

О.М. Ткаченко
Д.В. Богінський

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ІНФОРМАЦІЙНИХ СИСТЕМАХ УПРАВЛІННЯ БАЗОЮ ДАНИХ

Вінницький національний технічний університет

Анотація

У сучасних інформаційних системах управління базами даних (БД) питання безпеки є критично важливим. Захист даних від несанкціонованого доступу, витоків, кібератак та внутрішніх загроз є пріоритетом для організацій, що працюють з великими обсягами інформації. У цій роботі розглядаються основні методи забезпечення безпеки БД, зокрема аутентифікація, контроль доступу, шифрування даних, резервне копіювання та засоби моніторингу активності користувачів. Також проаналізовано сучасні виклики та перспективи розвитку технологій кібербезпеки у сфері управління БД.

Ключові слова: інформаційна безпека, захист даних, управління базами даних, кібербезпека, аутентифікація, контроль доступу, шифрування, резервне копіювання, моніторинг активності.

Abstract

In modern database management systems (DBMS), security is a critical issue. Protecting data from unauthorized access, leaks, cyberattacks, and insider threats is a priority for organizations that work with large amounts of information. This paper examines the main methods of ensuring database security, including authentication, access control, data encryption, backup, and user activity monitoring tools. It also analyzes current challenges and prospects for the development of cybersecurity technologies in the field of database management.

Keywords: information security, data protection, database management, cybersecurity, authentication, access control, encryption, backup, activity monitoring.

Вступ

У сучасних умовах цифрової трансформації безпека інформаційних систем управління базами даних відіграє ключову роль у збереженні конфіденційності, цілісності та доступності даних [1]. Зростання обсягів інформації, активне використання хмарних технологій, а також постійні загрози з боку кіберзлочинців зумовлюють необхідність розробки та впровадження ефективних механізмів захисту даних[2].

Основними викликами в цій сфері є ризик несанкціонованого доступу, виток конфіденційної інформації, маніпуляції з даними та кібератак. Відповідно, захист інформаційних систем потребує комплексного підходу, що включає аутентифікацію та авторизацію користувачів, багаторівневий контроль доступу, шифрування даних, резервне копіювання, моніторинг активності та використання засобів виявлення та запобігання загрозам.

У цій роботі розглядаються основні методи та технології забезпечення безпеки БД, їхнє практичне застосування, а також сучасні тенденції у сфері кібербезпеки для захисту інформаційних ресурсів підприємств та організацій.

Результати дослідження

Забезпечення безпеки та захисту даних в інформаційних системах управління базами даних (СУБД) є критично важливим для збереження конфіденційності, цілісності та доступності інформації. Основні аспекти захисту даних у СУБД включають забезпечення доступу до бази даних лише для авторизованих користувачів[3], встановлення правил та обмежень щодо доступу користувачів до певних даних або функцій системи, захист даних під час зберігання та передачі шляхом їхнього шифрування[4], створення копій бази даних для відновлення інформації у разі втрати або пошкодження, відстеження дій користувачів та системних процесів для виявлення та запобігання потенційним загрозам.

Реалізація комплексного підходу до безпеки баз даних допомагає мінімізувати ризики та забезпечити надійний захист інформаційних ресурсів організації.

Для забезпечення безпеки та захисту даних в інформаційних системах управління базами даних (СУБД) необхідно враховувати такі аспекти: види загроз безпеці інформації (несанкціонований доступ до даних сторонніми особами, несанкціоновані зміни або знищення даних, блокування доступу до даних для авторизованих користувачів), методи захисту інформації (розробка політик безпеки, навчання персоналу, контроль доступу, використання антивірусного ПЗ, мережових екранів, систем виявлення вторгнень, шифрування даних, електронні підписи для забезпечення цілісності та автентичності інформації) і правове регулювання захисту інформації (дотримання законодавчих норм та стандартів у сфері інформаційної безпеки, розробка внутрішніх нормативних документів щодо захисту даних).

Висновки

Забезпечення безпеки та захисту даних в інформаційних системах управління базами даних є ключовим фактором стабільної та ефективної роботи будь-якої організації. З огляду на зростання кіберзагроз, необхідно застосовувати комплексний підхід до захисту інформації, що включає організаційні, технічні та правові заходи.

До основних методів безпеки належать багаторівнева аутентифікація, контроль доступу, шифрування даних, резервне копіювання, моніторинг активності користувачів та використання сучасних антивірусних та мережових рішень. Впровадження таких заходів мінімізує ризики несанкціонованого доступу, витоку конфіденційної інформації та її пошкодження.

Окрім цього, важливим аспектом є дотримання міжнародних стандартів інформаційної безпеки, а також адаптація систем управління базами даних до нових загроз та викликів. Подальші дослідження у цій сфері повинні бути спрямовані на вдосконалення технологій кіберзахисту, розвиток штучного інтелекту для автоматичного виявлення загроз та інтеграцію безпекових механізмів у хмарні середовища.

Таким чином, ефективне управління безпекою баз даних є не лише технічною необхідністю, а й стратегічним пріоритетом для сучасних організацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies "Security in Computing" – Addison-Wesley Professional, 2023 – 1040 p
2. William Stallings, Lawrie Brown "Computer Security: Principles and Practice" – Pearson, 2017 – 800 p

3. Берко А.Ю., Верес О.М., Пасічник В.В. "Системи баз даних та знань. Книга 2. Системи управління базами даних та знань" – 680 с – Львів, 2013
4. William Stallings "Network Security Essentials: Applications and Standards" – Pearson, 2016 – 432 p

Богінський Денис Володимирович – студент групи ІПІ-24М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: denisboginskij137@gmail.com

Ткаченко Олександр Миколайович – доцент, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: ant@vntu.edu.ua

Bohinskiy Denys Volodymyrovych – student of the ІPI-24M group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, email: denisboginskij137@gmail.com

Supervisor: Tkachenko Oleksandr Mykolaiovych – Docent of Program Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ant@vntu.edu.ua