Національний університет “Львівська політехніка”

Тарасов Дмитро Олександрович

УДК 51.001.57+004.652.4:004.056.5

Моделювання системи захисту інформації у реляційних базах даних

Спеціальність 01.05.02 – Математичне моделювання та обчислювальні методи

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня

кандидата технічних наук

http://dtarasov.net

Львів - 2002

Дисертацією є рукопис.

Робота виконана в Національному університеті “Львівська політехніка”, Міністерства освіти і науки України

Науковий керівник - доктор технічних наук, доцент
Пасічник Володимир Володимирович,
завідувач кафедри “Інформаційні системи та мережі” Національного університету “Львівська політехніка”

Офіційні опоненти - доктор фізико-математичних наук, професор
Цегелик Григорій Григорович,
завідувач кафедри математичного моделювання соціально-економічних процесів Національного університету ім. Івана Франка (м. Львів)

доктор технічних наук, старший науковий співробітник
Русин Богдан Павлович,
завідувач відділу методів і систем обробки, аналізу і ідентифікації зображень Фізико-механічного інституту ім. Г.В. Карпенка НАН України (м. Львів)

Провідна установа - Харківський національний університет радіоелектроніки (м. Харків)

Захист відбудеться 14 березня 2003р. о $16^{\underline{00}}$ год. на засіданні спеціалізованої вченої ради Д 35.052.05 у Національному університеті “Львівська політехніка” (79013, м. Львів, вул. С.Бандери, 12)

З дисертацією можна ознайомитися у науково-технічній бібліотеці Національного університету “Львівська політехніка” (79013, м. Львів, вул. Професорська, 1)

Автореферат розісланий “___” лютого 2003р.

Вчений секретар спеціалізованої вченої ради
доктор технічних наук, професор Федасюк Д.В.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність роботи. Вирішення такої складної задачі як захист даних у інформаційних системах (ІС) базується на комплексному аналізі загроз та особливостей ІС і побудові математичної моделі системи захисту інформації (СЗІ). Відсутність адекватної моделі зменшує ефективність заходів щодо захисту інформації та призводить до складнощів та некерованості процесів підтримання належного рівня безпеки.

Враховуючи масовість використання реляційних баз даних (БД), велику кількість накопиченої в наявних БД інформації з різних предметних областей, існування стандартизованого інструментарію систем керування базами даних (СКБД), у роботі основна увага звертається на моделювання СЗІ саме реляційних баз даних, розглядаючи захист інших компонент ІС в міру необхідності.

Присвячені побудові моделей СЗІ БД роботи ґрунтуються на працях таких авторів, як Codd E., Maier D., Bell D., Griffiths P.G., LaPadula L., Wade B., Стогній А.А. За останні два десятиліття над розробленням моделей СЗІ та методів захисту інформації БД працювали Герасименко В.А., Гришин С.Г., Дейт К. Дж., Домарев В.В., Мельников В.В., Петров В.А., Пискарев А.С., Хорошко В.А., Хоффман Л.Дж., Шеин А.В., Bertino E., Chomicki J., Denning D., Fagin R., Gal-Oz N., Gertz M., Jajodia S., Lindsay B.G., Lipeck U. W., Lunt T.F., Qian X., Wilms P.F. та інші.

Проведений аналіз сучасного стану досліджень у галузі інформатики, теорії БД, теорії прийняття рішень, захисту інформації вказує на наявність ряду нерозв’язаних проблем. Серед них:

- відсутні математичні моделі СЗІ реляційних БД з врахуванням необхідності у статистичному захисті інформації, квотах, оптимізації ресурсоємності СЗІ, аудиті на рівні кортежів та значень атрибутів кортежів, забезпеченні можливості відтворити історію змін даних за довільний проміжок часу;
- недостатньо розроблена методологія проектування схем реляційних БД з врахуванням потреб у захисті інформації;
- наявні моделі недостатньо якісно вирішуються задачі авторизації для користувачів СКБД та ряд спеціальних задач захисту БД (статистичний захист, захист від отримання надлишкової інформації тощо).

Зв’язок роботи з науковими програмами, планами, темами.

Робота виконувалась в рамках пріоритетного наукового напрямку Міністерства освіти України “Перспективні інформаційні технології, прилади комплексної автоматизації, системи зв’язку” по темах: “Дослідження процесів проектування розподілених інтелектуальних інформаційних систем прийняття рішень для слабоструктурованих проблем на основі реляційних баз даних (на прикладі сфери фінансів, бізнесу та управління)”, шифр 0196U000179; “Розробка макетів та моделей для проектування розподілених інтелектуальних

інформаційних систем, алгоритмів і програм виявлення та апробації систем переваг особи, що приймає рішення, методів відсіювання та відбору альтернатив в слабоструктурованому середовищі", шифр 0198U002391. У межах цих робіт дисертантом розроблено основні підходи до побудови моделі системи захисту інформації розподілених інтелектуальних інформаційних систем прийняття рішень.

Метою дисертаційної роботи є розробка математичних моделей, методів та алгоритмів захисту інформації і їх застосування в інформаційних системах, побудованих на основі реляційних СКБД.

Мета дисертаційної роботи визначає необхідність розв'язання наступних задач:

- Аналіз наявних моделей СЗІ реляційних БД та загроз, які виникають при використанні ІС на основі реляційних БД.
- Побудова математичної моделі СЗІ БД, яка б врахувала особливості та характерні риси задач захисту інформації в інформаційних системах, що функціонують на основі реляційних БД.
- Побудова математичної моделі безпечної бази даних (ББД) як розширення реляційної моделі даних. Визначення операцій для роботи з безпечною базою даних та розроблення алгоритмів реалізації математичної моделі ББД засобами реляційної моделі.
- Визначення основних підходів до застосування методологій аналізу та проектування інформаційних систем при побудові інформаційних систем на основі розроблених математичних моделей.
- Апробація результатів дисертаційних досліджень шляхом створення СЗІ прикладної інформаційної системи.

Об'єктом досліджень виступають інформаційні системи, що працюють на основі реляційних БД та потребують захисту інформації.

Предметом досліджень є математичне моделювання комплексної системи захисту інформації реляційної БД, у тому числі, розроблення методів та алгоритмів для реалізації удосконаленої моделі авторизації користувачів, удосконаленої моделі аудиту дій користувачів реляційних БД.

Методи досліджень. Дослідження, виконані під час роботи над дисертацією, ґрунтуються на теорії реляційних БД, теорії функціональних залежностей, теорії нормалізації реляційних баз даних, апараті реляційної алгебри, дослідженнях у галузі захисту інформації, структурній та об'єктно-орієнтованій методології аналізу та проектування ІС, теорії формальних систем, теорії оптимізації, теорії імовірностей та математичній статистиці.

Наукова новизна роботи полягає у досягненні наступних результатів.

- Уперше введено поняття безпечної БД та сформульовано вимоги до математичної моделі безпечної БД з врахуванням потреб у статистичному захисті інформації, контролі квот інформації, оптимізації ресурсоємності СЗІ,

аудиті оновлень на рівні відношень, кортежів та значень атрибутів кортежів, забезпеченні можливості відтворити історію змін даних за довільний відрізок часу. Ці вимоги є основою для побудови комплексної системи захисту інформації реляційної БД.

- Уперше запропоновано математичну модель комплексної системи захисту інформації реляційної БД для статистичного захисту інформації, захисту від порушення конфіденційності шляхом отримання великих об'ємів інформації, детальному аудиті оновлення даних, реалізації примусового та довільного керування доступом, забезпечення цілісності даних, що дозволяє зменшити основні загрози інформації реляційної БД.
- Удосконалено модель примусового керування доступом для забезпечення сучасних потреб захисту інформації фінансово-економічних інформаційних систем та автоматизації керування системою захисту інформації ББД.
- Запропоновано нову математичну модель об'єкту захисту у реляційних БД, яка використовується для проектування схеми безпечної БД, що підвищує якість реалізації СЗІ БД засобами промислових реляційних СКБД.
- Введено обмежений набір операцій доступу до реляційної БД для запропонованої математичної моделі ББД. Цей набір операцій використовується для блокування виправлень в електронних документах, які зберігаються у БД та формування базової інформації для аудиту.

Практичне значення одержаних результатів полягає у наступному.

- Розроблено методи та алгоритми для захисту інформації реляційної БД з використанням запропонованої математичної моделі ББД та стандартних засобів промислових СКБД. Реалізація ББД блокує основні загрози конфіденційності, цілісності інформації реляційної БД, забезпечує аудит потрібної деталізації.
- Розроблено методи та алгоритми для реалізації удосконаленої моделі примусового керування доступом користувачів реляційних БД, удосконаленої моделі аудиту користувачів ББД. Ці механізми забезпечують швидку адаптацію СЗІ БД до змін політики безпеки, зменшення обчислювальних ресурсів, необхідних для СЗІ.
- Подано пропозиції щодо використання розроблених математичних моделей та налаштування СЗІ. Подані методики дозволяють будувати захищені ІС на основі серверів БД, інтегрувати СЗІ серверів БД з СЗІ інших корпоративних сервісів для забезпечення комплексного захисту даних підприємства.
- Розроблено систему захисту інформації інформаційної системи "Гермес", яка на практиці відображає результати теоретичних дисертаційних досліджень.

Впровадження результатів роботи. Розробки впроваджені у Львівській обласній державній адміністрації (м. Львів), фонді "Транспорт" (м. Ужгород), Львівському банківському інституті (м. Львів), Технологічному університеті "Поділля" (м. Хмельницький), а також в навчальному процесі, зокрема, в

курсах “Захист та безпека даних у інформаційних системах та мережах”, “Засоби забезпечення цілісності та достовірності даних”, “Комп’ютерні системи та мережі в автоматизованих системах керування технологічними процесами”, “Організація баз даних та знань”, “Основи системного аналізу об'єктів і процесів комп'ютеризації”, “Операційні системи комп'ютерних мереж”, “Комп'ютерні інформаційні мережі”, в яких використовувалися результати наукових досліджень як в окремих розділах лекційного курсу, так і в циклах лабораторних та практичних робіт.

Особистий внесок здобувача. Усі наукові результати, подані у дисертації, одержані здобувачем особисто. У друкованих працях, опублікованих у співавторстві, особистий внесок здобувача такий: [1] - належить аналіз функцій та тестової роботи прототипу інформаційної системи, додаткових вимог до захисту інформації та вибору інструментів розробки; [6] – дослідження засобів захисту серверів БД та систем аутентифікації користувачів БД; [9] - дослідження надійності користувацької компоненти інформаційних систем та моделі довірчих відношень; [11] - аналіз методів інформатизації планування виробничих процесів; [12] – аналіз загроз операцій зміни даних та методи захисту від неавторизованих або помилкових змін даних.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідалися на семінарах та конференціях: І міжнародна конференція з індуктивного моделювання “МКІМ’2002” – Львів 2002; міжгалузевий міжрегіональний семінар Наукової ради НАН України “Технічні засоби захисту інформації” - Львів 1999, 2000, 2001, 2002; п’ята та шоста Всеукраїнська наукова конференція “Застосування обчислювальної техніки, математичного моделювання та математичних методів у наукових дослідженнях” – Львів 1998, 1999; Всеукраїнський семінар кредитних спілок – Славське 2001; наукові семінари міжнародних комп’ютерних виставок “Комп’ютер і Офіс” – Львів 1998 - 2001; наукові семінари міжнародних комп’ютерних виставок “Комп’ютер+Бізнес” – Львів 1998 - 2001; щорічні (1998 - 2002) наукові семінари кафедри "Інформаційні системи та мережі" та наукові конференції викладачів і науковців Національного університету “Львівська політехніка”.

Публікації. По темі дисертації опубліковано 12 наукових праць, із них 7 праць – одноосібні. Загальний обсяг публікацій 106 сторінок. 10 праць опубліковані у фахових виданнях ВАК України.

Структура та обсяг роботи. Дисертаційна робота складається з переліку умовних скорочень, позначень та термінів, вступу, чотирьох розділів, висновку, списку літератури та додатків. Загальний обсяг дисертації 130 сторінок без додатків, список літератури включає 115 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується актуальність теми, формулюється мета та основні задачі досліджень, подається короткий зміст роботи.

<u>У першому розділі</u> наведено огляд більш як 110 літературних джерел та матеріалів конференцій у галузі захисту інформації в інформаційних системах на основі серверів БД за останні 20 років, розглядаються моделі СЗІ БД та види загроз інформації у ІС на основі серверів БД.

Захист інформації – комплекс заходів для забезпечення цілісності інформації, запобігання несанкціонованим змінам і отриманню даних. Основні характеристики захисту інформації – гарантована достовірність даних, конфіденційність, цілісність та доступність інформації. **СЗІ** – програмно апаратний комплекс, призначений вирішити завдання захисту ІС.

Політика безпеки (ПБ) – сукупність документів, цілей, правил, що визначає загальний напрямок робіт на підприємстві у галузі захисту інформації.

Задача СЗІ полягає у забезпеченні для заданої ІС, протягом часу $t_{ЗІС}$, $P_{ІС} \le P_{Дост} < 1$, де $P_{ІС}$ - імовірність порушення безпеки ІС протягом часу $t_{ЗІС}$, $P_{Дост}$ - максимально припустима імовірність порушення безпеки ІС. $P_{Дост}$ та $t_{ЗІС}$ визначаються політикою безпеки та залежать від цінності та особливостей використання інформації, відповідно і кваліфікації порушника безпеки та вартості СЗІ.

Об’єктами захисту у реляційних БД (об’єктами БД) є множини значень доменів, значення атрибутів, значення кортежів даних, набори кортежів, цілі відношення тощо.

Для подання прав доступу суб’єктів до об’єктів введена розширена матрична модель - куб $\mathbf{M}$, на осях якого позначаються суб’єкти, об’єкти та операції.

$$\mathrm{DAC}: S \times O \times F \to \mathbf{M}, \qquad \textbf{(1)}$$

де O – множина усіх об’єктів захисту, S – множина суб’єктів (користувачів БД, процесів, які діють від імені певного користувача тощо), F - множина можливих операцій з об’єктами БД. Основними **операціями** з об’єктами БД є введення, перегляд, зміна та знищення даних.

Для реалізації примусового керування доступом (Mandatory Access Control) із суб'єктами і об'єктами асоціюються мітки безпеки з множини L.

$$L = \left\{ l_i, i = \overline{1, k_L} \right\}, k_L \in N \qquad \textbf{(2)}$$

Мітка об'єкта описує ступінь закритості (конфіденційності) інформації, що міститься в об'єкті, мітка суб'єкта – максимальний рівень конфіденційності даних, доступних суб’єкту. За допомогою відображень $F_s : S \to L$ і $F_o : O \to L$, які ставлять множинам суб’єктів та об’єктів у відповідність множину міток безпеки та відношень на L, визначається можливість користувача s виконувати операції з o.

На L визначені бінарні відношення строгого домінування $\prec$, еквівалентності = та не строгого домінування $\preceq$:

$$l_i \preceq l_j \Rightarrow \left\{\left(l_i \prec l_j\right) \vee \left(l_i = l_j\right)\right\}. \quad \textbf{(3)}$$

Запис $l_1 \preceq l_2$ позначає домінування мітки l_2 над l_1.

Відображення $\mathrm{Top}: L \to L,\ \mathrm{Top}(l) = \left\{l_j \in L : l \preceq l_j\right\}$ визначає множину міток безпеки, які домінують над l.

Відображення $\top: L \to L,\ \top(l) = \left\{l_j \in \mathrm{Top}(l) : \forall l_i \in \mathrm{Top}(l), l_i \preceq l_j\right\}$ визначає множину міток безпеки верхнього рівня. Відображення $\mathrm{Bot}(l) = \left\{l_j \in L : l_j \preceq l\right\}$ та $\perp(l) = \left\{l_j \in \mathrm{Bot}(l) : \forall l_i \in \mathrm{Bot}(l), l_j \preceq l_i\right\}$ визначають множину міток безпеки, над якими домінує l, та множину міток безпеки нижчого рівня.

Здійснений аналіз показав, що у практичних реалізаціях використовуються (усі чи деякі) наступні обмеження на відношення =, $\preceq$ $\preceq$:

$$\left(\forall l_i, l_j, l \in L : l_i \preceq l, l \preceq l_j\right)\left\{\perp(l) \preceq l_i \preceq l_j \preceq \top(l)\right\}, \quad \textbf{(4)}$$

$$\left(\forall l_i, l_j \in L\right)(\exists!\perp)(\exists!\top)\left\{\perp\left(l_i\right) = \perp\left(l_j\right) \wedge \top\left(l_i\right) = \top\left(l_j\right)\right\}. \quad \textbf{(5)}$$

Обмеження (4), (5) не дозволяють адаптувати СЗІ СКБД для ряду практичних задач, наприклад, для фінансово-економічних ІС.

Для забезпечення універсальності математичної моделі ББД та гнучкості адміністрування СЗІ ББД у запропонованій у дисертації математичній моделі ББД знято зазначені штучні обмеження та введено поняття узагальненої мітки безпеки. Узагальнена мітка безпеки має вигляд

$$\hat{l} = \left\langle l^1, ..., l^n, \Phi^1, ..., \Phi^m \right\rangle \in \hat{L}, \quad \textbf{(6)}$$

де $l^i \in L$, $\Phi^j = \left\{\phi_k^j\right\}$ - множини категорій, $n, m, k \in \mathbb{N}$.

Мітка безпеки $\hat{l}_2$ строго домінує над $\hat{l}_1$ (позначається $\hat{l}_1 \lhd \hat{l}_2$), якщо

$$\hat{l}_1 \lhd \hat{l}_2 : \left(l_1^i \prec l_2^i, \Phi_1^j \subset \Phi_2^j, i = \overline{1,n}, j = \overline{1,m}\right). \quad \textbf{(7)}$$

Мітка безпеки $\hat{l}_2$ не строго домінує над $\hat{l}_1$ (позначається $\hat{l}_1 \trianglelefteq \hat{l}_2$), якщо

$$\hat{l}_1 \trianglelefteq \hat{l}_2 : \left(l_1^i \preceq l_2^i, \Phi_1^j \subseteq \Phi_2^j, i = \overline{1,n}, j = \overline{1,m}\right). \quad \textbf{(8)}$$

Доступ до об’єкту визначається наступними правилами:

- суб'єкт може читати інформацію з об'єкта, якщо $\hat{l}_s \trianglerighteq \hat{l}_o$;
- суб'єкт може записувати інформацію в об'єкт, якщо $\hat{l}_s \trianglelefteq \hat{l}_o$.

Завдяки використанню $\hat{l}$, запропонована у роботі модель ББД не має обмежень у застосуванні, характерних для моделі MRDB.

Забезпечення цілісності даних визначено, як забезпечення несуперечливості даних для процесів прийняття рішень, де суперечливість означає настання однієї з наступних подій:

1. У БД існують доступні користувачу набори даних A_1, A_2, які містять дані про один і той самий бізнес-об'єкт. Існує функція (запит, послідовність дій над даними) $Q(A_i)$, i=1 або 2, $Q(A_1)=B_1$, $Q(A_2)=B_2$. Для Q вірно $Q(A_1)\neq Q(A_2)$. Тобто, результати B_1, B_2 не рівні, або одне зі значень B_i не визначене. Причому Q логічно вірно опрацьовує дані у кожному окремо взятому випадку.
2. У БД існує набір даних A_3, які втратили зміст. Тобто, неможливо однозначно вказати, який бізнес-об'єкт або які характеристики бізнес-об'єкта описують дані A_3 і які значення мають ці характеристики.
3. Існує скінченна послідовність команд W (запит), виконання якої над однаковими даними повертає різні (навіть не передбачувані) результати. Непередбаченість результатів пов'язана з внутрішнім станом та принципами роботи СКБД, порушеннями атомарності транзакцій, особливостями фізичного розміщення даних тощо. Користувач БД не має засобів впливу на фізичну реалізацію послідовності команд W.

Для забезпечення доступності даних необхідно блокувати можливість захоплення користувачем (групою користувачів) ресурсів ІС. Для цього потрібно обмежувати кількість доступних користувачу ресурсів, що не можна зробити багатьма промисловими СКБД. Більш того, СКБД дозволяють контролювати лише використання ІС на фізичному рівні. Існує клас задач, які не можна описати на фізичному рівні, потрібно задати обмеження на логічному рівні. У дисертації розроблений механізм визначення та контролю **квот** доступу до об'єктів БД, який реалізує обмеження на логічному рівні за допомогою модифікованих SQL запитів.

Враховуючи наведені у дисертації недоліки СЗІ БД та особливості загроз інформації у реляційних БД, визначаються наступні задачі.

1. Формування безпечного середовища роботи для користувачів БД, у якому забезпечується цілісність даних, неможливе несанкціоноване розголошення та зміна даних іншими користувачами БД.
2. Мінімізація доступу користувачів до непотрібних даних, як на читання, так і на створення, зміну, знищення.
3. Забезпечення достовірності та цілісності даних в ІС.
4. Створення ефективних засобів адміністрування політики безпеки БД.
5. Забезпечення інтеграції СЗІ в ІС на етапі проектування схеми БД.

БД, яка вирішує наведені задачі, називається **безпечною БД** (**ББД**). Поняття ББД введено у дисертації вперше.

Основними завданнями моделі ББД є:

- усунення недоліків засобів авторизації, аудиту наявних моделей;

- спрощення адміністрування політики безпеки ІС на основі реляційних БД;
- забезпечення конфіденційності (у тому числі статистичний захист даних, захист на рівні кортежів тощо);
- забезпечення цілісності інформації (у тому числі контекстно залежний захист),

що на практиці неможливо досягнути за допомогою розглянутих у дисертації моделей СЗІ:

- реляційної СКБД та узагальненої моделі СЗІ РСКБД;
- Bell-LaPadula, Діона, багаторівневої реляційної бази даних (MRDB);
- комбінованої моделі.

Так, при використанні СКБД з моделлю MRDB виникає ряд проблем:

- Ієрархія рівнів доступу спеціалізованих СКБД не є розгалуженою, що не відображає особливості розподілу повноважень відповідно до функціональних обов'язків.
- Класичні механізми забезпечення багатоверсійності є надлишковими для ІС фінансово-економічного (і взагалі цивільного) характеру та є додатковим навантаженням на обчислювальні ресурси.
- Сфера використання спеціалізованих СКБД обмежується також недоступністю відповідного програмного забезпечення на ринку України (велика вартість та заборона експорту у інші країни, зокрема в Україну).

У дисертації вперше запропоновано використовувати модель ББД як модель СЗІ БД. Це дозволяє реалізувати нову політику безпеки з врахуванням потреб обмеження доступу на читання/запис окремих кортежів, атрибутів та груп кортежів БД, здійснювати статистичний захист інформації, аудит даних, забезпечити цілісність та контроль за СЗІ та її змінами, полегшити адміністрування СЗІ.

Використанню ББД передує заміна задачі обмеження доступу до інформації у наявних відношеннях на задачу захисту електронних документів з подальшим поданням документів у вигляді об'єктів БД. Нові об'єкти мають додаткові атрибути для збереження даних безпеки, відповідно до політики безпеки (мітки доступу, інформація аудиту тощо).

Форма та механізми фіксації авторства інформації стандартних засобів аудиту, наявних на ринку СКБД, складні для поточного використання та аналізу. Для забезпечення відслідковування авторства даних, створена у дисертації математична модель ББД містить функцію відповідності

$$Autor : O \to \{\langle s, time, \text{sysinfo}, \text{extrainfo}\rangle\}, \qquad \textbf{(9)}$$

де O – об'єкти доступу, s – суб'єкт, $time$ час створення об'єкту, sysinfo - додаткова системна та інша інформація, необхідна для проведення розслідування інцидентів, extrainfo - додаткова інформація, розміщена користувачем.

Значення extrainfo у дані аудиту БД автором введено вперше. Принципова можливість користувача БД впливати на аудит шляхом доповнення даних аудиту власною інформацією дозволяє:

- свідомо ставитись до процесу аудиту БД та захисту інформації в цілому;
- полегшувати розслідування інцидентів збереженням додаткової інформації про інцидент (часто цю інформацію не можна передбачити заздалегідь та описати формально);
- використовувати extrainfo як, свого роду, коментар або примітку щодо *O* для інших користувачів БД.

У системах, які проектувалися окремо від СЗІ, зміна прав доступу до інформації часто є складною для адміністрування задачею. Адміністрування користувачів СКБД та адміністрування прав доступу до конкретних об'єктів БД розглядають, як дві окремі задачі. Процеси фіксації в ІС даних щодо графіку роботи, посади, зміни статусу працівників тощо не змінюють права доступу працівників. Зміна прав доступу виноситься у окрему задачу адміністрування БД. Використання математичної моделі ББД спрощує адміністрування захисту завдяки інформаційній інтегрованості у моделі ББД компонент обліку людських ресурсів та підсистеми надання доступу користувачам.

Далі, у дисертації, розглянуто питання захисту БД як компоненти ІС, питання комплексності заходів щодо захисту інформації у БД, захисту від загроз, блокування яких засобами СКБД неможливе. Для цього створена модель надійної інформаційно-обчислювальної системи, захист елементів якої додатково розглянутий у розділі 3 та літературі (огляд у розділі 1).

<u>У другому розділі</u> розглядаються концептуальна та математична модель ББД. Запропоновано розв'язувати задачі захисту інформації з розділу 1 доповненням СЗІ БД рядом об'єктів (таблиць, переглядів, ролей, процедур тощо) та правил роботи з ІС та СЗІ. Ці об'єкти є захисним прошарком (проміжним рівнем) між об'єктами БД та діями користувачів БД, які пропущено обмеженнями СКБД (рис. 1).

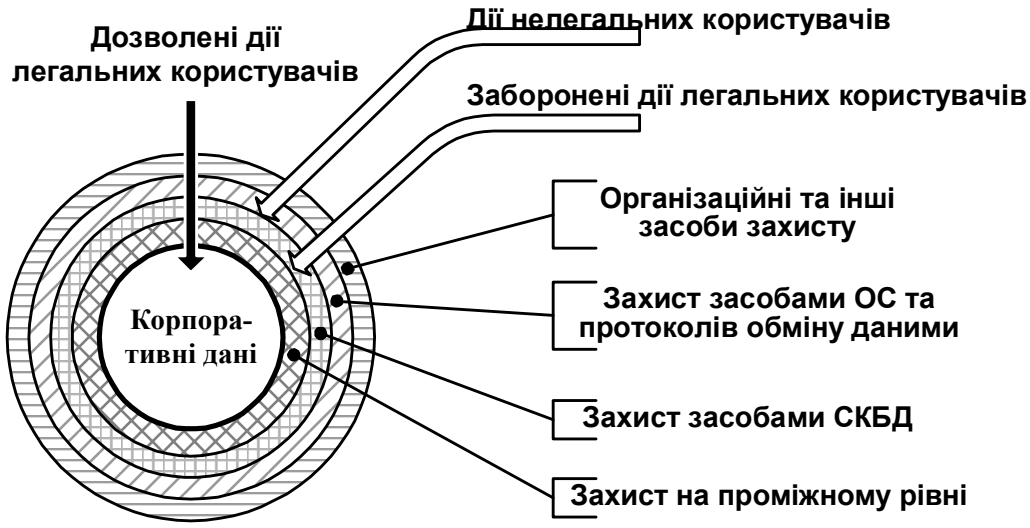

Рис. 1. Концептуальна модель СЗІ ББД.

Захисний прошарок забезпечує реалізацію прийнятої політики безпеки та виконує наступні функції:

1) обмеження доступу до даних,
2) забезпечення цілісності даних,
3) фіксація та контроль авторства,
4) автоматизацію адміністрування СЗІ,
5) забезпечення активності СЗІ (у т. ч. виконання превентивних дій),
6) контроль квот ресурсів.

Для надання користувачу результатів виконання запиту дані ББД проходять через наступні етапи опрацювання у СЗІ (рис. 2):

1) зчитування даних (з пристроїв збереження) та контроль використання квот ресурсів на фізичному рівні,
2) підготовка даних (наприклад, формування вибірки даних для статистичних розрахунків),
3) фіксація даних аудиту,
4) обмеження доступу за принципом MRDB та заміна результатів виконання запиту,
5) формування електронного документа, як єдиного цілого, відтворення історії об'єкту,
6) статистичний захист та логічні обмеження на кількість наданої інформації,
7) обмеження доступу з використанням переглядів та ролей (модель DAC),
8) контроль обмежень цілісності та контекстно залежний захист даних,
9) опрацювання результуючих даних за допомогою бізнес-алгоритмів (реалізація бізнес-правил),
10) надання результатів користувачу.

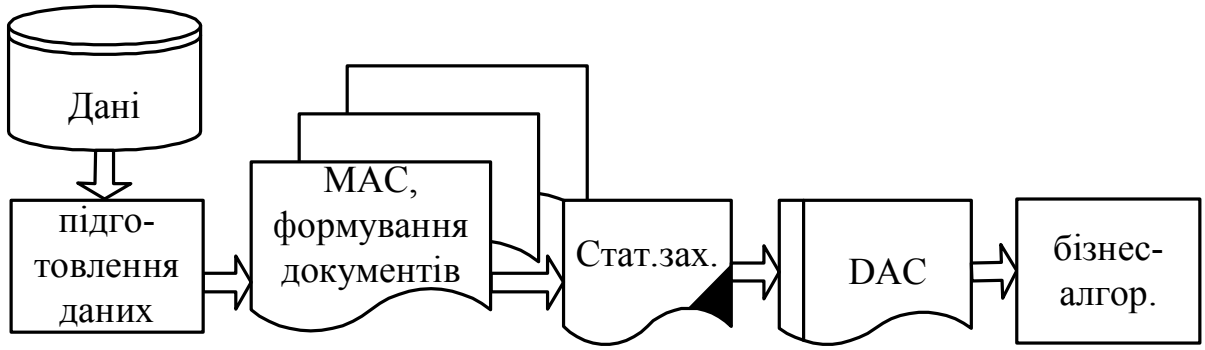

Рис. 2. Схема опрацювання даних СЗІ ББД

Побудована у дисертації **математична модель СЗІ безпечної БД** db^{S} зі схемою $S_{DB^{\mathrm{S}}}$ має вигляд:

$$SM = \left\langle O^{\mathrm{SA}}, S, G, \Omega^{\mathrm{S}}, \Sigma, S_{DB^{\mathrm{S}}}, D_{DB^{\mathrm{S}}}, \mathrm{DOM}^{\mathrm{S}}, \hat{L}, \trianglelefteq, Lab_S, \mathbf{M}^{\mathrm{S}}, Autor \right\rangle, \qquad \textbf{(10)}$$

де O^{SA} - множина атомів захисту, $\hat{L}$ - множина узагальнених міток безпеки, $\trianglelefteq$ - відношення на множині $\hat{L}$, Lab_S – функція, яка визначає мітку

безпеки суб'єкта. Множина доменів $D_{DB^{\mathrm{S}}} = D_{DB} \bigcup D_{\hat{L}} \bigcup D_{Hist}$ доповнена доменами: D_{Hist} - домени атрибутів даних аудиту та збереження історії зміни атомів захисту та $D_{\hat{L}}$ - домени для атрибутів $\hat{L}$. $\mathrm{DOM}^{\mathrm{S}}$ - функція відповідності між множинами доменів та атрибутів. $\mathbf{M}^{\mathrm{S}} = \left(m_{ijk}^{\mathrm{S}} \right)$ визначає права доступу користувача s_i на виконання операцій $\omega_k \in \mathbf{\Omega}^{\mathrm{S}}$ з атомом захисту $o_j^{\mathrm{SA}} \in O^{\mathrm{SA}}$.

Електронний документ – структурована сукупність об'єктів БД, які містять інформацію про певний факт, документ предметної області. Має спільні характеристики: дату та автора введення у систему, термін актуальності даних (термін початку дії документу, термін завершення). Об'єкт захисту $o_i^{\mathrm{S}} = \left\{ o_i^{\mathrm{I}} \right\} \in O -$ сукупність інформації (інформаційні об'єкти o_i^{I}) з єдиними правилами безпеки (правилами доступу, аудиту тощо), часом життя інформації, іншими важливими з точки зору захисту інформації характеристиками.

Атом захисту $o_i^{\mathrm{SA}} = \left\langle o_i^{\mathrm{S}}, \prod_i, I \right\rangle$, $\prod_i$ - правила безпеки, I – інформація захисту: історія o_i^{S}, історія захисту та системні дані.

Умови надання доступу для виконання операцій задані у вигляді впорядкованої четвірки $\left\langle o_i, s_j, f_m, rule \right\rangle$. Множина правил доступу

$$Rule = \left\{ \left\langle o, s, f, rule \right\rangle, o \in O, s \in S, f \in F \right\}, \qquad \textbf{(11)}$$

де *rule* - предикат, який задає додаткові обмеження на можливість виконання операції.

Досліджено операції з об'єктами ББД, загрози захисту інформації, які виникають при використанні операцій оновлення даних, методи блокування наведених загроз. Запропоновано використання обмеженого набору операцій для доступу до БД. А саме, обмежений набір операцій для користувачів БД містить операції INSERT, SELECT, DELETE (з деякими обмеженнями використання DELETE).

У дисертації запропонована методика використання обмеженого набору операцій та проектування схеми БД, забезпечення роботи ББД з обмеженим набором операцій. Показана функціональна повнота обмеженого набору операцій при дотриманні правил проектування схеми ББД.

Для об'єктів захисту O запропоновано створити своєрідний "накопичувач" інформації

$$\mathrm{Hist} = \left\langle A, Tr, h \right\rangle, \qquad \textbf{(12)}$$

де субнакопичувач A - зберігає інформацію, необхідну для аудиту використання об'єкту. Реалізація A стандартними системними засобами промислових СКБД не задовольняє багато вимог до повноти інформації.

Tr - забезпечує інформацією механізм транзакцій та зберігається до остаточного підтвердження користувачем необхідності виконання операції. Підтвердженням є команда завершення транзакції (у системах з підтримкою транзакцій), багатократне безпомилкове введення інформації про об'єкт, або інші події згідно з правилами роботи ІС.

h - інформація для забезпечення можливості повернення об'єкту у цілісний стан на заданий момент часу протягом тривалого терміну. Стандартними системними засобами промислових СКБД не реалізовано.

Типовими об'єктами захисту у реляційних БД є кортежі відношень БД - $o_i^{\mathrm{S}} = \langle a_1,...,a_n \rangle \in r$. Постає задача виправлення помилок без знищення наявної у кортежах інформації, іншими словами – забезпечення історичності БД.

Першим з методів збереження історичної інформації є використання часових (temporal) БД. Часові БД дозволяють реалізувати операцію оновлення даних зі збереженням попереднього значення за допомогою фіксації "станів" значень атрибутів кортежів.

Другим методом збереження історичної інформації є архівація інформації у альтернативні до *r* структури даних з подальшою заміною старих значень *o* на нові. Недоліками методу архівації є:

- практично двократне дублювання структур даних;
- розділення актуальної та історичної інформації ускладнює процедури аналізу;
- необхідність у використанні програмних кодів.

Третім методом збереження історичної інформації є проектування схеми БД для подальшого забезпечення накопичення історичної інформації спільно з "актуальним" останнім значенням o_i^{S}. Як накопичувачі у дисертації пропонується використовувати структури вигляду <об'єкт, історія об'єкту>. Таким чином, значення кортежу o_i^{S} зберігаються у вигляді o_i^{SA} у нових структурах даних $r_1,...r_m$. У відношеннях $r_i \in S^c, 1 \le i \le k \le m$ зберігається незмінна інформація o_i^{S}, у $r_j \in S^h, k+1 \le j \le m$ частина o_i^{S} – атрибути, які змінюються (довизначаються). Дані аудиту виділяються у окремі відношення $r_l \in S^a, 1 \le l \le v$ або зберігаються, як частина $r_j \in S^h$. Доцільно проектувати схему S^a з врахуванням функціональних залежностей між даними аудиту o_i^{SA} та стандартними атрибутами журналів аудиту СКБД.

У дисертації розроблені методи проектування схеми ББД для збереження даних з врахуванням потреб захисту інформації та забезпеченні історичності даних.

Здійснено аналіз специфічних для СКБД загроз конфіденційності інформації та методи блокування розглянутих загроз (агрегування даних, захист від отримання великих об'ємів інформації).

<u>У третьому розділі</u> розглядаються засоби реалізації математичної моделі ББД, введеної у розділі 2, за допомогою стандартних засобів промислових СКБД. Запропоновано методи та алгоритми реалізації обмежень доступу у ББД. Зокрема, запропоновано механізм обмеження доступу з використанням модифікованих SQL запитів. Проведано аналіз та класифікацію методів модифікації запитів. Сформульовано алгоритми автоматизованої модифікації запитів основних видів. Розроблено методику перепроектування схеми БД для реалізації ББД.

Модифікація SQL запитів дозволяє замість запиту Q_u, який отримано від користувача *u*, виконувати запит $Q_u^{'}$, який отримано з Q_u за допомогою правила модифікації запитів $MOD_{Rule}^{Q,u}$ та надати користувачу *u* результати виконання $Q_u^{'}$.

$$MOD_{Rule}^{Q,u} : Q(O,S) \to Q(O,S). \qquad \textbf{(13)}$$

Вихідними даними для $MOD_{Rule}^{Q,u}$ є інформація про користувача та сеанс зв'язку (ідентифікатор, час з'єднання, адреса, кількість відкритих сеансів зв'язку тощо), текст запиту (містить як перелік об'єктів доступу, так і дії).

Запропоновані у роботі методи модифікації ділиться на наступні види:

- просте обмеження доступу до окремих кортежів,
- обмеження доступу до окремих кортежів з підставлянням даних,
- заміна результатів запита.

$$\dot{Q}_u^{'} = \mathrm{MOD}_{\mathrm{Rule}}^{\mathrm{Q,u}}(Q_u) \qquad \textbf{(14)}$$

- елементарне обмеження доступу до кортежів.

Обмеження доступу до окремих кортежів з підстановлянням даних:

$$\ddot{Q}_u^{'} = \left\{ \begin{array}{l} t: \\ t = \langle f_1(r),...,f_n(r) \rangle, r = \langle a_1,...,a_n \rangle \in Q_u, f_i(r) \in DOM(a_i), \\ \mathrm{RULE}(r,t,u) = TRUE \end{array} \right\} \qquad \textbf{(15)}$$

Використовується для обмеження доступу користувача до окремих кортежів та підставляння замість реальних даних результатів обчислень деяких функцій.

Заміна результатів запиту Q_u результатами $Q_u^{'}$:

$$\dddot{Q}_u^{'} = \left\{ \begin{array}{l} t: \\ t = \langle b_1,...,b_n \rangle, r = \langle a_1,...,a_n \rangle \in Q_u, b_i \in DOM(a_i), \\ \mathrm{RULE}(r,t,u) = TRUE \end{array} \right\} \qquad \textbf{(16)}$$

Використовується для заміни результатів запиту Q_u результатами $\dddot{Q}_u^{'}$.

Прозора для користувачів модифікація запиту відбувається завдяки використанню додаткового перегляду (рис. 3).

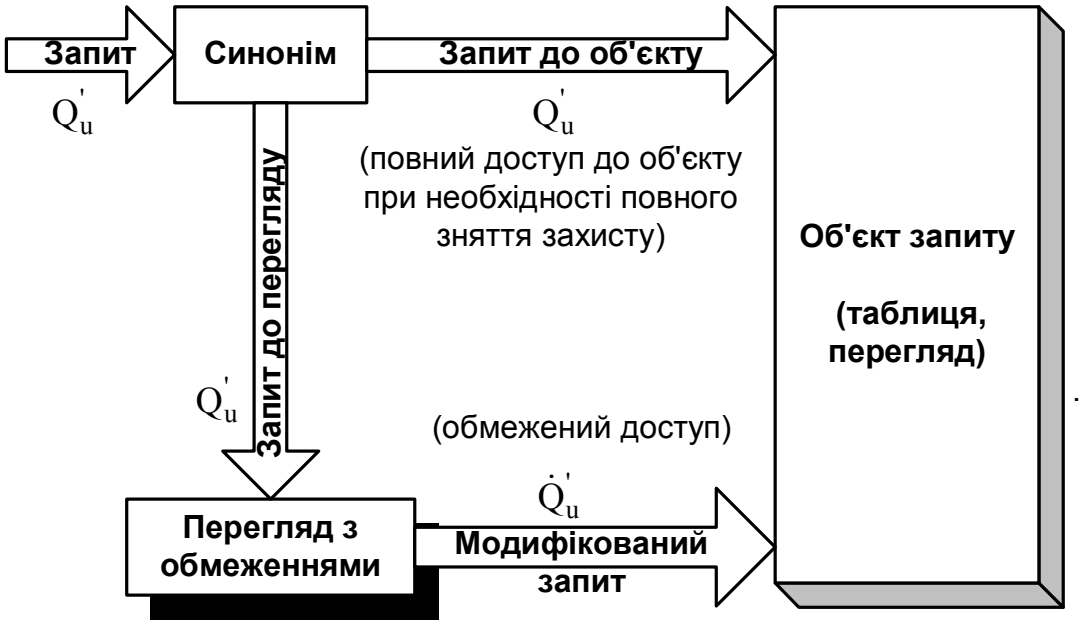

Рис. 3. Модифікація SQL запитів.

Модифікація запитів виду $\dot{Q}_u'$ дозволяє обмежити доступ не лише для операцій проекції (читання), а і для операцій введення, зміни та видалення даних. При операціях введення та зміни можливі фантоми – залежно від контролю даних, які вводяться.

Модифікація запитів виду $\ddot{Q}_u'$ дозволяє обмежити доступ для операцій проекції (читання), та, залежно від умов, дозволяє виконувати операції введення, зміни та видалення даних з обмеженням доступу до користувачів. Можливість виконувати операції введення, зміни та видалення даних з використанням переглядів залежить не лише від умов та функцій, які використовуються у запиті перегляду, а і від особливостей роботи СКБД, зокрема, транслятора запитів.

Модифікація запитів виду $\ddot{Q}_u'$ дозволяє обмежити доступ для операцій проекції (читання), та, в загальному випадку, не дозволяє виконувати операції введення, зміни та видалення даних.

Розроблено методи модифікації SQL запитів відповідно до правил $MOD_{Rule}^{Q,u}$.

Іншим методом обмеження доступу користувачів до окремих кортежів відношення R згідно з правилом RULE(u) є розділення відношення на кілька відношень.

$G_i = \left\{ s_j^i \in S \right\}, (i = \overline{1,n})$ - користувачі, які згідно з правилом RULE(u) мають доступ для здійснення операцій F_i до одних та тих самих кортежів $r_{U_i} = \langle a_1, ..., a_n \rangle \in r$.

Результатом розділення відношення $r = \{\langle a_1,...,a_n \rangle\}$ є множина відношень $\{r_i' = \{\tau_{G_i}\}\}$. Кожній групі користувачів G_i надають повноваження на здійснення операцій F_i з відповідним відношенням r_i'.

Описаний механізм розділення таблиці, є, фактично, статичним аналогом модифікації SQL запитів.

Досліджена задача надання дезінформації. Необхідність надання дезінформації користувачам БД виникає, як правило, після аналізу спроби НСД до об'єктів БД. Такий аналіз повинен показати напрям інтересів зловмисника та необхідні для реалізації НСД об'єкти БД.

Головними вимогами до механізмів надання дезінформації є:

1) швидкість реалізації (вмикання),
2) контрольованість (відомо, яка саме інформація/дезінформація передається, можливість тимчасового призупинення та вибіркове надання дезінформації),
3) непомітність для зловмисника.

Найефективнішим механізмом дезінформування є використання модифікації SQL запитів виду (16). Модифікації SQL запитів виду (16) дозволяє реалізувати правила утворення та надання дезінформації будь-якого рівня складності, робити це "на льоту" чи з використанням попередньо створених спеціальних масивів даних. Налаштування механізму за допомогою розробленого алгоритму, відбувається для користувача, групи користувачів, таблиць БД, переглядів, залежно або незалежно від часу запиту, терміналу тощо.

Для обмеження доступних користувачу ресурсів (створення та контролю **квот**) використовуються:

- обмеження на профайли користувачів;
- модифіковані SQL запити.

Обмеження на профайли користувачів використовуються для контролю за використанням ресурсів на фізичному рівні: кількість отриманої користувачам інформації (байтів за сесію, операцій введення/виведення тощо); розмір зайнятих користувачем областей пам'яті (буфер, об'єм табличного простору тощо); тривалість сесії, тривалість опрацювання запиту тощо.

Модифіковані SQL запити дозволяють реалізувати обмеження логічного рівня. Для цього у конструкцію WHERE додається умова "rownum<*x*", де *x* – максимальна кількість записів, яку зможе отримати користувач після кожного виконання запиту. У загальному випадку, кожен раз запит повертає не обов'язково однакові записи та не обов'язково у однаковому порядку.

Далі, у розділі, наведено умови доцільності використання СЗІ, запропонована методика впровадження ББД, досліджено питання захисту серверів БД при роботі у мережі та запропоновано методику використання БД як ядра системи безпеки підприємства (зокрема, СЗІ комплексної ІС).

<u>У четвертому розділі</u> дисертаційної роботи описано інформаційну систему “Гермес”, при проектуванні та розробці системи захисту інформації якої було використано теоретичні результати дисертаційних досліджень.

Зокрема, використовується елемент математичної моделі ББД - користувач ББД. Користувач ББД є користувачем СКБД, інформацією про якого внесено у список користувачів ББД із зазначенням місця у ієрархії підрозділів ББД. При зміні посади, підпорядкування підрозділів тощо відбувається автоматична зміна прав доступу. Для реалізації обмежень доступу використовуються ролі (role), перегляди даних (view), синоніми (synonym) та знімки даних (snap shot).

Механізми примусового керування доступом ІС “Гермес” ґрунтуються на узагальнених мітках безпеки. Залежно від потреб, таблиці атому захисту містять 1-3 додаткових атрибути для збереження $\hat{l}$. Мітки безпеки використовуються лише для вибраних таблиць БД. Кількість таблиць, які потребують примусового керування доступом, для задач ІС “Гермес” складає до 10% від загальної, що дозволяє зменшити затрати пам’яті та обчислювальних ресурсів порівняно з MRDB системами.

Для аудиту дій користувачів, розроблена СЗІ використовує інформацію, розміщену у атомах захисту, та журнали СКБД.

Використання у ІС “Гермес” запропонованої у дисертації моделі ББД дозволило реалізувати задачі експедиторського обліку зі збереженням значної кількості даних та забезпеченням їх цілісності, конфіденційності та аудиту.

Використання моделі ББД для реалізації ІС “Гермес” покращило захищеність даних (рис. 4.).

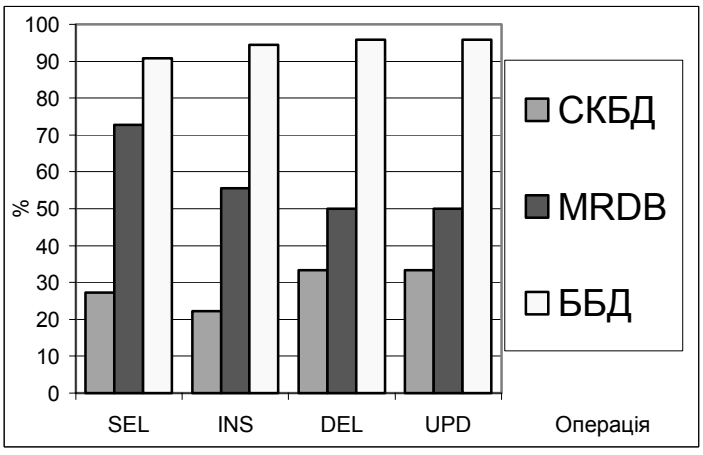

Рис. 4. Порівняння ефективності моделей СЗІ в розрізі операцій з БД.

На рис. 4 наведено співвідношення загроз від операцій з БД, заблокованих засобами: системи захисту інформації реляційної СКБД, MRDB, ББД, яка розроблена на основі запропонованих у роботі математичних моделей.

Порівняння ефективності реалізації методів блокування головних загроз засобами СЗІ СКБД і розробленою моделлю ББД та критичність загроз наведено на рис. 5.

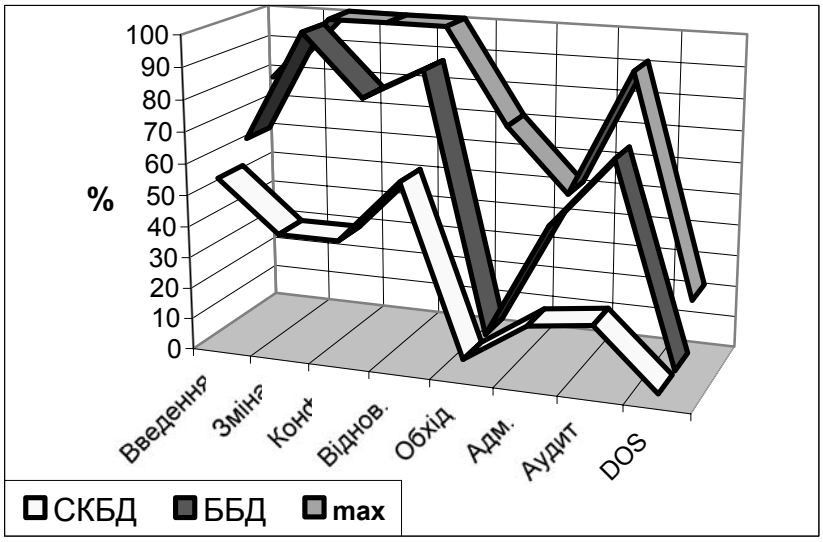

Рис. 5. Порівняння СЗІ СКБД та ББД.

Досліджено особливості адміністрування СЗІ ІС “Гермес”, виконаної з використанням СКБД ORACLE, засобів розробки ORACLE Developer/2000 та CASE засобу ORACLE Designer/2000.

У додатках наведено сценарії та програмні коди інформаційної системи “Гермес”, акти впроваджень результатів дисертаційних досліджень.

ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ.

Дисертантом отримано наступні основні результати.

- Введено поняття безпечної БД та визначено вимоги до математичної моделі безпечної БД з врахуванням потреб у статистичному захисті інформації, квотах інформації, аудиті та забезпеченні історичності даних.
- Розроблено математичну модель комплексної системи захисту інформації реляційної БД для статистичного захисту інформації, захисту від порушення конфіденційності шляхом отримання великих об’ємів інформації, детальному аудиті створення та змін даних, реалізації примусового та довільного керування доступом, забезпечення цілісності даних.
- Запропоновано нову математичну модель об’єкту захисту у реляційних БД. Ця математична модель використовується для проектування схеми ББД, реалізації комплексної системи захисту інформації реляційної БД.
- Для математичної моделі ББД введено новий обмежений набір операцій доступу до даних.
- Визначено методи реалізації математичної моделі ББД засобами реляційної моделі. Розроблено методи та алгоритми для реалізації математичної моделі комплексної системи захисту інформації реляційної БД з використанням стандартних засобів промислових СКБД, у тому числі, розроблено методи та алгоритми для реалізації удосконаленої моделі авторизації користувачів, удосконаленої моделі аудиту дій користувачів реляційних БД.

- Розроблено систему захисту інформації фінансово-економічної інформаційної системи “Гермес”, яка на практиці відображає результати теоретичних дисертаційних досліджень.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Нікольський Ю.В., Пасічник В.В., Тарасов Д.О. *Концепція інформаційної системи “Реєстр власників іменних цінних паперів”* // Вісник ДУ “Львівська політехніка” №315. – Львів, 1997. - с.153-168.
2. Тарасов Д.О. *Автоматизація операцій обліку іменних цінних паперів* // Вісник ДУ “Львівська політехніка” №330. – Львів, 1998. - с. 225-240.
3. Тарасов Д.О. *Засоби забезпечення цілісності даних на основі промислових стандартів* // Задачі та методи прикладної математики. Вісник Львівського університету ім. І. Франка. Випуск 50. – Львів, 1998. - с.194-196.
4. Тарасов Д.О. *Забезпечення цілісності даних у реляційних структурах* // Інформаційні системи та мережі. Вісник ДУ “Львівська політехніка” №383. - Львів 1999.- с. 213-226.
5. Тарасов Д.О. *Обмеження доступу з мережі до БД* // Вісник Львівського університету. Серія прикладна математика та інформатика. 1999. Випуск 1. - с. 213-216.
6. Катренко А.В., Тарасов Д.О. *Безпека систем управління розподіленими інформаційними ресурсами* // Защита информации, зб. наук. пр. КМУГА. - Київ, 1999. - с. 165-170.
7. Тарасов Д.О. *Основні задачі захисту баз даних* // Інформаційні системи та мережі. Вісник НУ “Львівська політехніка” №406. - Львів 2000. - с. 216-221.
8. Тарасов Д.О. *Аудит баз даних* // Защита информации: Сборник научных трудов. – Киев: КМУГА, 2000. - с. 136-140.
9. Катренко А.В., Тарасов Д.О. *Слабкі ланки захисту інформації в інформаційних системах* // Науково-технічний журнал “Захист інформації”. №3, 2000. - с. 58-63.
10. Тарасов Д.О. *Специфічні для СУБД, загрози захисту інформації* // Защита информации: Сборник научных трудов. – Киев: НАУ, 2001. - с. 53-60.
11. Кісь Я., Тарасов Д. *Застосування комп’ютерних інформаційних технологій для планування діяльності підприємств* // Комп’ютерна інженерія та інформаційні технології. Вісник НУ “Львівська політехніка” №433. - Львів, 2001. - с. 56-63.
12. Тарасов Д.О., Пелещищин А.М., Жежнич П.І. *Обмежений набір операцій для роботи з базами даних* // Інформаційні системи та мережі. Вісник НУ “Львівська політехніка” №438. – Львів, 2001. - с. 125-131.

АНОТАЦІЇ

Тарасов Д.О. Моделювання системи захисту інформації у реляційних базах даних. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – “Математичне моделювання та обчислювальні методи”. – Національний університет “Львівська політехніка”, 2002.

У дисертації досліджуються питання математичного моделювання системи захисту інформації реляційних баз даних. Сформульовано

концептуальне визначення безпечної бази даних, побудована математична модель системи захисту інформації безпечної бази даних. Запропонована модель дозволяє розв'язати спеціальні задачі захисту інформації реляційних баз даних: забезпечення авторизації та аудиту з деталізацією до рівня кортежів та атрибутів, статистичний захист інформації, захист від отримання надлишкової інформації. Досліджено операції доступу до інформації у реляційних базах даних. Запропоновано методи та алгоритми для реалізації обмеженого набору операцій доступу до даних з метою забезпечення підвищеного рівня конфіденційності, цілісності та аудиту. Запропоновано методи адаптації схеми бази даних для забезпечення цілісності шляхом реалізації безпечної бази даних.

Ключові слова: математичне моделювання, реляційні бази даних, захист інформації, системи керування базами даних, авторизація, SQL.

Тарасов Д.А. Моделирование системы защиты информации в реляционных базах данных. – Рукопись.

Диссертация на соискание научной степени кандидата технических наук по специальности 01.05.02 – "Математическое моделирование и вычислительные методы". – Национальный университет "Львовская политехника", 2002.

В диссертации исследуются вопросы метематического моделирования системы защиты информации в реляционных базах данных. Сформулировано концептуальное определение безопасной базы данных, построена математическая модель системы защиты информации безопасной базы данных. Предложенная модель позволяет решать специальные задачи защиты информации баз данных: обеспечение авторизации и аудита с детализацией до уровня кортежей и атрибутов, статистическая защита информации, защита от получения избыточной информации. Проведено исследование операций доступа к информации в реляционных базах данных. Предложено методы и алгоритмы для реализации ограниченного набора операций доступа к данным с целью обеспечения повышенного уровня конфиденциальности, целостности и аудита. Предложено методы адаптации схемы базы данных для обеспечения целостности путем реализации безопасной базы данных.

Ключевые слова: математическое моделирование, реляционные базы данных, защита информации, системы управления базами данных, авторизация, SQL.

Tarasov D.O. Modeling of the information protection system of relational databases. – Manuscript.

Thesis for a Ph.D. science degree by specialty 01.05.02 – "Mathematical modeling and calculating methods". – National university "Lvivska Polytechnika", Lviv, 2002.

In the thesis a question of mathematical modeling of the information protection system in relational databases is investigated. Conceptual definition of the safe database is formulated, the resulted requirements to security of databases are presented. The mathematical model of the information protection system of a safe database is constructed. The suggested model allows to solve special tasks of the information protection in relational databases: maintenance of authorization and audit with detailed elaboration to a level of trains and attributes.

In the Chapter 1 the review of references is resulted in the field of the information protection in information systems on the basis of DB servers, models DB information protection system and kinds of threats of the information in IS are considered on the basis of DB servers. It is considered to a task of maintenance of the information integrity, availability and confidentiality in the context of relational DB. The lacks of models analyzed IPS and concepts of the generalized label of safety entered.

In the Chapter 2 conceptual and mathematical model of a safe DB are considered. It is offered to solve to a task of the information protection by adding to system of the information protection of a DB by a line of objects (tables, views, roles, procedures, etc.) and rules. These objects are a protective layer (intermediate level) between a DB objects and actions of a DB users which are missed by restrictions DBMS. Concepts of electronic document and atom of the information protection relational DB are entered. There are considered operations with objects of a safe DB, threat of the information protection which arise at use of updating data operations, methods of the resulted threats blocking. Uses of the limited set of operations for access to DB are offered. The technique of the limited set of operations use and designing of the circuit of DB is suggested with maintenance of job safe DB with the limited set of operations. The limited set of operations functional completeness at observance of designing rules of circuit safe DB is shown.

In the Chapter 3 means of safe DB model realization, with the help of standard means industrial DBMS are considered. Realization methods and algorithms of access restrictions are offered. In particular, the mechanism of access restriction with the usage of modified SQL queries are offered. The analysis and classification of methods of searches updating. The automated updating algorithms of the basic kinds searches are formulated. It is resulted in recommendations on re-designing DB circuits for realization of a safe DB.

In the Chapter 4 of thesis information system "Hermes" is described, at designing and system engineering of which the information protection theoretical results of dissertational researches have been used. Features of administration information protection system of IS "Hermes" were executed with use DBMS ORACLE and means of development ORACLE Developer/2000 and CASE means of ORACLE Designer/2000 are investigated.

Keywords: mathematical modeling, relational database, information protection, database management system, authorization, SQL.

Підписано до друку 12.02.2003 р. Формат 60*90/16.
Папір офсетний. Друк на різографі. Умовн. друк. арк. 0,9.
Тираж 100 примірників. Безкоштовно.

Надруковано у Національному університеті “Львівська політехніка”
79013, м.Львів, вул., С.Бандери, 12