**УДК 004.67**

# ШИФРУВАННЯ ДАНИХ У МОДЕЛЯХ РЕЛЯЦІЙНОЇ БАЗИ ДАНИХ НА РІВНІ ТАБЛИЦЬ

**Поточняк Я.В., Мунзер Аль Абдо**

**Науковий керівник – проф. каф. «Системне програмне забезпечення»,**

**канд. техн. наук Кунгурцев О.Б.**

Багато способів підвищення продуктивності інформаційних систем (ІС) не можуть бути достовірно оцінені без їх випробування в умовах функціонуючої системи. У таких випадках вдаються до використання імітаційних моделей РБД. Однак дуже часто інформація, що міститься в базі даних, носить конфіденційний характер і не може бути представлена в моделі, оскільки випробування моделі звичайно виконують фахівці, які не мають допуску до цієї інформації. У таких умовах виникає завдання шифрування певних даних.

Відомі різні алгоритми шифрування, такі як *DES*, *AES* і т.д. Однак при моделюванні даних у РБД на рівні таблиць з'являються специфічні вимоги, що визначаються метою й способом випробування моделі. В основному, ці вимоги зводяться до наступного. Не можна змінювати тип даних, не можна змінювати ймовірність появи значень даних, потрібно зберігати співвідношення значень модельованих даних (“менше”, “більше”, “дорівнює”). Крім цього, зашифровані дані, немає потреби розшифровувати в звичайному режимі роботи з моделлю, оскільки результат моделювання – не змінені дані, а оцінка продуктивності моделі при певних налаштуваннях. Тому процес дешифрування присутній тільки на етапі апробації алгоритмів шифрування і способів побудови моделі.

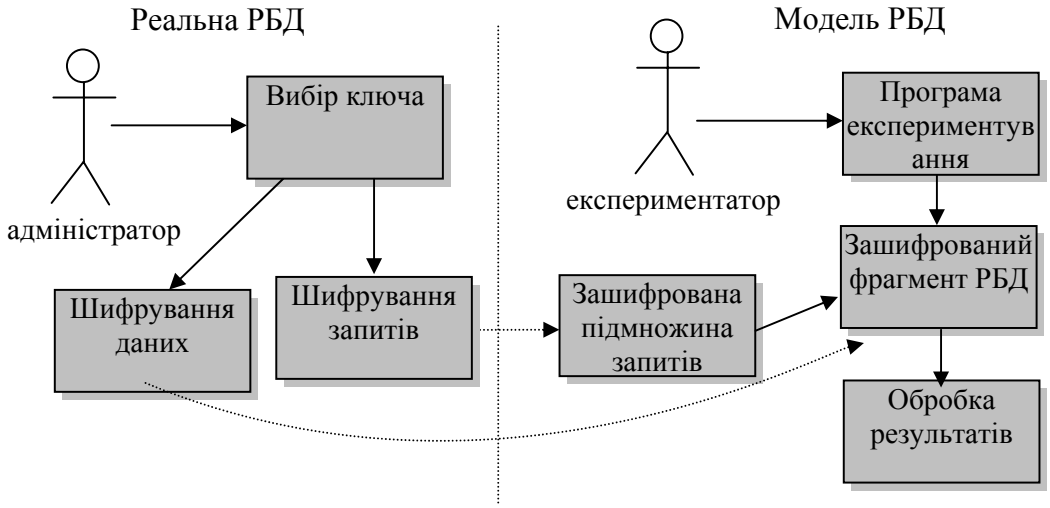


**Рис. 1. Схема роботи моделі БД при використанні шифрування даних**

На рисунку представлена схема шифрування даних і випробування моделі. Слід звернути увагу на те, що шифруванню піддаються не тільки дані, але і запити.

Моделювання на рівні таблиць – це мається на увазі, побудова моделі не всієї РБД, а тільки її фрагмента. Для виділення потрібного фрагменту попередньо слід визначити таблицю, або групу таблиць, які слід випробовувати за допомогою моделі. Після цього визначається множина запитів (з журналу трансакцій), в яких використовуються вказані таблиці. Аналіз цієї множини дозволяє визначити групу таблиць (фрагмент РБД), які слід моделювати і, відповідно, шифрувати. Одночасно потрібно шифрувати і згадану множену запитів. Очевидно, що в межах кожної таблиці немає потреби шифрувати всі поля. У пропонованій роботі розглядається шифрування тільки двох типів полів – числових і дат.

Для задоволення раніше сформульованих вимог до шифрування і збереження "правдоподібності" даних, був розроблений алгоритм шифрування, заснований на стисканні діапазону можливих значень поля. Ключ шифрування дозволяє отримати зашифровані значення в більш вузькому діапазоні, ніж це було для реального стовпця таблиці. Алгоритм шифрування містить наступні кроки.

1. Виділення граничних значень з генеральної сукупності значень кожного поля – $a_{min}$ & $a_{max}$ і $A=\{a_1, a_2, ..., a_n\}$.

2. Визначення кількості повторюваних значень – $m$ в сукупності значень кожного поля.

3. Визначення середнього інтервалу – $\Delta = (a_{max} - a_{min}) / (n - m)$, де $n$ кількість елементів генеральної сукупності.

4. Якщо середній інтервал більше 15, то це дозволяє використовувати шифрування стисненням інтервалу, оскільки дає можливість забезпечити достатню кількість вставок нових значень у процесі випробування моделі. Якщо середній інтервал виявляється менше вказаного значення, то слід застосувати шифрування методом розширення інтервалу, яке в даній роботі не розглядається.

5. Адміністратору пропонується вибрати ключ з певного діапазону значень, який і встановить ступінь стиснення зашифрованих даних.

6. Для шифрування запитів будується таблиця шифрування даних, за допомогою якої всі перетворені запити надходять у реальну РБД.

Запропонований алгоритм був випробуваний на фрагменті реальної РБД. Для перевірки його коректності було застосовано дешифрування, що в реальних умовах випробування моделі не передбачається.

Випробування показали ефективність і надійність запропонованого способу шифрування даних для моделей РБД.

## СПИСОК ЛІТЕРАТУРИ

1. Іщейнов В. Защита конфиденциальной информации / Іщейнов В., Мецатунян М. видавництво “Форум” 2009. - С. 256.

2. Панасенко С. Алгоритмы шифрования. Специальный справочник / Панасенко С. видавництво “БХВ-Петербург” 2009. - С. 576.