УДК 004.056. 5:004.7
DOI https://doi.org/10.32782/2521-6643-2025-1-69.16

Розломій І. О., кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету
ORCID: 0000-0001-5065-9004

Науменко С. В., викладач кафедри інформаційних технологій Черкаського національного університету імені Богдана Хмельницького
ORCID: 0000-0002-6337-1605

АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНІ ОСОБЛИВОСТІ ЗАХИЩЕНИХ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ НОВОГО ПОКОЛІННЯ З ПІДТРИМКОЮ SERVERLESS ТА EDGE-ОБЧИСЛЕНЬ

У статті представлено комплексне дослідження сучасних систем керування базами даних (СКБД), що функціонують на основі serverless- та edge-архітектур. Розглядаються новітні СКБД SurrealDB, Xata, Turso, Dolt і EdgeDB, які демонструють інноваційні підходи до зберігання, обробки та захисту даних у розподілених середовищах. З огляду на стрімке зростання обсягів даних, поширення IoT-пристроїв і зростання вимог до безпеки інформаційних систем, розробка ефективних архітектур захищених СКБД набуває особливої актуальності.

У роботі проаналізовано архітектурні та функціональні особливості зазначених систем, визначено їхні переваги, обмеження та потенціал до застосування в критично важливих сферах. Особливу увагу приділено питанням інформаційної безпеки, зокрема реалізації політик контролю доступу, підтримки шифрування, реплікації даних, стійкості до збоїв, а також наявності механізмів журналювання та аудиту. На основі проведеного аналізу розроблено узагальнену модель архітектури безпечної edge-орієнтованої СКБД, яка включає ключові компоненти – клієнтський рівень, edge-вузли, служби політик доступу, журналювання, централізоване сховище та службу керування ключами. Побудовано формальну модель оцінки ризиків, що враховує ймовірність реалізації загрози, ступінь вразливості та критичність впливу для кожного структурного елемента системи.

У результаті дослідження виділено архітектурні та захисн підходи, які показали високу ефективність у критичних розподілених системах. Зокрема, до них належать: ізоляція рівнів обробки, локалізація даних, атрибутивне управління доступом, наскрізне шифрування та системи журналювання в реальному часі. Застосування зазначених рішень сприяє зниженню рівня ризиків без втрати продуктивності або масштабованості, що є вирішальним для систем, які працюють у складних мережевих умовах або обслуговують чутливі дані. Отримані результати можуть бути використані для вдосконалення практик захисту у сфері медицини, енергетики, промислових IoT-рішень та інформаційних систем критичної інфраструктури.

Ключові слова: *розподілені бази даних, edge-обчислення, serverless-архітектура, інформаційна безпека, контроль доступу, оцінка ризиків.*

Rozlomii I. O., Naumenko S. V. Architecture and functional features of the next-generation secure database management systems with support for serverless and edge computing

This paper presents a comprehensive study of modern database management systems (DBMSs) designed to operate within serverless and edge computing architectures. The analysis focuses on recent DBMSs such as SurrealDB, Xata, Turso, Dolt, and EdgeDB, which implement innovative approaches to data storage, processing, and protection in decentralized environments. These systems have emerged in response to the growing demand for scalable, secure, and resilient data management solutions, especially in the context of increased data generation, the proliferation of IoT devices, and rising requirements for data privacy and integrity.

The study examines the architectural and functional characteristics of the mentioned DBMSs, identifying their advantages, limitations, and application potential in security-sensitive domains. Particular attention is paid to the integration of access control policies, support for data encryption, replication mechanisms, fault tolerance, and auditing capabilities. Based on the analysis, the authors propose a generalized architecture for a secure edge-oriented DBMS, which consists of a client tier, edge nodes, access policy engine, audit and logging service, centralized cloud storage, and key management service (KMS). Each component plays a distinct role in ensuring end-to-end data protection, context-aware authorization, local data processing, and synchronization with a centralized repository.

To assess system resilience and identify vulnerable components, a formal risk evaluation model is developed. The model calculates risk levels for each architectural component based on three parameters: the probability of threat realization, the

degree of vulnerability, and the criticality of impact. The resulting weighted risk scores allow for a quantitative comparison of different architectural configurations and help prioritize protection measures in systems operating under varying threat conditions.

The paper also identifies a set of architectural and security design principles that have proven effective in critical distributed systems. These include layered isolation of processing levels, data localization at the edge, attribute-based access control (ABAC), end-to-end encryption (both at rest and in transit), and real-time distributed logging. The combination of these principles is shown to enhance security without compromising scalability or system performance, making them highly suitable for applications in healthcare, industrial automation, energy systems, and critical infrastructure.

The results of this study can serve as a foundation for further improvement of secure DBMS design, offering practical insights for developers, system architects, and researchers working on the next generation of distributed and edge-integrated data platforms.

Key words: *distributed databases, edge computing, serverless architecture, information security, access control, risk assessment.*

Постановка проблеми. У сучасних умовах цифрової трансформації, коли обсяги даних зростають експоненційно, а вимоги до швидкості доступу, надійності та безпеки інформаційних систем постійно підвищуються, значну увагу фахівців привертають новітні системи керування базами даних (СКБД). На зміну класичним централізованим архітектурам приходять децентралізовані, розподілені та edge-орієнтовані підходи, що передбачають обробку та зберігання даних ближче до місця їхнього генерування [1, с. 27]. Такий підхід дозволяє значно зменшити затримки, підвищити продуктивність і знизити навантаження на центральні хмарні ресурси.

У цьому контексті зростає попит на СКБД, здатні ефективно працювати у розподілених середовищах, інтегруватися з edge-інфраструктурами, підтримувати serverless-парадигму та водночас гарантувати високий рівень безпеки збереження й обробки даних [2, с. 130]. Серед найперспективніших рішень нового покоління виділяються такі бази даних, як SurrealDB, Xata, Turso, Dolt та EdgeDB. Вони демонструють нові підходи до побудови структури даних, запитів, автентифікації, контролю доступу й інтеграції з сучасними інструментами розробки, що робить їх привабливими для широкого спектра застосувань – від вебзастосунків і IoT до систем реального часу [3, с. 85].

Ключовою перевагою таких СКБД є поєднання мультимодельності, можливостей горизонтального масштабування, автоматичного керування інфраструктурою та гнучких засобів безпеки. Вони дозволяють розробникам не лише спростити процес зберігання й обробки даних, а й ураховувати вимоги до конфіденційності, цілісності та доступності даних у критично важливих інформаційних системах. Водночас швидкий розвиток цих технологій вимагає детального аналізу їхніх архітектурних підходів, функціональних можливостей і наявних механізмів захисту.

Аналіз останніх досліджень та публікацій. Останніми роками спостерігається зростання кількості наукових і прикладних досліджень, присвячених проблематиці побудови безпечних, масштабованих та продуктивних систем керування базами даних, що відповідають викликам сучасної цифрової інфраструктури. У працях [4, с. 94; 5, с. 65; 6, с. 35] детально розглядаються особливості інтеграції баз даних у розподілені та serverless-середовища, акцентуючи увагу на важливості зменшення затримок, забезпечення стійкості до збоїв і підтримки автоматичного масштабування.

У роботах [7, с. 111] і [8, с. 1796] проаналізовано архітектурні особливості новітніх мультимодельних СКБД, таких як SurrealDB і EdgeDB. Автори підкреслюють їхню гнучкість у контексті одночасної підтримки графових, документних і реляційних моделей, що відкриває нові можливості для побудови адаптивних інформаційних систем. Особливу увагу дослідники приділяють уніфікованим мовам запитів і модульній архітектурі, яка дозволяє забезпечити високий рівень керованості даними.

Окремий науковий інтерес становлять публікації, присвячені питанням безпеки в serverless- та edge-інфраструктурах. Так, у дослідженнях [9, с. 3310] висвітлюються питання динамічного керування доступом, шифрування даних у розподіленому середовищі та забезпечення цілісності інформації в умовах обмежених обчислювальних ресурсів. Роботи [10, с. 170; 11, с. 24] фокусуються на ризиках, пов’язаних із використанням NoSQL-баз у хмарних і гібридних системах, зокрема вказується на відсутність стандартних механізмів транзакційного захисту, складність реалізації політик автентифікації та контролю доступу.

Огляд публікацій також засвідчує зростаючу увагу до інструментів, що орієнтовані на розробників. Наприклад, Xata і Turso, як об’єкти сучасних досліджень [12, с. 18], розглядаються з погляду інтеграції в DevOps-процеси, підтримки інтерфейсів REST/GraphQL та автоматизованого управління версіями схем баз даних. У той же час, автори наголошують на потребі вдосконалення захисних механізмів, особливо в умовах багатоагентної взаємодії та автономної реплікації даних.

Попри наявність значного наукового доробку, окремі аспекти безпечного функціонування СКБД нового покоління залишаються недостатньо вивченими. Зокрема, потребують подальшого опрацювання питання забезпечення цілісності та конфіденційності в умовах георозподіленої обробки даних, розробка уніфікованих моделей контролю доступу для мультимодельних СКБД, а також оцінювання ризиків при

serverless-розгортанні. Окрім того, актуальними залишаються дослідження щодо формалізації архітектурних патернів, що поєднують ефективність, масштабованість та високий рівень інформаційної безпеки.

Постановка завдання. Мета статті – аналіз архітектурних рішень, функціональних можливостей і засобів забезпечення безпеки в сучасних СКБД із підтримкою serverless та edge-обчислень, а також виявлення їхньої придатності для застосування у критичних та розподілених інформаційних системах.

Виклад основного матеріалу. Розвиток архітектур баз даних від централізованих до розподілених, а згодом і до serverless- та edge-орієнтованих рішень зумовив появу нових систем керування базами даних, які інтегрують властивості масштабованості, швидкодії та інформаційної безпеки. Серед сучасних представників такого класу особливе місце посідають SurrealDB, Xata, Turso, Dolt та EdgeDB. Зазначені системи орієнтовані на побудову інформаційних сервісів нового покоління, що функціонують у динамічних розподілених середовищах з високими вимогами до конфіденційності, доступності та цілісності даних.

SurrealDB належить до мультимодельних СКБД з підтримкою графової та документної структури даних, що забезпечує гнучкість у моделюванні складних зв'язків і об'єктів. Особливістю цієї системи є наявність вбудованих засобів автентифікації, розмежування доступу та підтримка ролей, що дозволяє реалізовувати політики безпеки на рівні окремих колекцій та записів. Платформа орієнтована на використання у високонавантажених середовищах, зокрема в edge-інфраструктурах, де критичною є мінімізація затримок доступу до даних.

Xata є хмарною документо-реляційною СКБД, що поєднує елементи класичних реляційних підходів із гнучкістю NoSQL. Особливу увагу в її реалізації приділено автоматичному масштабуванню, підтримці serverless-архітектури, а також вбудованим механізмам розмежування доступу, ізоляції середовищ та керування правами користувачів. Враховуючи орієнтацію на розробників вебзастосунків, система має зручні інтерфейси для інтеграції з популярними фреймворками, що забезпечує збереження безпеки при мінімізації зусиль на налаштування.

Turso позиціонується як легка база даних для edge-обчислень, побудована на основі libSQL – модифікованої версії SQLite [13, с. 9]. Основною ідеєю є забезпечення швидкого доступу до даних у географічно розподілених вузлах за рахунок наближення обробки до кінцевого користувача. Turso реалізує реплікацію, контроль доступу на основі токенів, ізоляцію регіональних інстанцій, що в сукупності дозволяє використовувати її в задачах, де критично важливими є локальність і безперервність доступу до даних.

Dolt поєднує можливості СКБД і системи контролю версій. Вона зберігає повну історію змін на рівні таблиць, дозволяє створювати гілки, виконувати злиття та відновлення стану, що робить її зручною для колективної роботи з даними, аналітичних досліджень і побудови систем із високими вимогами до прозорості змін. Серед механізмів безпеки – аудит дій, контроль відповідальності за зміни, а також підтримка автентифікації та прав доступу до окремих версій.

EdgeDB реалізує концепцію пост-SQL і поєднує реляційну модель з об'єктно-орієнтованими підходами до опису даних. Система вирізняється можливістю декларативного проєктування складних структур із чітким визначенням типів, автоматичним генеруванням API та контрольованим доступом до даних [14, с. 2010]. Безпека досягається за рахунок типізованості, контролю запитів, обмеження на доступ до полів і реалізації правил авторизації.

Узагальнення архітектурних і функціональних характеристик розглянутих СКБД представлено в таблиці 1, що дозволяє здійснити порівняльний аналіз їхніх можливостей з огляду на тип моделі даних, особливості архітектури, реалізацію механізмів захисту доступу, сферу застосування та ключові функціональні переваги. Аналіз порівняльних характеристик свідчить про те, що сучасні системи керування базами даних, орієнтовані на serverless- та edge-архітектури, демонструють високу гнучкість у реалізації моделей даних, масштабованості та безпеки.

Таблиця 1

Порівняльна характеристика сучасних СКБД з підтримкою serverless та edge-обчислень

СКБД	Тип моделі	Архітектура	Безпека доступу	Орієнтація	Особливості
SurrealDB	Графова + документна	Edge-ready	Ролі, автентифікація, ACL	Real-time, IoT	SQL-подібна мова, мультимодельність
Xata	Документо-реляційна	Serverless	RBAC, ізоляція середовищ	Вебзастосунки, JAMstack	Простота інтеграції, схеми, пошук
Turso	Key-value (libSQL)	Edge-distributed	Токени, реплікація	Mobile, geo-distributed	Легка вага, edge-розгортання
Dolt	Реляційна + контроль версій	Self-hosted/ serverless	Контроль змін, історія, права	Спільна робота, аналітика	Git-подібна модель керування
EdgeDB	Об'єктно-реляційна	Serverless	Типізація, правила доступу	Web, API-driven	Пост-SQL, декларативність

SurrealDB і EdgeDB вирізняються підтримкою складних структур даних із можливістю типізованого доступу та інтегрованих механізмів авторизації, що сприяє побудові систем з підвищеним рівнем керованості. Xata та Turso фокусуються на швидкій інтеграції з хмарною інфраструктурою та edge-оточеннями, надаючи прості у використанні інтерфейси для управління доступом і масштабування, що робить їх придатними для реалізації вебзастосунків та мобільних сервісів. У свою чергу, Dolt пропонує унікальну концепцію контролю версій даних, що відкриває нові можливості для реалізації безпечної командної роботи та аналітики зі збереженням історії змін.

Попри високу функціональність розглянутих СКБД, актуальними залишаються питання формалізації єдиних підходів до розмежування прав доступу у мультимодельних структурах, забезпечення наскрізного шифрування на рівні окремих запитів, а також створення типових рішень для автоматизованого контролю цілісності даних у розподілених і гібридних середовищах. Ці аспекти потребують подальшого дослідження з урахуванням специфіки побудови сучасних інформаційних систем.

Незважаючи на численні переваги розглянутих систем, поглиблений аналіз їхньої архітектури виявляє низку обмежень і технічних викликів, що можуть мати критичне значення при впровадженні в розподілених середовищах з підвищеними вимогами до безпеки, цілісності та безперервності обробки даних [15, с. 293].

У системі SurrealDB основним викликом є обмежена зрілість реалізації вбудованих засобів захисту. Незважаючи на підтримку механізмів автентифікації та розмежування доступу, відсутність повноцінної багатофакторної авторизації, детальної конфігурації прав на рівні атрибутів об'єктів і централізованого журналювання дій ускладнює її використання в умовах, що передбачають високий рівень аудиту та відповідності стандартам. Крім того, відсутність формалізованої моделі консистентності в умовах паралельного доступу до графових структур даних створює ризики конфліктів при одночасному оновленні.

Xata, зважаючи на свою cloud-native архітектуру, демонструє обмежену контрольованість з боку кінцевого користувача щодо налаштування середовищ безпеки, оскільки значна частина інфраструктури прихована за serverless-абстракціями. Це обмежує можливості інтеграції з існуючими системами автентифікації та політиками безпеки підприємства. Також слід зазначити відсутність підтримки повноцінного шифрування на рівні окремих запитів або політик шифрування на рівні колонок, що є критично важливим у сфері зберігання персональних або фінансових даних.

Turso, як легковагова база з орієнтацією на edge-середовища, забезпечує швидку доставку й обробку даних, однак її спрощена модель доступу через токени має обмежену гнучкість в адмініструванні складних ієрархій прав. Реплікація між інстанціями не забезпечує гарантій строгої консистентності, що унеможливлює використання цієї СКБД у задачах, де важлива узгодженість оновлень, наприклад, у фінансових системах. Також відсутність вбудованих засобів аналізу аномалій чи аудиту ускладнює контроль доступу в реальному часі.

У випадку Dolt головним недоліком є високі обчислювальні витрати на операції злиття (merge) при великій кількості паралельних гілок або складній історії змін. Через це система втрачає продуктивність при роботі в режимі високонавантажених транзакційних систем. Крім того, механізм контролю версій має низький рівень абстракції захисту – хоча історія змін зберігається, вона не захищена від модифікації без зовнішніх засобів перевірки, таких як цифрові підписи чи блокчейн-нотаріат. Відсутність тонкої конфігурації прав доступу до окремих версій чи гілок також знижує рівень гнучкості з погляду захисту інформації.

EdgeDB, попри свою типізовану структуру та декларативну модель даних, стикається з обмеженнями в реалізації складних схем розмежування доступу, зокрема у випадках, коли потрібна динамічна зміна політик на основі поведінкових факторів. У системі також бракує гнучких механізмів шифрування з підтримкою апаратного прискорення або роботи з розподіленими ключами. У випадках глибоко вкладених об'єктних структур складність управління дозволами може призводити до порушення принципів найменших привілеїв або до помилок у проєктуванні безпечної схеми доступу.

Усі зазначені обмеження свідчать про наявність актуальних задач, що потребують подальшого дослідження. Для формалізації та порівняння рівня захищеності таких СКБД доцільним є побудова узагальненої моделі оцінювання ефективності систем у контексті критичних параметрів безпеки. Нехай система S характеризується множиною параметрів $P = \{p_1, p_2, \ldots, p_n\}$, де кожен параметр описує окремий аспект безпеки (наприклад, p_1 – підтримка шифрування, p_2 – рівень розмежування доступу, p_3 – контроль змін, тощо). Для кожної системи S_i визначається вектор безпеки $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, а загальна ефективність може бути оцінена за допомогою зваженої норми:

$$E(S_i) = \sum_{j=1}^{n} w_j \cdot v_{ij}$$

де $w_j \in [0,1]$ – коефіцієнти вагомості параметрів безпеки відповідно до задачі. Застосування такої моделі дозволяє кількісно порівнювати СКБД між собою у визначеному контексті (наприклад, для систем з підвищеною відповідальністю, персональними даними або розподіленим обчисленням на периферії).

Аналіз наявних обмежень дозволяє окреслити вимоги до архітектури безпечної системи керування базами даних, орієнтованої на edge-обчислення [16, с. 65]. Така система має забезпечувати децентралізовану

обробку запитів, адаптивне масштабування, наскрізний захист даних та стійкість до втрат зв'язку з центральними вузлами. Її архітектура повинна підтримувати ізольовану обробку на периферійних вузлах, синхронізацію зі сховищем у хмарі, гнучке розмежування доступу та автоматизований аудит.

Формалізуючи архітектурну модель, можна визначити такі основні компоненти:

1. Клієнтський рівень (Client Tier) – включає мобільні, браузерні або вбудовані пристрої користувача, що взаємодіють із локальним edge-вузлом через захищені API (HTTPS, gRPC). Доступ контролюється за допомогою токенів або сертифікатів, з урахуванням контексту (геолокація, тип пристрою, поведінкові патерни).

2. Edge-вузол (Edge Node) – автономний обчислювальний компонент, розміщений ближче до джерел даних. Забезпечує локальне зберігання та обробку запитів, реалізує механізми кешування, валідації, розмежування доступу та шифрування. У разі втрати зв'язку з центральним сховищем може функціонувати у відключеному режимі з подальшою синхронізацією.

3. Менеджер політик доступу (Access Policy Engine) – модуль, який обслуговує запити авторизації на основі атрибутивної або ролейної моделі (ABAC/RBAC). Підтримує конфігурацію динамічних політик доступу, з урахуванням рівня чутливості даних та поточного контексту.

4. Журнальне сховище (Audit & Logging Service) – служба, що акумулює інформацію про всі події доступу, запити, оновлення та дії користувачів. Дані журналювання синхронізуються з центральною системою без втрати записів, навіть у разі нестабільного з'єднання.

5. Центральне сховище (Cloud Storage Core) – репозиторій, який зберігає повні резервні копії, агреговану аналітику, історію змін і виконує періодичну синхронізацію з edge-вузлами. Реалізує політики зберігання, реплікації та регламентованого доступу.

6. Служба керування ключами (KMS) – модуль, що забезпечує шифрування даних як у стані спокою, так і при передачі. Ключі зберігаються в апаратних сховищах (HSM) або програмно розділені за географічною ознакою.

Взаємодія основних компонентів безпечної системи керування базами даних, орієнтованої на edge-обчислення, представлена у вигляді узагальненої архітектурної моделі на рис. 1.

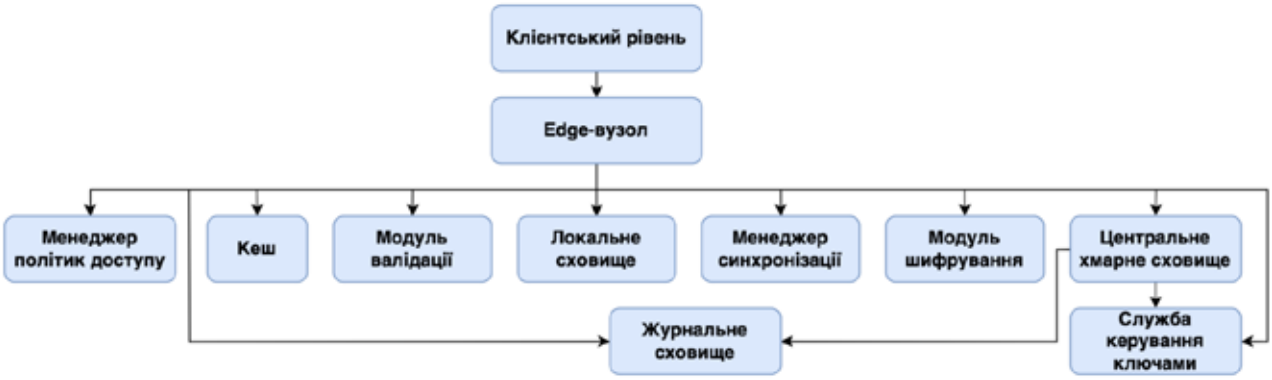

Рис. 1. Архітектура безпечної edge-орієнтованої СКБД

Описана архітектура дозволяє забезпечити баланс між продуктивністю та безпекою, характерний для критичних розподілених систем. Децентралізованість обробки, підтримка локального доступу, гнучке розмежування прав і журналювання створюють основу для побудови стійких до збоїв і атак баз даних, які відповідають сучасним вимогам щодо захисту інформації. Далі доцільно розглянути, як особливості цієї архітектури впливають на стійкість до загроз, та сформувати формальну модель для оцінки ризиків, характерних для кожного з компонентів системи.

Оцінка ризиків в архітектурі безпечної edge-орієнтованої системи керування базами даних потребує формалізованого підходу, що дозволяє враховувати вплив зовнішніх загроз, внутрішніх вразливостей та обмежень, пов'язаних з обчислювальними та мережевими ресурсами. З цією метою доцільно використовувати узагальнену модель, в якій рівень ризику для певного компонента системи визначається на основі ймовірності реалізації загрози, ступеня вразливості елемента та критичності потенційних наслідків.

Нехай архітектура системи складається з множини компонентів $C = \{c_1, c_2, \ldots, c_n\}$, а для кожного компонента c_i визначено відповідну трійку оцінок:

– $T_i \in [0,1]$ – ймовірність реалізації загрози;
– $V_i \in [0,1]$ – ступінь вразливості компонента;
– $I_i \in [0,1]$ – інтенсивність (критичність) впливу при реалізації загрози.

Формальний рівень ризику для кожного компонента визначається як:

$$R_i = T_i \cdot V_i \cdot I_i$$

Загальний ризик системи можна оцінити як агреговану функцію:

$$R_{total} = \sum_{i=1}^{n} \alpha_i \cdot R_i$$

де α_i – ваговий коефіцієнт для кожного компонента, який враховує його значущість для системи в цілому (наприклад, для edge-вузла або KMS ці значення можуть бути вищими, ніж для клієнтського рівня).

Для практичного використання така модель дозволяє: – ідентифікувати критичні точки, у яких ризики перевищують допустимі порогові значення; – обґрунтовано перерозподіляти ресурси безпеки між компонентами; – порівнювати різні варіанти архітектурних рішень щодо їхньої стійкості до загроз.

У процесі аналізу ефективності архітектурних підходів виявлено кілька принципів, які демонструють найкращі результати в критичних розподілених системах:

1. Ізоляція рівнів обробки. Розділення обчислень між клієнтським, edge- та хмарним рівнями з чітко визначеними інтерфейсами взаємодії дозволяє мінімізувати наслідки успішної атаки на окремий рівень, локалізуючи її вплив.

2. Локалізація доступу до даних. Зберігання та обробка даних на edge-вузлах з періодичною синхронізацією з центральним сховищем забезпечує зменшення обсягу переданих конфіденційних даних, що знижує ризики перехоплення та несанкціонованого доступу під час передачі.

3. Впровадження політик доступу на основі атрибутів (ABAC). Підхід до динамічного контролю доступу, який враховує контекст запиту, роль користувача, геолокацію, пристрій і поточний стан системи, дає змогу більш точно визначати дозволені дії та підвищувати адаптивність системи до загроз.

4. Наскрізне шифрування. Забезпечення шифрування даних як під час зберігання (at rest), так і під час передачі (in transit), із використанням незалежної служби керування ключами (KMS), дозволяє дотримуватись вимог безпеки навіть у разі компрометації окремих вузлів.

5. Журналювання та аудит у реальному часі. Запровадження розподілених механізмів журналювання подій з гарантованою доставкою до центральної системи аудиту дозволяє своєчасно виявляти аномалії, аналізувати спроби несанкціонованого доступу та підвищувати загальну стійкість системи до внутрішніх загроз.

Застосування описаних підходів у рамках запропонованої архітектури дозволяє підвищити рівень інформаційної безпеки без істотного зниження продуктивності або ускладнення масштабування. Саме комбінація децентралізованого зберігання, динамічного управління доступом і наскрізного контролю на рівні кожного компонента є визначальною для забезпечення стійкості до загроз у сучасних критичних розподілених системах.

Висновки. У ході дослідження проаналізовано архітектурні та функціональні особливості сучасних систем керування базами даних, зосереджених на підтримці serverless- та edge-обчислень. Розглянуто актуальні СКБД нового покоління – SurrealDB, Xata, Turso, Dolt та EdgeDB – з позиції їхньої здатності забезпечувати захист даних у розподілених середовищах. Встановлено, що ці системи пропонують інноваційні підходи до обробки запитів, зберігання даних та контролю доступу, однак мають певні обмеження, пов’язані з конфігурацією політик безпеки, підтримкою шифрування та аудитом дій користувачів.

На основі проведеного аналізу запропоновано узагальнену архітектуру безпечної edge-орієнтованої СКБД, яка передбачає інтеграцію локальної обробки даних, гнучкого управління доступом, наскрізного шифрування та централізованого журналювання. Побудовано формальну модель оцінки ризиків для таких систем, що дозволяє кількісно оцінити вплив потенційних загроз на кожен структурний компонент.

Сформульовано ключові архітектурні захисні підходи, поєднання яких є доцільним для побудови сучасних захищених інформаційних систем з високими вимогами до надійності, масштабованості та стійкості до зовнішніх і внутрішніх загроз.

Результати дослідження можуть бути використані як основа для подальшого вдосконалення підходів до захисту даних у новітніх СКБД, зокрема при проєктуванні платформ для IoT, медицини, фінансових систем і критичної інфраструктури.

Список використаних джерел:

1. Sulieman N. A., Ricciardi Celsi L., Li W., Zomaya A., Villari M. Edge-oriented computing: A survey on research and use cases. Energies. 2022. Vol. 15, No. 2. P. 452.

2. Xie R., Tang Q., Qiao S., Zhu H., Yu F. R., Huang T. When serverless computing meets edge computing: Architecture, challenges, and open issues. IEEE Wireless Communications. 2021. Vol. 28, No. 5. P. 126–133.

3. Wang S., Zhao Y., Xie Y., Liu Z., Hou X., Zou Q., Wang H. Towards Reliable Vector Database Management Systems: A Software Testing Roadmap for 2030. arXiv preprint. 2025. arXiv:2502.20812.

4. Sabbioni A., Rosa L., Bujari A., Foschini L., Corradi A. DIFFUSE: A DIstributed and decentralized platForm enabling Function composition in Serverless Environments. Computer Networks. 2022. Vol. 210. Article ID: 108993.

5. Magham R. K. Cloud-native distributed databases: a comprehensive overview. Management. 2024. Vol. 15, No. 2. P. 60–74.

6. De Heus M., Psarakis K., Fragkoulis M., Katsifodimos A. Distributed transactions on serverless stateful functions. Proceedings of the 15th ACM International Conference on Distributed and Event-based Systems. 2021. P. 31–42.

7. Lengweiler D., Vogt M., Schuldt H. MMSBench-Net: Scenario-Based Evaluation of Multi-Model Database Systems. International Journal of Data Management and Analytics. 2023. Vol. 8, No. 3. P. 145–158.

8. Kim J., Kim C., Son B., Ryu J., Kim S. A study on Time-series DBMS Application for EdgeX-based lightweight edge gateway. 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2020. P. 1795–1798.

9. Huang H., Zhang J., Hu J., Fu Y., Qin C. Research on distributed dynamic trusted access control based on security subsystem. IEEE Transactions on Information Forensics and Security. 2022. Vol. 17. P. 3306–3320.

10. Mansouri Y., Prokhorenko V., Babar M. A. An automated implementation of hybrid cloud for performance evaluation of distributed databases. Journal of Network and Computer Applications. 2020. Vol. 167. Article ID: 102740.

11. Zhang L., Pang K., Xu J., Niu B. JSON-based control model for SQL and NoSQL data conversion in hybrid cloud database. Journal of Cloud Computing. 2022. Vol. 11, No. 1. P. 23.

12. Goriparthi S. Streamlining API development: a comparative analysis of GraphQL and RESTful web services. Journal of Web Engineering and Services. 2023. Vol. 12, No. 4. P. 4587.

13. Enberg P., Tarkoma S., Rao A. Towards Database and Serverless Runtime Co-Design. Proceedings of the CoNEXT Student Workshop 2023. 2023. P. 9–10.

14. Katikeri R., Pepakayala A. N. R., Kuncham L., Barla R., Tarun K., Charan S., Vaid A. EVOLVE: Evaluation of Language-to-SQL Validity and Effectiveness – A Detailed Review Framework for Complex Text-to-SQL Queries. 2024 IEEE International Conference on Big Data (BigData). 2024. P. 1999–2004.

15. Voievodin Y., Rozlomii I., Yarmilko A. Approach to Evaluate Scheduling Strategies in Container Orchestration Systems. Modeling, Control and Information Technologies: Proceedings of the International Scientific and Practical Conference. 2023. No. 6. P. 292–295.

16. Voievodin Y. V., Rozlomii I. O. Advanced software framework for comparing balancing strategies in container orchestration systems. Proceedings of the International Scientific Conference «DOORS». 2024. April. P. 60–69.

References:

1. Sulieman, N. A., Ricciardi Celsi, L., Li, W., Zomaya, A., & Villari, M. (2022). Edge-oriented computing: A survey on research and use cases. *Energies, 15*(2), 452. https://doi.org/10.3390/en15020452

2. Xie, R., Tang, Q., Qiao, S., Zhu, H., Yu, F. R., & Huang, T. (2021). When serverless computing meets edge computing: Architecture, challenges, and open issues. *IEEE Wireless Communications, 28*(5), 126–133. https://doi.org/10.1109/MWC.001.2000458

3. Wang, S., Zhao, Y., Xie, Y., Liu, Z., Hou, X., Zou, Q., & Wang, H. (2025). Towards Reliable Vector Database Management Systems: A Software Testing Roadmap for 2030. *arXiv Preprint*. arXiv:2502.20812

4. Sabbioni, A., Rosa, L., Bujari, A., Foschini, L., & Corradi, A. (2022). DIFFUSE: A DIstributed and decentralized platForm enabling Function composition in Serverless Environments. *Computer Networks, 210*, 108993. https://doi.org/10.1016/j.comnet.2022.108993

5. Magham, R. K. (2024). Cloud-native distributed databases: A comprehensive overview. *Management, 15*(2), 60–74.

6. De Heus, M., Psarakis, K., Fragkoulis, M., & Katsifodimos, A. (2021). Distributed transactions on serverless stateful functions. In *Proceedings of the 15th ACM International Conference on Distributed and Event-based Systems* (pp. 31–42). https://doi.org/10.1145/3465481.3469195

7. Lengweiler, D., Vogt, M., & Schuldt, H. (2023). MMSBench-Net: Scenario-Based Evaluation of Multi-Model Database Systems. *International Journal of Data Management and Analytics, 8*(3), 145–158.

8. Kim, J., Kim, C., Son, B., Ryu, J., & Kim, S. (2020). A study on Time-series DBMS Application for EdgeX-based lightweight edge gateway. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1795–1798). IEEE. https://doi.org/10.1109/ICTC49870.2020.9289193

9. Huang, H., Zhang, J., Hu, J., Fu, Y., & Qin, C. (2022). Research on distributed dynamic trusted access control based on security subsystem. *IEEE Transactions on Information Forensics and Security, 17*, 3306–3320. https://doi.org/10.1109/TIFS.2022.3171182

10. Mansouri, Y., Prokhorenko, V., & Babar, M. A. (2020). An automated implementation of hybrid cloud for performance evaluation of distributed databases. *Journal of Network and Computer Applications, 167*, 102740. https://doi.org/10.1016/j.jnca.2020.102740

11. Zhang, L., Pang, K., Xu, J., & Niu, B. (2022). JSON-based control model for SQL and NoSQL data conversion in hybrid cloud database. *Journal of Cloud Computing, 11*(1), 23. https://doi.org/10.1186/s13677-021-00270-y

12. Goriparthi, S. (2023). Streamlining API development: A comparative analysis of GraphQL and RESTful web services. *Journal of Web Engineering and Services, 12*(4), 4587.

13. Enberg, P., Tarkoma, S., & Rao, A. (2023). Towards Database and Serverless Runtime Co-Design. In *Proceedings of the CoNEXT Student Workshop 2023* (pp. 9–10).

14. Katikeri, R., Pepakayala, A. N. R., Kuncham, L., Barla, R., Tarun, K., Charan, S., & Vaid, A. (2024). EVOLVE: Evaluation of Language-to-SQL Validity and Effectiveness – A Detailed Review Framework for Complex Text-to-SQL Queries. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 1999–2004). IEEE.

15. Voievodin, Y., Rozlomii, I., & Yarmilko, A. (2023). Approach to Evaluate Scheduling Strategies in Container Orchestration Systems. In *Modeling, Control and Information Technologies: Proceedings of the International Scientific and Practical Conference* (No. 6, pp. 292–295).

16. Voievodin, Y. V., & Rozlomii, I. O. (2024). Advanced software framework for comparing balancing strategies in container orchestration systems. In *Proceedings of the International Scientific Conference «DOORS»* (April, pp. 60–69).