УДК 004.056
DOI: 10.31673/2409-7292.2025.014247

Тишик І. Я.

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ СЕРВЕРІВ БАЗ ДАНИХ

Проаналізовано методи підвищення безпеки серверів баз даних при роботі в корпоративній мережі та застосовано базу даних як основу системи безпеки підприємства. Масовість використання баз даних та значної кількості накопиченої у них інформації з різних предметних областей, стандартизованого інструментарію систем керування ними, призводить до необхідності постановки завдання захисту як безпосередньо баз даних, так і систем керування ними. У роботі зроблений акцент на моделювання системи захисту саме реляційних баз даних, розглядаючи захист інших компонент інформаційної системи в міру необхідності. Введене поняття та дано обґрунтування необхідності використання безпечної бази даних. Розроблені методи та алгоритми для захисту інформації реляційної бази даних з використанням запропонованої математичної моделі безпечної бази даних. Надані пропозиції щодо використання розроблених математичних моделей та налаштування системи захисту інформації. Подані методики дозволяють будувати захищені інформаційні системи на основі серверів баз даних та інтегрувати системи захисту інформації цих серверів зі системами захисту інформації інших корпоративних сервісів для забезпечення комплексного захисту даних підприємства. Реалізація безпечної бази даних блокує основні загрози конфіденційності та цілісності інформації реляційної бази даних, забезпечуючи аудит потрібної деталізації. Також розроблені методи та алгоритми для реалізації удосконаленої моделі примусового керування доступом користувачів реляційних баз даних, проведення аудиту користувачів безпечної бази даних. Ці механізми забезпечують швидку адаптацію системи захисту інформації бази даних до змін політики безпеки та зменшення обчислювальних ресурсів. Досліджені механізми захисту серверів бази даних при роботі у корпоративній мережі та запропоновано використання безпечної бази даних як ядра системи безпеки підприємства.

Ключові слова: безпечна база даних, несанкціонований доступ, інформаційна система, політика безпеки, система захисту інформації, система керування базами даних.

Вступ

Швидкий розвиток галузі інформаційних технологій, широке застосування інформаційних систем для вирішення прикладних задач призводить до зростання вимог щодо ефективності використання методів та засобів захисту інформації. Основними підставами привертання уваги до питань безпеки інформації є розповсюдження інформаційних технологій у бізнесі, поширення Internet та широке використання розподілених обчислень.

Відомо, що дані є основними інформаційними компонентом організації, робота якої тісно пов’язана з інформаційними технологіями. Основний вид діяльності таких організацій пов'язаний, як правило, з опрацюванням та пересиланням даних використовуючи певні інформаційні та мережеві технології. Нині успішна діяльність організації щодо згаданого поводження з даними неможлива без забезпечення якісного їх захисту, тому актуальним питанням для неї є впровадження інформаційної системи, яка, по-перше, захищатиме дані від несанкціонованого доступу, по-друге, завжди буде готова надати їх своїм користувачам, а по-третє, надійно їх зберігатиме і гарантуватиме незмінність. Природно, що переважна більшість підприємств та організацій зацікавленні у збереженні життєво важливих для них даних як в процесі їх опрацювання, так і під час передачі. Частина даних інформаційної системи зберігається в базі даних. Такі дані є структурованими і зазвичай зберігаються у формі реляційних таблиць, і хоча більшість організацій використовує реляційні бази даних, нереляційні бази також отримали широку популярність за рахунок відсутності потреби структурувати дані та записувати їх в нетабличному вигляді. При використанні реляційної моделі даних, дані, які зберігаються в різних реляційних таблицях, пов’язані один з одним.

Не менш важливим для якісного опрацювання та захисту розміщених у базах даних є застосування відповідної системи керування базами даних (СКБД). Правильний вибір СКБД допомагає організувати дані для кращої продуктивності їх опрацювання та пришвидшити пошук завдяки підтримці індексів. Також сучасні СКБД ведуть журнали запитів, які

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

допомагають відновлювати дані та здійснювати їх моніторинг, контролюють паралельність опрацювання запитів та виконують операції щодо відновлення даних [1].

Оскільки інформація, яка зберігається у базах даних може бути критичною для організації, то важливо організувати належний захист баз даних від атак. Базу даних можна атакувати багатьма способами. Існує можливість атаки виключно на дані бази з метою їх несанкціонованого копіювання чи пошкодження, можна атакувати й сам додаток, який взаємодіє з відповідною базою даних, і, як наслідок, отримати доступ до бази. [2]

Критичним випадком розглядається ситуація, коли легальні користувачі бази даних (зумисно чи ні) просочують важливу для організації інформацію у зовнішній світ. Для нівелювання таких дій організація впроваджує політику інформаційної безпеки, яка ґрунтується на положеннях міжнародних стандартів з інформаційної безпеки. База даних є комп'ютерним активом, тому перед застосуванням будь-якої політики безпеки до систем баз даних слід враховувати аспекти конфіденційності, цілісності та доступності.

Існують інші вимоги щодо забезпечення безпеки бази даних, як-от фізична, логічна та безпека у вигляді контролю цілісності елементів, а також можливість перевірки прав доступу користувачів до певного виду даних. Фізична цілісність бази даних стосується проблем, які пов'язані з охороною обладнання опрацювання даних, обмеженням доступу до нього неуповноважених осіб, забезпечення безперебійної роботи серверів і т.д. До забезпечення логічної цілісності бази даних відносяться підтримка та збереження структури зв'язків у реляційних БД та цілісність колекцій в нереляційних базах. Моніторинг забезпечує можливість відстеження внесених змін у базі даних разом із користувачами, які їх внесли. Контроль доступу забезпечує користувачам доступ лише до даних, на які вони авторизовані.

Формулювання проблеми.

Враховуючи масовість використання реляційних баз даних та велику кількість накопиченої в них інформації з різних предметних областей, застосування стандартизованого інструментарію систем керування базами даних, постає проблема в ефективному їх захисті як від зовнішніх, так і від внутрішніх несанкціонованих втручань, що є важливим завданням, яке постає перед фахівцями в галузі захисту інформації.

Аналіз останніх досліджень і публікацій

Різні сфери застосування інформаційних систем (ІС) зумовлюють особливості роботи з інформацією та вимоги до її захисту. Разом з тим, існують загальні правила, які використовуються для побудови моделей систем захисту інформації (СЗІ). У наступних працях узагальнений практичний та теоретичний досвід у галузі питань щодо захисту інформації [1-6]. Особлива увага приділена політиці безпеки, технічним засобам захисту від несанкціонованих втручань, захисту апаратного забезпечення, криптографічним перетворенням і ін.. Розглядаються проблеми захисту великих ІС різного призначення, зокрема, організаційні, інженерно-технічні засоби захисту інформації, нормативно-правове забезпечення діяльності в галузі захисту інформації тощо.

Широко подана література та електронні джерела інформації, присвячені проблемам несанкціонованого доступу до обчислювальних ресурсів з використанням комунікаційних мереж [7], помилок програмного та апаратного забезпечення операційних систем ОС, систем керування базами даних (СКБД), прикладних систем та їх використання [4, 8].

У ряді закордонних та вітчизняних працях щодо моделювання СЗІ БД увага приділяється наступним питанням:

- реалізації механізму транзакцій;
- забезпеченню цілісності реляційних БД [5];
- принципам побудови та використання БД з примусовим контролем доступу (mandatory access control, MAC);

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

- використання БД з довільним контролем доступу (discretionary access control, DAC) [7];
- практичному втіленню теоретичних напрацювань у галузі захисту інформації (ЗІ) у СКБД, промислові стандарти (SQL) [3,6].

Враховуючи масовість застосування у ІС технології збереження інформації в БД, великі обсяги важливої інформації організації, яка зберігається у БД, постає ряд наступних задач.

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 розв′язує наведені задачі називається *безпечною БД* (ББД).

На практиці, засобами промислових СКБД неможливо повністю реалізувати усі задачі захисту, до яких можна віднести: забезпечення конфіденційності (у тому числі реалізувати статистичний захист); забезпечення цілісності інформації (у тому числі реалізувати контекстно-залежний захист); складність реалізації аудиту та адміністрування політики безпеки БД.

Промислові СКБД дозволяють обмежити доступ до об’єктів БД на рівні таблиць, переглядів (view), окремих атрибутів таблиць тощо [**Ошибка! Источник ссылки не найден.**, 6, 7]. Доступ розмежовується для читання даних, зміни, видалення, запису нових даних. Наприклад, для надання користувачу *scott* прав на читання даних з атрибутів *ПРОДУКЦІЯ (КОД, НАЗВА, ПРИМІТКА)* необхідно виконати команду:

GRANT SELECT ON *ПРОДУКЦІЯ (КОД, НАЗВА)* TO *scott*;

На практиці необхідно надавати доступ користувачам (наприклад, різних підрозділів) до конкретних кортежів (полів у деяких кортежах), обмежуючи доступ до інших кортежів. Стандартними командами CREATE ROLE…, GRANT…, REVOKE… це зробити неможливо [6, 7].

Для забезпечення деталізації захисту на рівні кортежів можливі два підходи: використання багаторівневої реляційної бази даних (multilevel relational database, MRDB) [8] та використання ББД.

Реалізація MRDB базується на доповнені наявної схеми БД додатковим атрибутом *L* для збереження міток безпеки або їх аналогів. Цей варіант фактично змінює реляційну БД на MRDB [5].

Існує ряд спеціалізованих СКБД (наприклад, Trusted ORACLE, INGRES/ Enhanced Security), які використовують багаторівневу систему захисту (multilevel) та моделі примусового контролю доступу Реалізація цієї моделі дозволяє обмежити доступ до окремих записів (полів записів) на основі ієрархії класів доступу [9].

При використанні СКБД на основі моделі 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.

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

Ведеться робота над СКБД, яка обмежує доступ до окремих записів таблиць шляхом модифікації SQL запитів користувачів. Дані продукти [10] фактично доповнюють SQL запити нескладними додатковими обмеженнями, лише частково реалізують механізм подібний на категорії міток безпеки.

Форма та механізми фіксації авторства інформації стандартних засобів аудиту, наявних на ринку СКБД, є складними для поточного використання та аналізу. Наприклад, кілька користувачів, у різний час, використовують команду INSERT для занесення у БД записів зі значеннями деякої складної функції багатьох аргументів. У журналі аудиту зберігаються дані про виконання команд, час, назви користувачів, можливо і текст команд. Подальший аналіз авторства конкретного запису вимагає пов'язаної зі записом позначки, яка вказує на автора. У БД ця мітка відсутня. Тому, необхідне, проведення наступного аналізу: оцінити проміжок часу за який міг бути створений запис; вибрати з журналів аудиту команди, які здійснюють операцію INSERT… у даний об'єкт (таблицю); вилучити з аналізу команди, які не відносяться до транзакцій, завершених у проміжок часу створення запису; серед вибраних команд провести співставлення значень у БД та результатів виконання команд і подальший аналіз з врахуванням відмінностей між значеннями у БД з результатами виконання команд. Складність проведення аналізу може завадити 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) [12].

У системах, які проектуються 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 модель компонент обліку людських ресурсів та підсистеми надання доступу користувачам [11,12].

Модель СЗІ реляційних СКБД повинна реалізувати:

1. Матричну модель доступу до основних об'єктів (відношень, окремих атрибутів відношень).
2. Обмеження доступу до даних на рівні відношень та окремих атрибутів відношень.

При цьому необхідно блокувати наступні загрози:

1. Перевищення повноважень користувачів (у тому числі на рівні окремих кортежів).
2. Мінімізація наслідків зламу системи автентифікації користувачів.
3. Підробка введених даних.
4. Захоплення ресурсів .
5. Неможливість використання стандартних засобів аудиту.
6. Помилки налаштування СЗІ БД (за рахунок складності адміністрування політики безпеки БД).

Метою статті є розробка математичних моделей, методів та алгоритмів захисту інформації і їх застосування в інформаційних системах, побудованих на основі реляційних систем керування базами даних.

Математична модель СЗІ реляційних СКБД

Математична модель СЗІ реляційних СКБД має вигляд:

$$SM^R = \langle O^R, S, G, \Omega^R, \sum, S_{DB}, D_{DB}, DOM, \mathbf{M}, Autor^R \rangle,$$

де об'єкти захисту $r_i \in O^R$ - 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); $\Omega^R = \{SEL, INS, DEL, UPD\}$ - операції з $r_i \in O^R$, де оператори

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

вибірки даних $SEL_p(r_1, r_2, \ldots, r_m)$, додавання кортежів у відношення $INS_p(r_1, r_2)$, знищення кортежів $DEL_p(r)$, та зміни значень атрибутів кортежів $UPD_p(r)$ реалізується шляхом застосування до $r_i \in O^R$ суперпозиції операторів реляційної алгебри $\delta_p, \Pi_X, \times, *, -, \cup$.

$\mathbf{M} = (m_{ijk})$ визначає права доступу користувача s_i на виконання операцій ω_k з об'єктом o_j.

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

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

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

$$SM^{R^*} = \langle SM^R, SR, QTYR, RESR, TR \rangle,$$

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'єкту БД $o \in O$ на виконання операції $\omega \in \Omega_{SR}^R = \Omega^R - \{SEL\}$.

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).

Математична модель СЗІ безпечної БД

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

$$SM = \langle O^{\text{SA}}, S, G, \Omega^S, \sum, S_{DB}s, D_{DB}s, DOM^S, \hat{L}, \trianglelefteq, Lab_S, \mathbf{M}^S, Autor \rangle,$$

де O^{SA} – множина атомів захисту, $\hat{L}$ – множина узагальнених міток безпеки, $\trianglelefteq$ – відношення на множині $\hat{L}$, Lab_{S} – функція, яка визначає позначку безпеки $\hat{l}$ суб'єкта.

Множина доменів $D_{DB}s = D_{DB} \cup D_{\hat{L}} \cup D_{Hist}$ 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.

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

З використанням додаткових засобів захисту промислових СКБД, узагальнена модель захисту безпечної БД має вигляд:

$$SM^* = \langle SM, SR, QTYR, RESR, TR \rangle.$$

Алгоритм надання доступу користувачам до ББД

Для забезпечення доступу користувачів до даних реляційні СКБД використовують спеціальні мови. Стандартом вважається SQL.

Для обмеження доступу користувачів до даних БД на рівні кортежів та значень атрибутів доцільно використати стандартні засоби промислових СКБД, зокрема засоби, наявні у мові SQL. До таких засобів належать ролі (ROLE) та перегляди.

За допомогою ролей визначають права доступу, зокрема, до відношень, переглядів та окремих атрибутів. За допомогою переглядів визначають права доступу до відношень, інших переглядів, окремих атрибутів, кортежів та окремих атрибутів кортежів.

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

1. Першим кроком є заборона доступу користувача до об'єктів БД за допомогою команд REVOKE. Додатково забороняється виконання команд типу HOST. Цей крок дозволяє сформувати політику *"що не дозволено – те заборонено"*.

2. Другий крок – визначення множини об'єктів БД, необхідних для роботи користувача O_N, які не потребують контекстно-залежного захисту $O_{NP} \subseteq O_N$, захисту на рівні кортежів і значень атрибутів та інших об'єктів, обмеження доступу до яких можливо описати засобами SQL. Надання користувачу доступу до визначених об'єктів БД.

Надання доступу до таблиць. Перегляди зумовлюється в окремих випадках призначенням цих об'єктів (наприклад, публічний доступ) та обмеженням ресурсів (велика таблиця використовується віддаленими користувачами для реплікації).

Зокрема, надають повноваження на: вибірку даних з відношень, переглядів та послідовностей; виконання необхідних користувачу програмних кодів, які зберігаються на сервері БД (процедур та функцій тощо); створення нових кортежів в O_N.

Для адміністрування прав доступу до даних для користувачів (груп користувачів) необхідні: класифікація об'єктів БД та визначення правил доступу; встановлення правила безпеки – по замовчуванню жоден користувач не повинен мати доступу до жодного об'єкту БД; призначення наступних прав:

- INSERT на певний об'єкт (таблицю, перегляд) лише для тих користувачів, яким це необхідно для виконання службових обов'язків;
- SELECT на таблиці (перегляди, послідовності тощо), з яких користувачі повинні отримувати інформацію за допомогою запитів, відповідно до своїх службових обов'язків;
- EXECUTE та інші на необхідні об'єкти.

Право DELETE не надавати, або обмежити шляхом надання права DELETE на певний об'єкт (таблицю, перегляд) лише для тих користувачів, яким це необхідно для виконання службових обов'язків та лише на об'єкти, які не містять історичної, фактографічної та іншої потрібної для подальшого використання інформації; заборона виконання операцій зміни даних для інших користувачів та інших об'єктів; не надання прав UPDATE; використання додаткових засобів захисту.

Захист серверів БД при роботі у корпоративній мережі

Сервер здійснює керування налагодженням різних компонентів корпоративної інформаційної системи (збір, опрацювання та збереження інформації про систему) відповідно до єдиного плану захисту ІС.

Активні агенти сервера встановлюються на робочі станції та сервери і забезпечують розділення прав доступу, реєстрацію дій користувачів, криптографічний захист даних. Додатково забезпечується інтеграція із засобами аналізу захищеності та виявлення атак. Засоби аналізу захищеності дозволяють перевіряти відомі шляхи порушення системи безпеки, знаходити очевидні паролі, формувати звіти та відслідковувати статистику роботи операційних систем. Найкращі засоби аналізу постійно оновлюють БД "дірок" системи захисту та мають вбудовані експертні системи з питань безпеки та адміністрування.

Використання корпоративних БД для збереження даних, зібраних серверами безпеки, дозволяє вести тривале дослідження параметрів системи безпеки, проводити аудит операцій. Використання промислових серверів БД дозволяє використати потужні OLAP та DSS системи для ефективного аналізу зібраних даних.

На рис. 1 зображена структура корпоративної мережі з використанням серверів безпеки та сертифікації. Для обліку інформації про політику безпеки ІС, про результати практичної реалізації політики безпеки, обліку та опрацювання даних користувачів ІС використовується сервер БД. Збереження переліченої інформації у БД дозволяє проектувати розподілену

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

систему безпеки з використанням добре відлагоджених механізмів розподілених обчислень та механізмів забезпечення цілісності інформації у СКБД.

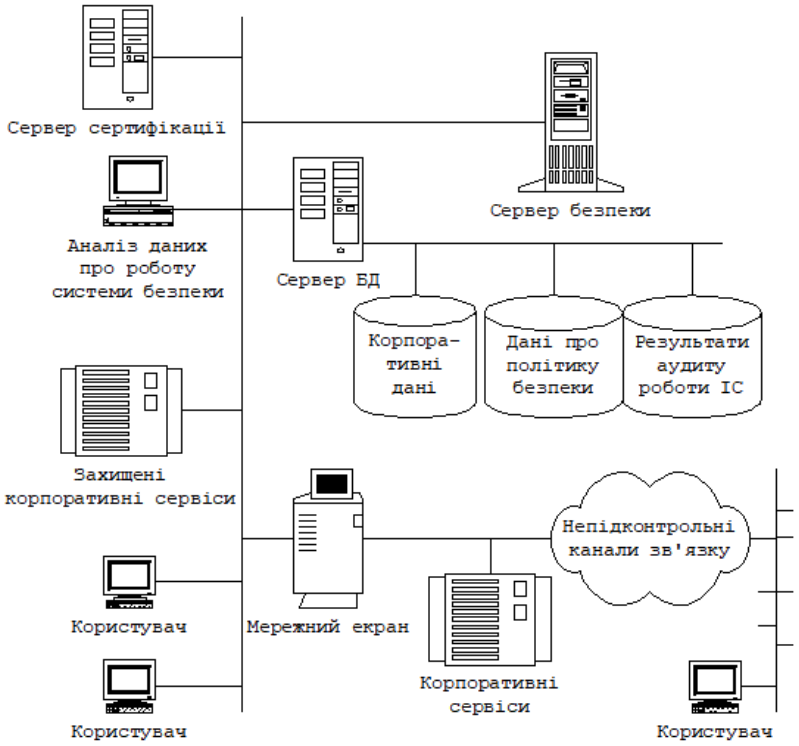

Рис. 1. Корпоративна мережа з використанням серверів безпеки та сертифікації

Сервери БД, зазвичай, складають основу автоматизованого опрацювання інформації у корпоративних ІС. Велика концентрація інформації в БД робить їх об’єктами уваги конкурентів та інших зацікавлених осіб. Порушення захисту БД загрожує втратою цінної інформації, неможливістю прийняття правильних рішень на основі хибних даних тощо.

Питанню атаки на сервери БД не приділяється у публікаціях потрібної уваги. При оцінці захищеності інформації мережевого сервера БД використовується наступна модель: Захист БД = Захист облікової інформації клієнта + Захист мережі + Захист ОС сервера + Захист СКБД.

Захист СКБД у наведеній моделі спрямовано на ідентифікацію та автентифікацію користувачів БД, захист каналу інформації “БД – автентифікований користувач”.

Використання технології клієнт/сервер дозволяє отримати доступ до СКБД навіть без попередньої ідентифікації як користувача корпоративної мережі, так і ОС сервера. Легальний користувач мережі може здійснити доступ до БД в обхід протоколів обміну даними СКБД. Подібні схеми доступу зображені на рис. 2.

Зображені на рис. 2 шляхи доступу користувачів БД та операційної системи до інформації БД контролюються наступними засобами захисту даних.

1. Криптографічний захист файлів БД засобами СКБД.
2. Захист даних на рівні користувачів БД (криптографічний захист об’єктів БД, розподіл повноважень доступу та операцій з об’єктами БД, семантичний захист даних тощо).
3. Автентифікація та авторизація користувачів СКБД, перевірка дозволеного часу роботи тощо.
4. Криптографічний захист інформації, абонентське шифрування тощо.
5. Захист даних на рівні користувачів ОС (криптографічний захист файлів, розділення доступу до системних ресурсів, розподіл повноважень доступу та операцій з ресурсами, налагодження параметрів середовища тощо).

6. Автентифікація та авторизація користувачів ОС сервера, виконання процедур ініціювання сеансу роботи користувача тощо.

7. Забезпечення цілісності та достовірності даних, збір даних для процедур автентифікації.

8. Виконання перевірок на робочому місці користувача, подання даних у потрібній формі.

9. Виконання загальних вимог безпеки до користувачів ІС.

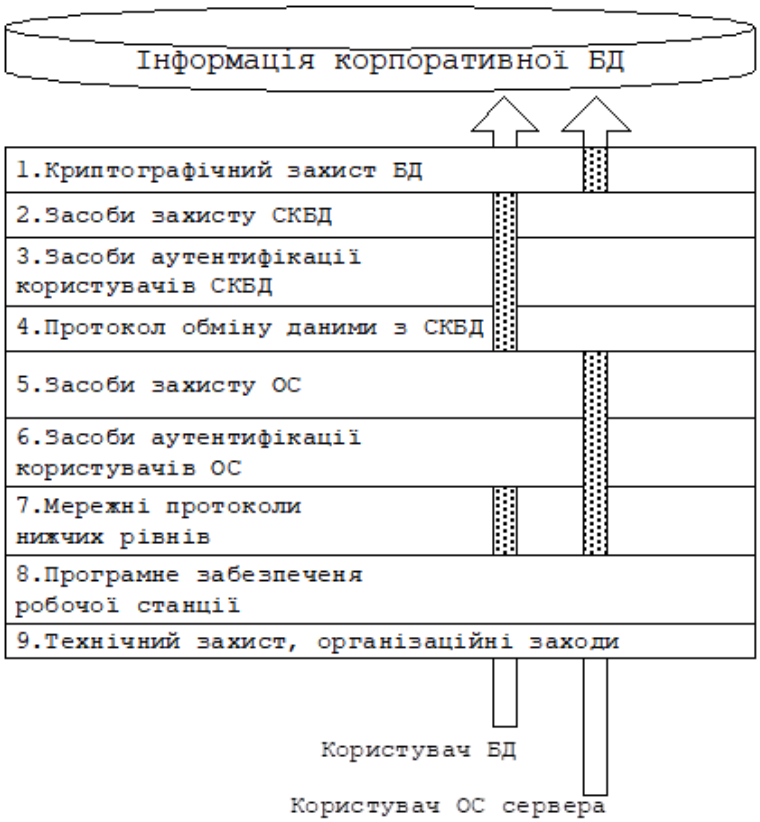

Рис. 2. Шляхи доступу користувачів СКБД та ОС сервера до БД

На рис. 2 розглядаються лише можливі канали несанкціонованого доступу користувачів через мережу. Варіанти фізичного доступу до сервера БД, до фізичних носіїв інформації, випромінювання апаратури та інше не розглядаються.

При роботі на одному мережевому сервері декількох сервісів (СКБД, Web та поштовий сервер, файл-сервер) стає можливою атака на один сервіс через недоліки у захисті іншого. Прикладом атак може бути як блокування сервісу шляхом захоплення ресурсів понад квоту, повне блокування роботи комп'ютера, так і прямий доступ до файлової системи та віртуальної пам'яті. Джерелом небезпеки для сервісів можуть бути навіть мережні протоколи, які використовує сервер через їх відкриті порти.

Встановлення декількох нових складних в інсталяції та адмініструванні програмних продуктів може спричинити непомітні для адміністратора зміни параметрів системи безпеки, обумовленої новими значеннями версій програмних продуктів. Взаємне перевизначення системних параметрів під час встановлення та адміністрування різних складних програмних продуктів може призвести до важко передбачуваних наслідків в умовах конкретної ОС.

Прикладом цього є поява системних паролів СКБД у відкритому вигляді в системних файлах ОС. У цьому випадку ряд користувачів файл-сервера, на якому працювала СКБД, мали доступ до паролів БД.

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

Отже, доцільно встановлювати різні сервіси на різних серверах. Особливо це стосується розділення внутрішньо корпоративних сервісів та сервісів для обслуговування сторонніх осіб. Доцільне розділення також за функціональними ознаками – відділення сервісів збереження та опрацювання даних від сервісів відображення та передавання інформації користувачу. Прикладом останнього є розміщення серверу БД та Web серверу на різних комп'ютерах.

Використання Web серверів як шлюзів між користувачем та СКБД дозволяє відійти від звичайної схеми автентифікації та використати автентифікацію користувача засобами Web сервера. Користувач може використати один із розповсюджених механізмів автентифікації, зокрема, електронні сертифікати. У свою чергу Web сервер, згідно з власними даними про паролі користувача у СКБД, відкриває сеанс роботи з БД із використанням внутрішніх корпоративних засобів автентифікації. Але у випадку порушення захисту Web сервера або зламу його системи автентифікації стає можливим несанкціонований доступ до СКБД.

Висновки

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 математичну модель об'єкту захисту у реляційних БД. Ця математична модель може бути використана для проектування ББД.

Введено поняття безпечної БД та визначено вимоги до математичної моделі безпечної БД та методи реалізації математичної моделі ББД засобами реляційної моделі. Розроблено 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.

Наведені умови доцільності використання СЗІ на основі ББД, дотримання яких дозволяє реалізувати ефективний захист БД від несанкціонованих втручань.

Проаналізовано механізми захисту серверів БД при роботі у корпоративній мережі, на основі чого встановлено, що використання Web-серверів як шлюзу між користувачем та СКБД дозволяє скористатися засобами автентифікації Web-сервера при отриманні доступу користувачів до корпоративних БД. При цьому, користувач може використати механізм автентифікації у вигляді електронного сертифіката, що значно підвищує захист БД від несанкціонованого доступу.

Перелік посилань

1. Доценко С.І. Організація та системи управління базами даних: Підручник. Харків: УкрДУЗТ, 2023. – 117 сторінок, 92 рисунки, 3 таблиці.

2. Пасічник В.В. та ін. Глобальні інформаційні системи та технології: Моделі ефективного аналізу, обробки та захисту даних. Монографія / В.В. Пасічник, П.І. Жежнич, Р.Б. Кравець, А.М. Пелещишин, Д.О. Тарасов. Львів: Видавництво Львівської політехніки, 2006. 348 сторінок. ISBN: 966-553-578-1.2. Chris J. Date. SQL and Relational Theory: How to Write Accurate SQL Code. Symbol-Plus, Series: High Tech. ISBN 978-5-93286-173-8, 978-0-596-52306-0; 2010.

3. Murach's SQL Server 2019 for Developers by Bryan Syverson and Joel Murach 19 chapters, 674 pages, 291 illustrations Published April 2020. ISBN 978-1-943872-57-2.

4. Dotsenko S.I. Organization and Database Management Systems: Textbook. Kharkiv: UkrDUZT, 2023. – 117 pages, 92 figures, 3 tables.

5. Formal models of information security systems for relational databases. Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems, 218-221. //URL: https://vspu.net/sit/index.php/ sit/article/view/2887(accessed: 2021).

6. Ivanov, T.; Pergolesi, M. The impact of columnar file formats on SQL-on-hadoop engine performance: A study on ORC and Parquet. Concurr. Comput. Pract. Exp. 2019, 32, e5523.

7. Dmytro Matveev, Daria Fedorenko. "The Problem of Personal Data Protection on the Internet" // ΛΌΓΟΣ.ONLINE: International scientific e-journal 2019. No. 4. 63. URL: https://ojs.ukrlogos.in.ua/index.php/2663-4139/article/view/530/545. EOI 10.11232/2663-4139.04.40 (accessed: 24.04.2021).

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.

8. Peter P. Chen. "Entity-Relationship Modeling: Historical Events, Future Trends, and Lessons Learned." URL: http://bit.csc.lsu.edu/~chen/pdf/Chen_Pioneers.pdf (accessed: 20.04.2021).

9. Managing Claims and Authorization with the Identity Model. https://learn.microsoft.com/ en-us/dotnet/framework/wcf/feature-details/managing-claims-and-authorization-with-the-identity-model (accessed: 06.01.2023).

10. Security Testing: SQL Injections. https://training.qatestlab.com/blog/technical-articles/ security-testing-sql-injection (accessed: 02.04.2020).

11. Popadyuk V. V. "Encryption in SQL SERVER Databases" // Cybersecurity in the Modern World: Materials of the II All-Ukrainian Scientific and Practical Conference (Odesa, November 20, 2020).

12. Basic Security Practices for SQLite: Safeguarding Your Data. https://dev.to/stephenc222/ basic-security-practices-for-sqlite-safeguarding-your-data-23lh (accessed: 03.02.24).

Надійшла 17.02.2025

© Тишик І. Я. (2025). Організація захисту інформаційних систем на основі серверів баз даних. Сучасний захист інформації, 1(61), 259–268.
https://doi.org/10.31673/2409-7292.2025.014247.