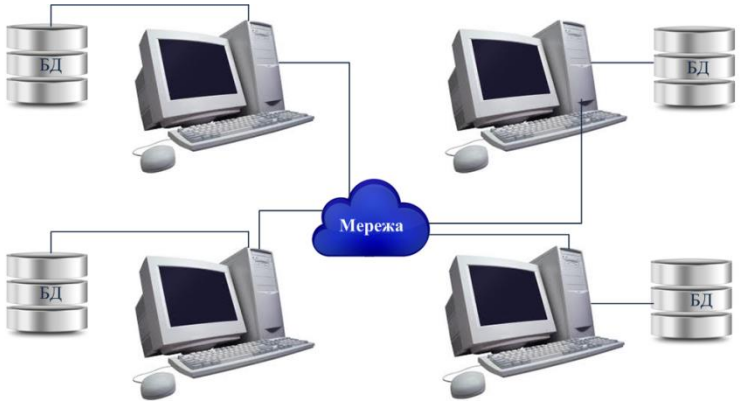


Лекція 8

Захист даних

Мета: ознайомитись з призначеннями обмежень цілісності даних; правилами застосування та формування обмежень цілісності; ознайомитись з заходами направленими на безпеку даних

---

1. **Поняття про обмеження цілісності.**
2. **Декларативні обмеження та семантичні обмеження.**
4. **Підтримка цілісності у разі виникнення перебоїв.**
5. **Поняття безпеки даних користувачів та керування правами доступу.**
6. **Обов’язкові методи захисту.**

8.1 Поняття про обмеження цілісності

Цілісність даних

- достовірність і точність інформації, що зберігається в базі

Обмеження цілісності

- це правила, які обмежують усі можливі стани бази даних, а також переходи з одного стану в інший

Класифікація обмежень цілісності

Обмеження цілісності за походженням

Семантичні

- випливають із властивостей структури даних

Структурні

- накладаються ПО, яка моделюється

Обмеження цілісності за способом підтримки

декларативні

- фіксують умови, яким має відповідати БД
- специфікуються фразою CONSTRAINT

процедурні

- забезпечують цілісності
- специфікуються тригерами

Обмеження цілісності за терміном перевірки

Негайна перевірка

- безпосередньо в момент виконання операції, яка може порушити цілісність

Відкладена перевірка

- для підтримки БД у несуперечному стані потрібно виконати дві або більше операції

Обмеження цілісності за областю дії

- відношення
- атрибута
- зв’язків між відношеннями
- зв’язків між атрибутами

Обмеження цілісності за можливими переходами БД з одного стану в інший

Статичні

- обмеження на можливі стани БД

Динамічні

- обмеження на можливі переходи БД з одного стану в інший

8.2 Декларативні обмеження цілісності

- на які об’єкти МД поширюються обмеження цілісності;
- якими є ці обмеження;
- як ті чи інші обмеження цілісності специфікуються;
- які існують механізми підтримання цілісності.

Цілісність відношень

Обмеження цілісності первинного ключа

- атрибути первинного ключа не можуть містити NULL-значень;
- значення первинного ключа (як окремого атрибута або сукупності атрибутів) не можуть дублюватися в межах відношення

CONSTRAINT<ім’я обмеження>
PRIMARY KEY(<перелік полів>**)**

Цілісність відношень. Приклад

```
CREATE TABLE КАФЕДРА
(
#D NUMBER(2),
Назва VARCHAR2(9),
Завідувач VARCHAR2(10),
CONSTRAINT DepPK PRIMARY KEY (#D)
);
```

Цілісність атрибутів

Обмеження цілісності атрибутів

- Зазначення типів даних та їхніх розмірів;
- Визначення обов’язковості значення;
- Визначення можливості дублювання
- Зміна значення атрибута після його введення;
- Встановленням умов на значення атрибута.

Цілісність атрибутів

CONSTRAINT<ім'я обмеження>
UNIQUE/CHECK (<перелік полів>**)**

CREATE TABLE *ГРУПА*
(*#G* NUMBER(3),
#D NUMBER(3),
Курс NUMBER(l) **CHECK** (Course IN(1.2.3.4.5)),
Номер NUMBER(3) **CHECK** (Номер > 0),
Кількість NUMBER(2) **CHECK** (Кількість > 0),
#Куратор NUMBER(3) **UNIQUE,**
CONSTRAINT GrpPK **PRIMARY KEY** (#G),
CONSTRAINT GrpUNQ **UNIQUE** (Курс, Номер)**);**

Цілісність зв'язків між відношеннями

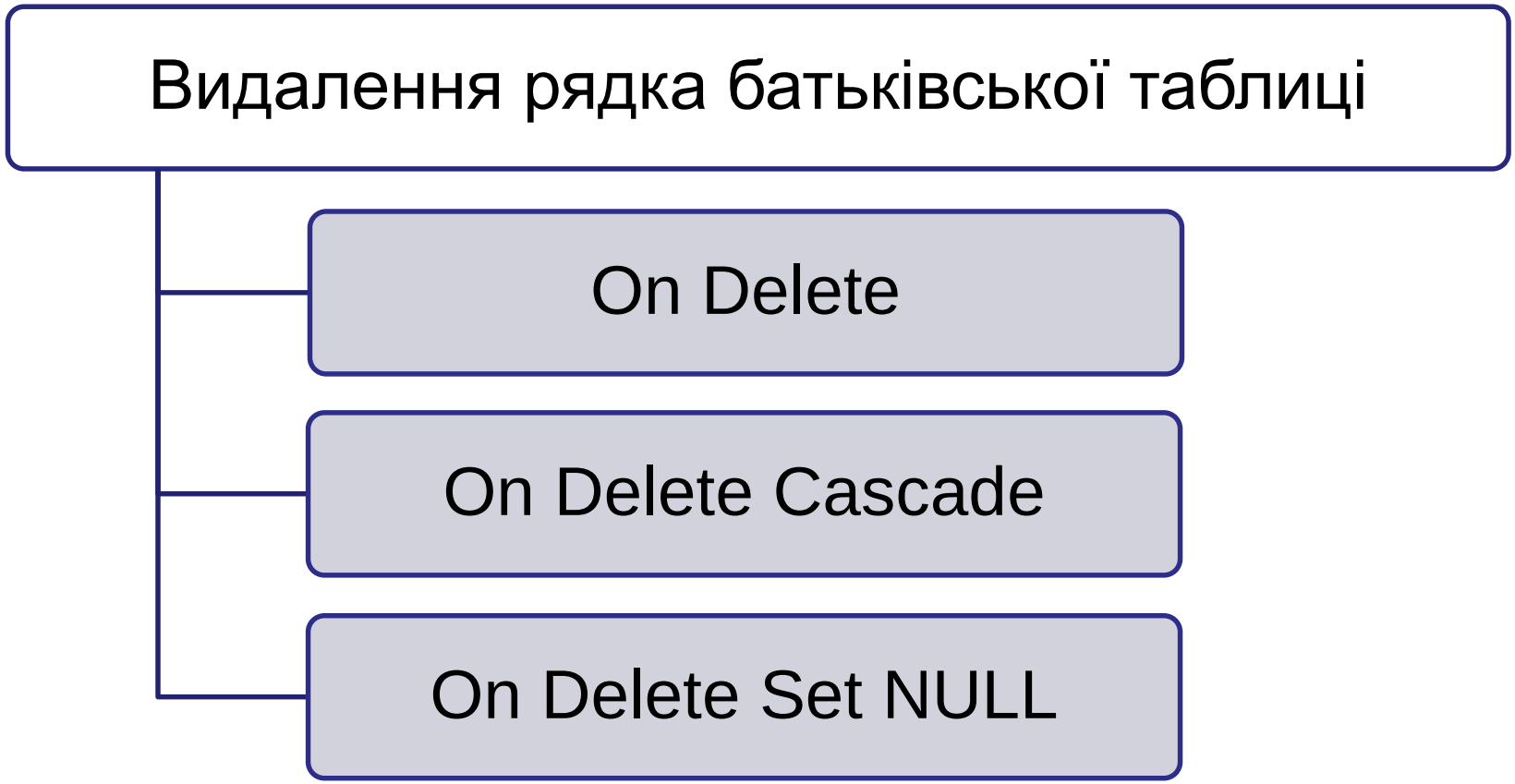
Обмеження зовнішнього ключа

- Якщо ЗК певного відношення може містити NULL-значення, то зв’язок даного відношення з іншим є **факультативним**.
- NOT NULL- специфікація стовпців зовнішнього ключа свідчить, що зв’язок є **обов’язковим**
- **цілісність за посиланням**: значення ЗК має посилатися на значення ПК іншого відношення.

Цілісність зв'язків між відношеннями

CONSTRAINT<назва обмеження>
FOREIGN KEY (<перелік полів 1>)
REFERENCES <ім'я таблиці (<перелік полів 2>)
[ON DELETE {CASCADE | SET NULL}]

Механізм забезпеченості цілісності зв'язків між відношеннями



Цілісність зв'язків між атрибутами

Обмеження сукупності атрибутів/відношень

```
CREATE TRIGGER Лекція Вставка Оновлення
BEFORE INSERT, UPDATE ON ЛЕКЦІЯ WHEN
(SELECT Місця
FROM АУДИТОРІЯ
WHERE АУДИТОРІЯ.#R =ЛЕКЦІЯ.#R) <
(SELECT Кількість FROM ГРУПА
WHERE ГРУПА.#Є = ЛЕКЦІЯ.#Є)
BEGIN ROLLBACK TRANSACTION END;
```

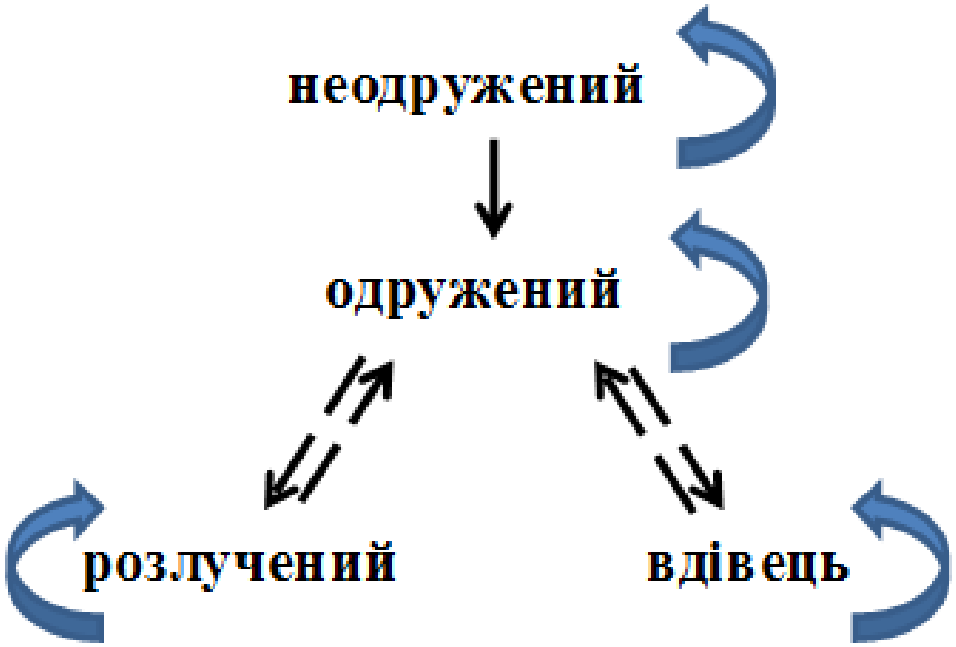
Динамічні обмеження

обмеження, які встановлюють залежність між різними частинами БД у різні моменти часу

- ситуаційно-орієнтовані
- операційно-орієнтовані

Ситуаційно - орієнтовані обмеження

- вимоги до послідовності станів БД



Можливі переходи значення атрибута Сімейний стан

8.3 Динамічні обмеження цілісності

```
CREATE TRIGGER Особа_Сімейний_Стан
BEFORE INSERT. UPDATE ON ОСОБА
WHEN (OLD.Сімейний_Стан = 'Неодружений' AND
NEW.Сімейний_Стан IN ('Розлучений'. 'Вдівець') ) OR
(OLD.Сімейний_стан='Одружений' AND
NEW.Сімейний_стан = 'Неодружений') OR
(OLD.Сімейний_стан='Розлучений' AND
NEW.Сімейний_стан IN ('Неодружений'.'Вдівець') ) OR
(OLD.Сімейний_стан='Вдівець' AND
NEW.Сімейний_стан IN ('Неодружений'.'Розлучений')
BEGIN
ROLLBACK TRANSACTION
END
```

8.3 Динамічні обмеження цілісності

Операційно - орієнтовані обмеження

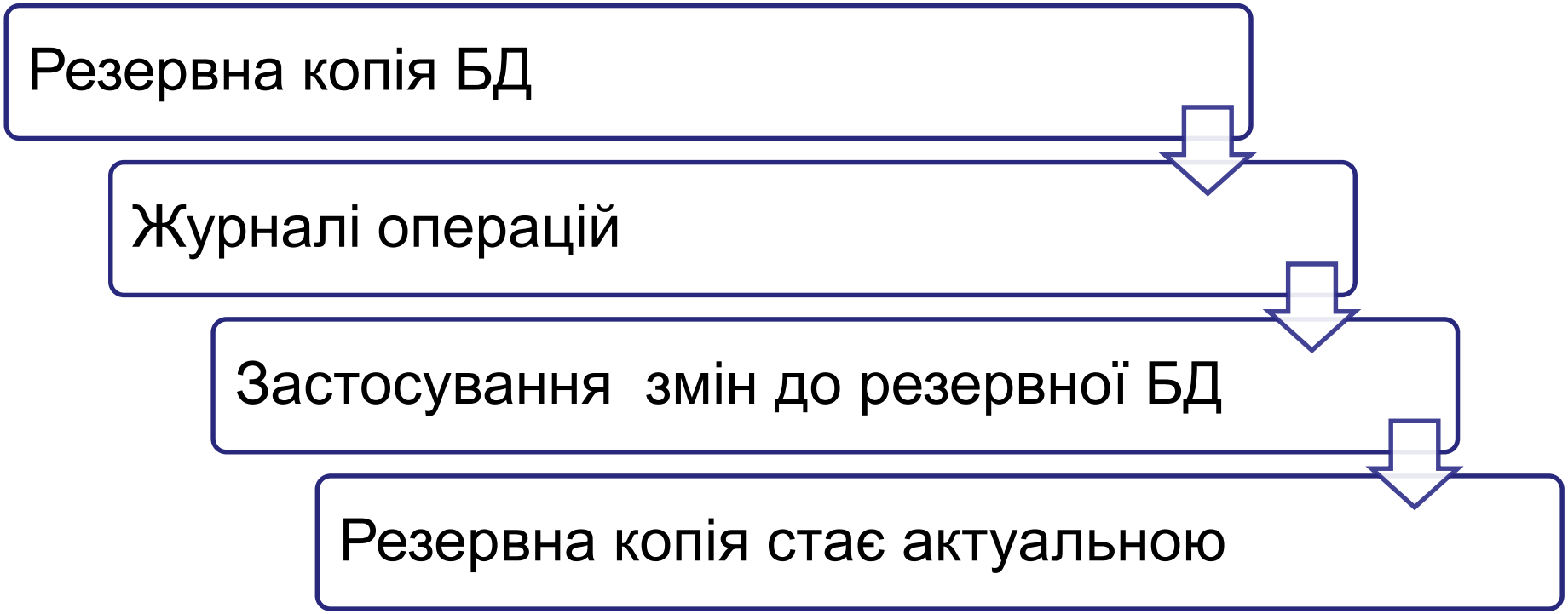
- вимоги до допустимих послідовностей операцій

```
CREATE TRIGGER Подружжя_Перевірка
BEFORE INSERT ON ПОДРУЖЖЯ
WHEN (ПОДРУЖЖЯ.Чоловік=ОСОБА.Прізвище AND
 ОСОБА.Сімейний_Стан = 'Одружений') AND NEW
(ПОДРУЖЖЯ.Жінка = ОСОБА.Прізвище AND
ОСОБА.СімейнийСтан = ‘Одружена’)
BEGIN
ROLLBACK TRANSACTION
END
```

Семантичні обмеження

Механізм підтримки цілісності у разі виникнення перебоїв

- періодичне створення резервної копії БД;
- ведення журналу всіх змін стану БД.



8.5 Поняття безпеки даних

Безпека даних

- захист даних від випадкового або спланованого доступу до них осіб, які не мають на це права, від несанкціонованого розкриття, зміни або видалення

Заходи і засоби

- Організаційно-методичні заходи
- Правові та юридичні заходи
- Технічні засоби
- Програмні засоби

Заходи і засоби

Організаційно-методичні заходи

- розроблення інструкцій та правил доступу і використання даних
- створення відповідних служб і підрозділів контролю

Заходи і засоби

Правові та юридичні заходи

- юридичне закріплення прав і обов’язків щодо зберігання, використання й передавання в електронному вигляді даних на рівні державних законів та інших нормативних документів.

Заходи і засоби

Технічні засоби захисту

- це комплекс технічних засобів для вирішення проблеми захисту даних

Програмні засоби захисту

- це комплекс математичних, алгоритмічних і програмних засобів для вирішення проблеми захисту даних

Програмні заходи безпеки даних

Система захисту

- це сукупність заходів, що вживаються в системі баз даних для гарантування необхідного рівня безпеки

Вибірковий метод

користувачі мають різні права доступу до різних або одних тих самих об’єктів бази даних

Обов’язковий метод

кожному об’єкту БД - рівень секретності, а кожному користувачу – певний рівень допуску

Механізми гарантування безпеки даних

- Реєстрація користувачів
- Керування правами доступу
- Ідентифікація та підтвердження автентичності користувачів /додатків
- Автоматичне ведення журналів доступу до даних
- Шифрування даних на зовнішніх носіях
- Довірче та адміністративне керування доступом

Довірче й адміністративне керування доступом

- Довірче керування
  - доступ користувачів до певних даних
  - передача повноваження на доступ іншим користувачам без адмін. втручання
- Адміністративне керування
  - доступ користувачів до певних даних
  - передача повноваження на доступ лише спец. авторизованому користувачу

Реєстрація користувачів

CREATE USER <користувач> **UDENTIFIED** <пароль>

Керування правами доступу

- Кому
- Умови
- Об'єкти БД
- Операції
- Передача прав іншим

8.6 Керування правами доступу

Роль – сукупність повноважень

CREATE ROLE <роль> **UDENTIFIED** <пароль>

- явно присвоєні повноваження
- повноваження, передані іншими ролями

Додаткові умови надання прав доступу

- це умови, за дотримання яких надаються певні права доступу

- часові характеристики
- локалізація комп’ютерів у локальній мережі

Класи об’єктів

- Системні об’єкти
  - База даних
  - Кластери
  - Тригери
  - Транзакції
- Об’єкти БД
  - Таблиці
  - Віртуальні таблиці
  - Процедури

Операції

- стандартні операції з маніпулювання об’єктами бази даних

- означення, переозначення й видалення таблиці або віртуальної таблиці;
- вибирання, додавання, видалення, оновлення рядків у таблиці або віртуальній таблиці;
- виконання збережених процедур

Передача повноважень користувачам/ролям

GRANT { <операція> | ALL} [(<список стовпців>)] **ON** <список об'єктів> **TO** {<користувач> | <роль> | PUBLIC} **WITH GRANT OPTION**

Приклад:

1. Надати користувачу на ім’я Джон права на виконання будь-яких операцій над таблицею ФАКУЛЬТЕТ і дозвіл на передавання цих прав іншим користувачам.

GRANT ALL ON ФАКУЛЬТЕТ **TO** Джон **WITH GRANT OPTION;**

2. Надати всім користувачам право переглядати дані з таблиці Лекція.

GRANT SELECT ON ЛЕКЦІЯ **TO PUBLIC;**

3. Надати користувачу на ім’я Джон право змінювати стовпець **фонд** у таблиці КАФЕДРА.

GRANT UPDATE (Фонд) **ON** КАФЕДРА **TO** Джон;

Обов'язкові методи захисту

- ✓ кожний об’єкт даних має певний рівень секретності
- ✓ кожний користувач – певний рівень доступу
- ✓ рівні утворюють строгий ієрархічний порядок

Ведення журналів доступу

- ✓ реєстрація всіх спроб отримання доступу до БД
- ✓ реєстрація дій користувачів
- ✓ надання адміністраторам можливості переглядати й аналізувати результати реєстрації

Засоби боротьби проти обходу системи захисту

- ✓ криптографія

Комплекс заходів і засобів направлених на безпеку даних:

- організаційно-методичні

- юридичні

- програмні

- технічні