УДК 004.056.53:004.732
DOI: 10.31673/2409-7292.2024.020006

**Легомінова С. В., Щавінський Ю. В.,
Будзинський О. В.**

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ БАЗ ДАНИХ

Стаття присвячена аналізу сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. Актуальність дослідження зумовлена збільшенням обсягу даних організацій і підприємств та зростаючою кількістю витоків конфіденційної інформації з корпоративних баз, які зафіксовані протягом останніх років. Актуальність підтверджена результатом прогнозу, проведеним в роботі за допомогою регресивного аналізу на основі статистичних даних. Аналіз публікацій виявив достатню кількість досліджень сучасних підходів до захисту корпоративних баз даних. Встановлено, що дослідження спрямовані на застосуванні штучного інтелекту, квантових обчислень та хмарних технологій у традиційних підходах до забезпечення безпеки баз даних. Особливістю сучасного підходу є використання стандартних бібліотек мови програмування Python при застосуванні штучного інтелекту в захисті корпоративних баз даних, що дозволяє автоматизувати процеси їх кіберзахисту. Разом з тим, при проведенні аналізу виявлено, що в основному дослідження науковцями проводяться в напрямку удосконалення захисту створених готових баз даних, без врахування вимог стандартів безпеки інформації на етапі проектування бази. Такий підхід створює в подальшому проблему корегування структури бази даних, що приведе до додаткових незапланованих затрат людських та матеріальних ресурсів. Для вирішення цієї проблеми в роботі запропонований превентивний підхід, який ґрунтується на поєднанні етапів створення бази та системи її захисту при проектуванні. Для цього розроблені концептуальні Entity-relationship моделі, суть яких полягає у встановленні сутностей організації захисту бази з їх атрибутами і зв'язками для побудови системи безпеки ще на етапі проектування.

Ключові слова: кібербезпека, корпоративні бази даних, захист інформації.

Вступ

Сьогодні інформація стала однією з найцінніших активів для бізнесу любої організації чи підприємства. Підтвердженням важливості цього твердження є зростання кількості кібератак на корпоративні бази з охопленням різних типів інформації: фінансові записи, відомості про клієнтів, дані про продажі і дослідження ринку, записи про співробітників тощо. Деколи інформація, що зберігається в корпоративних базах даних (КБД), або її частина, може складати комерційну таємницю, тому заволодіння такою інформацію і її використання в корисних цілях є метою зловмисників при проведенні кібератак. Разом з тим, не всі кібератаки призводять до витоку даних, деякі з них мають на меті спричинити збої в роботі, що може призвести до фінансових втрат та репутаційних збитків через відключення ключових операційних систем. Це змушує організації постійно адаптувати та удосконалювати свої стратегії та підходи до захисту інформації.

Постановка проблеми

Швидкі технологічні зміни роблять захист баз даних (БД) складним завданням. Географічна розгалуженість сучасних корпорацій на різних територіях, країнах і навіть континентах потребує нових підходів до забезпечення конфіденційності, доступності і цілісності інформації, яка зберігається в їхній базі. Впровадження Інтернет-речей (IoT) з обмеженими заходами безпеки і їх сумісність з системами управління базами даних (СУБД) робить бази даних вразливішими до атак. При цьому, основна проблема полягає в тому, що багато керівників організацій ще не до кінця розуміють, наскільки критичними є їхні дані.

Аналіз публікацій

Сьогодні, в умовах нестабільності сучасного інформаційного середовища та різноманітності кіберзагроз існує достатня кількість підходів до забезпечення кібербезпеки даних, які потребують постійного аналізу з метою наукового обгрунтування шляхів удосконалення кіберзахисту КБД.

Проведені науковцями дослідження проблем захисту корпоративних баз фіксують постійну еволюцію створення нових методів атак та нагальну потребу відпрацювання сучасних способів реагування на загрози. У своїх роботах [1–4] дослідники відзначають, що важливою складовою будь-якого надійного рішення безпеки КБД є методи виявлення

вторгнень (ID - Intrusion Detection), здатні виявляти аномальну поведінку додатків і користувачів на основі аналізу SQL-запитів шляхом групування запитів з іншими схожими за структурою. Такий підхід дозволяє використовувати алгоритми кластеризації для формування лаконічних профілів, що відображають нормальну поведінку користувачів баз в КБД. В подальшому це дозволяє виявити аномальну поведінку порівнянням профілів. Разом з тим, науковці відзначають, що при великих об'ємах бази даних для оперативного реагування на вторгнення існує потреба створення моделей на основі штучного інтелекту.

У статті [5] представлено уроки, отримані під час аналізу КБД, розроблених IBM Global Services (Австралія). Результати аналізу, проведеного співробітниками Австралійського науково-дослідного центру передового досвіду в галузі інформаційно-комунікаційних технологій виявили проблеми з базами даних, головним чином через відсутність зв'язків між різними таблицями даних. Фахівці вважають, що таких проблем можна уникнути, використовуючи варіант парадигми GQM (Goal-Question-Metric) для визначення ієрархії цілей та використовуючи моделі E-R (Entity-relationship model або Entity-relationship diagram) для виявлення проблем з існуючими базами даних і для проектування баз даних. При цьому, автори не прив'язують початок розробки бази даних з урахуванням розробки її безпеки.

В роботі [6] зазначено, що коли для роботи з БД використовуються корпоративні web-додатки, складно пов'язати конкретні операції щодо БД з конкретними співробітниками. Причиною цієї проблеми є відсутність застосування методів захисту інформації в базах даних на етапі її розробки в корпорації.

Аналіз публікацій зарубіжних і вітчизняних науковців виявив, що переважна більшість досліджень була зосереджена на проведенні власних пошуків ефективних способів захисту створених баз даних, в той час як порівняльного аналізу різних підходів недостатньо.

Мета дослідження полягає в проведенні аналізу сучасних підходів до організації захисту корпоративних баз даних та визначенні з них найбільш ефективних та перспективних, які забезпечать безпеку КБД з самого початку їх створення.

Виклад основного матеріалу

Корпоративні дані – це інформація, що генерується та збирається компанією під час її діяльності. Сучасні корпоративні бази даних зазвичай побудовані з використанням реляційної моделі даних, що базується на концепції таблиць, які містять рядки і стовпці. Однак, вони можуть також використовувати інші моделі даних, такі як NoSQL або NewSQL, залежно від специфіки бізнесу, обсягу даних та потреб користувачів. Незалежно від моделі, сьогодні актуальним завданням є забезпечення їх безпеки у зв'язку із різким збільшенням важливості інформації для організацій і підприємств, що зберігається у їх базах. Полювання за такою інформацією збільшується з кожним роком. Підтвердженням тому є статистичний аналіз витоків з корпоративних баз [7]. За результатами цього аналізу за допомогою пакету аналізу в Excel побудована діаграма, що показує різке зростання витоку інформації з КБД (рис.1).

Враховуючи нелінійність динаміки змін кількості витоків інформації з КБД, на основі цих статистичних даних можна, застосовуючи регресивний аналіз, спрогнозувати величину витоків на наступні роки за формулою (рис.1)

$$y = 171{,}52x^2 - 1346{,}4x + 3437{,}8 \qquad (1)$$

де y – кількість витоків інформації;

x – роки, на які здійснюється прогноз;

$171{,}52$; $1346{,}4$; $3437{,}8$ – коефіцієнти регресії поліноміальної регресивної моделі другого ступеню виду $y = ax^2 + bx + c$.

На якість регресивної моделі прогнозу вказує коефіцієнт детермінації R^2 (рис. 1.), розрахований за формулою [8]

© Легомінова, С. В., Щавінський, Ю. В., & Будзинський, О. В. (2024). Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. Сучасний захист інформації, 2(58), 50–58. https://doi.org/10.31673/2409-7292.2024.020006.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2} \quad (2)$$

де n – кількість результатів (років;
y_i – значення *i*-того результату в наборі;
$\hat{y}_i$ – апроксимоване регресійною моделлю значення *i*-того результату;
$\bar{y}$ – середнє значення з набору.

Рис.1. Динаміка змін кількості витоку інформації з корпоративних баз даних

Величина імовірності апроксимації (коефіцієнт детермінації R^2=*0,7893*) забезпечує достатній рівень достовірності прогнозу. Результат прогнозу з використанням формули регресії (1) наведений в таблиці 1.

Таблиця 1

Результат прогнозу витоку інформації

Рік	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026
Кількість витоків	1059	1429	1520	1677	2188	2369	2507	2320	1976	7149	11549	11980	14921	18206

Проведені розрахунки прогнозу кількості витоків інформації з баз даних на наступні три роки (рис. 1, табл.1) за допомогою поліноміальної регресивної моделі підтверджують актуальність пошуку ефективних підходів до захисту інформації в КБД.

Основні підходи до забезпечення безпеки корпоративних баз. Метою безпеки бази даних є захист конфіденційних даних і збереження конфіденційності, доступності та цілісності бази даних. Крім захисту інформації в базі даних, безпека бази даних повинна охоплювати також систему управління базами даних і пов'язані з нею програми, системи, фізичні та віртуальні сервери, мережеву інфраструктуру. Науковці у своїх дослідженнях розглядають традиційні підходи до захисту з метою їх удосконалення [9-10]:

- двофакторна і багатофакторна автентифікація;
- шифрування (статичне, динамічне, потокове);
- фільтрація вхідного і вихідного трафіку між довіреними і ненадійними мережами (брандмауери);

© Легомінова, С. В., Щавінський, Ю. В., & Будзинський, О. В. (2024). Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. Сучасний захист інформації, 2(58), 50–58. https://doi.org/10.31673/2409-7292.2024.020006.

- системи виявлення вторгнень в бази даних IDS/IPS (Intrusion Detection and Prevention System);
- резервне копіювання, в тому числі хмарне;
- навчання і підвищення обізнаності персоналу.

Переважна більшість науковців стверджують, що сучасні дослідження безпеки [11-14] зосереджені на застосуванні штучного інтелекту (ШІ) у перерахованих підходах (рис.2) та мають ряд переваг:

ШІ може ефективно обробляти великі обсяги даних, що надходять з баз даних, аналізувати зразки нормальної поведінки бази даних та користувачів і виявляти аномальні патерни, які можуть свідчити про потенційні атаки або вторгнення;

системи IDS/IPS можуть навчатися на основі історичних даних про атаки та вторгнення, щоб виявляти нові загрози, які можуть виникнути у майбутньому;

ШІ може використовувати алгоритми навчання без учителя для виявлення аномальних патернів в базі даних, не потребуючи попередньої інформації про конкретні типи атак;

ШІ може автоматично виявляти підозрілі активності та навіть реагувати на них, включаючи блокування атакуючих IP-адрес або виконання інших дій згідно з заздалегідь визначеними правилами;

ШІ може допомогти покращити рівень виявлення загроз та зменшити кількість фальшивих спрацювань, а також забезпечити швидку реакцію на реальні загрози.

Рис. 2. Застосування штучного інтелекту в основних підходах до забезпечення безпеки корпоративних баз даних

Використання штучного інтелекту в захисті КБД дозволяє:

- покращити здатність систем виявлення вторгнень в бази даних до рівня, що відповідає сучасним потребам безпеки інформації;
- оперативно реагувати та запобігати можливим атакам, що дозволяє зменшити шкоду та мінімізувати час простою системи;
- аналізуючи дані про попередні атаки, створювати моделі для прогнозування майбутніх загроз, що дозволяє підготувати заходи безпеки заздалегідь;
- навчатися на основі нових даних та адаптуватися до нових методів атак, що дозволяє постійно покращувати рівень захисту корпоративних баз даних.

В останній час набув широкого застосування підхід, який ґрунтується на використанні стандартних бібліотек мови програмування Python при застосуванні ШІ в захисті КБД, що дозволяє автоматизувати процеси їх безпеки:

- TensorFlow, Keras, PyTorch - ці бібліотеки машинного навчання використовуються для побудови моделей, які можуть виявляти аномалії в активах баз даних або прогнозувати можливі атаки на їх безпеку, наприклад, можна створити модель для виявлення незвичайної активності, яка може свідчити про вторгнення;
- Scikit-learn - популярна бібліотека машинного навчання для Python, яка має широкий спектр алгоритмів, таких як класифікація, кластеризація та аналіз даних, може бути використана для створення моделей для виявлення аномальної поведінки або класифікації потенційних загроз;
- OpenAI Gym - може бути використана для створення середовища тестування, де можна навчати агентів на основі змістовних даних та імітувати потенційні атаки;
- NLTK (Natural Language Toolkit) – використовується для аналізу тексту, зокрема, виявлення аномальних або підозрілих патернів у журналах аудиту а також для обробки природної мови;
- IBM Watson - може допомогти виявляти аномалії та підозрілу активність в корпоративних даних шляхом використання мовного аналізу, аналізу зображень та інших інтелектуальних сервісів;
- DeepArmor Enterprise - приклад рішення, яке використовує глибоке навчання для виявлення й блокування загроз кібербезпеки у реальному часі на різних рівнях корпоративних мереж та систем.

Ці бібліотеки та інструменти можуть використовуватися як окремо, так і в поєднанні для створення рішень з захисту корпоративних баз даних за допомогою штучного інтелекту.

Досить новим та досліджуваним напрямком для захисту корпоративних баз даних є використання квантових обчислень, суть яких полягає у використанні принципів квантової механіки (фізичні властивості квантових частин, таких як квантові біти (або кубіти), для забезпечення конфіденційності та цілісності передачі даних) для забезпечення безпеки при шифруванні, автентифікації, виявленні загроз, пошуку великих обсягів даних. Загалом, квантові обчислення мають потенціал стати важливим інструментом для захисту корпоративних баз даних, проте наразі це ще завдання наукових досліджень, і більшість застосувань ще потребують подальшого розвитку та випробувань [15].

Важливу роль в захисті КБД грають хмарні технології, які надають компаніям різноманітні інструменти і можливості для забезпечення безпеки даних, використовуючи всі перераховані вище підходи. Використання хмарних технологій для захисту корпоративних баз даних дозволяє компаніям забезпечити високий рівень безпеки та надійності своїх даних, зменшуючи витрати та складність управління інфраструктурою, але при цьому ставить захист даних в залежність від постачальників хмарних послуг. Зберігання даних у хмарних сервісах може створити додаткові виклики у виконанні вимог щодо захисту даних, які встановлені законодавством або стандартами відповідності. Компанії можуть потребувати спеціальних домовленостей з провайдерами хмарних послуг або додаткових заходів безпеки для забезпечення відповідності.

Розроблення превентивного підходу до захисту корпоративних баз даних. Аналіз перерахованих підходів до захисту КБД свідчить про те, що в основному дослідження науковцями проводяться в напрямку удосконалення захисту створених баз даних. Це інколи потребує при розробленні системи захисту КБД реорганізації самої структури бази даних та вимагає додаткових матеріальних та часових затрат. Тому, на підставі висновків, зроблених в роботі [6], організацію захисту БД доцільно розпочинати одночасно з розробленням самої бази.

Щоб полегшити процес розробки захисту БД при проектуванні бази, використовуються так звані семантичні концептуальні моделі. Найбільш відомою є ER-модель даних (Entity-

© Легомінова, С. В., Щавінський, Ю. В., & Будзинський, О. В. (2024). Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. Сучасний захист інформації, 2(58), 50–58. https://doi.org/10.31673/2409-7292.2024.020006.

relationship model або Entity-relationship diagram) в різних нотаціях. В основі ER-моделі лежать поняття “сутність”, “зв’язок” та “атрибут” та зв’язки між ними у вигляді наочних графічних діаграм. ER-модель – це тільки концептуальний рівень моделювання, який не містить деталей реалізації, але полегшує процес проектування.

Концептуальні ER моделі будуть корисним інструментом при розробці захисту корпоративних баз даних. Вони дозволяють візуалізувати структуру даних та відносини між різними сутностями в системі. Їх застосування на етапі проектування КБД має наступні переваги:

- шляхом аналізу ER-моделі можна виявити потенційні вразливості та слабкі місця в системі, що можуть стати точками входу для атак або порушень безпеки;
- ER-модель може допомогти у визначенні необхідних рівнів доступу для різних сутностей в системі, допомагає визначити, які дані потребують вищого рівня захисту і кого можна допустити до певних частин бази даних;
- аналізуючи залежності між сутностями в ER-моделі, можна визначити, які дані можуть бути компрометовані внаслідок атаки або порушення безпеки в певній частині КБД;
- ER-модель може також вказати, які дані є найбільш критичними для бізнесу і потребують регулярного резервного копіювання та захисту;
- на основі ER-моделі може бути здійснена ідентифікація ключових точок в системі, де потрібно встановити контроль доступу та інші заходи безпеки.

Загальні складові частини ER-моделі захисту КБД, які допоможуть при розробці системи захисту, показані на рисунку 3.

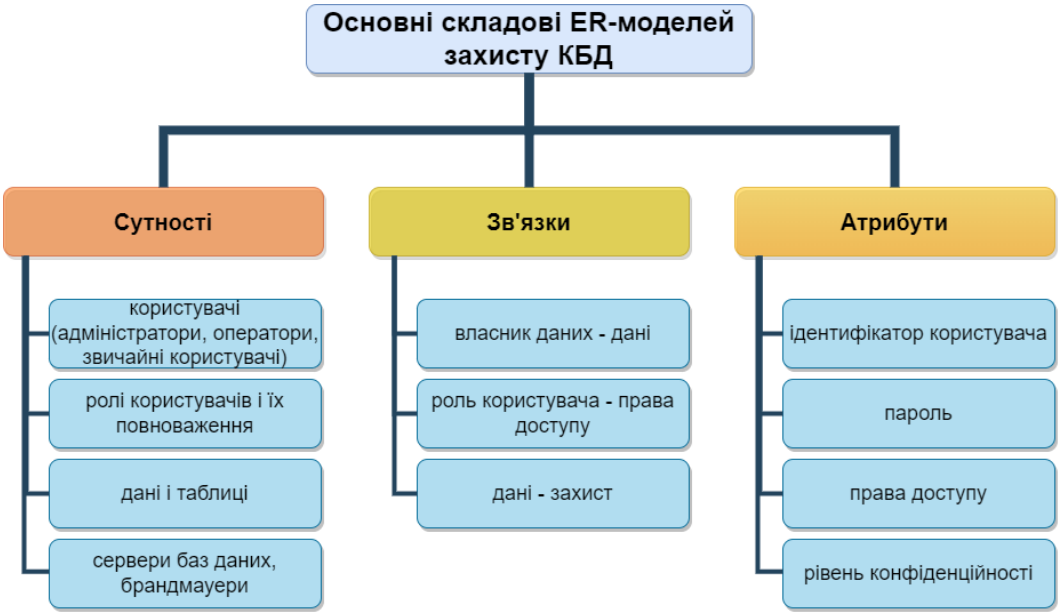

Рис. 3. Основні складові Entity-relationship моделі захисту КБД

Ці сутності, зв'язки та атрибути допомагають візуалізувати структуру та організацію захисту корпоративної бази даних, що дозволяє ефективно розробляти та впроваджувати стратегії захисту.

Наприклад, для концептуальної моделі шифрування КБД можуть бути (рис. 3):

- сутності:

a) дані, які потрібно зашифрувати, має атрибути: ID даних (Data_ID), назва даних (Data_Name), тип даних (Data_Type), вміст даних (Data_Content);

b) ключ шифрування, який використовується для шифрування або розшифрування даних, має атрибути: ID ключа (Key_ID), назва ключа (Key_Name), тип шифрування (Encryption_Type);

c) користувач, який має доступ до зашифрованих даних, має атрибути: ID користувача (User_ID), ім'я користувача (Username), пароль (Password), роль користувача (Role).

- зв'язки:

a) дані - ключ шифрування: вказує, які дані зашифровані за допомогою конкретного ключа шифрування. Кожні дані можуть бути зашифровані лише одним ключем;

b) ключ шифрування - користувач: визначає, які ключі шифрування доступні для кожного користувача. Кожен користувач може мати доступ до одного або більше ключів шифрування;

c) користувач - дані: вказує, до яких даних має доступ кожен користувач. Кожен користувач може мати доступ до різних категорій зашифрованих даних.

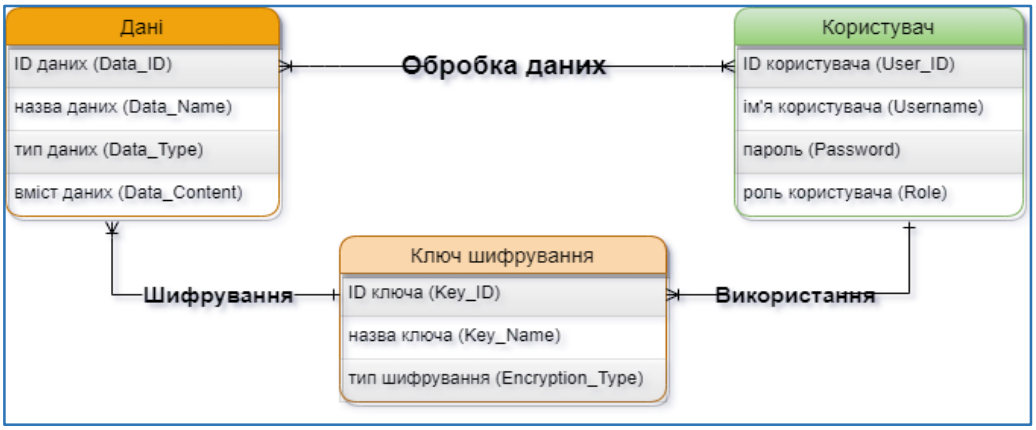

Рис. 3. Концептуальна ER-модель шифрування КБД

У цій моделі реалізовано основні зв'язки між сутностями, необхідні для реалізації системи шифрування в КБД.

Наступний приклад концептуальної моделі контролю доступу в КБД включає (рис. 4):

- сутності:

a) користувач, який має доступ до бази даних та його атрибути: ID користувача (User_ID), ім'я користувача (Username), пароль (Password), роль користувача (Role);

b) роль та повноваження користувачів системи, має атрибути: ID ролі (Role_ID), назва ролі (Role_Name);

c) права доступу користувачів до певних об'єктів бази даних, має атрибути: ID дозволу (Permission_ID), тип доступу (Access_Type), об'єкт доступу (Access_Object).

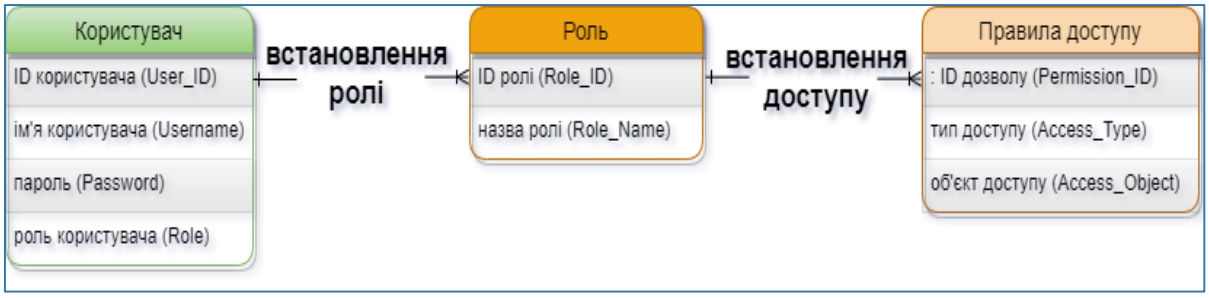

Рис. 4. Концептуальна ER-модель встановлення доступу до КБД

- зв'язки:

a) користувач - роль: визначає, які користувачі належать до яких ролей. Кожен користувач може мати одну або більше ролей;

b) роль - права доступу: вказує, які дозволи доступу надаються для кожної ролі. Кожна роль може мати різні права доступу до об'єктів бази даних.

У цій моделі реалізовано основні зв’язки між сутностями, необхідні для реалізації системи контролю доступу в корпоративній базі даних. Користувачі наділяються ролями, а ролі мають відповідні дозволи доступу до об’єктів бази даних.

Концептуальна модель для моніторингу корпоративної бази даних включає (рис. 5):

- сутності:

a) подія моніторингу, яка сталася в системі, може включати доступ до даних, внесення змін, авторизацію тощо. Має атрибути: ID події (Event_ID), тип події (Event_Type), дата та час (Timestamp), додаткова інформація (Additional_Info);

b) користувач системи, який здійснює дії, має атрибути: ID користувача (User_ID), ім'я користувача (Username), IP-адреса (IP_Address), роль користувача (Role);

c) об’єкти моніторингу, які моніторяться, такі як таблиці, записи, запити тощо, має атрибути: ID об’єкта (Object_ID), назва об'єкта (Object_Name), тип об’єкта (Object_Type).

- зв’язки:

a) користувач - подія моніторингу: вказує, які події пов’язані з кожним користувачем системи. Кожна подія моніторингу пов’язана з одним користувачем;

b) об’єкт моніторингу - подія моніторингу: визначає, які події пов’язані з кожним об’єктом моніторингу. Кожна подія моніторингу пов’язана з одним об'єктом моніторингу.

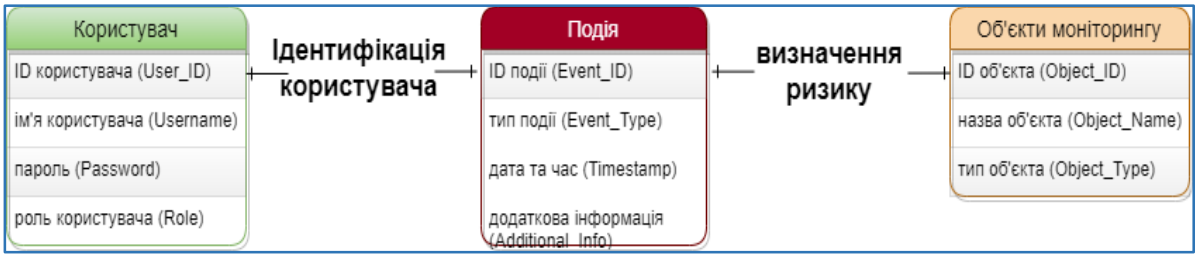

Рис. 5. Концептуальна ER-модель встановлення доступу до КБД

У цій моделі реалізовано основні зв’язки між сутностями, необхідні для відслідковування та моніторингу дій користувачів та об’єктів в КБД. Кожна подія моніторингу зберігається разом з інформацією про користувача, який її здійснив, та об'єктом, до якого вона відноситься.

Таким чином, запропонований підхід з використанням Entity-relationship моделей може допомогти організаціям ще на етапі проектування розробляти ефективні системи захисту своїх корпоративних баз даних.

Висновок

Проведений в роботі аналіз підходів до забезпечення кібербезпеки корпоративних баз даних виявив достатню кількість досліджень щодо захисту інформації в корпоративних базах, суть яких полягає в застосуванні штучного інтелекту, хмарних технологій та квантових обчислень при створенні систем захисту. Разом з тим встановлено, що основні зусилля в дослідженнях науковців спрямовані за застосуванні сучасних інформаційних технологій захисту уже готових корпоративних баз, що може в подальшому привести до необхідності реконфігурації структури і додаткових матеріальних і людських затрат. Тому запропонований підхід створення системи захисту бази даних ще на етапі її проектування методом створення концептуальних моделей. Враховуючи переваги моделей типу Entity-Relationship, їх використання може сприяти розробці більш ефективних та надійних стратегій захисту корпоративних баз даних, принесе користь споживачам, допомагаючи організаціям у розробці безпечних систем.

Перелік посилань

1. Kamra, A., Terzi, E. & Bertino, E. (2008). Detecting anomalous access patterns in relational databases. The VLDB Journal 17, 1063–1077. https://doi.org/10.1007/s00778-007-0051-4.

2. Gokhan, Kul., Duc, Thanh, Anh, Luong., Ting, Xie., Patrick, Coonan., Varun, Chandola., Oliver, Kennedy., Shambhu, Upadhyaya. (2016). Ettu: Analyzing Query Intents in Corporate Databases. WWW '16 Companion: Proceedings of the 25th International Conference Companion on World Wide WebApril 2016, pp. 463-466. https://doi.org/10.1145/2872518.2888608.

3. Gaurang, Gavai., Kumar, Sricharan., Dave, Gunning., Rob, Rolleston., John, Hanley., Mudita, Singhal. (2015). Detecting Insider Threat from Enterprise Social and Online Activity Data. MIST '15: Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security ThreatsOctober 2015, pp. 13–20. https://doi.org/10.1145/2808783.2808784.

4. Natalia, Arzamasova., Klemens, Böhm., Bertrand, Goldman., Christian, Saaler., Martin, Schäler. (2020). On the Usefulness of SQL-Query-Similarity Measures to Find User Interests. IEEE Transactions on Knowledge and Data Engineering, 32(10), 1982-1999. https://doi.org/10.1109/TKDE.2019.2913381.

5. Kitchenham, Barbara & Kutay, Cat & Jeffery, R. & Connaughton, Colin. (2006). Lessons learnt from the analysis of large-scale corporate databases. Proceedings - International Conference on Software Engineering. 2006. 439-444. https://doi.org/10.1145/1134285.1134347.

6. Спасітєлєва, С. О., Бурячок, В. Л. Комплексний захист гетерогенних корпоративних сховищ даних. Сучасний захист інформації №1, 2017. С. 58-65

7. Iqbal, A., Khan, S.U., & Niazi, M. et al. (2023). Advancing database security: a comprehensive systematic mapping study of potential challenges. Wireless Netw (5), 1-28. https://doi.org/10.1007/s11276-023-03436-z

8. Conte, S.D. & De Boor, C. (2018). Elementary Numerical Analysis: An Algorithmic Approach. Classics in Applied Mathematics. Society for Industrial and Applied Mathematics (SIAM, 3600 Market Street, Floor 6, Philadelphia, PA 19104). 259 p.

9. Adewusi, Okolo, Olorunsogo, Asuzu, & Daraojimba. Business intelligence in the era of big data: a review of analytical tools and competitive advantage. Computer Science & IT Research Journal Volume 5, Issue 2, P.415-431, 2024. DOI: https://doi.org/10.51594/csitrj.v5i2.791.

10. Cheng, L., Liu, F., Yao, D. Enterprise data breach: causes, challenges, prevention, and future directions //Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2017. – Т. 7. – №. 5. – С. e1211.

11. Савченко, В. А. Основні напрями застосування технологій штучного інтелекту у кібербезпеці / Савченко В. А., Шаповаленко О. Д // Сучасний захист інформації №4(44), 2020. – С. 6–11.

12. Unuriode, Austine & Yusuf, Babatunde & Durojaiye, Olalekan & Okunade, Lateef. (2023). The integration of Artificial Intelligence Into Database Systems (ai-db integration review). International Journal on Cybernetics & Informatics. Vol 12, No 6, 161-172. https://doi.org/10.5121/ijci.2023.1206012.

13. Ogoniba, Bemologi. (2023). Protecting Privacy in the Age of AI: Understanding Data Security Challenges in AI- Powered Technology. By Ogoniba unity Bemologi (LLB, BL, LLM). https://doi.org/10.6084/m9.figshare.22795703.

14. Timan, T., Mann, Z. (2021). Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In: Curry, E., Metzger, A., Zillner, S., Pazzaglia, JC., García Robles, A. (eds) The Elements of Big Data Value. Springer, Cham. Pp. 153-175. https://doi.org/10.1007/978-3-030-68176-0_7

15. Соколов, О. К., Штангей, С. В. Перспективи квантового шифрування у системах інфокомунікацій. Матеріали Міжнародної науково-технічної конференції «Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023))». Харків, Україна, 7 – 8 грудня 2023 р. С. 123-126.

Надійшла 21.04.2024