УДК 004.65

А.В. Миргородський[1]
О.В. Романюк[1]

МЕТОДИ ЗАХИСТУ ДАНИХ В СИСТЕМАХ КЕРУВАННЯ БАЗАМИ ДАНИХ

[1]Вінницький національний технічний університет

Анотація

Проаналізовано сучасні методи захисту даних у системах керування базами даних. Досліджено моделі управління доступом, включаючи дискреційний та мандатний контроль, а також рольовий та атрибутивний підходи. Розглянуто криптографічні методи захисту, як-от прозоре шифрування даних, шифрування на рівні полів та застосування еліптичної криптографії. Проаналізовано механізми проактивного виявлення загроз із застосуванням систем SIEM та інструментів машинного навчання.

Ключові слова: СКБД, програмна інженерія, управління доступом, RBAC, ABAC, прозоре шифрування даних, SIEM, машинне навчання, архітектура нульової довіри, розподілені системи.

Abstract

The paper analyses modern methods of data protection in database management systems. It examines access control models, including discretionary and mandatory control, as well as role-based and attribute-based approaches. Cryptographic protection methods are considered, such as transparent data encryption, field-level encryption, and the use of elliptic cryptography. Proactive threat detection mechanisms using SIEM systems and machine learning tools are analysed.

Keywords: DBMS, software engineering, access control, RBAC, ABAC, transparent data encryption, SIEM, machine learning, zero trust architecture, distributed systems.

Вступ

Сучасний стан інформаційної безпеки баз даних характеризується принциповим зсувом від реактивних до проактивних стратегій захисту, що охоплюють весь життєвий цикл даних в інформаційних системах. Зростаюча складність цифрових інфраструктур, що включають хмарні середовища, пристрої Інтернету речей та мобільні платформи, суттєво розширила поверхню потенційних атак, зробивши традиційні підходи недостатніми для нейтралізації сучасних загроз [1]. Зокрема, хмарні бази даних попри свою масштабованість та економічну ефективність породжують специфічні ризики: спільне розміщення даних, неналежне конфігурування та залежність від механізмів безпеки третіх сторін. У свою чергу, пристрої IoT часто позбавлені надійних вбудованих засобів захисту та слугують точками входу до ізольованих мереж для атак зсередини [2]. Тому, актуальним є питання аналізу сучасних методів захисту даних в системах керування базами даних та виявлення перспективних шляхів їх покращення.

Метою дослідження є аналіз методів захисту даних в системах керування базами даних.

Об'єктом дослідження є процес захисту даних в системах керування базами даних.

Предмет дослідження – методи захисту баз даних.

Основна частина

Одним з основних елементів захисту баз даних є управління доступом. До класичних моделей управління доступом можна віднести дискреційний (англ. Discretionary Access Control, DAC) та мандатний (англ. Mandatory Access Control, MAC) контроль, що передбачають доступ за допомогою матриці дозволів або ж централізованих політик безпеки відповідно [3]. Проте, дедалі популярнішими стають моделі з більш гнучкими підходами: рольовим (англ. Role-Based Access Control, RBAC) та атрибутивним (англ. Attribute-Based Access Control, ABAC) управлінням доступом. Рольовий контроль, що ґрунтується на принципі найменших привілеїв, дозволяє обмежити можливість несанкціонованого доступу шляхом суворого розмежування повноважень відповідно до функціональних обов'язків

користувача. Наприклад, співробітник може мати лише права на читання фінансових записів при одночасних адміністративних правах у межах кадрового модуля. Атрибутивний контроль ще більш гнучкий: рішення про надання доступу приймається на основі комплексу атрибутів [4]. Наприклад, це може бути роль, місцезнаходження, тип пристрою або навіть поточний стан системи. Цей підхід може бути більш гнучким для хмарних обчислень та IoT, де статичні рольові конфігурації можуть стати функціональним обмеженим.

Криптографічний захист залишається важливою складовою будь-якої сучасної інформаційної системи. В сфері СКБД можна побачити як розвиток класичних підходів, так і появу принципово нових технологічних рішень. Серед традиційних методів можна виділити поширення прозорого шифрування даних (англ. Transparent Data Encryption, TDE), що автоматично захищає файли бази даних, а також шифрування на рівні полів, яке застосовується до конкретних атрибутів записів, як-от ідентифікаційних номерів або фінансових реквізитів [3]. Криптографія на основі генетичних алгоритмів є прикладом нетривіального міждисциплінарного підходу: методи еволюційних обчислень застосовуються для генерації стійкіших ключів шифрування та вдосконалення протоколів автентифікації. Також можна виділити застосування еліптичної криптографії (англ. Elliptic Curve Cryptography, ECC) на рівні кешу як засіб підвищення безпеки без суттєвого впливу на продуктивність системи [5].

Іншим методом захисту даних, що набуває популярності, є проактивне виявлення загроз під час функціонування СКБД, а не постфактум. Структури даних, що оптимізовані для запису, як-от інструменти на основі RocksDB, забезпечують моніторинг безпеки у реальному часі з мінімальними затримками [6]. Така швидкодія є критичною для систем виявлення вторгнень та платформ запобігання шахрайству, де навіть незначна затримка може мати невиправні наслідки. Прикладом є інформаційні системи банкових установ, які подібним чином перевіряють всі транзакції в режимі онлайн без перерв. Крім того, відбувається інтеграція технологій великих даних у системи управління інформаційною безпекою: алгоритми машинного навчання здатні виявляти аномальні патерни доступу або нетипові операції та автоматично ініціювати протоколи реагування. Поєднання систем управління подіями та інформацією про безпеку (англ. Security Information and Event Management, SIEM) [7] з базами даних дозволяє створити єдину аналітичну платформу, що забезпечує не лише виявлення, а й кореляцію подій, атрибуцію загроз та підтримку прийняття рішень.

Якщо традиційні системи захисту даних функціонують на основі статичних правил та відомих сигнатур загроз, то ШІ-орієнтовані підходи забезпечують динамічну, постійно оновлювану оцінку ризиків на основі моніторингу в реальному часі. Тобто, сучасні інструменти машинного навчання доповнюють уже описану концепцію SIEM. Це дозволяє не лише виявляти відомі типи атак, а й прогнозувати потенційні вектори загроз, що ще не були зафіксовані раніше. Адаптивне забезпечення захисту даних передбачає перехід від концепції одноразової сертифікації до постійного переоцінювання стану захисту, де ШІ автоматизує процеси перевірки відповідності нормативним вимогам та формування звітності. Це дозволяє розширити відому архітектуру нульової довіри (англ. Zero Trust Architecture, ZTE), в основу якої покладено принцип максимального захисту навіть в ізольованих мережах та інших «безпечних» середовищах. Застосування ШІ разом з ZTE дозволяє розробити методи захисту нового рівня, де рівень довіри динамічно переоцінюється при кожній транзакції незалежно від попередньої поведінки суб'єкта [8]. Особливо корисним це може бути в розподілених системах керування базами даних, де є ризик компрометації окремих вузлів.

Розглянуті методи та підходи демонструють певну обмеженість: запропоновані механізми захисту, включаючи криптографічні засоби або RBAC/ABAC, розглядаються переважно в ізольованому контексті класичних інформаційних систем. Сучасні гібридні середовища часто є гетерогенними, тобто об’єднують різнорідне програмне забезпечення або ж моделі даних [9], як-от розподілені СКБД в складі хмарних ресурсів в поєднанні з кордонними обчисленнями або IoT. Застосування методів захисту та потенційні нові загрози в такому контексті залишаються недостатньо дослідженими. Крім того, реалізація будь-яких методів захисту даних повинна враховувати фактор людського чинника – більшість запропонованих рішень передбачає технічну досконаліть реалізації, але не аналізує організаційні, когнітивні та поведінкові особливості сучасних безпекових інцидентів.

Висновок

Було досліджено сучасний стан методів захисту даних у системах керування базами даних з

урахуванням актуальних викликів, зумовлених розширенням поверхні атак у хмарних, IoT та мобільних середовищах. Проведено аналіз класичних і сучасних моделей управління доступом, зокрема дискреційного, мандатного, рольового та атрибутивного контролю, виявлено переваги гнучких підходів RBAC та ABAC у динамічних розподілених середовищах. Розглянуто криптографічні методи захисту, включаючи прозоре шифрування даних, шифрування на рівні полів та застосування еліптичної криптографії і генетичних алгоритмів. Досліджено механізми проактивного виявлення загроз на основі структур даних, оптимізованих для запису, а також інтеграцію систем SIEM з інструментами машинного навчання. Окремо розглянуто ШІ-орієнтовані підходи до захисту даних у контексті архітектури нульової довіри як перспективного напряму динамічної оцінки ризиків.

Дослідження показало, що розглянуті методи та механізми є важливими складовими сучасної архітектури захисту СКБД, проте їхня ефективність у гетерогенних гібридних середовищах залишається недостатньо вивченою. З урахуванням цього, подальші напрями розвитку у сфері захисту баз даних можуть охоплювати розробку адаптивних безпекових фреймворків, що інтегрують криптографічні методи із засобами штучного інтелекту та машинного навчання; вдосконалення архітектури нульової довіри для застосування у розподілених СКБД з динамічною переоцінкою рівня довіри на рівні окремих транзакцій; а також формалізацію метрик оцінювання ефективності безпекових рішень з урахуванням організаційних і поведінкових чинників, що залишаються малодослідженими у наявних підходах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Naseer F. Security paradigms in advanced database management systems [Electronic resource] / Fahad Naseer // Journal of innovative computing and emerging technologies. – 2025. – Vol. 3, no. 1. – Mode of access: https://doi.org/10.56536/jicet.v3i1.225 (date of access: 18.02.2026). – Title from screen.
2. IoT data security in outsourced databases: a survey of verifiable database [Electronic resource] / Ailin Chen [et al.] // Heliyon. – 2024. – Vol. 10, no. 7. – P. e28117. – Mode of access: https://doi.org/10.1016/j.heliyon.2024.e28117 (date of access: 18.02.2026). – Title from screen.
3. Merilena Jonnada N. Database and system security [Electronic resource] / Nikitha Merilena Jonnada // International journal of network security & its applications. – 2025. – Vol. 17, no. 6. – P. 41–47. – Mode of access: https://doi.org/10.5121/ijnsa.2025.17603 (date of access: 18.02.2026). – Title from screen.
4. Rewriting Graph-DB queries to enforce attribute-based access control [Electronic resource] / Daniel Hofer [et al.] // Lecture notes in computer science. – Cham, 2023. – P. 431–436. – Mode of access: https://doi.org/10.1007/978-3-031-39847-6_34 (date of access: 18.02.2026). – Title from screen.
5. GECC: A GPU-based high-throughput framework for Elliptic Curve Cryptography [Electronic resource] / Qian Xiong [et al.] // ACM transactions on architecture and code optimization. – 2025. – Mode of access: https://doi.org/10.1145/3736176 (date of access: 18.02.2026). – Title from screen.
6. Database security [Electronic resource] / Prof K. R. Ingole [et al.] // International journal for research in applied science and engineering technology. – 2023. – Vol. 11, no. 4. – P. 1568–1576. – Mode of access: https://doi.org/10.22214/ijraset.2023.50415 (date of access: 18.02.2026). – Title from screen.
7. Mahajan S. The role of SIEM in modern cybersecurity [Electronic resource] / Shilpa Mahajan // Cybersecurity and privacy in the era of smart technologies. – [S. l.], 2025. – P. 301–324. – Mode of access: https://doi.org/10.4018/979-8-3373-2282-7.ch010 (date of access: 18.02.2026). – Title from screen.
8. Vineel Bala. Zero trust security framework for federated and centralized enterprise data architectures: a comparative analysis of AI-enhanced database integration models [Electronic resource] / Vineel Bala // Journal of information systems engineering and management. – 2025. – Vol. 10, no. 59s. – P. 839–854. – Mode of access: https://doi.org/10.52783/jisem.v10i59s.12963 (date of access: 18.02.2026). – Title from screen.
9. Миргородський А. В. Аналіз архітектурних принципів сучасних розподілених систем керування базами даних / Андрій Вікторович Миргородський, Оксана Володимирівна Романюк // Матеріали LIV Всеукраїнської науково-технічної конференції підрозділів ВНТУ, Вінниця, 24–27 берез. 2025 р. – Вінниця, 2025.

Миргородський Андрій Вікторович – аспірант групи 121-24а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: mirgorodskijav@gmail.com

Романюк Оксана Володимирівна – к.т.н., доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: romaniukoksanav@gmail.com

Myrhorodskyi Andrii – graduate student of group 121-24a, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mirgorodskijav@gmail.com

Oksana Romaniuk – Candidate of Technical Sciences, Associate Professor of the Software Chair, Vinnytsia NationalTechnical University, Vinnytsia, e-mail: romaniukoksanav@gmail.com