https://orcid.org/0000-0002-5080-1856
https://orcid.org/0000-0003-3370-4584

УДК 004.056

Ю.М. ЛИСЕЦЬКИЙ[*], Д.Й. КАЛБАЗОВ[**]

ІНФОРМАЦІЙНА БЕЗПЕКА КОРПОРАТИВНИХ БАЗ ДАНИХ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна
[**]ТОВ «Інформаційні спеціалізовані системи», м. Київ, Україна

Анотація. *Щодня компанії по всьому світу збирають та генерують велику кількість даних. Тепер інформація прийняла цифрову форму та зберігається в автоматизованих цифрових базах даних, використання яких дає можливість обробляти великі масиви даних, що були важкодоступними для обробки раніше. Важливим для економічної безпеки підприємства є захист корпоративних баз даних та інформації в них, який містить фізичний захист; захист продуктивності та їх моніторинг; захист даних від знищення чи пошкодження; контроль доступу; облік нових даних, які з'являються в інфраструктурі. З огляду на те, що до баз даних мають доступ користувачі різних типів та рівнів доступу (внутрішні користувачі, системні адміністратори, підрядники та партнери, Machine-to-Machine комунікації), вони можуть зловживати наданим доступом у таких напрямах: зловживання та використання надмірних прав доступу; зловживання об'єктивно необхідними правами доступу; зловживання правами, які не використовуються. Слабо контрольований процес видачі прав доступу до баз даних, як правило, формує надмірні права доступу, що завжди створює надлишковий ризик для інформаційної безпеки. До заходів безпеки відносять, по суті, запровадження процесу видачі та обліку виданих доступів, видачу мінімально необхідних прав доступу та впровадження механізму контролю й блокування виданих доступів. У статті розглянуто такі види загроз для баз даних, як SQL Injections і NoSQL injection атаки; низький рівень деталізації подій баз даних; витік через резервні копії; вразливості та налаштування; DDoS-атаки і методи протидії цим загрозам. Наведено, що найбільш дієвим способом захисту баз даних є впровадження Imperva DBS та Imperva WAF – спеціалізованих програмно-апаратних комплексів, розроблених для захисту баз даних. Застосування Imperva DBS допоможе вирішити усі ключові завдання захисту баз даних і забезпечить повну видимість та контроль їх використання в інфраструктурі підприємства.*

Ключові слова: *бази даних, права доступу, загрози, атаки, захист даних, методи протидії.*

Abstract. *Every day, companies all over the world collect and generate a large amount of data. Now information is digital and is stored in automated digital databases, the use of which allows for processing large amounts of data that previously were difficult to process. Protecting corporate databases and the information within them is essential for economic security. It includes their physical protection, productivity assurance and monitoring, data protection from destruction or damage, access control, and recording of new databases appearing in the infrastructure. However, since users of different types and levels of access (internal users, system administrators, contractors, partners, and M2M communications) have access to databases, they can abuse their access rights in several ways. These may be an abuse of excessive, objectively necessary, or non-used rights. As a rule, an inefficiently controlled process of granting access rights creates excessive access rights which in turn may cause new information security risks. Security measures include implementing an access management process, granting minimally necessary access rights, and implementing a mechanism to control and block the given access rights. This article discusses such threats to databases as SQL Injections and NoSQL injection attacks, insufficient detailing of events in databases, backup leaks, vulnerabilities and configurations, DDoS attacks, and methods to counter these threats. The most effective way to protect databases is to implement specialized software and hardware complexes such as Imperva DBS and Imperva WAF developed for database protection. The use of*

ISSN 1028-9763. Математичні машини і системи. 2023. № 3

Imperva DBS will help to solve all the key tasks of database protection and provide complete visibility and control over their usage in the enterprise infrastructure.
Keywords: *databases, access rights, threats, attacks, data protection, countermeasures.*

DOI: 10.34121/1028-9763-2023-3-31-37

1. Вступ

В епоху інформатизації та діджиталізації захист інформації – одне з важливих завдань, а цифрові дані – це критичний актив сучасного підприємства. Щодня компанії по всьому світу збирають та генерують велику кількість даних. У 2020 р. об'єм створених та спожитих даних у світі складає 64 ZBytes (зеттабайт), що становить 64 000 000 000 000 GB (64 трільярди GB) [1]. У 2021 р. прогнозують ріст до 79 ZBytes, а у 2025 р. – 181 ZBytes, тобто у 3 рази більше, ніж у 2020 р. (рис. 1). Сюди відносяться, в першу чергу, медіа-контент, big-data та корпоративні дані.

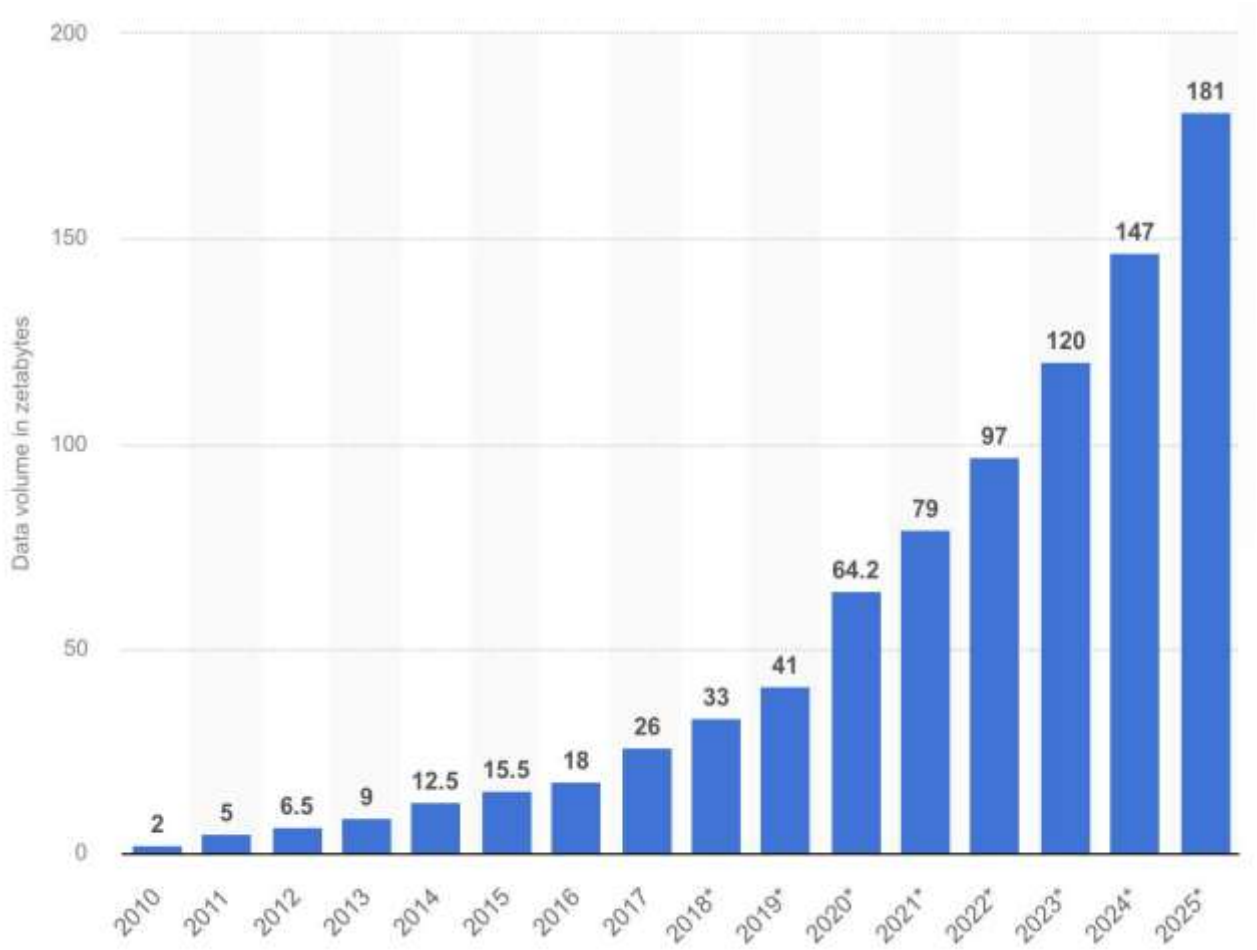

Рисунок 1 – Об'єми даних у глобальній мережі

Таке динамічне зростання обсягу даних формує нові завдання для підприємств: їх зберігання та захист [2]. Проте не завжди підприємства усвідомлюють важливість захисту власних даних.

Метою статті є розгляд ролі автоматизованих баз даних (БД) у роботі підприємства, основних загроз, пов'язаних з їх захистом та методами протидії.

2. Особливості використання корпоративних БД

У доцифрову епоху носіями інформації були паперові носії, що зберігалась в архівах. Тепер інформація прийняла цифрову форму й зберігається в автоматизованих цифрових БД. Серед них найбільш відомі Oracle, MS SQL, MySQL, PostgreSQL, MongoDB та ін.

Використання автоматизованих БД дає можливість обробляти великі масиви даних, які були важкодоступними для обробки раніше. Підприємство в короткий термін може підготувати та опрацювати дані по продажах за тривалий період по всій номенклатурі товарів всім замовникам та відділенням. Без використання БД така аналітика потребує значних трудовитрат. Використання БД значно підвищує ефективність підприємства та забезпечує цілий пласт даних для подальшого аналізу й обробки.

Без використання автоматизованих БД не обходиться жодна IT-система обліку та управління підприємством. Як наслідок, БД зайняли ключове місце в бізнес-процесах підприємства будь-якого масштабу (рис. 2). До переліку основних застосувань БД можна віднести:

- системи обліку контрагентів, контрактів та замовлень;
- облік товарів;
- історію та облік транзакцій;
- систему оформлених замовлень;
- систему управління продажами;
- кадровий облік;
- управління виробництвом.

Рисунок 2 – Приклад застосування БД в інфраструктурі підприємства

Перелік доповнюється масою спеціалізованих застосувань, таких, як складський облік, логістика, управління транспортом, управління магазином, моніторинг продуктивності обладнання та ін. Де-факто, усі операції підприємства, від дзвінка потенційному замовнику до звільнення працівника, від прийняття товару на склад до відвантаження його замовнику, фіксуються у корпоративних БД, а інформація використовується на наступних етапах роботи.

Отже, у процесі бізнес-активності підприємство генерує велику кількість цифрових даних на усіх етапах реалізації своєї бізнес-моделі.

3. Захист корпоративних БД

Важливим для економічної безпеки підприємства є захист корпоративних БД та інформації в них. Захист інформації – це основне завдання процесу управління БД, який у англомовних джерелах називають database security. Захист БД містить такі компоненти (рис. 3):

1) фізичний захист БД;
2) захист продуктивності БД та їх моніторинг;
3) захист даних у БД від знищення чи пошкодження;
4) контроль доступу;
5) облік нових БД, які з'являються в інфраструктурі.

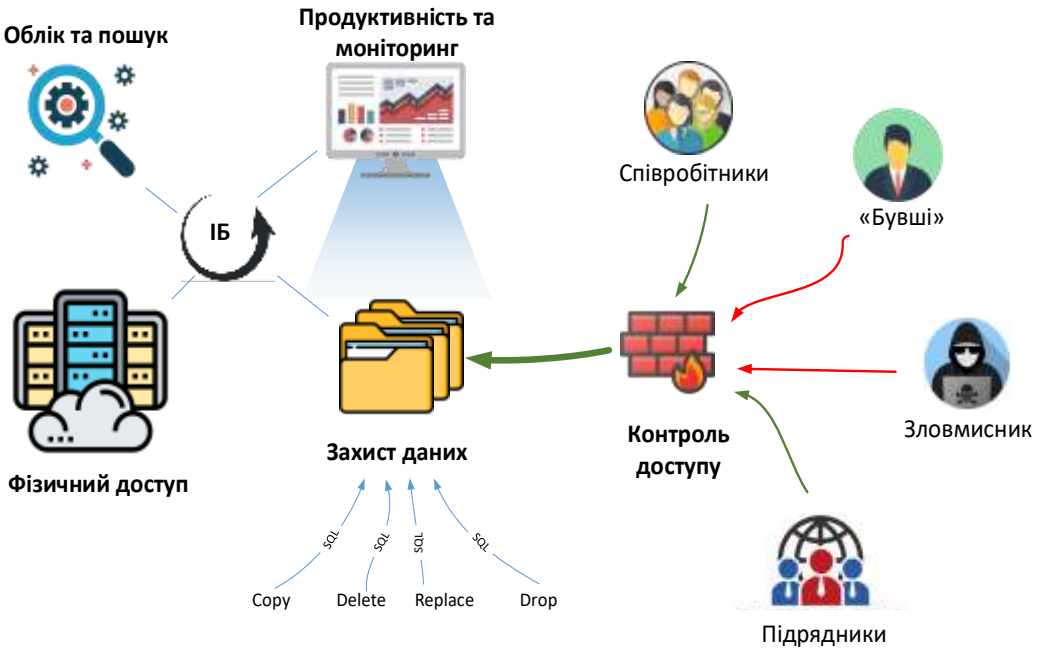

Рисунок 3 – Компоненти інформаційної безпеки БД

У першу чергу, захист БД складається з фізичного захисту. Фізичний доступ до БД повинен бути обмеженим та доступним тільки для авторизованого персоналу. З розвитком хмарних технологій цей компонент інформаційної безпеки (ІБ) втратив свою актуальність, адже питанням фізичного доступу до обладнання, де зберігається інформація, займається постачальник хмарних сервісів. Проте існує багато інших внутрішніх та зовнішніх загроз. Основні з них ми розглянемо далі.

3.1. Надмірні права доступу

До БД мають доступ користувачі різних типів та рівнів доступу. Серед них:

• *Внутрішні користувачі* – працівники, які мають доступ до БД напряму або через сторонні додатки.

• *Системні адміністратори* – як правило, мають повні права доступу, а кількість адміністраторів може сягати десятків людей, тому виникає проблема контролю дій адміністраторів, використання паролів доступу, видачі ти видалення прав доступу адміністраторам.

• *Підрядники та партнери,* серед яких аутсорсери, розробники програмного забезпечення (ПЗ), замовники, яким доступ до БД надається для розробки та тестування нового

ПЗ, оформлення замовлень дочірніми компаніями, самообслуговування on-line чи технічного супроводу БД.

• *Machine-to-Machine (M2M) комунікації* – комунікація між технологічними системами. Це впровадження мобільних додатків, on-line сервісів, взаємна інтеграція управлінських систем та ін. Характерною особливістю є використання API (Application Programming Interface).

Прикладом таких комунікацій є інтеграція інтернет-магазину зі складськими запасами, сервіс-деск із контакт-центром, мобільних додатків із системою управління підприємством. Більшість корпоративних даних обробляється з застосуванням M2M комунікацій (рис. 4).

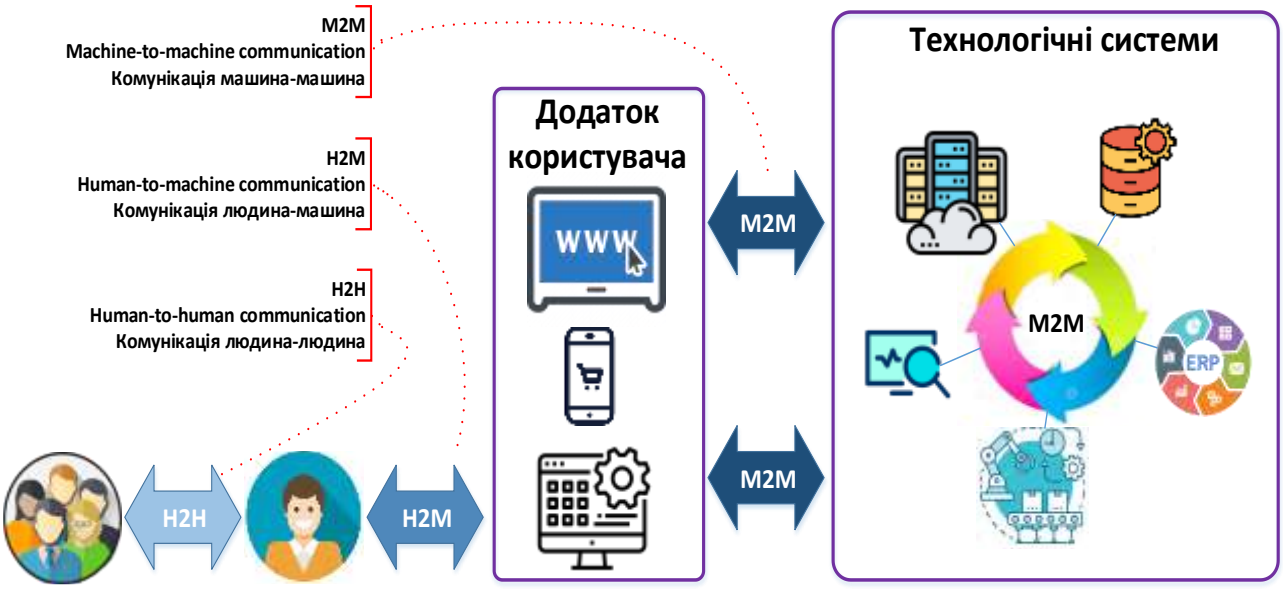

Рисунок 4 – Комунікативні моделі людина-людина, людина-машина, машина-машина

Користувачі можуть зловживати наданим доступом до БД у таких напрямах:

• зловживання та використання надмірних прав доступу;

• зловживання об'єктивно необхідними правами доступу;

• зловживання правами, які не використовуються.

Слабо контрольований процес видачі прав доступу до БД, як правило, формує надмірні права доступу, що завжди створює надлишковий ризик для інформаційної безпеки. Згідно зі статистикою, 80% атак корпоративних БД виконуються працівниками або екс-працівниками.

До заходів безпеки відносять, по суті, запровадження процесу видачі та обліку виданих доступів, видачу мінімально необхідних прав доступу та впровадження механізму контролю й блокування виданих доступів.

3.2. SQL Injections

SQL Injections – це вид атаки, при якому зловмисний SQL-код вбудовується в веб-додатки або вставляється зловмисником у текстові поля-форми на веб-сайті (для заповнення ПІБ, № телефону, e-mail тощо) [3].

Без відповідного захисту такий SQL-код може бути переданий від frontend (веб-сайт, з яким працює користувач) до backend (внутрішня «сторона» веб-сайту) та викона-

ний. Кіберзлочинець може отримати необмежений доступ до бази та виконувати SQL-команди безпосередньо в БД, наприклад, видалити чи скопіювати базу.

Розділяють два види атак:

• SQL-injection атаки, спрямовані на традиційні БД;

• NoSQL-injection атаки, спрямовані на big data БД.

Як протидію визначають:

• використання Stored Procedure та API замість прямих SQL-команд [4];

• впровадження MVC (Model-View-Controller) архітектури [5];

• впровадження фаєрволу БД Imperva Database Security [6].

3.3. Низький рівень деталізації подій БД

У першу чергу це важливо для банківської та фармацевтичної галузей, оскільки низький рівень відслідковування подій у БД представляє ризик невідповідності вимогам національних та міжнародних регуляторів стосовно обробки та зберігання конфіденційних даних. Всі транзакції БД повинні фіксуватись в автоматичному режимі з обов'язковим використанням сторонніх автоматизованих систем обстеження БД. Невиконання цих вимог формує значні ризики для БД на різних рівнях.

Способом зниження ризику в даному випадку є використання сторонніх автоматизованих систем аудиту БД (Audit Trail). Використання Imperva Database Security є найкращим технологічним рішенням галузі.

3.4. Витік через резервні копії

Хорошою практикою є впровадження процесу регулярного резервування БД. Не менш важливим є впровадження механізму перевірки цілісності резервних копій та можливості відновлення бази з резервної копії.

Важливо також забезпечити захист резервних копій БД. Як правило, резервні копії, навіть із найбільш критичними даними, залишаються не захищеними від викрадення, знищення чи внесення змін. Незахищеність резервних копій формує високий ризик інформаційної безпеки підприємства.

Методи протидії:

• шифрування і бази з резервних копій. Зберігання інформації в зашифрованому вигляді дозволяє забезпечити захист як продуктивної бази, так і її резервні копії. Imperva DBS – найкращий спосіб вирішити цю задачу;

• відстежувати та регламентувати доступ до БД та її резервних копій.

3.5. Вразливості та налаштування

Часто БД повністю незахищена в результаті некоректного налаштування. Більшість БД мають власні системні облікові записи та конфігураційні параметри за замовчуванням. Крім того, розробка програмного коду завжди супроводжується програмними дефектами. Для їх усунення компанії-виробники ПЗ випускають оновлення, патчі, інструкції щодо безпечного використання. Програмні дефекти формують вразливості ПЗ.

Зловмисники, як правило, досить кваліфіковані для того, щоб знати, які вразливості вбудовані в ту чи іншу БД та які налаштування системи можна використати для несанкціонованого доступу.

Методи протидії:

• видалення облікових записів, створених за замовчуванням;

• підвищення кваліфікації ІТ персоналу;

• використання Imperva DBS для захисту БД від використання вразливостей ПО, виявлення використання підозрілих облікових записів та ін.

3.6. Denial of Service

Досить «старий», але ефективний вид атаки, який сповільнює роботу БД або виводить її з ладу, не дає можливості виконувати продуктивну роботу [7].

У складних випадках для зупинки DDoS-атаки компанії вдаються до відключення БД від мережі інтернет. Це дозволить відновити роботу бази, проте включення інтернет-каналів знову активує DDoS-активність, що, у свою чергу, знову виводить базу з робочого стану.

Хоча DDoS-атака не має на меті викрадення чи пошкодження даних, така атака може дорого обійтись підприємству, адже неможливість роботи з даними робить БД безкорисною.

Методи протидії:

• використання Intrusion Detection System [8];

• постійний моніторинг активності БД, вивчення її вразливостей та блокування можливості їх використання;

• очистка трафіка за допомогою хмарних сервісів типу Imperva Cloud WAF (Web Application Firewall) [9].

4. Висновки

У статті розглянуто особливості використання корпоративних БД, основні існуючі загрози для них та методи протидії. Наведено, що найбільш дієвим способом захисту БД є впровадження Imperva DBS та Imperva WAF – спеціалізованих програмно-апаратних комплексів, розроблених для захисту БД, захисту веб-додатків, очистки нелегітимного трафіка, захисту від використання вразливостей.

Отже, застосування Imperva DBS допоможе вирішити усі ключові завдання захисту БД та забезпечить повну видимість і контроль використання БД у інфраструктурі підприємства.

СПИСОК ДЖЕРЕЛ

1. Total data volume worldwide 2010–2025 – Statista. URL: https://www.statista.com/statistics/871513/worldwide-data-created/ (дата звернення: 17.02.2023).
2. Лисецький Ю.М., Козаченко С.В. Програмно-визначені системи зберігання даних. Переваги і особливості. *Математичні машини і системи.* 2021. № 1. С. 17–23.
3. Что такое SQL-инъекции и как им противостоять? URL: https://highload.today/sql-inektsii/ (дата звернення: 18.02. 2023).
4. What is a Stored Procedure? – Definition from WhatIs.com. URL: https://www.techtarget.com/searchoracle/definition/stored-procedure#:~:text=A%20stored%20procedure%20is%20a,and%20shared%20by%20multiple%20programs (дата звернення: 18.02.2023).
5. The Model View Controller Pattern – MVC Architecture and Frameworks Explained. URL: https://www.freecodecamp.org/news/the-model-view-controller-pattern-mvc-architecture-and-frameworks-explained/ (дата звернення: 19.02.2023).
6. Imperva Database Security. URL: https://www.imperva.com/resources/datasheets/Imperva-Database-Security-Datasheet-2020.pdf (дата звернення: 19.02.2023).
7. Лисецкий Ю.М. Информационная безопасность: защита от DDoS-атак. *Системный анализ и информационные технологии*: сб. тезисов междунар. научн.-практ. конф. (Киев, 26–30 июня 2014 г.). К.: НТУ «КПИ», 2014. С. 405–406.
8. Intrusion Detection Systems: A Modern Investigation. URL: https://www.academia.edu/13787335/Intrusion_Detection_Systems_A_Modern_Investigation (дата звернення: 20.02.2023).
9. Imperva Web Application Firewall (WAF) | App & API Protection. URL: https://www.imperva.com/products/web-application-firewall-waf/ (дата звернення: 20.02. 2023).

Стаття надійшла до редакції 27.04.2023