_list.genre\_id = genres.genre\_id

WHERE serial\_name != 'Кухня'

ORDER BY serials\_list.serial\_name

Error at Command Line : 13 Column : 6

Error report -

SQL Error: ORA-00942: таблица или представление пользователя не существует

00942. 00000 - "table or view does not exist"

\*Cause:

\*Action:

1. **От лица пользователя user2**

INSERT ALL

INTO system.managers(id, manager\_name)VALUES (1, 'James Smith')

SELECT \* FROM DUAL;

Error starting at line : 1 in command -

INSERT ALL

INTO system.managers(id, manager\_name)VALUES (1, 'James Smith')

SELECT \* FROM DUAL

Error at Command Line : 2 Column : 13

Error report -

SQL Error: ORA-00942: таблица или представление пользователя не существует

00942. 00000 - "table or view does not exist"

\*Cause:

\*Action:

1. **От лица пользователя user1**

GRANT CREATE SESSION TO c##trainee;

Error starting at line : 1 in command -

GRANT CREATE SESSION TO c##trainee

Error report -

ORA-01031: привилегий недостаточно

01031. 00000 - "insufficient privileges"

\*Cause: An attempt was made to perform a database operation without

the necessary privileges.

\*Action: Ask your database administrator or designated security

administrator to grant you the necessary privileges

1. **От лица пользователя user2**

SELECT id, serial\_name from system.serials\_list;

ID SERIAL\_NAME

---------- ------------------------------

1 Кухня

2 Физрук

3 Мажор

4 Шерлок

5 Игра Престолов

6 Острые козырьки

6 rows selected.

1. **От лица пользователя trainee**

CREATE INDEX idx\_serials

ON serials\_list(serial\_name);

SELECT serial\_name, annotation FROM serials\_list

WHERE serial\_name != 'Кухня';

Error starting at line : 3 in command -

SELECT serial\_name, annotation FROM serials\_list

WHERE serial\_name != 'Кухня'

Error at Command Line : 3 Column : 37

Error report -

SQL Error: ORA-00942: таблица или представление пользователя не существует

00942. 00000 - "table or view does not exist"

\*Cause:

\*Action:

1. **От лица пользователя trainee**

CREATE USER c##user3 identified by user3;

Error starting at line : 1 in command -

CREATE USER c##user3 identified by user3

Error report -

ORA-01031: привилегий недостаточно

01031. 00000 - "insufficient privileges"

\*Cause: An attempt was made to perform a database operation without

the necessary privileges.

\*Action: Ask your database administrator or designated security

administrator to grant you the necessary privileges

1. **От лица пользователя trainee**

SELECT \* FROM system.countries;

COUNTRY\_ID COUNTRY\_NAME

---------- ------------------------------

5 Россия

6 Великобритания

7 США