гические основы нарушений мышления при афазии. – М.: Наука, 1996. – 230 с. 3. Брагина Н.Н., Доброхотова Т.А. Функциональные асимметрии человека. – М: Медицина, 1981. – 287 с. 4. Харламов А.А., Ермаков А.Е., Кузнецов Д.М. Технология обработки текстовой информации с опорой на семантическое представление на основе иерархических структур из динамических нейронных сетей, управляемых механизмом внимания // Информационные технологии. – 1998. – № 2. – С. 26–32. 5. Орлова Л.В. Структура сверхфразового единства в научных текстах. – К.: Наукова думка, 1998. – 154 с. 6. Ахутина Т.В. Порождение речи. Нейролингвистический анализ синтаксиса. – М.: МГУ, 1989. – 215 с.

УДК 681.3

Д.О. Тарасов
Національний університет “Львівська політехніка”,
кафедра “Інформаційні системи та мережі”

ФОРМАЛЬНІ МОДЕЛІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ РЕЛЯЦІЙНИХ БАЗ ДАНИХ

© *Тарасов Д.О., 2003*

This paper describes the formal models of relational databases information protection system. We propose new formal model of relational databases information protection system.

Розглянуто формальні моделі систем захисту інформації реляційних баз даних та методи їх реалізації. Запропоновано нову формальну модель захисту інформації реляційної БД.

1. ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ

Використання технологій баз даних дозволяє ефективно та швидко аналізувати інформацію, формалізувати процес проектування інформаційних систем (ІС), швидко опрацьовувати великі об’єми інформації. Для найбільш розповсюджених баз даних – реляційних баз даних (БД) створено стандартизований інструментарій систем управління базами даних (СУБД) [1].

Питанням захисту інформації БД, засобам захисту інформації СУБД постійно приділяється увага [1, 3, 4, 6–8, 10]. Це зумовлено інформацією про знайдені недоліки захисту СУБД, появою нових методів аналізу інформації, винекненням нових задач захисту інформації. Для вирішення проблеми захисту інформації у БД необхідний комплексний підхід, який базується на формальних моделях системи захисту інформації (СЗІ) [12–14].

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ

У дослідженнях СЗІ БД розглядають такі аспекти захисту:

- механізми транзакцій;
- забезпечення цілісності реляційних БД;
- принципи побудови та використання БД з примусовим контролем доступу (mandatory access control, MAC);

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

- БД з довільним контролем доступу (discretionary access control, DAC);
- практичне втілення теоретичних наробок у галузі захисту інформації у СУБД, промислові стандарти (SQL);
- надійність СУБД.

Додаткові питання захисту БД розглядаються у роботах:

- захист об'єктно-реляційних та дедуктивних БД [13, 16];
- статистичний та контекстно-залежний захист [2, 9].

Найбільш поширеними з використаних формальних моделей СЗІ є:

- серед фінансово-економічних ІС – модель довільного керування доступом [1, 12];
- серед ІС з додатковими вимогами до захисту – модель довільного керування доступом, модель примусового керування доступом, інші [15, 16].

2.1. Модель довільного керування доступом

Довільне керування доступом (Discretionary Access Control, DAC) – це метод обмеження доступу до об'єктів, що ґрунтується на обліку особи суб'єкта чи групи, у яку входить суб'єкт.

Під об'єктом захисту (об'єктом) розуміють будь-який елемент, здатний зберігати дані. *O* – множина усіх об'єктів захисту БД

$$O = \left\{ o_i, i = \overline{1, k_O} \right\}, k_O \in N \text{ .} \tag{2.1}$$

Як об'єкти захисту у реляційних БД розглядають множини значень доменів, значення атрибутів, значення кортежів даних, набори кортежів, відношення. У СУБД відношення реалізуються за допомогою таблиць (table) та переглядів (view). Отже, до об'єктів захисту належать таблиці і перегляди.

Множина *O* не містить службові об'єкти СУБД, які не використовуються у реляційній моделі, але самі можуть бути описані та зберігаються за допомогою об'єктів реляційної БД та потрібні для розширення функцій СУБД. До службових об'єктів належать послідовності, семафори, процедури, функції, тригери, правила цілісності тощо. Перелік та характеристики службових об'єктів залежать від версії конкретної СУБД.

Створення та адміністрування службових об'єктів є задачею адміністратора БД. Відповідно користувачі БД не повинні мати повноважень на створення, знищення, зміну та визначення характеристик та вихідних кодів як згаданих службових об'єктів, так і кодів переглядів даних та синонімів, ролей тощо.

S – множина суб'єктів (користувачів БД, процесів, які діють від імені певного користувача)

$$S = \left\{ s_i, i = \overline{1, k_S} \right\}, k_S \in N \text{ .} \tag{2.2}$$

Користувач – це ініціатор команд (людина, автоматизована система, сервіс автоматизованої системи тощо), який успішно пройшов процедури ідентифікації та аутентифікації та не отримав адміністративні права для роботи з БД.

Під адміністративними правами розуміємо привілеї виду SELECT ALL (читати з будь-якої таблиці, перегляду), UPDATE ALL (робити оновлення кортежів будь-якої таблиці), DROP ANY (знищити будь-яку таблицю, перегляд) тощо.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Для запобігання порушення безпеки з боку користувачів, які мають адміністративні права для керування всією БД (адміністратор БД, адміністратор безпеки тощо), необхідно виконувати цілий ряд запобіжних організаційних та технічних заходів, детальний розгляд яких виходить за межі даної роботи.

$$G = \left\{ g_i \subseteq S, i = \overline{1, k_G} \right\}, k_G \in N$$

– множина груп суб'єктів.

Множина можливих операцій з об'єктами

$$F = \left\{ f_i, i = \overline{1, k_F} \right\}, k_F \in N \text{ .} \tag{2.3}$$

Основними операціями з об'єктами БД є введення даних, перегляд даних, зміна даних, знищення даних.

Довільність керування полягає в тому, що деяка особа (зазвичай власник об'єкта) може на власний розсуд давати іншим суб'єктам чи відбирати в них права доступу до об'єкта. Отже, права доступу при довільному управлінні доступом описується матрицею **M** (матрична модель доступу, access matrix model), у рядках якої перераховані суб'єкти, а в стовпцях – об'єкти.

У комірках, розташованих на перетині рядків і стовпців, фіксуються способи доступу, дозволені для суб'єкта стосовно об'єкта, наприклад: читання, запис, виконання, можливість передачі прав іншим суб'єктам тощо. Інший варіант представлення – куб **M** , на осях якого позначаються суб'єкти, об'єкти та операції

$$\text{DAC} : S \times O \times F \to \mathbf{M} \text{ .} \tag{2.4}$$

Для реалізації матричної моделі доступу СУБД використовують поняття привілеїв, ролей (SQL privileges, Role-Based Access Control) для додаткової деталізації об'єктів БД (таблиць, переглядів) використовують проекцію відношень (перегляди, database views).

2.2. Модель примусового керування доступом

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

$$L = \left\{ l_i, i = \overline{1, k_L} \right\}, k_L \in N \text{ .} \tag{2.5}$$

Відображення $Lab_s : S \to L$ ставить множині суб'єктів у відповідність множину міток безпеки. Відображення $Lab_o : O \to L$ ставить множині об'єктів у відповідність множину міток безпеки.

Мітка об'єкта описує ступінь закритості (конфіденційності) інформації, що міститься в об'єкті, мітка суб'єкта – максимальний рівень конфіденційності даних, доступних суб'єкту.

Визначимо бінарні відношення строгого домінування $\prec$ та еквівалентності = на множині L.

Семантика $\prec$ – якщо $l_i \prec l_j$ (тобто мітка l_j домінує над l_i), то суб'єкти з міткою l_i не мають доступу до об'єктів з міткою l_j, суб'єкти з міткою l_j мають доступ до об'єктів з міткою l_i.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Семантика = – якщо $l_i=l_j$ (тобто мітка l_j еквівалентна l_i), то суб'єкти з міткою l_i мають доступ до об'єктів з міткою l_j.

Надалі для зручності використовується також відношення не строгого домінування $\preceq$:

$$l_i \preceq l_j \Rightarrow \left\{\left(l_i \prec l_j\right) \vee \left(l_i = l_j\right)\right\}. \quad (2.6)$$

Таке відношення є антисиметричним та не обов'язково лінійним (зв'язним).

2.2.1. Модель Bell-LaPadula

Одна з перших математичних моделей безпеки БД, модель Bell-LaPadula використовує наведене вище відношення $\preceq$ та визначає такі правила доступу.

1. Просте правило безпеки. Суб'єкту дозволено отримувати (читати) кортежі (дані) тільки, якщо рівень позначки безпеки (конфіденційності) суб'єкта дорівнює або більший, ніж рівень позначки безпеки об'єкта доступу $l_o \preceq l_s$.

2. * – правило. Суб'єкту дозволено писати (змінювати) кортежі (дані) тільки, якщо рівень позначки безпеки (конфіденційності) суб'єкта дорівнює або менший, ніж рівень позначки безпеки об'єкта доступу $l_s \preceq l_o$.

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 $\mathrm{Bot}: L \to L,\ \ \mathrm{Bot}(l) = \left\{l_j \in L : l_j \preceq l\right\}$ визначає множину міток безпеки, над якими домінує l.

Відображення $\perp: L \to L,\ \ \perp(l) = \left\{l_j \in \mathrm{Bot}(l) : \forall l_i \in \mathrm{Bot}(l), l_j \preceq l_i\right\}$ визначає множину міток безпеки нижчого рівня.

Модель Bell-LaPadula не накладає явних обмежень на множину L та відношення $\prec$, =, $\preceq$, але у практичних реалізаціях використовуються (усі чи деякі) такі обмеження на $\preceq$:

$$\left(\forall l_i, l_j, l \in L : l_i \preceq l, l \preceq l_j\right)\left\{\perp(l) \preceq l_i \preceq l_j \preceq \top(l)\right\}, \quad (2.7)$$

$$\left(\forall l_i, l_j \in L\right)\left(\exists! \perp\right)\left(\exists! \top\right)\left\{\perp\left(l_i\right) = \perp\left(l_j\right) \wedge \top\left(l_i\right) = \top\left(l_j\right)\right\}. \quad (2.8)$$

2.2.2. Модель Діона

Модель Діона забезпечує реалізацію політики безпеки (контроль доступу) за допомогою рівнів конфіденційності та цілісності інформації. З об'єктами та суб'єктами заставляються мітки:

- мітки рівня конфіденційності (абсолютна – ACL, читання – RCL, запису – WCL);
- мітки рівня цілісності (абсолютна – AIL, читання – RIL, запису – WIL);

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

На множинах мітки визначені відношенням домінування міток $\preceq$. Встановлені співвідношення між позначками об'єктів та суб'єктів, виконання яких забезпечує збереження конфіденційності та цілісності даних, які зберігаються та передаються між суб'єктами та об'єктами.

Модель Діона узагальнює відоміші моделі безпеки (Bell-LaPadula і Biba). Вона, як і модель Bell-LaPadula, передбачає можливість передавання інформації шляхом організації односпрямованих каналів між об'єктами.

2.2.3. Модель MRDB з категоріями у складі міток безпеки

У деяких реалізаціях MRDB мітки безпеки складаються з двох частин: рівня конфіденційності l і списку категорій $\Phi^1=\left\{\phi_k^1\right\}$. Рівні конфіденційності, які підтримуються СУБД, утворюють впорядковану множину (відношення $\prec$).

Категорії утворюють невпорядковану множину. Категорія – незалежний від рівня конфіденційності критерій обмеження доступу, їх призначення – описати предметну область, до якої належать дані. Наприклад, категорія може містити {"кадри", "фінанси"}. У деяких реалізаціях (СУБД INGRES) категорії доповнені областями $\Phi^2=\left\{\phi_k^2\right\}$, утворюючи три критерії обмеження доступу $\hat{l}=\left\langle l,\Phi^1,\Phi^2\right\rangle$.

Для задач захисту інформації, які потребують кількох міток (як у моделі Діона) та кількох категорій (областей), введемо поняття узагальненої мітки безпеки. Узагальнена мітка безпеки має вигляд

$$\hat{l}=\left\langle l^1,...,l^n,\Phi^1,...,\Phi^m\right\rangle\in\hat{L}, \tag{2.9}$$

де $l^i\in L$, $\Phi^j=\left\{\phi_k^j\right\}$, $n,m,k\in\square$.

Оскільки на відношення $\prec$ на L не накладаються додаткові умови (лінійність, зв'язність тощо), то використання спільної множини L для визначення l^i не зменшує загальності узагальненої мітки безпеки.

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

$$\hat{l}_1\lhd\hat{l}_2:\left(l_1^i\prec l_2^i,\Phi_1^j\subset\Phi_2^j,i=\overline{1,n},j=\overline{1,m}\right). \tag{2.10}$$

Тобто, рівень безпеки l_2 строго більший, ніж у l_1, та набір категорій $\hat{l}_1$ є власною підмножиною набору категорій $\hat{l}_2$.

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

$$\hat{l}_1\trianglelefteq\hat{l}_2:\left(l_1^i\preceq l_2^i,\Phi_1^j\subseteq\Phi_2^j,i=\overline{1,n},j=\overline{1,m}\right). \tag{2.11}$$

Доступ до об'єкта визначається такими 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 $\hat{l}_s\trianglelefteq\hat{l}_o$.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

3.ФОРМУВАННЯ ЦІЛЕЙ

При використанні СУБД з моделлю MRDB виникає ряд проблем:

- ієрархія рівнів доступу спеціалізованих СУБД не є розгалуженою, що не відображає особливості розподілу повноважень відповідно до функціональних обов'язків;
- класичні механізми забезпечення багатоверсійності є надлишковими для ІС фінансово-економічного характеру та є додатковим навантаженням на обчислювальні ресурси;
- сфера використання спеціалізованих СУБД обмежується також недоступністю відповідного програмного забезпечення на ринку України (велика вартість та заборона експорту).

Ведеться робота над СУБД, яка обмежує доступ до окремих записів таблиць шляхом модифікації SQL запитів користувачів. Дані продукти фактично доповнюють SQL запити нескладними додатковими обмеженнями, лише частково реалізують механізм, подібний на категорії міток безпеки.

На практиці засобами промислових СУБД неможливо повністю реалізувати такі задачі захисту БД, як:

- забезпечення конфіденційності (у тому числі статистичний захист);
- забезпечення цілісності інформації (у тому числі контекстно залежний захист);
- аудит.

Адміністрування СУБД проводиться окремо від адміністрування політики безпеки ІС, що створює додаткові труднощі.

Для покращання захищеності БД необхідно використати формальну модель СЗІ БД, реалізація якої дозволяє виправити вказані недоліки існуючих моделей. Цю модель названо безпечною базою даних (ББД).

4. ОСНОВНИЙ МАТЕРІАЛ

4.1. Модель СЗІ реляційних СУБД

Математична модель СЗІ реляційних СУБД має вигляд

$$SM^{\mathrm{R}} = \left\langle O^{\mathrm{R}}, S, G, \Omega^{\mathrm{R}}, \Sigma, S_{DB}, D_{DB}, \mathrm{DOM}, \mathbf{M}, Autor^{\mathrm{R}} \right\rangle, \qquad (4.1)$$

де об'єкти захисту $r_i \in O^{\mathrm{R}}$ – відношення, результати застосування операцій проекції, вибірки і об'єднання відношень та їх подання у вигляді переглядів даних; S, G – множини суб'єктів та груп суб'єктів (користувачів); $\Omega^{\mathrm{R}} = \{SEL, INS, DEL, UPD\}$ – операції з $r_i \in O^{\mathrm{R}}$, де оператори вибірки даних $SEL_p(r_1, r_2, ..., r_m)$, додавання кортежів у відношення $INS_p(r_1, r_2)$, знищення кортежів $DEL_p(r)$ та зміна значень атрибутів кортежів $UPD_p(r)$ реалізуються шляхом застосування до $r_i \in O^{\mathrm{R}}$ суперпозиції операторів реляційної алгебри $\delta_p, \Pi_X, \times, *, -, \cup$. Для визначення умов виконання операцій використовуються предикати $\{p_j\}$; Σ – множина залежностей між атрибутами. Σ разом зі $S_{DB}, D_{DB}, \mathrm{DOM}$ визначає правила цілісності

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

відношень, атрибутів, первинних та зовнішніх ключів; $\mathbf{M}=\left(m_{ijk}\right)$ визначає права доступу користувача s_i на виконання операцій ω_k з об'єктом o_j

$$m_{ijk}=\begin{cases}1, & \text{якщо доступ дозволено,}\\ 0, & \text{якщо доступ заборонено.}\end{cases} \tag{4.2}$$

$Autor^{\mathrm{R}}: O^{\mathrm{R}} \to \{\langle s, time, \mathrm{sysinfo}\rangle\}$ – функція аудиту SM^{R}.

Промислові реляційні СУБД містять додаткові засоби захисту, які здійснюють операції та використовують критерії, не передбачені реляційною моделлю даних. Узагальнена модель СЗІ промислових реляційних СУБД має вигляд

$$SM^{\mathrm{R}^*}=\left\langle SM^{\mathrm{R}}, SR, QTYR, RESR, TR\right\rangle, \tag{4.3}$$

де $SR=\{\langle o,\omega,act\rangle\}$ – додаткові (процедурні) правила захисту. Реалізуються за допомогою тригерів БД та інших програмних засобів для опису прикладної логіки. Правила *SR* визначають необхідність виконання програмного коду *act* у випадку доступу до об'єкта БД $o\in O$ на виконання операції $\omega\in\Omega^{\mathrm{R}}_{SR}=\Omega^{\mathrm{R}}-\{SEL\}$; *QTYR* – обмеження кількості інформації (кортежів) у результатах виконання команд *SEL*; *RESR* – обмеження кількості ресурсів системи (часу процесора, об'ємів пам'яті тощо), використаних під час виконання команд користувача; *TR* – засоби забезпечення цілісності БД у випадку збоїв обладнання, при паралельному доступі до даних, роботі розподілених БД (механізми транзакцій та розподілених обчислень).

4.2. Модель СЗІ MRDB

Реалізація MRDB базується на доповненні наявної схеми БД додатковим атрибутом L для збереження міток безпеки або їх аналогів. Цей варіант фактично змінює реляційну БД на MRDB.

Існує ряд спеціалізованих СУБД (наприклад, Trusted ORACLE, INGRES/Enhanced Security), які використовують багаторівневу систему захисту (multilevel), моделі примусового контролю доступу. Реалізація цієї моделі дозволяє обмежити доступ до окремих записів (полів записів) на основі ієрархії класів доступу.

СУБД з багаторівневою системою захисту дозволяють реалізувати багатоверсійність даних. Користувачі отримують "версії" документів залежно від рівня доступу.

Загально прийнята багаторівнева реляційна модель з мітками рівню кортежів (MRDB) має наступний вигляд.

Визначено множину L з відношенням домінування $\preceq$.

Існують і єдині $\top=\top(l)$ – верхній (домінуючий) та $\bot=\bot(l)$ – нижній елементи L.

Схемою багаторівневого відношення r^{L} є

$$S^{\mathrm{L}}_R=\langle R[U_R], L\rangle=\left\langle A^{\mathrm{R}}_1,\ldots,A^{\mathrm{R}}_{n_R}, L\right\rangle. \tag{4.4}$$

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Відношення $r_i^{\mathrm{L}} = \left\{ \tau^{\mathrm{L}}{}_j^{\,i} \right\}$ – множина кортежів вигляду

$$\tau^{\mathrm{L}}{}_j^{\,i} = \left\langle a_1^i, a_2^i, \ldots, a_{\mathrm{n_i}}^i, l \right\rangle,$$

де $a_j^i \in A_j^{R_i}$, $l \in L$.

БД db^{L} зі схемою S_{DB}^{L} це $db^{\mathrm{L}} = \left\{ r_i^{\mathrm{L}} \right\}$, $1 \le i \le n$.

$$L_{l_1}^{l_2} = \mathrm{Top}(l_1) \bigcap \mathrm{Bot}(l_2). \tag{4.5}$$

$$\left(r_i^{\mathrm{L}} \right)_{l_1}^{l_2} = \left\{ \tau^{\mathrm{L}} = \left\langle a_1^i, a_2^i, \ldots, a_{\mathrm{n_i}}^i, l \right\rangle \in r_i^{\mathrm{L}} : l \in L_{l_1}^{l_2} \right\}. \tag{4.6}$$

$$\left(db^{\mathrm{L}} \right)_{l_1}^{l_2} = \left\{ \left(r_i^{\mathrm{L}} \right)_{l_1}^{l_2} \right\}, \quad 1 \le i \le n. \tag{4.7}$$

Позначимо $r_i^{\mathrm{L}} \left| l = \left(r_i^{\mathrm{L}} \right)_l^l \right.$ однорівневе відношення, однорівнева БД $db_i^{\mathrm{L}} \left| l = \left(db_i^{\mathrm{L}} \right)_l^l \right.$.

Математична модель СЗІ MRDB має вигляд

$$SM^{\mathrm{L}} = \left\langle O^{\mathrm{L}}, S, L, \preceq, Lab_{\mathrm{S}}, \Omega^{\mathrm{R}} \right\rangle, \tag{4.8}$$

де користувачі *S*, над об'єктами захисту $O^{\mathrm{L}} = \left\{ r_i^{\mathrm{L}} \left| l : l \in L, r_i^{\mathrm{L}} \in db^{\mathrm{L}} \right. \right\}$, як над звичайними відношеннями, здійснюють операції з множини Ω^{R}.

Запропоноване вище визначення O^{L} реалізує функцію Lab_{O} та дозволяє побудувати модель SM^{L} з використанням операцій SM^{R}.

Введемо позначення $O_{\omega_i, s_j}^{\mathrm{L}}$ – множина об'єктів $o^{\mathrm{L}} \in O^{\mathrm{L}}$, доступних користувачу s_j для виконання операції ω_i.

При реалізації у MRDB правил моделі Bell-LaPadula отримуємо:

$$O_{SEL, s_j}^{\mathrm{L}} = \left(db^{\mathrm{L}} \right)_{\perp}^{Lab_{\mathrm{S}}(s_j)}, \tag{4.9}$$

$$O_{UPD, s_j}^{\mathrm{L}} = db^{\mathrm{L}} \left| Lab_{\mathrm{S}}(s_j) \right.. \tag{4.10}$$

Оскільки окреме відношення у MRDB не має загальної мітки безпеки, приймемо такі правила.

1. Кортежі, створені користувачем s_i, мають мітку $l = Lab_{\mathrm{S}}(s_j)$.
2. $O_{INS, s_j}^{\mathrm{L}} = db^{\mathrm{L}}$.
3. $O_{DEL, s_j}^{\mathrm{L}} = db^{\mathrm{L}} \left| Lab_{\mathrm{S}}(s_j) \right.$.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Спеціалізовані СУБД використовують комбіновану математичну модель СЗІ БД, яка містить елементи моделей SM^{R} та SM^{L}:

$$SM^{\mathrm{RL}} = \left\langle O^{\mathrm{L}}, S, G, \Omega^{\mathrm{R}}, \sum, S_{DB}^{\mathrm{L}}, D_{DB}^{\mathrm{L}}, \mathrm{DOM}^{\mathrm{RL}}, L, \preceq, Lab_{\mathrm{S}}, \mathbf{M}^{\mathrm{RL}}, Autor^{\mathrm{R}} \right\rangle, \quad (4.11)$$

де $D_{DB}^{\mathrm{L}} = D_{DB} \bigcup \{L\}$, $\mathrm{DOM}^{\mathrm{RL}}$ – функція відповідності між множинами доменів та атрибутів. $\mathbf{M}^{\mathrm{RL}} = \left(m_{ijk}^{\mathrm{RL}}\right)$ визначає права доступу користувача s_i на виконання операцій ω_k з об'єктом o_j^{L}.

4.3. Модель СЗІ безпечної БД

Характерною відмінністю моделі СЗІ безпечної БД від моделей СЗІ реляційних СУБД та СЗІ MRDB повинно бути покращання можливостей аудиту. Аналіз журналів аудиту БД є складною задачею [5]. Складність зумовлена специфікою задачі, особливостями реалізації аудиту у стандарті SQL та інформаційною недостатністю журналів аудиту СУБД. Це заважає знайти точний час створення запису та його автора. У практичних задачах спростити процедуру аналізу авторства дозволяє співставлення мітки автора (наприклад назви користувача) з об'єктами аудиту (наприклад, записами).

Для забезпечення можливості визначення авторства даних ББД повинна містити функцію відповідності

$$Autor : O \to S, \quad (4.12)$$

або у загальному випадку функція аудиту має вигляд

$$Autor : O \to \{\langle s, time, \mathrm{sysinfo}, \mathrm{extrainfo} \rangle\}, \quad (4.13)$$

де s – суб'єкт; $time$ – час створення об'єкта; sysinfo – додаткова системна та інша інформація, необхідна для розслідування інцидентів; extrainfo – додаткова інформація, розміщена користувачем.

Принципова можливість користувача БД впливати на аудит шляхом доповнення даних аудиту власною інформацією дозволяє:

- виховувати у користувачів свідоме ставлення до процесу аудиту БД та захисту інформації загалом;
- полегшувати розслідування інцидентів збереженням додаткової інформації про інцидент (часто цю інформація не можна передбачити заздалегідь та описати формально);
- використовувати extrainfo як, свого роду, коментар або примітку щодо О для інших користувачів БД.

Математична модель СЗІ безпечної БД db^{S} зі схемою $S_{DB^{\mathrm{S}}}$ має вигляд:

$$SM = \left\langle O^{\mathrm{SA}}, S, G, \Omega^{\mathrm{S}}, \sum, S_{DB^{\mathrm{S}}}, D_{DB^{\mathrm{S}}}, \mathrm{DOM}^{\mathrm{S}}, \hat{L}, \trianglelefteq, Lab_{\mathrm{S}}, \mathbf{M}^{\mathrm{S}}, Autor \right\rangle, \quad (4.14)$$

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 $\hat{l}$ суб'єкта.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Множина доменів $D_{DB^S} = D_{DB} \bigcup D_{\hat{L}} \bigcup D_{Hist}$ доповнена доменами: D_{Hist} – домени атрибутів даних аудиту та збереження історії зміни атомів захисту та $D_{\hat{L}}$ – домени для атрибутів $\hat{L}$. DOM^S – функція відповідності між множинами доменів та атрибутів.

$\mathbf{M}^S = \left(m_{ijk}^S \right)$ визначає права доступу користувача s_i на виконання операцій $\omega_k \in \Omega^S$ з атомом захисту $o_j^{SA} \in O^{SA}$.

З використанням додаткових засобів захисту промислових СУБД, аналогічно до (4.3), узагальнена модель захисту безпечної БД має вигляд

$$SM^* = \langle SM, SR, QTYR, RESR, TR \rangle. \quad (4.15)$$

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 [11]. 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.

5. ВИСНОВКИ

Реалізація моделі ББД ґрунтується на:

- проектуванні схеми БД з врахуванням вимог захисту інформації, зокрема, необхідності використання нового об'єкта захисту;
- модифікації базових SQL запитів за допомогою переглядів даних;
- використанні обмеженого набору операцій.

Для реалізації моделі ББД достатньо використати промислову реляційну СУБД, яка підтримує стандарт SQL. Тестування ББД на платформі СУБД Oracle показало покращення захищеності БД без помітних втрат швидкодії та об'ємів дискового простору. Використання запропонованої у роботі моделі безпечної БД дозволяє покращити такі параметри захисту БД, як:

- деталізація аудиту;
- цілісність (забезпечення можливості відновлення змін даних протягом тривалого часу, неможливість знищення даних тощо);
- конфіденційність (деталізація прав доступу на отримання інформації, статистичний захист тощо).

Використання запропонованої моделі дозволяє, у перспективі, автоматизувати процес проектування захищених ІС на основі серверів БД за допомогою спеціалізованих CASE засобів.

1. Дейт, К. Дж. Введение в системы баз данных: Пер. с англ. – 6-е изд. – К.: Диалектика, 1998. – 784 с. 2. Дудикевич В.Б., Ковела С.І. Алгоритм проектування механізму захисту контекстно-залежної інформації в автоматизованих банках даних // Наук.-техн.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

журн. "Захист інформації". – 1999. – № 1. – С. 24–30. 3. Катренко А.В., Тарасов Д.О. Безпека систем управління розподіленими інформаційними ресурсами // Защита информации: Зб. наук. пр. КМУГА. – К., 1999. – С. 165–170. 4. Пейдж, Вильям, Дж. и др. Использование Oracle8/8i. Специальное издание: Пер. с англ. – М.: Издательский дом "Вильямс", 1999. – 1024 с. 5. Тарасов Д.О. Аудит баз даних // Защита информации: Сборник научных трудов. – К.: КМУГА, 2000. – С. 136-140. 6. Тарасов Д.О. Забезпечення цілісності даних у реляційних структурах // Вісн. Держ. ун-ту "Львівська політехніка". – 1999. – № 383. – С. 213–226. 7. Тарасов Д.О. Моделювання інформаційної інфраструктури комп'ютерних мереж та інформаційна безпека // Вісн. Нац. ун-ту "Львівська політехніка". – 2002. – № 464. – С. 302–311. 8. Тарасов Д.О. Обмеження доступу з мережі до БД // Вісн. Львів. ун-ту. Серія прикладна математика та інформатика. – 1999. – Вип. 1. – С. 213–216. 9. Тарасов Д.О. Основні задачі захисту баз даних // Вісн. Нац. ун-ту "Львівська політехніка". – 2000. – № 406. – С. 216–221. 10. Тарасов Д.О. Специфічні для СУБД, загрози захисту інформації // Защита информации: Сб. науч. тр. – К.: НАУ, 2001. – С. 53-60. 11. Тарасов Д.О., Пелещицин А.М., Жежнич П.І. Обмежений набір операцій для роботи з базами даних // Вісн. Нац. ун-ту "Львівська політехніка". – 2001. – № 438. – С. 125–131. 12. Baldwin R.W. Naming and Grouping Privileges to Simplify Security Management in Large Databases. Proc. // IEEE Symposium Security and Privacy, Oakland, Calif. P. 116–132, Apr. 1990. 13. Bonatti P.A, Kraus S., Subrahmanian V.S., Foundations of Secure Deductive Databases // IEEE Transactions on Knowledge and Data Engineering. – June 1995. – Vol. 7, No. 3. – P. 406–422. 14. Chomicki J. and Toman D., Implementation Temporal Integrity Constraints Using An Active DBMS // IEEE Transactions on Knowledge and Data Engineering. – August 1995. – Vol. 7, No. 4. – P. 566–582. 15. Qian X. Inference channel-free integrity constraints in multilevel relational databases., Proc. // IEEE Symposium on Research in Security and Privacy, Oakland, Calif. – 1994. – P. 158–167, 16. Thuraisingham B. and Ford W., Security Constraint Processing in a Multilevel Secure Distributed Database Management System // IEEE Transaction on knowledge and data engineering. – April 1995. – Vol. 7, No. 2. – P. 274–293.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua