УДК 004.056.5:004.5
DOI: 10.31673/2409-7292.2025.029259

Будзинський О.В.

МЕТОД ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА АВТОМАТИЗОВАНОГО РЕАГУВАННЯ В СИСТЕМАХ ЗАХИСТУ КОРПОРАТИВНИХ БАЗ ДАНИХ

У статті запропоновано науково обґрунтований метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних, що функціонують в умовах сучасної мережевої інфраструктури. Актуальність дослідження зумовлена зростанням складності кібератак, збільшенням обсягів даних та поширенням хмарних технологій, що значно ускладнюють контроль за доступом та унеможливлюють застосування лише традиційних підходів до забезпечення безпеки систем управління базами даних. Запропоновано багаторівневу архітектуру, яка базується на поєднанні моделей аналізу поведінки користувачів, математичного оцінювання ризиків запитів до бази даних. Кожен SQL-запит описується вектором ознак, які аналізуються із застосуванням моделі Isolation Forest. Визначений рівень загрози дозволяє сформувати комбіновану оцінку ризику, що інтегрує поведінкову аномальність та критичність запиту. На основі цієї оцінки реалізовано механізм автоматичного реагування в режимі реального часу – зокрема блокування доступу, сповіщення SOC та можливий запуск сценаріїв через плагін для SIEM-системи. Особливістю методу є можливість його адаптації до реальних IT-інфраструктур, що забезпечується модульністю системи та сумісністю з існуючими засобами моніторингу. Запропонований метод є інноваційним поєднанням поведінкового аналізу, адаптивного машинного навчання та автоматизованої реакції в єдиній архітектурі захисту корпоративних баз даних. Його відмінністю є проактивність, гнучкість реагування, попереджувальна дія до виконання запиту та можливість інтеграції з існуючими SOC-рішеннями. Ефективність методу підтверджена результатами моделювання, зокрема порівнянням з іншими підходами за метриками повноти та ROC-кривими. Запропоноване рішення має практичне значення для підвищення стійкості корпоративних систем управління базами даних до внутрішніх і зовнішніх загроз.

Ключові слова: інформаційна безпека, захист баз даних, виявлення аномалій доступу, автоматизація реагування.

Вступ

У сучасних умовах стрімкого розвитку інформаційних технологій корпоративні бази даних (БД) відіграють ключову роль у функціонуванні організацій, забезпечуючи збереження та доступ до критично важливої інформації. Проте зростання обсягів оброблюваних даних, розширення мережевої інфраструктури та активне впровадження хмарних і віртуалізованих середовищ значно ускладнюють завдання забезпечення безпеки корпоративних БД.

Особливої актуальності набуває проблема виявлення вразливостей у системах управління базами даних (СУБД) і своєчасного реагування на спроби несанкціонованого доступу. Традиційні методи, засновані на сигнатурному аналізі або ручному втручанні аналітиків центру моніторингу безпеки (SOC), виявилися недостатньо ефективними в умовах високої динаміки сучасних атак, які часто є багатоетапними, використовують легітимні облікові дані та відзначаються складною поведінковою моделлю. Додаткову загрозу становлять атаки з використанням штучного інтелекту, які здатні обійти стандартні механізми захисту та знаходити нові вектори проникнення. Разом з тим, час між початком атаки та нанесенням шкоди дедалі скорочується, що вимагає переходу до автоматизованих рішень виявлення й реагування в реальному часі. Крім того, посилення регуляторних вимог у сфері захисту персональних даних (зокрема, GDPR, ISO/IEC 27001, Закону України «Про захист персональних даних») зобов'язує суб'єктів господарювання впроваджувати дієві методи моніторингу доступу, виявлення вразливостей та запобігання витокам інформації.

У цьому контексті важливим завданням є розроблення методу, що дозволяє: виявляти потенційні вразливості в корпоративних БД; проводити поведінковий аналіз запитів до СУБД; здійснювати автоматизоване реагування – блокування небезпечних запитів або обмеження доступу та інформування SOC у випадках підозрілої активності.

Формулювання проблеми

Сьогодні існуючі засоби моніторингу та аналізу безпеки баз даних здебільшого орієнтовані на постфактум-аналіз логів, що унеможливлює реагування в реальному часі та

потребує ручного втручання фахівців і знижує ефективність захисту в умовах складної мережевої інфраструктури.

З іншого боку, для забезпечення цілісності та конфіденційності даних у корпоративних базах даних необхідне своєчасне виявлення загроз та негайне реагування на спроби несанкціонованого доступу, включаючи блокування потенційно небезпечних запитів ще до їх виконання.

Таким чином, наукове протиріччя полягає у неузгодженості між необхідністю реагування в реальному масштабі часу та наявними методами виявлення і обробки інцидентів безпеки, які є переважно пасивними та запізнілими.

Аналіз літератури

Враховуючи актуальність та необхідність вирішення проблеми, пошуку ефективних методів захисту корпоративних БД присвячена велика кількість вітчизняних та зарубіжних наукових досліджень. У кількох дослідженнях проведено вивчення та класифіковано ризики та загрози кібербезпеки в системах баз даних.

В роботі [1] проведений всебічний огляд, щоб визначити основні елементи контролю безпеки в системах баз даних. Це дозволило розділили ці засоби контролю на п'ять груп: методи підвищення конфіденційності, системи виявлення вторгнень (IDS), аудит, шифрування, а також контроль доступу та автентифікація.

У дослідженні [2, 3] проаналізовані критичні кібератаки в системах баз даних, заснованих на технології блокчейн. Їхні результати показали, що основні кібератаки в системах баз даних включають DoS, несанкціонований доступ, внутрішні загрози, чорну діяльність, соціальну інженерію, SQL-ін'єкції та зловживання надмірними привілеями, які зловмисники можуть використовувати для компрометації систем баз даних.

Проведене науковцями [4] порівняння з традиційними методами захисту БД і машинними методи навчання (ML) виявило як переваги машинного навчання так і деякі недоліки, такі, як слабке узагальнення, відхилення від реальності при зосередженні тільки на застосуванні програмних методів.

В роботі [5] наведений комплексний аналіз кіберризиків у системах управління базами даних, включаючи класифікацію загроз, вразливостей, впливів та заходів протидії, які полягають у проведенні технічних контрзаходів для захисту систем БД від кіберзагроз. Разом з тим, запропоновані заходи протидії не мають превентивного характеру та не зовсім забезпечують виявлення нових загроз і потребують подальших досліджень.

У дослідженні [6] автори всебічно охопили та дослідили проблеми забезпечення безпеки баз даних у інформаційно-телекомунікаційних мережах, провели аналіз загроз та вразливостей, які завдають шкоди інформаційній мережі та провели дослідження методів протидії сучасним загрозам інформаційно-телекомунікаційних мереж. При цьому, зосередження на двох найбільш ефективних методах, а саме використання фаєрволу та Suricata, не забезпечить захист від внутрішніх загроз безпеці БД.

У роботі [7] запропонований метод прогнозного моделювання як надійної стратегії пом’якшення вразливостей бази даних на основі створення системи виявлення нерегулярних дій, таких як несанкціонований доступ або незвичайні шаблони використання даних, за допомогою моніторингу в реальному часі та алгоритмів машинного навчання. На думку дослідників, ці системи здатні розрізняти законну та зловмисну поведінку, значно покращуючи можливості раннього виявлення порушень.

Дослідження [8] спрямоване на аналіз актуальних проблем безпеки корпоративних баз даних в умовах сучасної інфраструктури, розробку моделі виявлення аномальної активності доступу до баз даних та інтеграцію її в SIEM-систему AlienVault для автоматичного реагування на загрози. Встановлено, що одною із головних проблем захисту баз даних є потреба в негайному виявленні аномалій доступу та реагуванні на загрози конфіденційності, доступності та цілісності баз даних і потребує пошуку науково обґрунтованих методів.

© Будзинський О.В. (2025). Метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних. Сучасний захист інформації, 2(62), 180–186. https://doi.org/10.31673/2409-7292.2025.029259

У роботі [9] запропонована методика виявлення аномалій взаємодії користувачів з інформаційними активами на підставі даних мережі з використанням дводольного графа для відображення та для практичної реалізації адміністраторами інформаційної безпеки. Переважна більшість науковців у своїх дослідженнях визначають проблему автоматизації реагування на загрози безпеці БД.

Метою дослідження є розроблення методу виявлення вразливостей і забезпечення автоматизованого реагування на інциденти інформаційної безпеки в корпоративних системах баз даних, що дозволяє в режимі реального часу виявляти загрози, здійснювати динамічну оцінку ризиків та ініціювати відповідні захисні дії без втручання людини.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- на основі аналізу існуючих підходів до виявлення вразливостей в системах баз даних визначити основні вектори атак на СУБД, характерні для сучасної мережевої інфраструктури;
- розробити узагальнену архітектуру рішення, що забезпечує моніторинг, виявлення загроз та автоматизоване реагування;
- запропонувати формальний метод, який дозволяє поєднати виявлення аномальної поведінки із класифікацією рівня загрози;
- провести тестування запропонованого методу на навчальному середовищі та оцінити ефективність.

Основна частина

1. Загальний аналіз існуючих підходів до виявлення вразливостей і реагування в системах захисту баз даних

У сучасних корпоративних інформаційних системах бази даних виступають критичними активами, які постійно зазнають ризику зовнішніх і внутрішніх атак. У зв'язку з цим науковцями у своїх дослідженнях розроблена низка підходів до виявлення вразливостей та реагування на інциденти безпеки.

Аналіз публікацій [1-9] дозволяє зробити висновок про те, що жоден з існуючих підходів, крім методів машинного навчання, не забезпечує повною мірою виявлення та блокування спроб несанкціонованого доступу в реальному часі без затримки запиту до бази даних, що обґрунтовує потребу в розробці нового методу, орієнтованого на превентивне реагування ще до виконання потенційно небезпечної операції.

2. Основні вектори атак на СУБД, характерні для сучасної мережевої інфраструктури

Основні вектори атак на системи управління базами даних у сучасній мережевій інфраструктурі відображають актуальні загрози, що спрямовані на порушення конфіденційності, цілісності або доступності даних. Вони поділяються за джерелом, технікою атаки та рівнем доступу. Основними векторами є:

- SQL-ін'єкції;
- атаки через слабку автентифікацію та компрометацію облікових даних;
- атаки на вразливості налаштування СУБД (відкриті порти, надмірні привілеї, відсутність шифрування, відкритий доступ за замовчуванням з Інтернету, вразливості розширення, переповнення буфера);
- атаки зсередини (Insider Threats);
- атаки через додатки (впровадження команд через API, використання вразливостей ORM-бібліотек, атаки на механізми гешування або ORM-запити);
- DoS/DDoS-атаки на СУБД;
- шкідливі тригери та збережені процедури для створення бекдорів або деструктивної логіки; компрометація точок входу через сервіси передачі даних.

Основні вектори атак разом з джерелами атак (зовнішні/внутрішні користувачі) та цілями атак показані на рисунку 1. Граф відображає не лише вектори атак і їх цілі а й логіку реагування на ці атаки: виявлення → класифікація → оцінка → дія.

3. Опис методу виявлення вразливостей та автоматизованого реагування

© Будзинський О.В. (2025). Метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних. Сучасний захист інформації, 2(62), 180–186. https://doi.org/10.31673/2409-7292.2025.029259

З метою підвищення ефективності систем захисту корпоративних БД запропоновано метод виявлення вразливостей та автоматизованого реагування. В основі методу – принципи проактивного захисту, де ключовим є запобігання несанкціонованому впливу ще до виконання запиту до СУБД. Метод базується на аналізі SQL-запитів у реальному часі з метою виявлення потенційно небезпечної активності. Формалізуємо ключові компоненти моделі.

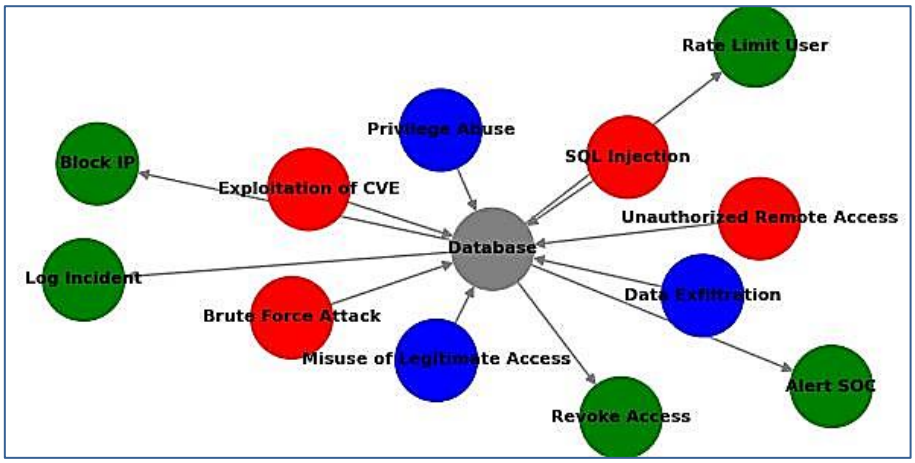

Рис. 1. Граф векторів атак на СУБД (червоні вузли – зовнішні атаки, сині вузли – внутрішні загрози, сірий вузол – сама база даних, зелені вузли – автоматизовані дії у відповідь).

3.1.Математична формалізація запропонованого методу

Нехай маємо множину SQL-запитів: $Q=\{q_1,q_2,...,q_n\}$, $q_i \in Q$, де Q – множина всіх можливих SQL-запитів. Кожен запит q_i описується вектором ознак:

$$\vec{x}=[f_i(q_i),f_2(q_i),...f_m(q_i)]\in R^m, \tag{1}$$

де $f_k(q_i)$ – функція, що виділяє *k*-ту ознаку запиту, k=1,2,…,m (наприклад довжина запиту, наявність операторів DROP, UNION, SLEEP, час виконання, частота доступу до таблиць); m – розмірність вектора ознак (тобто кількість ознак).

Визначимо функцію оцінки рівня загрози:

$$R(\vec{x})=w_1f_1+w_2f_2+...+w_mf_m=\vec{w}^T\vec{x}, \tag{2}$$

де $\vec{w}=[w_1,...,w_m]$ – ваговий вектор, визначений шляхом навчання (наприклад, логістична регресія або SVM); $\vec{w}^T$ – транспонований вектор.

Нормалізуємо результат $R(\vec{x})$ до інтервалу [0,1] і визначимо порогові значення для класифікації запиту *Kl*:

$$Kz:\begin{cases} N_r, & \text{if } R(\vec{x})<\theta_1 \\ S_r, & \text{if } \theta_1 \le R(\vec{x})<\theta_2 \\ V_r, & \text{if } R(\vec{x})\ge\theta_2 \end{cases}, \tag{3}$$

де N_r, S_r, V_r – низький, середній, високий ризик; θ_1, $\theta_2 \in [0,1]$ – емпірично визначені пороги.

Для прийняття рішення визначимо *функцію дії:*

© Будзинський О.В. (2025). Метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних. Сучасний захист інформації, 2(62), 180–186. https://doi.org/10.31673/2409-7292.2025.029259

$$\delta(\vec{x}) = \begin{cases} Allow, & \text{if } R(\vec{x}) < \theta_1 \\ \text{Alert}, & \text{if } \theta_1 \le R(\vec{x}) < \theta_2 \\ Block, & \text{if } R(\vec{x}) \ge \theta_2 \end{cases}. \quad (4)$$

Функція (4) може реалізовуватись через просту логіку або складнішу модель прийняття рішень (наприклад, дерево рішень або нейромережу). Для складнішої моделі з метою визначення аномалій та поведінкового аналізу потрібно застосувати модуль виявлення з використанням алгоритму штучного інтелекту Isolation Forest [8, 10].

Нехай $S(q_i)$ – функція оцінки аномальності запиту, яка повертає значення $S(q_i) \in [0,1]$, $S(q_i) \to 1 \Rightarrow$ *аномалія.* У цьому випадку комбінований ризик буде визначатись:

$$R'(q_i) = \alpha R(\vec{x}) + (1-\alpha) S(q_i), \quad (5)$$

де $\alpha \in [0,1]$ – відіграє роль вагового коефіцієнта, що визначає співвідношення впливу двох компонентів ризику: $R(\vec{x})$ – ризик на основі профілю користувача/джерела доступу (наприклад, історія дій, права, поведінкові аномалії) та $S(q_i)$ – ризик, що базується на характеристиках самого SQL-запиту (наприклад, спроба доступу до чутливих таблиць, складність запиту, тип операції – SELECT/UPDATE/DELETE тощо).

Рішення приймається на основі $R'(q_i)$, що дозволяє враховувати як контекст запиту, так і поведінкову відмінність від "нормального" профілю. Наприклад, користувач має середній ризик (0.5), але намагається виконати складний запит із потенційною SQL-ін'єкцією (0.9). Якщо α=0.6, то: $R'(q_i)$ =0.6·0.5 + 0.4·0.9 = 0.3 + 0.36 = 0.66. Це дозволяє більш гнучко та об'єктивно врахувати обидва аспекти – хто виконує запит і що саме він виконує.

3.2.Інтеграція з SIEM

При досягненні рівня ризику $R'(q_i) \ge \theta_1$ (рис. 2) формується подія *Alert* і надсилається в систему типу AlienVault OSSIM у форматі Syslog або JSON для подальшої кореляції з іншими джерелами для сповіщення: Event(q_i)=$\{id, \text{time,source\_ip,user}, R'(\vec{x}), \delta(\vec{x})\}$.

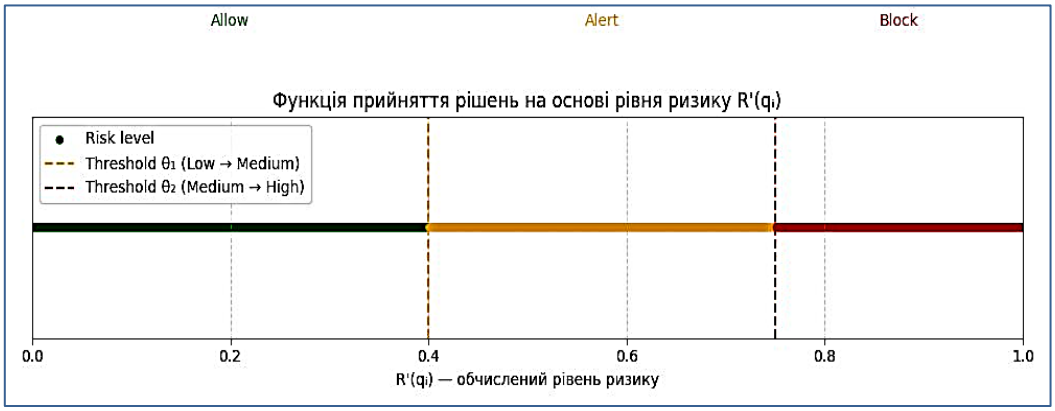

Рис.2. Графік порогів

3.3.Алгоритм і архітектура методу показані на рис.3

3.4. З метою перевірки працездатності та ефективності запропонованого методу виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних було проведено моделювання створеного програмного продукту на мові

програмування Python у лабораторному середовищі. Для порівняльного аналізу з відомими підходами використовувалися загальноприйняті метрики оцінювання класифікаторів у задачах виявлення аномалій, а саме: Precision (точність позитивного класу); Recall (повнота); F1-score (гармонійне середнє); Time to Detect (TTD) – середній час реакції на аномальний запит; False Positive Rate (FPR) – частка хибно позитивних спрацьовувань (табл.1).

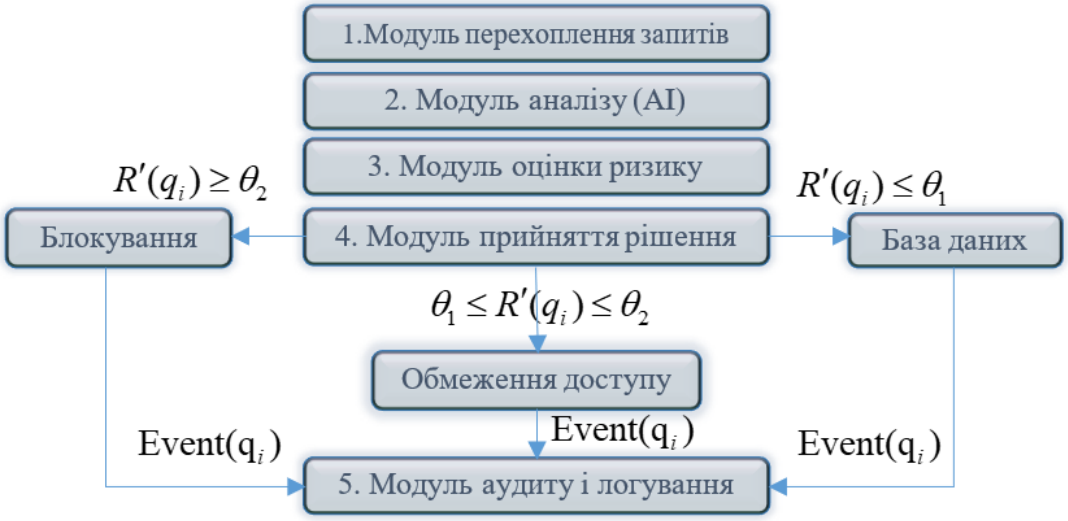

Рис. 3. Архітектура методу

Таблиця 1

Результати порівняння

Метод	Precision	Recall	F1-score	FPR	TTD (середнє, мс)
Isolation Forest	0.92	0.86	0.89	0.07	110
One-Class SVM	0.90	0.83	0.86	0.09	135
AutoEncoder (нейромережа)	0.95	0.88	0.91	0.05	160
Запропонований метод	**0.93**	**0.90**	**0.91**	**0.04**	**95**

Запропонований підхід демонструє найкращу повноту (recall), що є критично важливою метрикою для систем виявлення загроз, де пропуск атаки є значно шкідливішим, ніж хибне спрацьовування. Також спостерігається найменший середній час виявлення – менше 100 мс, що забезпечує практично реальний режим реагування. Метод забезпечує надійне виявлення атак на рівні запитів до БД та буде також забезпечувати оперативне автоматизоване реагування в рамках SOC.

Висновки

Таким чином, розроблений метод виявлення вразливостей та автоматизованого реагування в системах корпоративних баз даних із використанням моделей машинного навчання об'єднує поведінковий аналіз запитів до СУБД, механізм динамічного визначення рівня загрози запиту (з поділом на високий, середній, низький), та автоматизоване реагування на виявлені інциденти (блокування, обмеження доступу, сповіщення SOC). У роботі вперше запропоновано інтегрувати підхід як розширення функціоналу SIEM-системи, з можливістю прийняття рішень до обробки запиту СУБД. Запропонований метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних відрізняється від відомих підходів за кількома важливими аспектами: інтеграція виявлення та реагування в реальному часі у автоматизованому режимі; контекстна обробка запиту перед доступом до СУБД; гнучкий механізм прийняття рішень (реакцій) з масштабуванням порогових рівнів;

© Будзинський О.В. (2025). Метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних. Сучасний захист інформації, 2(62), 180–186. https://doi.org/10.31673/2409-7292.2025.029259

емпірична оцінка та візуалізація. Оцінка ефективності запропонованого методу показала його високу придатність для інтеграції у системи захисту корпоративних баз даних, особливо в умовах сучасного загрозоорієнтованого середовища.

Перелік посилань

1. Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of Cyber Security, 115–133. https://doi.org/10.58496/mjcsc/2023/016.

2. Touil, H., El Akkad, N., Satori, K., Soliman, N. F., & El-Shafai, W. (2024). Efficient Braille Transformation for Secure Password Hashing. IEEE Access, 1. https://doi.org/10.1109/access.2024.3349487.

3. Pan, X., Obahiaghon, A., Makar, B., Wilson, S., & Beard, C. (2024). Analysis of Database Security. OALib, 11(04), 1–19. https://doi.org/10.4236/oalib.1111366.

4. Wang, Y., Xi, J., & Cheng, T. (2021). The Overview of Database Security Threats' Solutions: Traditional and Machine Learning. Journal of Information Security, 12(01), 34–55. https://doi.org/10.4236/jis.2021.121002.

5. Almaiah, M. A., Saqr, L. M., Al-Rawwash, L. A., Altellawi, L. A., Al-Ali, R., & Almomani, O. (2024). Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems. Computers, Materials & Continua, 1–10. https://doi.org/10.32604/cmc.2024.057673.

6. Ilyenko, A., Ilyenko, S., Diana, K., & Mazur, Y. (2023). Практичні підходи щодо виявлення вразливостей в інформаційно-телекомунікаційних мережах. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 96–108. https://doi.org/10.28925/2663-4023.2023.19.96108.

7. Mosope Williams & Tina Charles Mbakwe-Obi. (2024). Integrated strategies for database protection: Leveraging anomaly detection and predictive modelling to prevent data breaches. World Journal of Advanced Research and Reviews, 24(3), 1098–1115. https://doi.org/10.30574/wjarr.2024.24.3.3795.

8. Щавінський, Ю., & Будзинський, О. (2025). Аналіз актуальних проблем безпеки корпоративних баз даних в умовах сучасної інфраструктури та шляхи їх вирішення . Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 390–405. https://doi.org/10.28925/2663-4023.2025.27.726.

9. Савченко,В. А., Смолєв,Є. С., & Гамза,Д. Є.(2023). Методика виявлення аномалій взаємодії користувачів з інформаційними ресурсами організації. Сучасний захист інформації, 4(56), 6–12. https://doi.org/10.31673/2409-7292.2023.030101.

10. Xu, H., Pang, G., Wang, Y., Wang, Y. (2023). Deep Isolation Forest for Anomaly Detection. IEEE Trans. on Knowl. and Data Eng. 35(12), 12591–12604. (2023). https://doi.org/10.1109/TKDE.2023.3270293.

Надійшла 30.05.2025