КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1221
УДК 004.056.5:004.7

Будзинський Олександр Володимирович
аспірант кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0002-2402-0711
oleksandr.email@gmail.com

Щавінський Юрій Віталійович
канд. техн. наук, доцент,
доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-2319-8983
yushchavinsky@ukr.net

Мужанова Тетяна Михайлівна
канд. наук з держ. управління, доцент,
доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Якименко Юрій Михайлович
канд. військ. наук, доцент,
доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-6848-852X
yakum14@ukr.net

Примаченко Діана Володимирівна
викладач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

МЕТОДИКА ІНТЕЛЕКТУАЛЬНОЇ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ БАЗ ДАНИХ

Анотація. У статті запропоновано методику інтелектуальної оцінки ризику захисту корпоративних баз даних, що базується на використанні ансамблевого підходу до виявлення аномалій. На основі проведеного аналізу сучасних підходів і досліджень безпеки баз даних зроблено висновок про необхідність застосування штучного інтелекту в системі захисту для врахування комплексного впливу негативних факторів на безпеку корпоративних баз даних. На відміну від традиційних методів, які орієнтовані на окремі аспекти поведінки користувачів, запропоноване рішення забезпечує багатовимірний аналіз за рахунок інтеграції декількох моделей машинного навчання. Зокрема, використано алгоритм Isolation Forest для виявлення точкових аномалій у просторі ознак, модель Long Short-Term Memory для аналізу часових залежностей та Autoencoder для виявлення структурних відхилень у багатовимірних даних. Запропоновано інтегральну оцінку аномальності, яка формується шляхом зваженого поєднання результатів окремих моделей, що дозволяє підвищити точність виявлення складних сценаріїв атак. На основі отриманого показника аномальності реалізовано перехід до оцінки ризику з врахуванням критичності ресурсів і типів операцій доступу до бази даних. Це забезпечує можливість адаптивного прийняття рішень щодо реагування на інциденти інформаційної безпеки. Розроблено програмний прототип запропонованої методики засобами мови програмування Python із використанням сучасних бібліотек машинного навчання. Проведено експериментальне дослідження на синтетичному наборі даних, що імітує нормальні та аномальні сценарії

доступу. Отримані результати підтверджують підвищення ефективності ансамблевої моделі порівняно з окремими підходами за метриками Precision, Recall, F1-score та ROC-AUC. Запропонована методика може бути використана у системах моніторингу безпеки (SOC) для автоматизованого виявлення аномалій та оцінки ризику в режимі реального часу.

Ключові слова: інформаційна безпека, корпоративні бази даних, оцінка ризиків, інтелектуальні методи, машинне навчання, кіберзагрози.

ВСТУП

Сучасні корпоративні інформаційні системи функціонують в умовах постійного зростання кількості та складності кіберзагроз, спрямованих на бази даних як ключові елементи зберігання критично важливої інформації. Особливої актуальності набувають атаки, що поєднують використання вразливостей програмного забезпечення із поведінковими аномаліями користувачів, зокрема SQL-ін’єкції, несанкціонований доступ із використанням скомпрометованих облікових записів, а також інсайдерські загрози. Поряд зі стрімким зростанням потенційних ризиків від неочікуваних кібератак, збитки від незліченних порушень кібербезпеки зростають безпрецедентними темпами та стають серйозною економічною проблемою та небезпекою для користувачів, організацій та країн. За оцінками міжнародних організацій, наслідки кібератак коштують світу близько 10,5 трильйонів доларів кожного року та продовжують зростати на 15% щороку [1]. Зростання обумовлює необхідність удосконалення підходів до оцінки ризиків інформаційної безпеки та удосконалення методів їх оцінки, що є особливо важливим для забезпечення оцінювання безпеки державних інформаційних ресурсів в умовах сучасних інформаційних війн [2-3].

Постановка проблеми. Існуючі підходи до оцінювання ризиків інформаційної безпеки, зокрема ті, що базуються на міжнародних стандартах, мають низку обмежень. Вони, як правило, орієнтовані на статичний аналіз загроз і вразливостей, використовують експертні оцінки та не враховують динамічні зміни стану інформаційної системи. Крім того, такі підходи недостатньо інтегровані з сучасними засобами моніторингу безпеки, зокрема системами SIEM та IDS/IPS, що ускладнює їх застосування в умовах реального часу та знижує їх ефективність у сучасних умовах, де атаки мають адаптивний характер.

Окремою проблемою є відсутність формалізованого підходу до кількісного врахування поведінкових характеристик користувачів та результатів роботи алгоритмів машинного навчання при оцінюванні ризику. Існуючі моделі або не використовують ці дані, або інтегрують їх фрагментарно, що знижує точність оцінювання та ефективність реагування на інциденти.

Таким чином, виникає науково-прикладна задача розробки методики інтелектуальної оцінки ризиків інформаційної безпеки корпоративних баз даних, яка повинна забезпечувати інтеграцію класичних моделей ризику з даними систем моніторингу та результатами аналізу аномалій, а також здійснювати оцінювання ризиків у режимі реального часу з можливістю автоматизації процесів реагування.

Аналіз останніх досліджень і публікацій. Враховуючи актуальність проблем захисту корпоративних баз даних, у науковій літературі існує достатня кількість публікацій, які фокусуються на вирішенні таких проблем окремо.

У роботі [4] пропонується кількісний аналіз поширених ризиків безпеки в національній базі даних вразливостей на основі прикладних методів як початкові кроки до оптимальних, орієнтованих на безпеку, інвестиційно-орієнтованих оцінок технологічних рішень та економічно ефективних процесів прийняття рішень для найкращого управління та визначення пріоритетів зменшення ризиків. Автором зроблений висновок про те, що кількісні алгоритми є більш конкурентоспроможними, практичними, цілеспрямованими, функціональними та економічно вигідними, ніж традиційно обмежені описові та категоріальні варіанти оцінки та управління ризиками кібербезпеки.

У дослідженні [5] проаналізовані загрози інформаційній безпеці баз даних та запропоновані рішення для їх пом’якшення. Науковцями підтверджена актуальність постійного удосконалення механізмів боротьби із загрозами баз даних, складність яких постійно зростає.

Метою є дослідження [6] є розвиток інформаційної технології «людина-машина» для оцінки ризиків, яка є критично важливою для системи управління ризиками інформаційної безпеки компанії. Акцент у роботі робиться на забезпеченні систематичної оцінки ризиків та надійності процесу впровадження, досліджуються численні методи, моделі та методології окремих компонентів оцінки ризиків. У дослідженні підкреслюється домінуюча важливість «людського фактора» в системах управління ризиками, зокрема проблеми, пов'язані зі складністю аналізу та потребою у великих ресурсах.

Для покращення управління ризиками науковці підкреслюють необхідність переходу до інформаційних технологій на основі сучасних систем підтримки прийняття рішень. розробки інструментів, що покращують систематизацію, формалізацію та стандартизацію процедур оцінки.

У дослідженні [7] застосований алгоритм Isolation Forest для створення моделі виявлення аномалій доступу до баз даних. з використанням бібліотек вільного доступу мови програмування Python та проведена інтеграція моделі через механізм виклику зовнішніх скриптів у SIEM-системи AlienVault. Разом з тим, використання лише одного алгоритму Isolation Forest є недостатнім для повноцінного виявлення загроз інформаційної безпеки корпоративних баз даних, що обумовлено багатовимірністю та динамічністю поведінкових характеристик користувачів і системних процесів. Isolation Forest ефективно виявляє точкові аномалії у багатовимірному просторі ознак, однак має низку суттєвих обмежень: не враховує часову залежність подій; не аналізує послідовність дій користувача; не здатний виявляти повільні або приховані атаки (low-and-slow attacks); чутливий до вибору ознак і масштабу даних.

Дослідження [8-11] зосереджені на захисті інформаційних ресурсів на основі ризик-орієнтованого підходу для малого та середнього бізнесу з акцентом на якісній оцінці ризиків інформаційної безпеки за допомогою SWOT-аналізу, статистичного методу, методу експертної оцінки та методу Монте-Карло. Науковці вважають, що комплексне застосування інструментів захисту із застосуванням штучного інтелекту дозволить забезпечити надійну безпеку баз даних

Не зважаючи на існування значної кількості підходів до аналізу ризиків, більшість із них мають загальне значення для інформаційної безпеки, не враховують особливості кіберзахисту корпоративних баз даних, відображають в основному якісний підхід та не враховують динаміку загроз у реальному часі.

Оцінювання ризиків інформаційної безпеки є ключовим елементом побудови ефективної системи захисту корпоративних інформаційних ресурсів. На сьогодні найбільш поширеними є підходи, що базуються на міжнародних стандартах та методологіях, зокрема ISO/IEC 27005, NIST SP 800-30, а також моделі оцінювання вразливостей, такі як CVSS.

Стандарт ISO/IEC 27005 визначає загальні принципи управління ризиками інформаційної безпеки та передбачає ідентифікацію активів, загроз і вразливостей із подальшою оцінкою ймовірності та впливу. Основною перевагою даного підходу є його універсальність і можливість застосування до різних типів інформаційних систем. Однак він значною мірою базується на експертних оцінках, що знижує об’єктивність результатів та ускладнює автоматизацію процесу оцінювання [12].

Методологія NIST SP 800-30 орієнтована на проведення оцінки ризиків у державних та корпоративних інформаційних системах і передбачає поетапний аналіз загроз, вразливостей, ймовірності їх реалізації та можливих наслідків. Вона забезпечує більш деталізований підхід до аналізу ризиків, проте, як і ISO/IEC 27005, має переважно статичний характер і не враховує змін у поведінці користувачів або систем у реальному часі [13].

Незважаючи на широке впровадження систем класу SOAR, які забезпечують автоматизацію реагування на інциденти інформаційної безпеки, проблема кількісної оцінки ризику залишається актуальною. SOAR-системи, як правило, не виконують глибокого аналізу ризику, а використовують результати, отримані від SIEM або інших джерел, що обмежує їх здатність до обґрунтованого прийняття рішень.

Окреме місце серед підходів до оцінювання безпеки займає система CVSS (Common Vulnerability Scoring System), яка використовується для кількісної оцінки критичності вразливостей. CVSS дозволяє отримати числове значення рівня небезпеки вразливості на основі таких параметрів, як складність експлуатації, рівень доступу та вплив на систему [14]. Незважаючи на це, дана система оцінює лише окремі вразливості і не враховує контекст їх використання в конкретній інформаційній системі, а також не дозволяє оцінити ризик як інтегральний показник.

Аналіз наведених підходів дозволяє виділити їх спільні недоліки. По-перше, більшість із них мають статичний характер і передбачають періодичну, а не безперервну оцінку ризиків. По-друге, вони практично не враховують поведінкові фактори, такі як аномальна активність користувачів або відхилення від нормальної роботи системи, що є критично важливим у контексті сучасних кіберзагроз. По-третє, існує слабка інтеграція з сучасними системами моніторингу безпеки (SIEM, IDS/IPS), що обмежує можливості автоматизації процесів виявлення та реагування на інциденти.

Таким чином, існуючі підходи до оцінювання ризиків інформаційної безпеки не повною мірою відповідають вимогам сучасних інформаційних систем. Це зумовлює необхідність розробки нових методик, які б поєднували формалізовані математичні моделі з можливостями аналізу даних у реальному часі, зокрема із використанням методів машинного навчання та інтеграцією з SIEM-системами.

Метою статті є розроблення методики інтелектуальної оцінки ризиків інформаційної безпеки корпоративних баз даних, яка поєднує класичні підходи оцінювання ризиків із методами машинного навчання та даними систем моніторингу безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Архітектура методики інтелектуальної оцінки ризику. У сучасних умовах функціонування корпоративних інформаційних систем особливого значення набуває побудова комплексних підходів до обробки подій інформаційної безпеки, які забезпечують не лише їх реєстрацію, але й інтелектуальний аналіз у режимі реального часу. Ефективність такого підходу визначається здатністю інтегрувати різнорідні джерела даних, враховувати поведінкові характеристики користувачів та застосовувати адаптивні алгоритми виявлення аномалій. У цьому контексті запропонована методика орієнтована на формування єдиного аналітичного середовища, що поєднує традиційні механізми моніторингу з сучасними методами машинного навчання.

Архітектура запропонованої методики (рис. 1) реалізує багаторівневу систему обробки подій інформаційної безпеки, що забезпечує інтеграцію різнорідних джерел даних, аналітичних модулів та механізмів реагування.

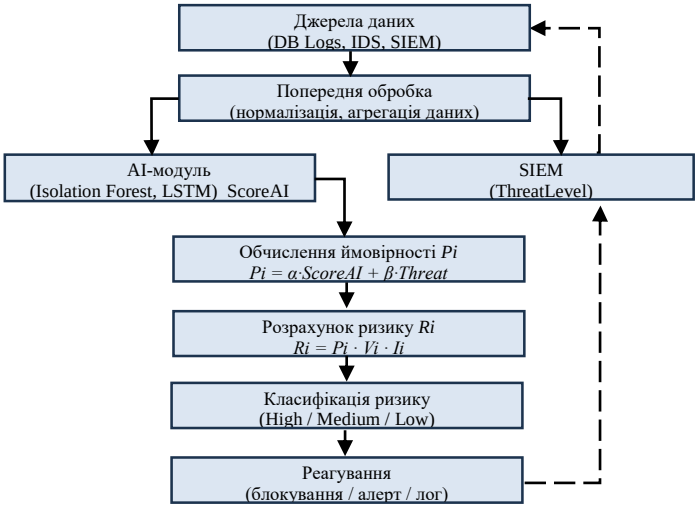

Рис. 1. Архітектура методики інтелектуальної оцінки ризиків інформаційної безпеки корпоративних баз даних

Формування вхідного потоку даних здійснюється з кількох категорій джерел:

– журнали баз даних (DB Logs) – записи SQL-запитів, операцій SELECT/INSERT/UPDATE/DELETE, інформація про користувачів, час доступу, IP-адреси;
– системні журнали (Audit Logs) – події автентифікації, зміни привілеїв, системні виклики;
– мережеві джерела (IDS/IPS) – події мережевого трафіку, сигнатури атак (наприклад, Suricata);
– SIEM-системи – агреговані події безпеки, кореляційні правила, індикатори компрометації.

Таким чином, формується багатовимірний потік подій, який відображає як поведінку користувачів, так і технічний стан системи. Попередня обробка є критично важливим етапом, що забезпечує підготовку даних до аналізу. Різнорідні дані приводяться до єдиного числового масштабу, для чого використовується міні–макс нормалізація:

$$x = \frac{x' - x_{\min}}{x_{\max} - x_{\min}} \quad (1)$$

де x – нормалізоване значення, x' –. початкове значення ознаки.

З метою агрегації події групуються у часові вікна (наприклад, Δt = 1–5 хв) для формування узагальнених характеристик:

$$F_k = \sum_{i=1}^{n} x_i \quad (2)$$

де F_k – агрегована ознака (наприклад, кількість запитів), x_i – окремі події в межах вікна.

На основі сирих даних формуються інформативні ознаки:

– кількість SQL-запитів за інтервал часу;
– частоту помилок автентифікації;

– кількість доступів до критичних таблиць;
– середній час сесії;
– відхилення від типового профілю користувача.

Згруповані інформативні ознаки $X = \{x_1, x_2, ..., x_n\}$ передаються в інтелектуальний модуль (AI-модуль), який є ключовим компонентом запропонованої методики та призначений для виявлення аномальної активності, аналізу поведінкових характеристик користувачів і системи на основі методів машинного навчання. AI-модуль реалізовано у вигляді ансамблю моделей, що поєднує різні підходи до виявлення аномалій:

– Isolation Forest – для виявлення точкових (point anomalies) відхилень у багатовимірному просторі ознак на основі принципу їх ізоляції [15-16];
– LSTM (Long Short-Term Memory) – для аналізу часових залежностей та послідовностей подій [17-18];
– автоенкодери – для виявлення відхилень шляхом реконструкції нормальної поведінки [19].

На відміну від класичних статистичних методів, алгоритм Isolation Forest є ефективним у задачах виявлення рідкісних подій, не потребує попереднього припущення щодо розподілу даних та базується на побудові ансамблю випадкових дерев (ізоляційних дерев – ізоляції аномальних точок), у яких кожна подія послідовно розділяється за випадково обраними ознаками (рис. 2).

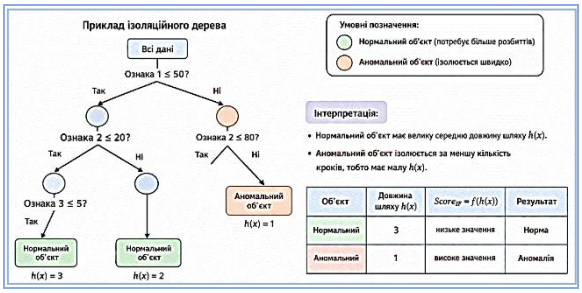

Рис.2. Принцип функціонування моделі Isolation Forest

Аномалії визначаються як об'єкти, які ізолюються за меншу кількість розбиттів від кореня дерева до листа, в який потрапляє об'єкт x (кількість вузлів (split-операцій), які потрібно пройти, щоб ізолювати об'єкт). У рамках алгоритму Isolation Forest об'єктом аналізу є вектор ознак, сформований на основі параметрів доступу до бази даних. Типовими ознаками для визначення аномалій доступу до бази даних в модулі Isolation Forest є: час доступу (ніч / робочий час); IP-адреса; кількість SQL-запитів; тип запитів (SELECT/DELETE/DROP); розмір вибірки; частота звернень.

Наприклад, на етапі попередньої обробки (рис.1) потрібні значення запиту (timestamp: 03:12; ip: 192.168.1.50; user: admin; query: DROP; rows: 0; status: FAIL) після перетворення будуть мати вигляд вектору ознак, як вхідні величини для алгоритму Isolation Forest – *x = [3, 1, 5, 0, 0, 1, 3232235826]*, де: 3 – година; 1 – ніч; 5 – тип запиту (DROP); 0 – admin; 0 – кількість рядків (rows); 1 – статус запиту (FAIL); 3232235826 – IP. Кожен такий вектор відповідає окремій події або агрегованому набору подій та використовується для оцінювання аномальності шляхом визначення довжини шляху ізоляції у дереві. Аномальність доступу до бази даних визначається як функція від середньої довжини шляху ізоляції запиту в ансамблі випадкових дерев. Для нормалізації значення використовується експоненціальна функція, що враховує розмір вибірки та дозволяє інтерпретувати результат у вигляді ймовірнісної оцінки аномалії в діапазоні (0,1):

$$Score_{IF} = f(h(x)) = 2^{-\frac{E(h(x))}{c(n)}} \quad (3)$$

де $h(x)$ – довжина шляху в одному дереві, $E(h(x))$ – середня довжина шляху по всіх деревах, $c(n)$ – нормалізаційний показник, n – кількість об'єктів у вибірці, яка використовується для побудови одного дерева.

Нормалізаційний показник $c(n)$, як еталон нормальної глибини, використовується для приведення середньої довжини шляху ізоляції до відносної шкали, незалежної від розміру вибірки, ще дозволяє інтерпретувати значення функції аномальності (3) у стандартизованому діапазоні та забезпечує коректне порівняння результатів для наборів даних різного розміру:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n} \quad (4)$$

де H – гармонічне число, $H(n)=1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n}$.

Водночас, даний алгоритм Isolation Forest не враховує часову залежність між подіями, що обмежує його ефективність у випадках складних поведінкових атак. Наприклад, є три запити (03:00 → SELECT…; 03:02 → SELECT…; 03:05 → SELECT…) і їх розглядати окремо – вони представляють норму, але якщо розглядати разом – це уже буде аномалія, яку Isolation Forest може не побачити.

Для усунення цього недоліку в інтелектуальному модулі застосовується LSTM-архітектура, яка на відміну від традиційних методів, що аналізують окремі події незалежно одна від одної, обробляє впорядковані у часі послідовності дій користувачів (наприклад, серії SQL-запитів), формуючи внутрішнє представлення поведінкового профілю. Це дозволяє виявляти аномалії, які не можуть бути ідентифіковані при розгляді окремих подій ізольовано. Таким чином, на відміну від класичних алгоритмів (зокрема Isolation Forest), які аналізують події як незалежні об’єкти у просторі ознак, LSTM враховує:

- порядок виникнення подій;
- часові інтервали між ними;
- залежності між попередніми та наступними діями користувача.

Агрегація подій у часові вікна здійснюється на етапі попередньої обробки даних (рис.1) перед подачею їх у модель LSTM. Це дозволяє сформувати узагальнені вектори ознак F_k (2), що відображають інтенсивність та характер активності у відповідному часовому інтервалі. Надалі отримана послідовність векторів використовується як вхідні дані для LSTM, яка моделює часові залежності між агрегованими характеристиками. Для формалізації процесу моделювання поведінки користувачів та виявлення аномалій у доступі до бази даних наведено відповідність між математичними залежностями LSTM [17] та їх кібербезпековою інтерпретацією (табл. 1, рис. 3).

Таблиця 1

Математична інтерпретація механізму LSTM у задачі виявлення аномалій доступу до бази даних

№	Формула	Математичний зміст	Кібербезпекова інтерпретація (доступ до БД)
1	$f_t=\sigma(W_f\cdot[h_{t-1},F_t]+b_f)$	Forget gate (забування)	Визначає, яку частину попередньої активності користувача (історії доступу) слід враховувати. Дає змогу відфільтрувати застарілі або нерелевантні дії (наприклад, старі сесії).
2	$i_t=\sigma(W_i\cdot[h_{t-1},F_t]+b_i)$	Input gate (вхід)	Оцінює важливість поточних подій (наприклад, інтенсивність SQL-запитів, помилки автентифікації) для формування поведінкового профілю.
3	$\tilde{C}=\tanh(W_c\cdot[h_{t-1},F_t]+b_c)$	Кандидат нового стану	Формує нову інформацію про поведінку користувача (наприклад, різке зростання запитів або доступ до критичних таблиць).
4	$C_t=f_t\cdot C_{t-1}+i_t\cdot\tilde{C}_t$	Оновлення пам’яті	Формує актуальний оновлений поведінковий профіль користувача шляхом поєднання історичних і поточних даних. Відображає зміну характеру доступу до БД.
5	$h_t=\sigma(W_o\cdot[h_{t-1},F_t]+b_o)\cdot\tanh(C_t)$	Вихідний стан	Узагальнене представлення поточної поведінки користувача в системі (контекст безпеки в момент часу t).
6	$\hat{F}_t=f(F_{t-1},F_{t-2},...)$	Прогноз	Очікуваний (нормальний) стан активності користувача на основі попередньої поведінки.
7	$E_t=\left\|F_t-\hat{F}_t\right\|$	Помилка прогнозу	Відхилення фактичної поведінки від очікуваної. Велике значення свідчить про потенційну аномалію доступу.
8	$Score_{LSTM}=\frac{1}{T}\sum_{t=1}^{T}\left\|F_t-\hat{F}_t\right\|^2$	Оцінка аномальності	Узагальнена міра аномальності всієї послідовності дій користувача. Використовується для прийняття рішення в SOC.

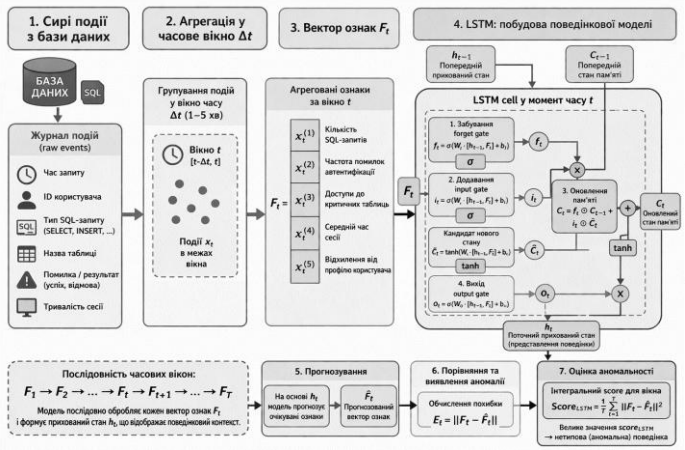

Рис. 3. Алгоритм застосування LSTM для визначення аномалій в захисті баз даних

У наведених формулах (табл. 1, рис. 3) використано позначення:

F_t – вектор агрегованих ознак активності користувача за часовий інтервал Δt;

$\hat{F}_t$ – прогнозоване значення вектора ознак;

h_t – прихований стан LSTM, що відображає поточний поведінковий контекст;

C_t – стан пам’яті (cell state), який акумулює довгострокові залежності;

f_t – яку частину минулої поведінки вважати актуальною;

i_t – важливість нової події (чи враховувати її);

$\tilde{C}_t$ – кандидат нового стану пам’яті (нова поведінкова інформація - ознаки активності);

W , b – параметри моделі (ваги та зміщення);

σ () – сигмоїдна функція активації;

tanh () – гіперболічний тангенс;

E_t – похибка прогнозу (відхилення фактичної поведінки від очікуваної);

$Score_{LSTM}$ – узагальнена оцінка аномальності послідовності.

У контексті захисту баз даних вектор F_t відповідає агрегованим характеристикам активності користувача за певний часовий інтервал, таким як кількість SQL-запитів, частота помилок або доступ до критичних таблиць. Прихований стан h_t та стан пам’яті C_t відображають накопичений поведінковий профіль користувача.

Механізм забування f_t визначає, які аспекти попередньої активності залишаються релевантними, тоді як вхідний механізм i_t контролює вплив нових подій на формування поведінкового контексту. Оновлення стану пам’яті забезпечує інтеграцію історичних і поточних даних, формуючи актуальну модель поведінки.

На основі сформованого контексту модель прогнозує очікувані значення ознак $\hat{F}_t$, а відхилення між прогнозованими та фактичними значеннями використовується для виявлення аномалій доступу до бази даних.

Незважаючи на високу ефективність Long Short-Term Memory у моделюванні часових залежностей та виявленні аномалій у вигляді нетипових послідовностей дій користувачів, даний підхід має певні обмеження. Зокрема, LSTM орієнтована переважно на аналіз динаміки змін ознак у часі та може бути менш чутливою до аномалій, що проявляються у вигляді нетипових комбінацій ознак у межах окремого часового інтервалу. У зв’язку з цим доцільним є використання додаткових методів, здатних виявляти структурні відхилення у багатовимірному просторі ознак. Одним із таких підходів є автоенкодер, який дозволяє здійснювати нелінійне стиснення та відновлення вхідних даних, формуючи компактне представлення нормальної поведінки.

Основною ідеєю автоенкодера є навчання компактного представлення вхідних даних шляхом їх стискання (encoding) та подальшого відновлення (decoding), що дозволяє моделі формувати узагальнений опис нормальної поведінки.

На відміну від LSTM, яка аналізує часові залежності між послідовностями подій, автоенкодер працює з окремими векторами ознак F_t, сформованими на основі агрегованих характеристик доступу до бази даних. Архітектура автоенкодера (рис. 4) складається з двох основних частин: енкодера, який перетворює вхідний вектор у латентне представлення меншої розмірності, та декодера, який відновлює початкові дані з цього представлення.

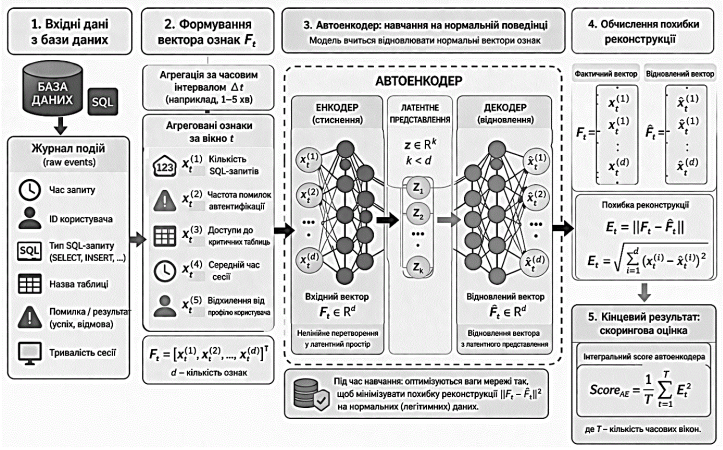

Рис. 4. Алгоритм автоенкодера

У процесі навчання модель мінімізує похибку реконструкції між вхідним та відновленим вектором. У контексті задачі виявлення аномалій автоенкодер навчається на нормальних даних доступу до бази даних, формуючи компактну модель типових комбінацій ознак (наприклад, характерного співвідношення між кількістю запитів, частотою помилок та доступом до критичних таблиць). Для нових даних обчислюється похибка реконструкції:

$$E_t = \left\| F_t - \hat{F}_t \right\| \tag{5}$$

де F_t – фактичний вектор ознак, $\hat{F}_t$ – його відновлене значення.

Похибка реконструкції характеризує ступінь відповідності вхідних даних навченій моделі нормальної поведінки. У випадку, коли вхідний вектор ознак відповідає типовим сценаріям доступу до бази даних, автоенкодер здатний точно його відновити, що призводить до малого значення похибки. Натомість для аномальних даних, які не представлені у навчальній вибірці, точність відновлення суттєво знижується, що проявляється у зростанні похибки реконструкції. Таким чином, величина похибки використовується як індикатор відхилення від нормальної поведінки.

Значне перевищення цієї похибки свідчить про те, що вхідні дані не відповідають навченому профілю нормальної поведінки та можуть бути інтерпретовані як аномалія. Таким чином, автоенкодер дозволяє ефективно виявляти аномалії, що проявляються у вигляді нетипових комбінацій ознак у межах окремого часового інтервалу, доповнюючи можливості LSTM у частині аналізу часових залежностей. Використання цих підходів у сукупності забезпечує більш повне охоплення потенційних сценаріїв атак на корпоративні бази даних.

Кінцева оцінка автоенкодера визначається як середня квадратична похибка реконструкції по всіх часових інтервалах (рис. 4):

$$Score_{AE} = \frac{1}{T}\sum_{t=1}^{T} E_t^{\,2} \tag{6}$$

Дана величина характеризує ступінь відхилення вхідних даних від навченого підпростору нормальної поведінки. Низькі значення $Score_{AE}$ відповідають типовим сценаріям доступу до бази даних, тоді як високі значення свідчать про наявність аномалій, зумовлених нетиповими комбінаціями ознак.

Розглянуті підходи до виявлення аномалій мають різну природу та спрямованість: алгоритм Isolation Forest ефективно виявляє точкові відхилення у просторі ознак, LSTM – аномалії у часових залежностях, а автоенкодер – нетипові структурні комбінації ознак. Водночас жоден із зазначених методів не забезпечує повного охоплення всіх можливих сценаріїв атак на корпоративні бази даних.

Тому, з метою підвищення точності та надійності виявлення аномалій доцільним є використання ансамблевого підходу (рис. 5), що передбачає інтеграцію результатів декількох моделей у єдину скорингову оцінку:

$$Score_{AI} = w_1 \cdot Score_{IF} + w_2 \cdot Score_{LSTM} + w_3 \cdot Score_{AE} \quad (7)$$

де w_1, w_2, w_3 – вагові коефіцієнти ($w_1 + w_2 + w_3 = 1$).

Вагові коефіцієнти w_1, w_2, w_3 визначають внесок кожної моделі у формування інтегральної оцінки та відображають ступінь довіри до відповідного підходу. Значення ваг можуть бути визначені експертним шляхом або на основі оптимізації на валідаційній вибірці з урахуванням метрик якості класифікації за F1-score або ROC-AUC, при цьому нормування вагових коефіцієнтів ($w_1 + w_2 + w_3 = 1$) забезпечує коректне поєднання результатів моделей у єдиній шкалі.

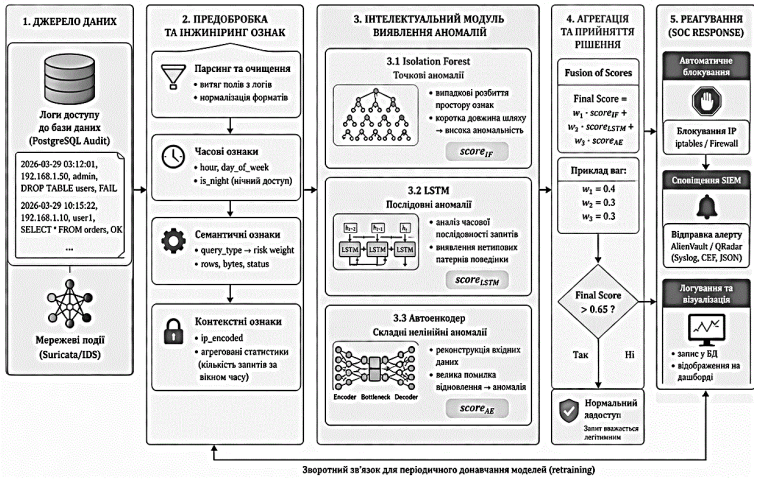

Рис. 5. Інтегрована архітектура інтелектуального модуля виявлення аномалій доступу до корпоративної бази даних на основі Isolation Forest, LSTM та автоенкодера

Отримана інтегральна оцінка $Score_{AI}$ характеризує інтегральну ступінь аномальності та відображає відхилення від нормальних сценаріїв доступу до бази даних. Водночас для прийняття управлінських рішень у системах забезпечення інформаційної безпеки доцільним є перехід від оцінки аномальності до оцінки ризику. Для переходу від оцінки аномалій до оцінки ризику використано підхід, що враховує не лише ступінь аномальності доступу, але й потенційні наслідки інциденту. Узагальнений рівень ризику визначається як:

$$Risk = Score_{AI} * I \qquad Risk \in [0,1], \quad (8)$$

де I, як показник потенційних наслідків інциденту, характеризує критичність ресурсу або операції з базою даних, до якої здійснюється доступ, $I \in [0,1]$.

Показник потенційних наслідків інциденту I може формуватись (табл. 2) як функціональна залежність між критичністю таблиці C, типом операції з базою даних T та рівнем доступу до інформації в базі A:

$$I = f(C, T, A) \quad (9)$$

Таблиця 2

Принцип формування потенційних наслідків інциденту

Подія	I
SELECT звичайної таблиці	0.1
SELECT критичної таблиці	0.5
UPDATE	0.7
DROP / DELETE	0.9–1.0

Для забезпечення автоматизованого реагування введено порогову модель прийняття рішень (Θ_{high} – високий пороговий рівень ризику, Θ_{low} – низький пороговий рівень ризику). У разі перевищення високого порогового значення ризику здійснюється автоматичне блокування доступу (наприклад, блокування IP-адреси або облікового запису). При середньому рівні ризику формується повідомлення для оператора SOC, тоді як низький рівень ризику передбачає лише моніторинг без активного втручання. критично для SOC:

$$\begin{cases} Risk > \Theta_{high} \rightarrow \text{automatic locking} \\ \Theta_{low} < Risk \leq \Theta_{high} \rightarrow \text{SOC notification} \\ Risk \leq \Theta_{low} \rightarrow \text{monitoring} \end{cases} \quad (10)$$

Формування моделі інтелектуальної оцінки ризиків інформаційної безпеки корпоративних баз даних. Експериментальна частина спрямована на перевірку здатності розробленої моделі адекватно виявляти аномалії доступу до бази даних та коректно трансформувати їх у показник ризику. Для цього реалізовано програмний прототип засобами мови програмування Python із використанням сучасних бібліотек машинного навчання, зокрема scikit-learn для реалізації алгоритму Isolation Forest та TensorFlow/Keras для побудови моделей LSTM і Autoencoder, в яких закладені всі перераховані математичні залежності, що визначені у формулах (1-6), в таблиці 1 та на рисунках 3-5.

У межах експерименту сформовано навчальний набір даних (1000 інцидентів), що імітує як нормальні сценарії доступу до бази даних, так і аномальні події, включаючи спроби несанкціонованого доступу, підбір облікових даних, а також виконання нетипових запитів до критичних ресурсів. Дані були попередньо оброблені та агреговані у часові вікна з формуванням інформативних ознак, що використовуються як вхідні параметри моделей.

Для забезпечення коректності експерименту дані розділено на навчальну, валідаційну та тестову вибірки у відсотковому співвідношенні 60/20/20, що дозволяє оцінити узагальнюючу здатність моделей. Навчання кожної складової ансамблю здійснюється незалежно, після чого виконується оцінювання їх ефективності як окремо, так і в сукупності у складі інтегрованої моделі.

Оцінювання якості моделей проводиться з використанням стандартних метрик класифікації, таких як Precision (точність), Recall (повнота), F1-score (якість) та ROC-AUC (ефективність), що дозволяє комплексно проаналізувати їх здатність до виявлення аномалій [19]. Особлива увага приділяється порівняльному аналізу ефективності окремих моделей та ансамблевого підходу, що дає змогу обґрунтувати доцільність їх інтеграції у рамках запропонованої методики (табл. 3, рис. 6).

Таблиця 3

Порівняння ефективності моделей

Модель	Precision	Recall	F1-score	ROC-AUC
Isolation Forest	0.81	0.76	0.78	0.88
LSTM	0.85	0.82	0.83	0.91
Autoencoder	0.83	0.79	0.81	0.89
Ансамбль (Score_AI)	**0.91**	**0.88**	**0.89**	**0.94**

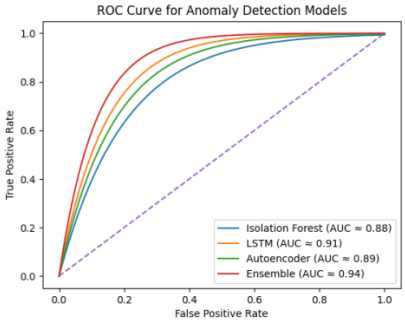

Рис. 6. Порівняння ефективності моделей за ROC-AUC

Отримані результати свідчать про те, що ансамблева модель демонструє найкращі показники за всіма метриками:

– підвищення F1-score на 6-11% порівняно з окремими моделями;
– зростання Recall вказує на зменшення пропущених атак;
– підвищення ROC-AUC свідчить про кращу роздільну здатність моделі.

Таким чином, використання ансамблевої моделі дозволяє підвищити точність та надійність виявлення аномалій, а також забезпечує більш обґрунтовану оцінку ризику в системах захисту корпоративних баз даних.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі запропоновано методику інтелектуальної оцінки ризику захисту баз даних, що базується на ансамблевому поєднанні моделей машинного навчання. На відміну від існуючих підходів, запропонована модель забезпечує багатовимірний аналіз аномалій, враховуючи просторові, часові та структурні характеристики поведінки користувачів. Інтеграція результатів моделей у єдину оцінку $Score_{AI}$ та її подальше перетворення у показник ризику дозволяє перейти від виявлення аномалій до підтримки прийняття рішень у системах кібербезпеки. Запропонований підхід забезпечує адаптивне та автоматизоване реагування на інциденти безпеки залежно від рівня загрози. Отримані експериментальні результати підтверджують підвищення точності виявлення аномалій та зменшення кількості хибних спрацьовувань у порівнянні з використанням окремих моделей.

Перспективи подальших досліджень полягають у вдосконаленні методів адаптивного налаштування вагових коефіцієнтів ансамблю, а також інтеграції запропонованого підходу з системами управління інформаційною безпекою та SIEM-платформами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gracy, S. (2025). *A global analysis of data breaches from 2004 to 2024*. Information Security Group, Royal Holloway, University of London. https://doi.org/10.48550/arXiv.2502.05205
2. Lysetskyi, Y. M., & Kalbazov, D. Y. (2023). Information security of corporate databases. *Mathematical Machines and Systems*, (3), 31-37. https://doi.org/10.34121/1028-9763-2023-3-31-37
3. Kyrychok, R. V., Skladannyi, P. M., Buryachok, V. L., Gulak, G. M., & Kozachok, V. A. (2016). Problems of ensuring control of corporate network security and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications*, 3(43), 48-61. https://journals.dut.edu.ua/index.php/sciencenotes/article/view/772/716
4. Sahinoglu, M. (2024). Cyber security risk assessment and optimal risk management of a national vulnerability database. *International Journal of Computer Theory and Engineering*, 16, 104-126. https://doi.org/10.7763/IJCTE.2024.V16.1359
5. Pevnev, V., & Kapchynskyi, S. (2018). Database security: Threats and preventive measures. *Advanced Information Systems*, 2(1), 69-72. https://doi.org/10.20998/2522-9052.2018.1.13
6. Khlaponin, Y., Izmailova, O., Krasovska, H., Krasovska, K., Bodnar, N., & Abbas, S. Q. (2024). Base of models of the information security risks assessment system. In *2024 35th Conference of Open Innovations Association (FRUCT)*. IEEE. https://doi.org/10.23919/fruct61870.2024.10516397
7. Shchavinskyi, Y., & Budzynskyi, O. (2025). Analysis of current problems of security of corporate databases in the conditions of modern infrastructure and ways to solution them. *Cybersecurity: Education, Science, Technique*, 3(27), 390-405. https://doi.org/10.28925/2663-4023.2025.27.726
8. Shevchenko, S., Zhdanova, Y., & Kravchuk, K. (2021). Information protection model based on information security risk assessment for small and medium-sized business. *Cybersecurity: Education, Science, Technique*, 2(14), 158-175. https://doi.org/10.28925/2663-4023.2021.13.158175
9. Dziuba, L. F., & Chmyr, O. Y. (2022). Information security risk assessment using mathematical statistics methods. *Bulletin of Lviv State University of Life Safety*, 26, 47-54. https://doi.org/10.32447/20784643.26.2022.06
10. de Wit, J., Pieters, W., & van Gelder, P. (2025). Sources of security risk information: What do professionals rely on for their risk assessment? *The Information Society*, 41(3), 157-172. https://doi.org/10.1080/01972243.2025.2475311
11. Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology projects. *International Journal of Information Management*, 32(1), 50-65. https://doi.org/10.1016/j.ijinfomgt.2011.07.002
12. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information technology-Security techniques-Information security risk management*. ISO. https://www.iso.org/standard/80585.html

13. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1
14. FIRST. (2019). *Common vulnerability scoring system (CVSS) v3.1: Specification document*. https://www.first.org/cvss/specification-document
15. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining (ICDM)*. IEEE. https://doi.org/10.1109/icdm.2008.17
16. Chater, M., Borgi, A., Slama, M. T., Sfar-Gandoura, K., & Landoulsi, M. I. (2022). Fuzzy isolation forest for anomaly detection. *Procedia Computer Science*, 207, 916-925. https://doi.org/10.1016/j.procs.2022.09.147
17. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735
18. Kalchbrenner, N., Danihelka, I., & Graves, A. (2015). Grid long short-term memory. *arXiv*. https://arxiv.org/abs/1507.01526
19. Li, X., Li, J., Qu, Y., & He, D. (2020). Semi-supervised gear fault diagnosis using raw vibration signal based on deep learning. *Chinese Journal of Aeronautics*, 33(2), 418-426. https://doi.org/10.1016/j.cja.2019.04.018
20. Powers, D. M. W. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. *Journal of Machine Learning Technologies*, 2(1). https://doi.org/10.9735/2229-3981

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Oleksandr Budzynskyi
Postgraduate Student, Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0002-2402-0711
oleksandr.email@gmail.com

Yurii Shchavinskyi
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-2319-8983
yushchavinsky@ukr.net

Tetiana Muzhanova
Candidate of Science in Public Administration, Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Yuriy Yakymenko
Candidate of Military Sciences, Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-6848-852X
yakum14@ukr.net

Diana Primachenko
Lecturer at the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

METHODOLOGY OF INTELLECTUAL ASSESSMENT OF INFORMATION SECURITY RISKS OF CORPORATE DATABASES

Abstract. The article proposes a methodology for intelligent risk assessment of corporate database security based on the use of an ensemble approach to anomaly detection. Based on the analysis of modern approaches and research in database security, it is concluded that the use of artificial intelligence in protection systems is necessary to account for the complex impact of negative factors on the security of corporate databases. Unlike traditional methods that focus on individual aspects of user behavior, the proposed solution provides a multidimensional analysis through the integration of multiple machine learning models. In particular, the Isolation Forest algorithm is used to detect point anomalies in the feature space, the Long Short-Term Memory model is applied for analyzing temporal dependencies, and the Autoencoder is utilized to identify structural deviations in multidimensional data. An integrated anomaly score is proposed, which is formed by a weighted combination of the outputs of individual models, enabling improved detection accuracy for complex attack scenarios. Based on the obtained anomaly score, a transition to risk assessment is implemented, taking into account the criticality of resources and the types of database access operations. This approach enables adaptive decision-making for responding to information security incidents. A software prototype of the proposed methodology has been developed using the Python programming language with modern machine learning libraries. An experimental study was conducted on a synthetic dataset simulating both normal and anomalous access scenarios. The obtained results confirm the improved effectiveness of the ensemble model compared to individual approaches in terms of Precision, Recall, F1-score, and ROC-AUC metrics. The proposed

methodology can be applied in Security Operations Center (SOC) systems for automated anomaly detection and real-time risk assessment.

Keywords: information security, corporate databases, risk assessment, intelligent methods, machine learning, cyber threats.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Gracy, S. (2025). *A global analysis of data breaches from 2004 to 2024*. Information Security Group, Royal Holloway, University of London. https://doi.org/10.48550/arXiv.2502.05205
2. Lysetskyi, Y. M., & Kalbazov, D. Y. (2023). Information security of corporate databases. *Mathematical Machines and Systems*, (3), 31-37. https://doi.org/10.34121/1028-9763-2023-3-31-37
3. Kyrychok, R. V., Skladannyi, P. M., Buryachok, V. L., Gulak, G. M., & Kozachok, V. A. (2016). Problems of ensuring control of corporate network security and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications*, 3(43), 48-61. https://journals.dut.edu.ua/index.php/sciencenotes/article/view/772/716
4. Sahinoglu, M. (2024). Cyber security risk assessment and optimal risk management of a national vulnerability database. *International Journal of Computer Theory and Engineering*, 16, 104-126. https://doi.org/10.7763/IJCTE.2024.V16.1359
5. Pevnev, V., & Kapchynskyi, S. (2018). Database security: Threats and preventive measures. *Advanced Information Systems*, 2(1), 69-72. https://doi.org/10.20998/2522-9052.2018.1.13
6. Khlaponin, Y., Izmailova, O., Krasovska, H., Krasovska, K., Bodnar, N., & Abbas, S. Q. (2024). Base of models of the information security risks assessment system. In *2024 35th Conference of Open Innovations Association (FRUCT)*. IEEE. https://doi.org/10.23919/fruct61870.2024.10516397
7. Shchavinskyi, Y., & Budzynskyi, O. (2025). Analysis of current problems of security of corporate databases in the conditions of modern infrastructure and ways to solution them. *Cybersecurity: Education, Science, Technique*, 3(27), 390-405. https://doi.org/10.28925/2663-4023.2025.27.726
8. Shevchenko, S., Zhdanova, Y., & Kravchuk, K. (2021). Information protection model based on information security risk assessment for small and medium-sized business. *Cybersecurity: Education, Science, Technique*, 2(14), 158-175. https://doi.org/10.28925/2663-4023.2021.13.158175
9. Dziuba, L. F., & Chmyr, O. Y. (2022). Information security risk assessment using mathematical statistics methods. *Bulletin of Lviv State University of Life Safety*, 26, 47-54. https://doi.org/10.32447/20784643.26.2022.06
10. de Wit, J., Pieters, W., & van Gelder, P. (2025). Sources of security risk information: What do professionals rely on for their risk assessment? *The Information Society*, 41(3), 157-172. https://doi.org/10.1080/01972243.2025.2475311
11. Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology projects. *International Journal of Information Management*, 32(1), 50-65. https://doi.org/10.1016/j.ijinfomgt.2011.07.002
12. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information technology-Security techniques-Information security risk management*. https://www.iso.org/standard/80585.html
13. National Institute of Standards and Technology. (2012) .*Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1
14. FIRST. (2019). *Common vulnerability scoring system (CVSS) v3.1: Specification document*. https://www.first.org/cvss/specification-document
15. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining (ICDM)*. IEEE. https://doi.org/10.1109/icdm.2008.17
16. Chater, M., Borgi, A., Slama, M. T., Sfar-Gandoura, K., & Landoulsi, M. I. (2022). Fuzzy isolation forest for anomaly detection. *Procedia Computer Science*, 207, 916-925. https://doi.org/10.1016/j.procs.2022.09.147
17. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735
18. Kalchbrenner, N., Danihelka, I., & Graves, A. (2015). Grid long short-term memory. *arXiv*. https://arxiv.org/abs/1507.01526

19. Li, X., Li, J., Qu, Y., & He, D. (2020). Semi-supervised gear fault diagnosis using raw vibration signal based on deep learning. *Chinese Journal of Aeronautics*, 33(2), 418-426. https://doi.org/10.1016/j.cja.2019.04.018
20. Powers, D. M. W. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. *Journal of Machine Learning Technologies*, 2(1). https://doi.org/10.9735/2229-3981

Отримано редакцією журналу / Received: 16.02.26
Прорецензовано / Revised: 27.02.26
Схвалено до друку / Accepted: 25.06.26