В. С. Лаврентьев (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)
В. А. Петров (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ПО КУРСУ «БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ» КАК ОДИН ИЗ ОСНОВНЫХ КОМПОНЕНТОВ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье приведена методика обучения технологиям безопасности современной СУБД (на примере СУБД Oracle) [1]. Отличительной особенностью методики является направленность на обучение студента не только знанию предмета, но и уверенному овладению практическими навыками в работе с технологиями безопасности информационных систем.

Двухсеместровый курс «Безопасность систем баз данных» является частью профилирующей подготовки и входит в цикл общепрофессиональных дисциплин (ОПД.Ф.09). Цель преподавания дисциплины: во-первых, дать студенту представление о проблематике, типовых задачах обеспечения информационной безопасности средствами СУБД системотехнического ядра информационной системы — базы данных; во-вторых, научить студента умению самостоятельно решать типовые задачи обеспечения безопасности баз данных на примере баз данных, реализованных под управлением современной СУБД.

МИФИ заключен договор с корпорацией Oracle об участии МИФИ в программе Advanced Computer Sciense & Business (ACSB), в соответствии с которой МИФИ получил для использования в учебном процессе комплект лицензионных продуктов Oracle и в их числе — СУБД Oracle10g.

Программой курса предусмотрено 64 часа лекционных и столько же часов лабораторных работ. Первая часть курса (7-й семестр) знакомит студента с вопросами реализации баз данных на основе современной СУБД, закладывая фундамент для освоения во второй части курса (8-й семестр) технологий обеспечения безопасности средствами СУБД.

Всего по технологиям обеспечения безопасности системы баз данных средствами современной СУБД предусмотрено 12 лабораторных работ. Первая лабораторная работа знакомит студента с архитектурой Oracle, с практической реализацией сетевых, клиентских настроек для работы с сервером Oracle.

Тематика остальных лабораторных работ покрывает практически все основные разделы информационной безопасности: конфиденциальность, целостность, доступность.

Наибольший акцент сделан на вопросах разграничения полномочий и контроле действий пользователя. Восемь лабораторных работ посвящены этой тематике. Здесь студенты осваивают на практике управление системными, объектными привилегиями, ролями и реализуемым на их основе дискреционным методом доступа, а также — аудит действий пользователя. Отдельные лабораторные работы из этих восьми знакомят студентов с практической реализацией технологий Virtual Private Database, Fine Grained Audit, Oracle Label security (мандатный метод доступа). Одна лабораторная работа из этой группы знакомит студентов с вопросами глобальной аутентификации (Oracle Internet Directory).

Одна лабораторная работа знакомит студентов с технологиями обеспечения доступности базы данных (Backup & Recovery), одна — с технологиями обеспечения целостности и шифрованием информации при удаленном общении клиента с сервером.

Вышесказанное позволяет сделать вывод об относительном превышении объема работы студента по тематике разграничения полномочий по сравнению с контролем целостности и доступности. Это связано с тем, что вопросы защиты информации от атак в целях обеспечения ее доступности рассматриваются в других курсах, а вопросы обеспечения целостности — создание constarints для объектов схемы — рассматривались в первой части курса.

Методика выполнения лабораторных работ следующая: по каждой лабораторной работе есть описание лабораторной работы, скрипты ее выполнения на учебной предметной области. Скрипты составлены так, что возможно их многократное повторное выполнение без дополнительных настроек. Студент осваивает тематику очередной лабораторной работы, выполняя скрипты лабораторной работы, — это вводная демонстрационная часть лабораторной работы. Вслед за тем студент выполняет задание по лабораторной работе уже на выданной преподавателем другой предметной области, с другими объектами и субъектами информационной базы. Студент по заданию лабораторной работы должен будет создать пользователя — владельца схемы, объекты, субъекты информационной базы своего индивидуального задания, администраторов контроля осваиваемых технологий безопасности, написать собственные скрипты, реализующие задание на лабораторную работу. Общее количество разных предметных областей — 20. В каждой предметной области разные группы объектов и субъектов формируют исходные данные для разных заданий на выполнение лабораторной работы (обычно на одну предметную область — три задания). Таким образом, каждый студент получает индивидуальное задание для выполнения лабораторной работы. Этим снимается проблема списывания.

Приведем пример предметной области демонстрационной учебной информационной системы и скриптов (для дисплейного класса Б-408ст) для выполнения лабораторной работы по технологиям Virtual Private Database. На рис. 1 приведена схема базы данных учебной информационной системы «Учет использования дисплейных классов».

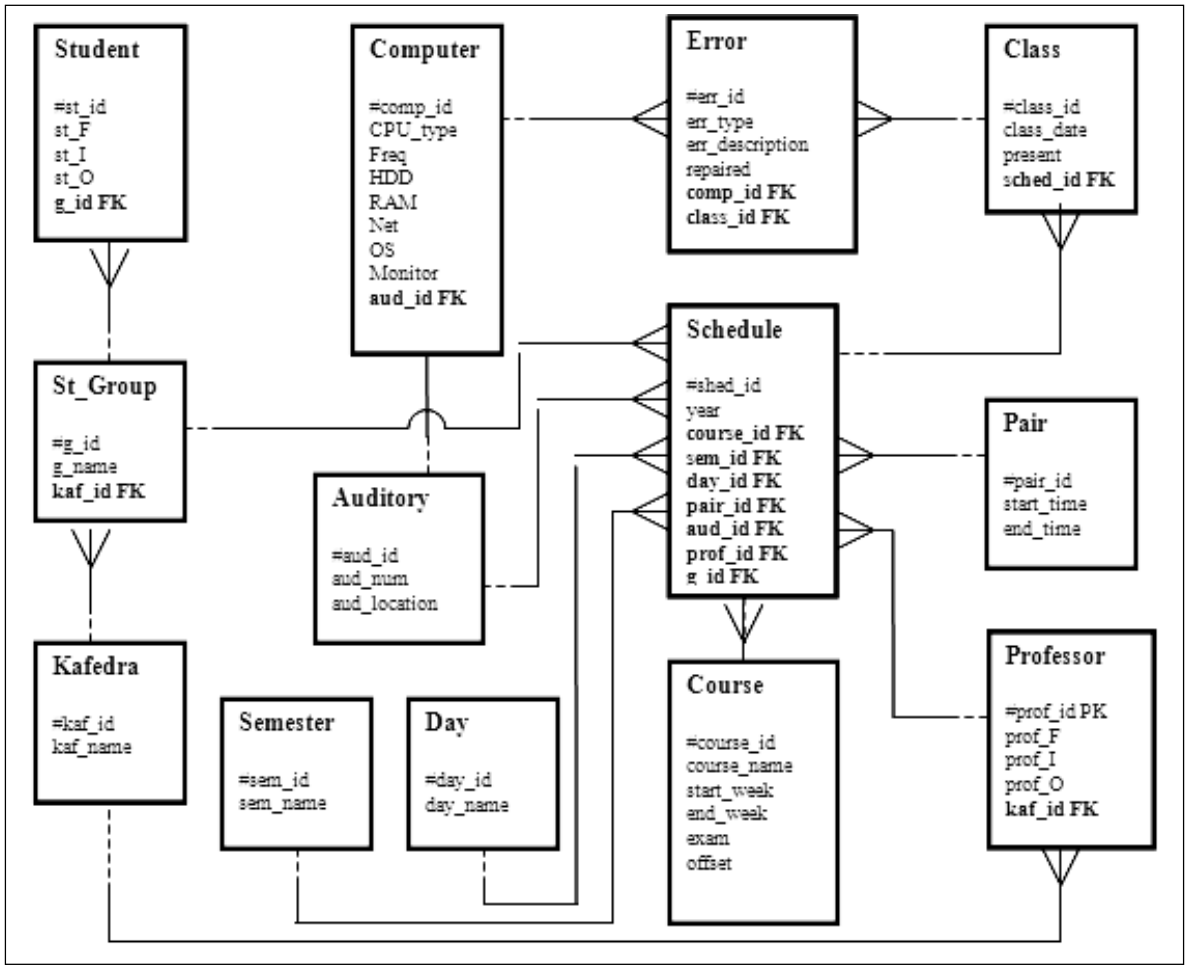

Рис 1. Схема базы данных учебной информационной системы «Учет использования дисплейных классов».

Задание для вводной демонстрационной части: преподаватели (пользователи с именами, совпадающими со значениями столбца prof_F таблицы Professor) могут просматривать в таблице Error записи, касающиеся неисправностей компьютеров, только в тех аудиториях, в которых эти преподаватели проводят занятия. Приведем скрипты, реализующие решение сформулированной задачи.

Сначала командный файл (Рис. 2):

```
@set ORACLE_SID=orcl
@set ORACLE_HOME=D:\oracle\product\10.2.0\db_1
@chcp 1251
rem @set nls_lang= RUSSIAN_CIS.RU8PC866
@%ORACLE_HOME%\bin\sqlplus system/system  @c:\tmp\fga.sql
```

Рис. 2. Командный файл для выполнения скрипта решения сформулированной задачи.

Затем фрагмент исполняемого sql скрипта, в котором реализуется «контекстный» вариант Virtual Private Database. Фрагмент включает комментарии к решению, отмеченные сдвоенным тире (Рис. 3).

Текст программы для решения сформулированной задачи представлен на рис. 4 — рис. 6.

```
- Задание: Преподаватель (таблица Professor) может просматривать
--в таблице Error записи, касающиеся неисправностей компьютеров
--только в тех  аудиториях, в которых этот преподаватель проводит занятия
--В таблице Professor 3 записи:
--(1,'Лаврентьев','Валерий','Сергеевич',3);
--(2,'Зотов','А','А',1);
--(3,'Беззубцев','Б','Б',2);
--первая колонка – это prof_id, вторая – prof_f
--очевидно, что надо создавать пользователей Лаврентьев,
--Зотов, Беззубцев. Создадим их из консоли Enterprise Manager
--по образцу пользователя scott. Отметим, здесь, пароль на кириллице
--Oracle не принимает
--Владельцем схемы "Учет использования дисплейных классов"
--установим пользователя t2/t2. Создадим его из консоли Enterprise
--Manager
--по образцу пользователя scott, а потом добавим ему
--необходимые привилегии (см. ниже)
--Полезный совет для работы в ходе контрольной (да и при
--выполнении ДЗ сгодится): открыть две сессии, в одной из
--которых соединиться sys-ом, в другой – владельцем схемы
--в моем случае t2. Кроме того, полезно открыть консоль
--Enterprise Manager, из которой удобно создавать, удалять
--пользователей, просматривать схемы и т. д.
```

Рис. 3. Комментарии к исходным данным, используемым для решения сформулированной задачи.

```
@D:\oracle\product\10.2.0\db_1\BIN\connect 'sys/sys@orcl as sysdba'
--предварительно созданному владельцу схемы даются привилегии
grant CREATE ANY CONTEXT to t2;
grant drop any context to t2;
grant EXECUTE_CATALOG_ROLE to t2;
grant execute on dbms_rls to t2;
grant execute on DBMS_FGA to t2;
grant create user to t2;
grant CREATE SESSION, RESOURCE TO t2 with admin option;
grant create view to t2;
grant select any table to t2 with admin option;
grant create public synonym to t2;
```

```
grant drop public synonym to t2;
grant select on professor to public;
create public synonym professor for t2.professor;
grant select on error to public;
create public synonym error for t2.error;
--****************************************
--Теперь задействуем использование контекста
--****************************************
create or replace context professor_sec_ctx USING GET_PROF_ID;
```

Рис. 4. Первый фрагмент текста программы решения сформулированной задачи.

```
Create or replace procedure GET_PROF_ID as
  v_PROF_ID number;
 begin
 select PROF_ID
 into
 v_PROF_ID
  from professor
  where upper(prof_f)=sys_context('userenv', 'session_user');
 dbms_session.set_context('professor_sec_ctx','prof_id1',v_PROF_ID);
 exception
 when no_data_found then
  NULL;
 end GET_PROF_ID;
/
GRANT EXECUTE ON GET_PROF_ID to public;
create public synonym GET_PROF_ID for t2.GET_PROF_ID;
 @D:\oracle\product\10.2.0\db_1\BIN\connect 'sys/sys@orcl as sysdba'
create or replace trigger DB_TRIGGER
 AFTER LOGON ON DATABASE
  Begin
 t2.get_PROF_ID;
end;
/
@D:\oracle\product\10.2.0\db_1\BIN\connect t2/t2@orcl;
create or replace function f4_1
(obj_schema IN VARCHAR2, obj_name IN VARCHAR2)
RETURN VARCHAR2
is
v_return varchar2(500);
begin
v_return:='comp_id in (
select comp_id from
computer,auditory,schedule,professor
where
computer.aud_id=auditory.aud_id and
auditory.aud_id=schedule.aud_id and
schedule.prof_id=professor.prof_id and
professor.prof_id=sys_context(''professor_sec_ctx'', ''prof_id1''))';
RETURN  v_return;
end;
/
grant execute on f4_1 to public;
create public synonym f4_1 for t2.f4_1;
--проверка работы функции
```

```
create table tv4_1 (
clm1 varchar2(500));
create public synonym tv4_1 for t2.tv4_1;
/
```

Рис. 5. Второй фрагмент текста программы решения сформулированной задачи.

```
declare
 v_test varchar2(500);
  begin
 v_test:=f4_1('T2','ERROR');
 insert into tv4_1 values(v_test);
 end;
/
select * from tv4_1;
—проверка работы функции завершена
BEGIN
DBMS_RLS.ADD_POLICY(
OBJECT_SCHEMA => 't2',
OBJECT_NAME => 'error',
POLICY_NAME => 'prof_id_policy',
FUNCTION_SCHEMA => 't2',
POLICY_FUNCTION => 'f4_1');
END;
/
@D:\oracle\product\10.2.0\db_1\BIN\connect зотов/z@orcl
select * from error;
@D:\oracle\product\10.2.0\db_1\BIN\connect лаврентьев/l@orcl
select * from error;
@D:\oracle\product\10.2.0\db_1\BIN\connect t2/t2@orcl;
BEGIN
DBMS_RLS.drop_POLICY(
OBJECT_SCHEMA => 't2',
OBJECT_NAME => 'error',
POLICY_NAME => 'prof_id_policy');
end;
/
--для обеспечения повторного безошибочного выполнения программы
drop public synonym error;
drop public synonym f4_1;
drop public synonym professor;
drop public synonym GET_PROF_ID;

 @D:\oracle\product\10.2.0\db_1\BIN\connect 'sys/sys@orcl as sysdba'
drop trigger db_trigger;
```

Рис. 6. Последний фрагмент текста программы решения сформулированной задачи.

А теперь — пример задания по этой лабораторной работе (для варианта этой же предметной области): студенты из таблицы student (столбец st_F) видят в таблице Schedule строки расписания занятий только своих групп.

Аналогичные образцы и задания на лабораторную работу даются и по другим темам.

По двум темам (обычно FGA, OLS) студенты выполняют контрольные работы в дисплейном классе. Студент на контрольной должен не только написать, но и отладить решение, а также убедиться в его работоспособности. Задания контрольной похожи на задания лабораторной работы — только даются они для другой предметной области.

При написании контрольных работ студент отчитывается о выполненной контрольной работе PL/SQL скриптами, spool-файлом (протоколом) работы PL/SQL скрипта. Для PL/SQL скрипта студент формирует выдаваемой преподавателем хэш-функцией электронную подпись, которая заносится студентом в бланк регистрации результатов контрольной [2]. Наличие электронной подписи гарантирует аутентичность проверяемого преподавателем скрипта выполнения задания контрольной работы. На рис. 7 представлен пример заполнения такого бланка.

Кафедра 43 Курс _____БСБД2_____
(этот пункт и все последующие заполняются студентом)

Контрольная работа ___FGA_____

Группа___Б8-02_____Вариант №_____25_____Дата___31.03.2007_____

Фамилия И.О.___Тагунова Е.С. _____

Результат вычисления хэш-функции, примененной к текстовому файлу с решением контрольной, – электронная подпись (заполняется студентом):

FCBY VJO$ VGWQ 2QGY
Подпись студента_____

Рис. 7. Заполненный бланк регистрации электронной подписи для текста решения задачи контрольной работы.

Представленная в статье методика обучения делает акцент на обучении студента не только знанию, но и практическому овладению изучаемым предметом. Многолетний опыт общения со студентами показывает, что студент, добросовестно прошедший обучение по представленной методике, быстро трудоустраивается на работу по тематике безопасности баз данных.

СПИСОК ЛИТЕРАТУРЫ:

1. http://academy.oracle.com.
2. *Ткаченко С. И., Лаврентьев В. С.* Опыт регистрации работы студентов на контрольной с использованием электронной подписи // Тезисы докладов конференции МИФИ 2007 г.