Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего профессионального образования

**«Национальный исследовательский ядерный университет «МИФИ»**

**ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ**

**Кафедра №42 (криптологии и кибербезопасности)**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2-5**

«Аудит БД»

по дисциплине: «Безопасность систем баз данных»

**Выполнил:**  
Студент учебной группы Б19-515

Родионов Дмитрий Александрович

**Принял:**

Ассистент НИЯУ МИФИ

Куприяшин М.А.

**Москва, 2022**

**СОДЕРЖАНИЕ**

[Лист с диаграммой отношения сущностей 3](#_Toc123415298)

[Описание разработанных политик аудита 4](#_Toc123415299)

[Тестирование политик аудита 5](#_Toc123415300)

[Вывод унифицированного журнала аудита 7](#_Toc123415301)

[Заключение 8](#_Toc123415302)

# **Лист с диаграммой отношения сущностей**

Диаграмма базы данных:



# **Описание разработанных политик аудита**

Унифицированный аудит базы данных осуществляется следующим образом:

* политика *admin\_pol* используется для аудита:
  + действий *SELECT*, *INSERT*, *UPDATE* и *DELETE* с данными в таблице *players*,
  + всех проверяемых действий с данными таблицы *clubs*,
  + административных ролей *CONNECT* и *DBA*;
* политика *table\_pol* используется для аудита:
  + системных привилегий *CREATE ANY TABLE* и *DROP ANY TABLE*,
  + действий *SELECT*, *INSERT*, *UPDATE* и *DELETE* с данными в таблице *players*,
  + всех проверяемых действий с данными таблицы *clubs*.

Запросы к базе данных:

* CREATE AUDIT POLICY admin\_pol  
   ACTIONS  
   SELECT ON administrator.players,  
   INSERT ON administrator.players,

UPDATE ON administrator.players,

DELETE ON administrator.players,

ALL ON administrator.clubs

ROLES

CONNECT,

DBA

CONTAINER = CURRENT;

* AUDIT POLICY admin\_pol BY administrator;
* CREATE AUDIT POLICY table\_pol

PRIVILEGES

CREATE ANY TABLE,

DROP ANY TABLE

ACTIONS

SELECT ON administrator.players,

INSERT ON administrator.players,

UPDATE ON administrator.players,

DELETE ON administrator.players,

ALL ON administrator.clubs

CONTAINER = CURRENT;

* AUDIT POLICY table\_pol BY USERS WITH GRANTED ROLE app\_manager\_role;

# **Тестирование политик аудита**

Запросы к базе данных от пользователя *administrator*:

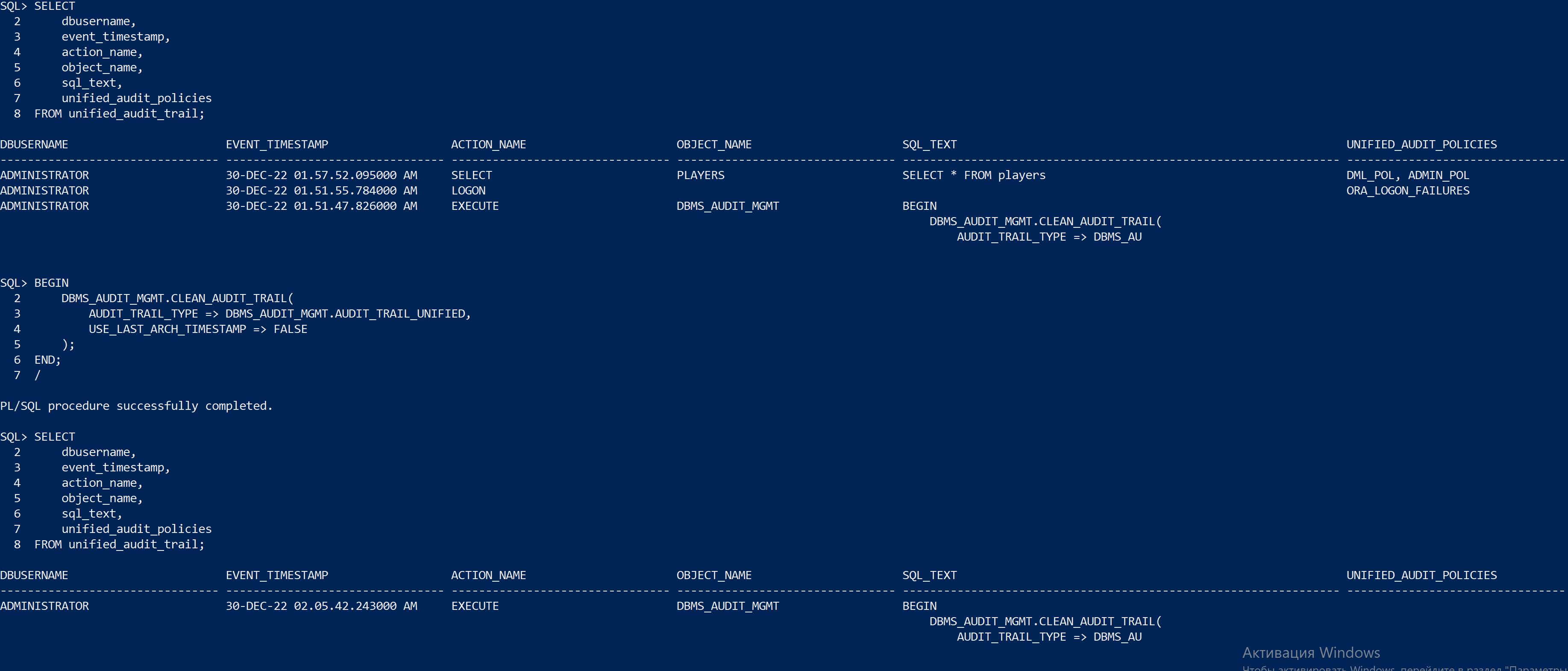
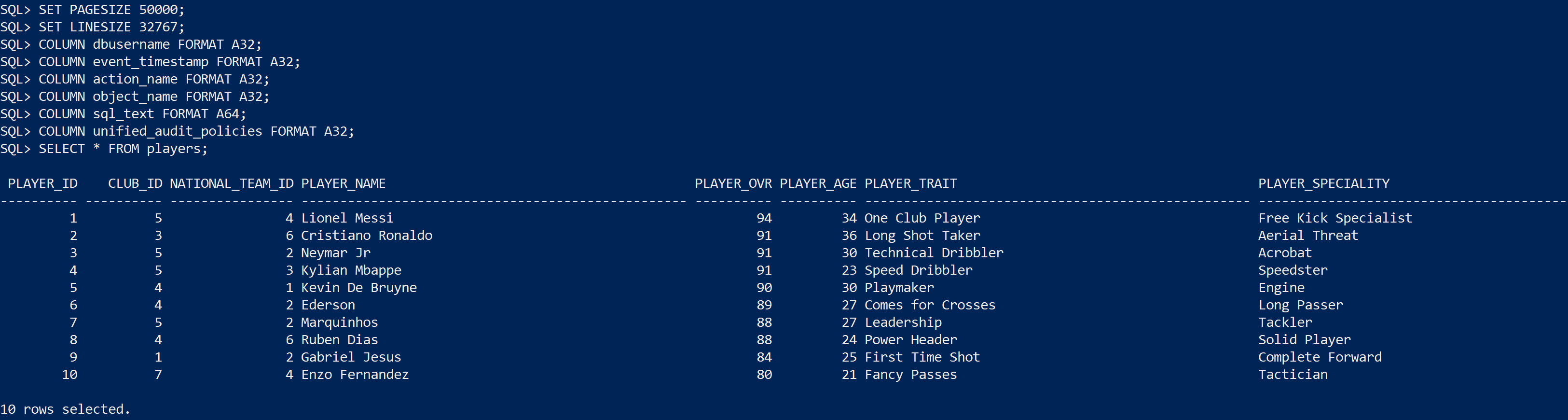
* SELECT \* FROM clubs;
* INSERT ALL  
   INTO clubs(club\_id, league\_id, club\_name, club\_stadium) VALUES (11, 4, 'KAA Gent', 'Ghelamco Arena')  
  SELECT \* FROM dual;
* SELECT \* FROM clubs;
* UPDATE clubs  
   SET club\_stadium = 'Parc des Princes'  
   WHERE club\_id = 5;
* SELECT \* FROM clubs;
* DELETE  
   FROM clubs  
   WHERE club\_name = 'Atletico Mineiro';
* SELECT \* FROM clubs;
* SELECT \* FROM players;
* INSERT ALL  
   INTO players(player\_id, club\_id, national\_team\_id, player\_name, player\_ovr, player\_age, player\_trait, player\_speciality) VALUES (11, 1, 2, 'Gabriel Jesus', 84, 25, 'First Time Shot', 'Complete Forward')  
  SELECT \* FROM dual;
* SELECT \* FROM players;
* UPDATE players  
   SET player\_ovr = 91  
   WHERE player\_name = 'Kevin De Bruyne';
* SELECT \* FROM players;
* DELETE  
   FROM players  
   WHERE player\_name = 'Mehdi Taremi';
* SELECT \* FROM players;
* GRANT AUDIT\_VIEWER TO manager;
* CREATE TABLE timestamps(  
   timestamp\_id NUMBER(4, 0) NOT NULL,  
   day NUMBER(2, 0),  
   month NUMBER(2, 0),  
   year NUMBER(4, 0),  
   PRIMARY KEY (timestamp\_id)  
  );
* SELECT  
   dbusername,  
   event\_timestamp,  
   action\_name,  
   object\_name,  
   sql\_text,  
   unified\_audit\_policies  
  FROM unified\_audit\_trail  
  WHERE dbusername = 'ADMINISTRATOR'  
  ORDER BY event\_timestamp;

Запросы к базе данных от пользователя *manager*:

* SELECT \* FROM clubs;
* SET ROLE app\_manager\_role IDENTIFIED BY password;
* CREATE TABLE timestamps(  
   timestamp\_id NUMBER(4, 0) NOT NULL,  
   day NUMBER(2, 0),  
   month NUMBER(2, 0),  
   year NUMBER(4, 0),  
   PRIMARY KEY (timestamp\_id)  
  );
* DROP TABLE administrator.timestamps;
* SELECT \* FROM administrator.clubs;
* INSERT ALL  
   INTO administrator.clubs(club\_id, league\_id, club\_name, club\_stadium) VALUES (13, 5, 'Atletico Mineiro', 'Estadio Governador')  
  SELECT \* FROM dual;
* SELECT \* FROM administrator.clubs;
* UPDATE administrator.clubs  
   SET club\_stadium = 'Estadio do Sport Lisboa'  
   WHERE club\_id = 7;
* SELECT \* FROM administrator.clubs;
* DELETE  
   FROM administrator.clubs  
   WHERE club\_name = 'Atletico Mineiro';
* SELECT \* FROM administrator.clubs;
* SELECT \* FROM administrator.players;
* INSERT ALL  
   INTO administrator.players(player\_id, club\_id, national\_team\_id, player\_name, player\_ovr, player\_age, player\_trait, player\_speciality) VALUES (13, 6, 3, 'Valentine Rongier', 78, 28, 'Finesse Shot', 'Complete Midfielder')  
  SELECT \* FROM dual;
* SELECT \* FROM administrator.players;
* UPDATE administrator.players  
   SET player\_ovr = 80  
   WHERE player\_name = 'Enzo Fernandez';
* SELECT \* FROM administrator.players;
* DELETE  
   FROM administrator.players  
   WHERE player\_name = 'Raheem Sterling';
* SELECT \* FROM administrator.players;
* SELECT  
   dbusername,  
   event\_timestamp,  
   action\_name,  
   object\_name,  
   sql\_text,  
   unified\_audit\_policies  
  FROM unified\_audit\_trail  
  WHERE dbusername = 'ADMINISTRATOR'  
  ORDER BY event\_timestamp;

# **Вывод унифицированного журнала аудита**

Запросы к базе данных от пользователя *administrator*:



# **Заключение**

В данной лабораторной работе приобретены базовые навыки аудита в базе данных и анализа журнала аудита. В частности, согласно легенде разработаны политики унифицированного аудита, которые используются для аудита всех проверяемых действий с таблицами, системных привилегий пользователей и их ролей.

Также произведено тестирование разработанных политик аудита и изучено содержание журнала аудита.