

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет» РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-1 «Защита информации»

ОТЧЁТ

# по практическому занятию №2

**по дисциплине «Безопасность систем баз данных»**

Студент: Кутьин З.

Шифр учебной группы:

БББО-05-20

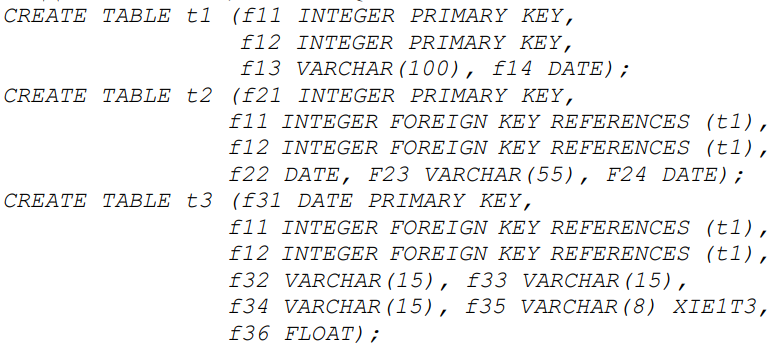
Принял: Кунин Н.Т.

Москва, 2022

# Ход работы

**Задание 1**

**Дано:** *база данных, заданная SQL-командой*



Совокупность степеней конфиденциальности информации:

"ООО" – колонки f11, f14, f24, f35, f36;

"ОО" – колонки f12, f21, f23, f31;

остальные колонки имеют степень "О". Наивысшей степенью является "ООО".

Система уровней благонадежности пользователей:

"ООО" – пользователи U1, U4, U8;

"ОО" – пользователи U3, U6;

"О" – пользователи U2, U5, U7, U9.

АСУ предоставляет в распоряжение пользователей типовые SQL-запросы.

Построить матрицу безопасности, привилегии назначить произвольно.

**Решение:**

В качестве привилегий выберем: INSERT (вставка), SELECT (выборка), UPDATE (обновление), DELETE (удаление).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | f11\*(3) | f12\*(2) | f13(1) | f14(3) | f21\*(2) | f22(1) | f23(2) | f24(3) | f31\*(2) | f32(1) | f33(1) | f34(1) | f35(3) | f36(3) |
| U1(3) | i, s, d, u | i, s, d, u | i, s, d, u | i, s, d | - | s | - | s, u | - | s, u | s | s, u | s | s |
| U2(1) | i | i | s, i | i | i | s, i | s, i | i | i | s, i | s, i | s, i | i | i |
| U3(2) | i | s, i | s, i | i | s, i | s, i | s, i | i, u | s, u | s | s | s | - | - |
| U4(3) | s, d, i | s, d, i | s, d, i | s, d, i | s, d, i, u | s, d, i | s, d, i, u | s, d, i, u | s | s | s | s | s | s |
| U5(1) | i | i | i, s | i | i | s, i, u | i | i | - | s | s | s | - | - |
| U6(2) | - | i, s | s | - | s, d, i | s, d, i | s, d, i | s, d, i | s, i | s, i | s, i | s, i | s, i | s, i |
| U7(1) | - | - | - | - | - | - | - | - | i | s, i, u | s, i, u | s, i, u | s, i | s, i |
| U8(3) | s | s | s | s | s, d, i | s, d, i | s, d, i | s, d, i, u | s, d, i, u | s, d, i | s, d, i | s, d, i | s, d, i, u | s, d, i, u |
| U9(1) | - | - | - | - | i | i | i | i | - | - | - | - | - | - |

Матрица безопасности основана на следующих основаниях:

* U1 — субъект, ответственный за таблицу *t1*. Только он может изменять её первичные ключи, а также обновлять данные непосредственно в ячейках.
* U4 — субъект, ответственный за таблицу *t2*. Только он может изменять её первичные ключи, а также обновлять данные непосредственно в ячейках.
* по большей части матрица основана на принципах «No read up» и «No write down». Однако, в некоторых ситуациях возможны отступления от них.
* на отдельные столбцы могут быть назначены только привилегии SELECT и UPDATE.
* привилегии, распространяющиеся на всю таблицу, должны соответствовать максимальному из уровней доступа её столбцов.

# Задание 2.

Разработать SQL-предложения для внедрения матрицы безопасности в действующую базу данных по условиям задачи 1.

**Решение:**

GRANT INSERT ON t1 TO u1

GRANT SELECT ON t1, t2(f22, f24), t3 TO u1

GRANT UPDATE ON t1(f11,f12,f13), t2(f24), t3(f32,f34) TO u1

GRANT DELETE ON t1 TO u1

GRANT INSERT ON t1, t2, t3 TO u2

GRANT SELECT ON t1(f13) t2(f22,f23) t3(f32, f33, f34) TO u2

GRANT INSERT ON t1, t2 TO u3

GRANT SELECT ON t1(f12, f13), t2(f21, f22, f23), t3(f31, f32, f33, f34) TO u3

GRANT UPDATE ON t2(f24), t3(32) TO u3

GRANT INSERT ON t1, t2 TO u4

GRANT SELECT ON t1, t2, t3 TO u4

GRANT UPDATE ON t2(f21, f23, f24) TO u4

GRANT DELETE ON t1, t2 TO u4

GRANT INSERT ON t1, t2 TO u5

GRANT SELECT ON t1(f13) t2(f22) t3(f32, f33, f34) TO u5

GRANT INSERT ON t2, t3 TO u6

GRANT SELECT ON t1(f12, f13), t2, t3 TO u6

GRANT DELETE ON t2 TO u6

GRANT INSERT ON t3 TO u7

GRANT SELECT ON t3(f32, f33, f34, f35, f36) TO u7

GRANT UPDATE ON t3(f32, f33, f34) TO u7

GRANT INSERT ON t2, t3 TO u8

GRANT SELECT ON t1, t2, t3 TO u8

GRANT UPDATE ON t2(f24), t3(f31, f35, f36) TO u8

GRANT DELETE ON t2, t3 TO u8

GRANT INSERT ON t2 TO u9

# Задание 3

**Дано:**в базе данных предусмотрено три таблицы с именами Ф1, Ф2 и Ф3. В каждой таблице по 6 колонок. База данных обслуживает 146 пользователей и управляется двумя администраторами. Пользователям и администраторам предоставляются привилегии по использованию 12 функций

**Определить:**размер занимаемого матрицей безопасности пространства на диске сервера.

**Решение:**

* для упрощения матрицу безопасности БД можно разбить на три матрицы безопасности (для каждой таблицы) одинакового размера
* размер одной матрицы, в которой *n* строк, *m* столбцов, одна ячейка занимает *K* байт, а первичный ключ имеет размер *Vpk* равняется:

𝐼 = 𝑛 ∗ (𝑚 ∗ 𝐾 + 𝑉𝑝𝑘)

* количество строк *n* равняется количеству пользователей (включая администраторов):

𝑛 = 146 + 2 = 148

* количество столбцов *m* равняется количеству объектов базы данных (1 таблица, 6 её столбцов и 12 функций)

𝑚 = 1 + 6 + 12 = 19

* размер одной ячейки примем за 1 байт (этого хватит для обозначения 12 функций)
* размер первичного ключа примем за 4 байта

𝐼 = 148 ∗ (19 ∗ 1 + 4) = 3404 байта

𝐼общ = 3𝐼 = 3 ∗ 3404 = 10 212 байт

Ответ: 9,9 Кбайт

# Задание 4

**Дано***:* база данных обслуживает 165 пользователей, предоставляя в их распоряжение 6 разнотипных функций, и содержит 2 таблицы по 12 полей, 1 таблицу – 4 поля, 3 таблицы – по 8 полей и 2 таблицы – по 6 полей

**Определить:**объем, занимаемый матрицей безопасности на диске сервера, при условии, что защищаемая БД функционирует под управлением СУБД PARADOX, на хранение индекса выделяется 4 байта, а логическое имя пользователя может иметь длину до 16 символов.

**Решение:**

𝐼 = 𝑛 ∗ (𝑚 ∗ 𝐾 + 𝑉𝑝𝑘)

𝑛 = 165

𝐾 = 4, 𝑉𝑝𝑘 = log2 16 = 4

* таблицы по 12 полей:

𝑚 = 2 + 2 ∗ 12 = 26

𝐼 = 165 ∗ (26 ∗ 4 + 4) = 17 820 байт

* таблица 4 поля:

𝑚 = 1 + 4 = 5

𝐼 = 165 ∗ (5 ∗ 4 + 4) = 3960 байт

* таблицы по 8 полей:

𝑚 = 3 + 3 ∗ 8 = 27

𝐼 = 165 ∗ (27 ∗ 4 + 4) = 18 480 байт

* таблицы по 6 полей:

𝑚 = 2 + 2 ∗ 6 = 14

𝐼 = 165 ∗ (14 ∗ 4 + 4) = 9900 байт

* По итогу:

𝐼общ = 17 820 + 3960 + 18 480 + 9900 = 50 160 байт

Ответ: 48,9 Кбайт

**Задание 5**

Создать роль для сотрудников отдела маркетинга с правами ведения базы данных и репликации снимков.

**Решение:**

* создание базы данных:

CREATE DATABASE sales

GO

* создание роли:

CREATE ROLE staff

GO

* предоставление привилегий:

GRANT ALTER ON DATABASE::sales TO staff

GRANT REPLICATION SLAVE ON sales TO staff

**Задание 6**

Создать учетную запись для сотрудника отдела маркетинга без прав администрирования базы данных

**Решение:**

* создание учётной записи:

CREATE LOGIN ord\_staff

WITH PASSWORD=N’staff12345’,

DEFAULT\_DATABASE=sales

GO

**Задание 7**

Создать учетную запись администратора базы данных с данными аутентификации dbadmin/A32oY4Fd

**Решение:**

* создание учётной записи:

CREATE LOGIN dbadmin

WITH PASSWORD=N’A32oY4Fd’,

DEFAULT\_DATABASE=sales

GO

**Задание 8**

Для учетной записи пользователя STUD\_MIREA/Pass\_2022 предоставить

привилегию подключения к базе данных и привилегию ведения данных

Решение:

* создание учётной записи:

CREATE LOGIN STUD\_MIREA

WITH PASSWORD=N’Pass\_2022’,

DEFAULT\_DATABASE=sales

GO

* создание пользователя:

CREATE USER \_user\_mirea FOR LOGIN STUD\_MIREA

* выдача привилегий:

GRANT CONNECT ON DATABASE::sales TO \_user\_mirea

GRANT ALTER ON DATABASE::sales TO \_user\_mirea

**Задание 9**

Пользователю с учетной записью STUD\_MIREA присвоить роль админи-

стратора базы данных

**Решение:**

* добавление роли участнику:

ALTER ROLE db\_owner ADD MEMBER \_user\_mirea

**Задание 10**

У пользователя с учетной записью STUD\_MIREA отнять привилегию ад-

министратора базы данных

**Решение:**

* удаление роли у участника:

ALTER ROLE db\_owner DROP MEMBER \_user\_mirea

**Задание 11**

Удалить учетную запись пользователя STUD\_MIREA

**Решение:**

* удаление учётной записи:

DROP LOGIN STUD\_MIREA

**Домашнее задание**

CREATE DATABASE depart

GO

USE depart

GO

CREATE ROLE TRANS\_DEP

GO

GRANT CONNECT ON DATABASE::depart TO TRANS\_DEP

GRANT BACKUP ON DATABASE::depart TO TRANS\_DEP

GRANT RESTORE ON DATABASE::depart TO TRANS\_DEP

CREATE LOGIN RACE\_DEP

WITH PASSWORD=N’race12345’,

DEFAULT\_DATABASE=depart

GO

GRANT CONNECT ON DATABASE::depart TO RACE\_DEP

GRANT ALTER ON DATABASE::depart TO RACE\_DEP

GRANT CREATE TABLE ON DATABASE::depart TO RACE\_DEP

CREATE TABLE TAB\_RACE (

id integer Primary key,

race\_date timestamp not null,

point\_out varchar(250),

point\_in varchar(250),

note\_race varchar(500)

)

INSERT INTO TAB\_RACE values(1, 2022-06-11 06:35:00, ‘Mos-

cow’, ‘Pervomaysk’, null)

INSERT INTO TAB\_RACE values(7, 2022-07-12 06:35:00, ‘Mos-

cow’, ‘Nizhny Novgorod’, ‘transit’)

INSERT INTO TAB\_RACE values(14, 2022-08-13 06:35:00, ‘Mos-

cow’, ‘Arzamas’, null)

INSERT INTO TAB\_RACE values(952, 2022-09-14 06:35:00, ‘Mos-

cow’, ‘Vladimir’, ‘express’)

INSERT INTO TAB\_RACE values(71, 2022-10-15 06:35:00, ‘Mos-

cow’, ‘Davydkovo’, null)