**УДК 004.49**
**Б. Петльовий**
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

## СПОСОБИ ТА ЗАСОБИ ЗАХИСТУ БАЗ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

**UDC 004.49**
**B. Petlovyi**

## METHODS AND TOOLS TO PROTECT DATABASES FROM UNAUTHORIZED ACCESS

Захист баз даних від несанкціонованого доступу є одним із ключових аспектів інформаційної безпеки, що забезпечує конфіденційність, цілісність та доступність даних. У сучасному світі інформаційних технологій бази даних стають важливим елементом роботи різних організацій, а ризики втрати чи компрометації даних зростають разом із розвитком кіберзагроз. У зв'язку з цим важливим є дослідження способів та засобів захисту баз даних від потенційних атак.

Одним із найефективніших підходів до захисту є використання механізмів аутентифікації та авторизації. Автентифікація забезпечує перевірку особи користувача, який запитує доступ до бази даних, тоді як авторизація встановлює рівні доступу до конкретних ресурсів системи. Сучасні технології пропонують багатофакторну аутентифікацію MFA, яка поєднує кілька елементів для підвищення рівня безпеки.

Важливим способом захисту є шифрування даних, що забезпечує збереження конфіденційності інформації навіть у разі її перехоплення. Використання симетричних алгоритмів таких як AES, DES та асиметричних алгоритмів шифрування до прикладу RSA, дає змогу захистити як дані, що зберігаються, так і ті, що передаються в мережі. Особливого значення набуває технологія управління ключами SSL/TLS, яка гарантує надійне зберігання та обмін ключами.

Моніторинг активності в базах даних і аудит дозволяють своєчасно виявляти підозрілі дії, такі як несанкціоновані спроби доступу чи аномалії в поведінці користувачів. Аналітичні системи на основі штучного інтелекту здатні такі як IBM Guardium, Splunk, Elastic Security, та інші здатні розпізнавати складні шаблони атак і забезпечувати оперативну реакцію на інциденти. Системи захисту баз даних також використовують методи виявлення вторгнень, які базуються на аналізі мережевого трафіку та поведінкових характеристик користувачів.

Таким чином, ефективний захист баз даних від несанкціонованого доступу є багаторівневим процесом, що включає поєднання технічних, організаційних та процедурних заходів. Постійний розвиток інформаційних технологій та кіберзагроз вимагає впровадження новітніх підходів до безпеки, що базуються на інноваційних технологіях та інструментах.

**Література**

1. Bishop, M., & Venkatramanayya, S. Introduction to Computer Security. Addison-Wesley, 2022.
2. Kim, H., & Solomon, M. G. Database Security and Auditing. Jones & Bartlett Learning, 2023.
3. Elmasri, R., & Navathe, S. Fundamentals of Database Systems. Pearson, 2021.
4. Mirkovic, J., & Reiher, P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM Computing Surveys, 2022.
5. O’Reilly Media. Defensive Security Handbook: Best Practices for Securing Systems and Organizations, 2023.