УДК 004.056.5:004.652

МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ БАЗАМИ ДАНИХ

Гамза С. С.[1]; Нестеров Ю. М.[2]
[1, 2]Національний університет «Одеська політехніка»
Україна, Одеса
[1]s.gamza@gmail.com; [2]nesterov@op.edu.ua

Анотація. *У роботі розглянуто основні механізми захисту інформації в системах керування базами даних, зокрема контроль доступу, шифрування, аудит та резервне копіювання. Акцентовано увагу на багаторівневій архітектурі безпеки та сучасних практиках забезпечення конфіденційності, цілісності й доступності даних. Запропоновано підходи до реалізації політик безпеки у поширених СУБД.*
Ключові слова: *інформаційна безпека; бази даних; контроль доступу; шифрування; аудит.*

Вступна частина. У сучасних умовах цифрової трансформації суспільства питання захисту інформації набуває особливого значення. Стрімке зростання обсягів даних, активне впровадження хмарних технологій, розподілених обчислень і мобільних застосунків створюють нові виклики у сфері інформаційної безпеки. Бази даних є основою будь-якої інформаційної системи, адже саме в них зберігається критично важлива інформація – персональні дані користувачів, фінансові записи, комерційна таємниця, результати наукових досліджень тощо. Втрата, пошкодження або несанкціонований доступ до таких даних може мати серйозні наслідки для функціонування організацій і держави в цілому [1].

Актуальність теми зумовлена тим, що із розвитком інформаційних технологій зростає і кількість кіберзагроз, спрямованих на системи управління базами даних (СУБД). Серед найпоширеніших загроз можна виділити несанкціонований доступ до даних, ін’єкції SQL-коду, зловмисне програмне забезпечення, соціальну інженерію, а також внутрішні помилки адміністраторів і користувачів. Зважаючи на це, захист інформації у базах даних є не просто технічною вимогою, а необхідною складовою стратегічної безпеки будь-якої організації.

Метою дослідження є аналіз і систематизація механізмів захисту інформації в сучасних системах керування базами даних, а також визначення найефективніших підходів до запобігання загрозам та забезпечення цілісності даних.

Основна частина. Інформаційна безпека баз даних – це сукупність організаційних, технічних та програмних заходів, спрямованих на захист даних від несанкціонованого доступу, модифікації, знищення або розголошення. Її основною метою є гарантування збереження та достовірності інформації, забезпечення доступності даних для авторизованих користувачів і запобігання будь-яким спробам порушення цілісності бази даних.

Ключовими принципами інформаційної безпеки вважаються складові так званої «CIA-тріади» (Confidentiality, Integrity, Availability): конфіденційність (Confidentiality) означає обмеження доступу до даних лише для уповноважених осіб і захист від несанкціонованого ознайомлення; цілісність (Integrity) передбачає збереження точності, узгодженості та достовірності даних протягом усього життєвого циклу; доступність (Availability) гарантує, що авторизовані користувачі мають змогу отримати доступ до інформації у потрібний момент часу без необґрунтованих затримок [2].

Дотримання принципів CIA є основою побудови будь-якої стратегії захисту баз даних, незалежно від типу СУБД чи обраної архітектури системи.

Усі загрози безпеці баз даних умовно поділяються на зовнішні та внутрішні.

Зовнішні загрози – це кібератаки, шкідливе програмне забезпечення, мережеві злами, фішинг, DDoS-атаки, спроби SQL-ін'єкцій та інші дії, що походять поза межами організації.

Внутрішні загрози – це несанкціоновані дії співробітників, помилки адміністраторів, зловживання привілеями або порушення політик безпеки. Статистика свідчить, що внутрішні інциденти часто становлять більшу небезпеку, ніж зовнішні атаки, оскільки відбуваються у межах системи й важче виявляються.

Для побудови ефективної системи безпеки у базах даних застосовуються різні моделі захисту інформації, серед яких найвідомішими є:

– модель Bell–LaPadula – орієнтована на забезпечення конфіденційності. Вона обмежує доступ до інформації на основі рівнів секретності, забороняючи читання або запис даних користувачами з нижчими привілеями;

– модель Biba – фокусується на забезпеченні цілісності даних, забороняючи запис у дані нижчого рівня або зміну інформації користувачами без належних прав;

– модель Clark–Wilson – базується на принципі «обмеження доступу через контрольовані програми» і спрямована на запобігання несанкціонованим модифікаціям;

– модель Role-Based Access Control (RBAC) – визначає доступ на основі ролей користувачів і є найпоширенішою у сучасних СУБД (MySQL, PostgreSQL, Oracle, SQL Server).

Важливою складовою теоретичних засад захисту є нормативно-правова база. У світовій практиці функціонують стандарти, які регламентують вимоги до систем безпеки інформації. ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, який визначає вимоги до створення системи захисту даних в організаціях. GDPR (General Data Protection Regulation) – загальний регламент ЄС про захист персональних даних, який встановлює правила обробки та зберігання інформації про користувачів. NIST SP 800-53 – американський стандарт, що визначає набір контролів безпеки для інформаційних систем і баз даних. Застосування цих стандартів забезпечує уніфікований підхід до побудови систем безпеки, підвищує довіру до інформаційних технологій та сприяє захисту даних на глобальному рівні.

Архітектура систем захисту інформації в СУБД являє собою комплексну багаторівневу структуру, що поєднує технічні, програмні та організаційні засоби для забезпечення конфіденційності, цілісності та доступності даних. Основна мета цієї архітектури – створити інтегроване середовище безпеки, у межах якого усі компоненти бази даних взаємодіють у спосіб, що мінімізує ризики несанкціонованого доступу або втрати інформації [3].

У сучасних СУБД логічна структура захисту передбачає поєднання таких ключових механізмів, як аутентифікація користувачів, авторизація дій, шифрування даних, аудит операцій і системи резервного копіювання. Всі ці елементи організовані у три основні рівні безпеки: фізичний, логічний та адміністративний, кожен з яких виконує власну функцію в єдиній архітектурі захисту. Усі три рівні архітектури перебувають у тісній взаємодії. Фізичний рівень створює основу для логічного, який, у свою чергу, реалізує політики, розроблені на адміністративному рівні. Важливу роль у цій взаємодії відіграє адміністратор бази даних, який забезпечує узгодженість дій між технічними засобами та організаційними процесами [4]. Ефективна архітектура системи захисту інформації передбачає не лише

впровадження технологій, а й постійний моніторинг, оновлення політик і реагування на потенційні інциденти безпеки.

Механізми захисту інформації в базах даних формують практичну основу системи безпеки. Вони включають комплекс технічних рішень і процедур, які запобігають несанкціонованому доступу, спотворенню або втраті даних. До найважливіших належать контроль доступу, шифрування, резервне копіювання та аудит дій користувачів.

Одним із базових механізмів є контроль доступу, який визначає, хто саме має право виконувати певні операції з даними. Він забезпечує розмежування прав користувачів і мінімізує ризик несанкціонованого використання ресурсів бази даних. У сучасних СУБД застосовуються різні моделі управління доступом, зокрема дискреційна, мандатна, ролева та атрибутна. Найбільш поширеною є ролева модель, оскільки вона дозволяє групувати користувачів за функціональними обов'язками та надавати права на основі ролей.

Іншим ключовим засобом безпеки є шифрування даних, яке гарантує їх конфіденційність навіть у разі перехоплення чи несанкціонованого доступу. Воно може бути реалізоване як на рівні фізичних носіїв, так і на рівні окремих таблиць або полів. Симетричне шифрування (наприклад, за алгоритмом AES) використовується для швидкого захисту великих обсягів інформації, тоді як асиметричне (RSA) – для більш безпечної передачі ключів і автентифікації. На практиці застосовуються також гібридні підходи, що поєднують переваги обох методів. У PostgreSQL і Oracle реалізовано шифрування з'єднань за допомогою SSL/TLS, а Microsoft SQL Server підтримує технологію Transparent Data Encryption, яка забезпечує автоматичне шифрування всіх файлів бази даних.

Ще одним важливим механізмом є резервне копіювання, яке забезпечує збереження даних у випадках технічних збоїв або кібератак. Системи резервного копіювання дають змогу створювати як повні, так і інкрементальні копії бази даних. Автоматизовані інструменти, наприклад pg_dump у PostgreSQL або SQL Server Agent у Microsoft SQL Server, дозволяють проводити резервування за розкладом та зберігати копії у віддалених сховищах. Ефективна стратегія резервування завжди поєднується з планом відновлення після збоїв (Disaster Recovery Plan), що визначає послідовність дій для швидкого відновлення працездатності системи.

Не менш важливим компонентом є аудит і моніторинг, які забезпечують контроль за діяльністю користувачів та своєчасне виявлення підозрілої активності. Аудит фіксує всі значущі події – від входу користувача в систему до виконання критичних запитів. Залежно від мети він може бути обліковим, операційним або безпековим.

Таким чином, механізми захисту інформації в базах даних формують цілісну систему, у якій кожен елемент виконує свою роль: контроль доступу запобігає несанкціонованим діям, шифрування забезпечує конфіденційність, резервування гарантує відновлення після збоїв, а аудит створює умови для прозорості та підзвітності. Комплексне застосування цих засобів дозволяє досягти високого рівня інформаційної безпеки та стабільності роботи сучасних систем керування базами даних.

Для підтвердження теоретичних положень і демонстрації ефективності розглянутих механізмів безпеки було проведено практичне дослідження на основі системи керування базами даних PostgreSQL, яка належить до найпоширеніших реляційних СУБД із відкритим вихідним кодом. PostgreSQL відома своєю надійністю, високим рівнем безпеки та широким набором вбудованих засобів захисту, що робить її зручною платформою для експериментальної перевірки.

Одним із перших етапів практичної реалізації було налаштування ролевої моделі доступу. Для цього були створені окремі ролі з різними рівнями привілеїв: адміністратор бази даних (admin), розробник (developer) і користувач (user). Адміністратор мав повні права на створення, зміну та видалення об'єктів бази даних, тоді як розробник міг працювати лише в межах певної схеми, а звичайний користувач – виконувати операції вибірки даних без можливості модифікації. Такий підхід забезпечив розмежування доступу відповідно до принципу «мінімально необхідних привілеїв». Політики авторизації реалізовувалися за допомогою команд GRANT і REVOKE, які дозволяють гнучко керувати дозволами для кожного користувача.

Другим етапом стало впровадження механізмів шифрування даних. У PostgreSQL реалізовано кілька рівнів захисту інформації – від шифрування під час передавання даних до шифрування окремих полів таблиць. Для забезпечення захищеного з'єднання між клієнтом і сервером використовувалося SSL/TLS-шифрування, яке запобігає перехопленню переданих даних у мережі. На наступному етапі було проведено аудит дій користувачів; для цього використано модуль pgaudit.

Результати проведених експериментів показали, що комплексне застосування механізмів безпеки забезпечує високий рівень захисту даних у PostgreSQL. Ефективна інтеграція цих механізмів дозволяє створити стійку до загроз систему, здатну гарантувати конфіденційність, цілісність і доступність інформації навіть за умов підвищених навантажень і спроб несанкціонованого доступу.

Висновки. Побудова ефективної системи захисту інформації в СУБД вимагає комплексного підходу, який поєднує технічні рішення, організаційні заходи й постійний моніторинг безпеки. Лише завдяки інтеграції всіх рівнів захисту можна гарантувати стабільність роботи баз даних і надійність зберігання інформації у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Iqbal, A., Khan, S. U., Niazi, M., Humayun, M., Us Sama, N., & Ali Khan, A. (2024). *Advancing database security: A comprehensive systematic mapping study of potential challenges*. *Wireless Networks*, 30, 1234-1254.

[2] Parmar, V., Patel, D., & Padghawala, M. (2023). *Current trends in database security: A comprehensive review. Scientific and Practical Cyber Security Journal*, 9(3), 45-67.

[3] Mailewa, A. (2022). *Mechanisms and techniques to enhance the security of big database systems*. *Procedia Computer Science*, 200, 152-161.

[4] Khan, H. S., Mustufa, A., & Irshad, A. (2025). *Security challenges and solutions in DBMS: A theoretical analysis*. *Scientific & Practical Cyber Security Journal*, 9(3), 78-87.

Gamza S. S., Nesterov Yu. M.

Information security mechanisms in database management systems

Abstract. *The paper explores key information security mechanisms in database management systems, including access control, encryption, auditing, and backup. Particular attention is paid to the multi-level security architecture (physical, logical, and administrative levels) and modern practices for ensuring data confidentiality, integrity, and availability. The study outlines approaches to implementing security policies in popular DBMS platforms.*

Keywords: *information security; databases; access control; encryption; auditing*.