УДК 004.056:004.658:004.8 DOI: 10.31673/2409-7292.2026.027402

Будзинський Олександр Володимирович
аспірант кафедри Управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0002-2402-0711
E-mail: o.budzynskyi@duikt.edu.ua

ЗАХИСТ КОРПОРАТИВНИХ БАЗ ДАНИХ НА ОСНОВІ РИЗИК-ОРІЄНТОВАНОЇ СЕГМЕНТАЦІЇ ДОСТУПУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

У статті розглянуто проблему підвищення рівня захисту корпоративних баз даних в умовах зростання кількості складних багатокрокових атак та внутрішніх загроз. Проаналізовано обмеження традиційних підходів до контролю доступу, що базуються на статичних політиках і не враховують контекст взаємодії суб'єктів у мережі. Запропоновано метод захисту корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту, який ґрунтується на представленні процесів доступу у вигляді графової моделі. У межах підходу вводиться поняття шляху доступу до бази даних та формується інтегральна оцінка ризику, що враховує критичність вузлів, ймовірність переходів і структуру взаємодії. На основі отриманих значень ризику реалізовано механізм адаптивного реагування, що передбачає динамічне оновлення політик доступу, ізоляцію аномальних потоків у quarantine-сегментах мережі та блокування небезпечних сценаріїв взаємодії. Особливістю запропонованого підходу є орієнтація не на окремі вузли чи події, а на цілісні шляхи доступу, що дозволяє ефективно виявляти та нейтралізувати складні атаки, включаючи латеральне переміщення та приховані аномалії поведінки. Використання методів штучного інтелекту забезпечує адаптивність системи до змін у поведінці користувачів та динаміці мережевого середовища. Перевірка методу у навчальному середовищі та отримані результати експерименту за критеріями F1-score, FPR, ASR підтверджують ефективність запропонованого методу ризик-орієнтованої сегментації доступу, який забезпечує підвищення точності виявлення аномалій, зменшення частки успішних атак та своєчасне реагування на загрози. Запропонований підхід може бути інтегрований у сучасні системи моніторингу безпеки (SIEM/SOC) та використаний для підвищення ефективності захисту інформаційних ресурсів корпоративних систем.

Ключові слова: кібербезпека, корпоративні бази даних, захист інформації, метод сегментації, штучний інтелект, графові моделі доступу.

Вступ

У сучасних умовах цифрової трансформації корпоративні бази даних є ключовими елементами інформаційної інфраструктури, що забезпечують зберігання, обробку та аналіз критично важливої інформації. Зростання обсягів даних, ускладнення архітектур інформаційних систем, а також поширення хмарних і розподілених середовищ призводять до суттєвого підвищення вимог до забезпечення безпеки баз даних.

Одночасно спостерігається збільшення кількості складних кіберзагроз, зокрема атак, що реалізуються через багатокрокові сценарії доступу, включаючи латеральне переміщення всередині мережі, використання легітимних облікових записів та приховані аномалії поведінки користувачів. Традиційні підходи до захисту баз даних, які базуються на статичних моделях контролю доступу (RBAC, DAC), виявляються недостатньо ефективними в умовах динамічного мережевого середовища, оскільки не враховують контекст взаємодії між суб'єктами, часові характеристики доступу та структурні особливості маршрутів доступу до ресурсів.

Сучасні тенденції розвитку кіберзахисту орієнтовані на впровадження адаптивних механізмів управління доступом, які враховують поточний рівень ризику та поведінкові характеристики користувачів. У цьому контексті особливого значення набуває застосування методів штучного інтелекту для виявлення аномалій та підтримки прийняття рішень у системах безпеки. Одним із перспективних напрямів є використання графових моделей для представлення процесів доступу до баз даних, що дозволяє враховувати не лише окремі події, а й цілісні шляхи взаємодії в інформаційній системі. Такий підхід створює передумови для переходу від подієво-орієнтованого до шляхово-орієнтованого аналізу ризиків, що є більш адекватним сучасним сценаріям атак.

Постановка проблеми

Незважаючи на значну кількість досліджень у галузі захисту баз даних та мережевої безпеки, існуючі підходи мають ряд обмежень, що знижують їхню ефективність у сучасних умовах. Зокрема, більшість рішень орієнтовані на аналіз окремих подій або дій користувачів, не враховуючи їх взаємозв'язок у межах складних сценаріїв доступу. Це ускладнює виявлення багатокрокових атак, які реалізуються через послідовність легітимних на перший погляд дій. Крім того, традиційні механізми сегментації мережі та контролю доступу, як правило, є статичними та не адаптуються до зміни рівня загроз у реальному часі. Вони не враховують динаміку формування шляхів доступу до баз даних, що призводить до появи "прихованих" каналів доступу та підвищення ризику несанкціонованого використання ресурсів.

Існує також проблема відсутності інтегрованих підходів, які б поєднували оцінювання ризику доступу, структурний аналіз взаємодій у мережі та механізми автоматизованого реагування. Зокрема, недостатньо дослідженим залишається питання формалізації ризику не окремого суб'єкта або події, а цілісного шляху доступу до бази даних, що включає множину вузлів і переходів між ними.

Таким чином, науковою проблемою є розроблення методу захисту корпоративних баз даних, який повинен забезпечувати оцінювання ризику на рівні шляхів доступу з урахуванням їх структури та динаміки, виявлення аномальних сценаріїв взаємодії в інформаційній системі, адаптивну зміну політик доступу та сегментації мережі залежно від рівня ризику, інтеграцію із сучасними системами моніторингу безпеки для автоматизованого реагування. Вирішення зазначеної проблеми потребує застосування графових моделей представлення доступу та методів штучного інтелекту для аналізу поведінкових характеристик і прогнозування ризиків.

Аналіз публікацій

Проблема захисту корпоративних баз даних та виявлення аномалій доступу активно досліджується у сучасній науковій літературі, особливо в контексті застосування методів штучного інтелекту, машинного навчання та графових моделей. Науковцями у роботі [1] встановлено, що пріоритетною сферою забезпечення безпеки мереж і захисту даних є застосування штучного інтелекту. У роботах останніх років визначено, що традиційні сигнатурні та правило-орієнтовані системи виявлення атак не здатні ефективно реагувати на нові та складні загрози, тоді як моделі машинного навчання дозволяють швидко аналізувати поведінкові характеристики користувачів та виявляти відхилення від нормальної активності. Зокрема, широко застосовуються такі алгоритми, як Isolation Forest, One-Class SVM, Random Forest та градієнтний бустинг, які демонструють ефективність при обробці журналів доступу до баз даних [2].

В дослідженні [3] отримали подальший розвиток методи глибокого навчання, здатні враховувати часову та послідовну структуру подій. Дослідники стверджують, що використання рекурентних нейронних мереж (LSTM) та Автоенкодерів (AE) дозволяє моделювати складні залежності в послідовностях запитів і транзакцій, що є характерним для сучасних атак. Дослідження демонструють, що такі підходи забезпечують високу точність виявлення аномалій і знижують рівень хибних спрацювань.

Окремим напрямом є мережеві та інфраструктурні системи виявлення вторгнень, у яких застосовуються ансамблеві та гібридні моделі [4-5]. Оглядові дослідження підтверджують, що поєднання різних методів машинного навчання дозволяє підвищити стійкість систем до атак і покращити узагальнювальні властивості моделей [6]. Водночас науковцями підкреслюється проблема масштабованості, інтерпретації та адаптації моделей до змін у середовищі.

У сучасних дослідженнях [7-10] пропонуються багатомодельні архітектури, що поєднують виявлення, класифікацію та адаптацію в єдиному циклі, забезпечуючи цілісну систему захисту. Суттєвий інтерес становлять адаптивні системи виявлення аномалій у реальному часі, які здатні реагувати на нові типи загроз без необхідності повного перенавчання моделей. Такі підходи особливо актуальні для критичної інфраструктури та

© Будзинський О.В. Захист корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту. Сучасний захист інформації, 2(66), 21–30.
https://doi.org/10.31673/2409-7292.2026.027402

корпоративних систем. Останнім часом науковцями у дослідженнях [11-13] активно розвивається напрям графових моделей і графових нейронних мереж (GNN) для задач кібербезпеки. У цих підходах користувачі, ресурси, сесії та мережеві взаємодії представляються у вигляді графа, що дозволяє враховувати структурні залежності між об'єктами. Дослідження показують, що графові методи є ефективними для виявлення багатокрокових атак, латерального переміщення та складних сценаріїв взаємодії, які проявляються як аномальні шляхи або зміни структури зв'язків. Крім того, використання графових нейронних мереж дозволяє враховувати як локальні, так і глобальні залежності в мережі. Разом з тим, як показує аналіз досліджень, більшість існуючих рішень орієнтовані на окремі події або записи журналів, ізольовані аномалії або на поведінку окремих користувачів. При цьому, недостатньо уваги приділяється аналізу цілісних шляхів доступу до баз даних, які формуються як послідовність взаємодій між різними вузлами системи. Також недостатньо досліджені питання інтеграції оцінювання ризику з механізмами мережевої сегментації та автоматизованого реагування. Крім того, науковці зазначають про необхідність переходу до адаптивних і контекстно-орієнтованих систем кіберзахисту, які повинні враховувати поведінкові характеристики та динаміку середовища, швидкість їх еволюції та адаптації до захисних механізмів [14-15]. Зокрема, зростаюча роль концепцій Zero Trust та безперервної оцінки довіри потребує розроблення нових моделей оцінювання ризику доступу.

Таким чином, аналіз публікацій свідчить про наявність наукової прогалини, пов'язаної з відсутністю комплексного підходу, який повинен поєднувати графове представлення доступу до баз даних, кількісне оцінювання ризику на рівні шляхів, адаптивну сегментацію та механізми реагування, використання методів штучного інтелекту для підтримки прийняття рішень. Заповнення цієї прогалини і визначає актуальність та наукову новизну запропонованого в роботі підходу.

Мета та завдання дослідження

Мета дослідження полягає у підвищенні рівня захисту корпоративних баз даних шляхом розроблення методу ризик-орієнтованої сегментації доступу на основі аналізу шляхів доступу та використання методів штучного інтелекту. Для досягнення мети необхідно: здійснити аналіз існуючих підходів; побудувати графову моделі доступу та оцінювання ризику шляхів; розробити механізм адаптивної сегментації; експериментально перевірити ефективність запропонованого методу**.**

Виклад основного матеріалу

У сучасних корпоративних інформаційних системах забезпечення безпеки баз даних потребує переходу від статичних механізмів контролю доступу до адаптивних моделей, що враховують динаміку взаємодії суб'єктів та ресурсів. Одним із перспективних напрямів є застосування ризик-орієнтованої сегментації доступу, який дозволяє приймати рішення щодо обмеження або дозволу доступу на основі поточного рівня загрози. На відміну від традиційних підходів, у яких сегментація здійснюється на рівні вузлів або мережевих зон, у даній роботі пропонується підхід, заснований на аналізі шляхів доступу до бази даних, що формуються як послідовності взаємодій вузлів та сегментів у мережі. Такий підхід дозволяє враховувати складні багатокрокові сценарії атак, включаючи латеральне переміщення та використання легітимних облікових записів. Для реалізації запропонованого підходу використовується графова модель представлення доступу, а також методи штучного інтелекту для оцінювання ймовірностей переходів і виявлення аномальних сценаріїв. Це забезпечує можливість адаптивного управління доступом до баз даних у реальному масштабі часу.

Графова модель доступу до корпоративної бази даних

Використання графових моделей для представлення процесів доступу до баз даних (рис. 1) є одним із перспективних напрямів, який дозволяє враховувати не лише окремі події, а й цілісні шляхи взаємодії в інформаційній системі. Для формалізації процесів доступу до корпоративної бази даних запропоновано використовувати орієнтовану графову модель $G =$

© Будзинський О.В. Захист корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту. Сучасний захист інформації, 2(66), 21–30.
https://doi.org/10.31673/2409-7292.2026.027402

(V, E), де V – множина вузлів, що відповідають суб'єктам (користувачам, процесам), ресурсам (сервери, бази даних,), сегментам мережі (VLAN) та проміжним елементам інфраструктури, а E– множина ребер, що відображають можливі переходи доступу між вузлами. Кожному вузлу v ∈ Vставиться у відповідність вагова характеристика I(v), яка відображає рівень його критичності або потенційного впливу на безпеку системи. Ребра графа характеризуються ймовірностями переходів за різними шляхами, що можуть змінюватися в часі та відображають динаміку доступу.

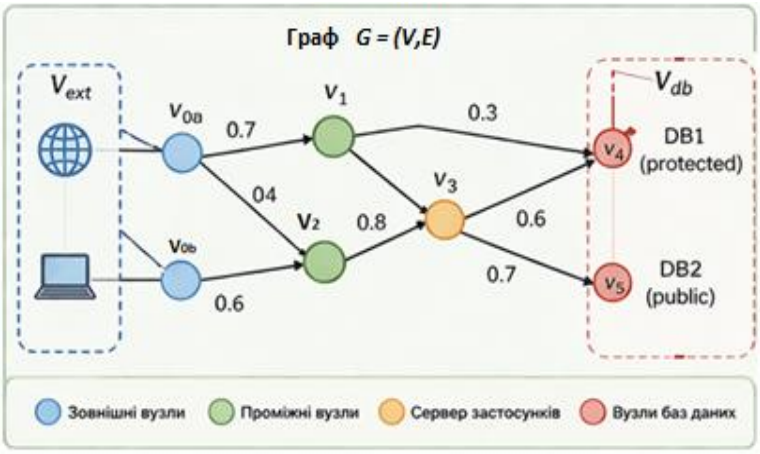

Рис. 1. Принципова графова модель

У такій постановці доступ до бази даних розглядається не як окрема подія, а як послідовність переходів, тобто шлях: $\pi = (v_1, v_2, \ldots, v_n), v_n = \text{DB}$. Кожне ребро v∈E характеризується коефіцієнтом p_{uv}, який інтерпретується як імовірність успішного поширення атаки між відповідними вузлами (від v-1 до v):

$$p_{uv}(t) = \sqrt{q_{v-1}(t) \cdot q_v(t)}\,, \tag{1}$$

де $q_{v-1}(t), q_v(t)$ – інтегральні оцінки аномальності вузла v та попереднього вузла *v-1* в момент часу t, $q_v \in [0,1]$.

З метою своєчасного реагування на загрози, що динамічно змінюють поверхню ризиків оцінювання аномальності у вузлах здійснюється із використанням ансамблю моделей машинного навчання у вигляді створеного AI-контролера (Isolation Forest (IF) – наскільки вузол/сесія нетипові, Long Short-Term Memory (LSTM) – наскільки нетипова послідовність дій, Autoencoder (AE) – наскільки поточний стан відхиляється від норми), на основі їх результатів формується інтегральний показник аномальності:

$$q_v(t) = \sigma(\alpha s_{IF}(v,t) + \beta s_{LSTM}(v,t) + \gamma s_{AE}(v,t))\,, \tag{2}$$

де $q_v(t)$ – інтегральна оцінка аномальності вузла v у момент часу t, $q_v \in [0,1]$; $s_{IF}(v,t)$ – оцінка аномальності, отриманий методом Isolation Forest; $s_{LSTM}(v,t)$ – оцінка поведінкової аномалії за LSTM; $s_{AE}(v,t)$ – помилка реконструкції Автоенкодера; α, β, γ – вагові коефіцієнти моделей, $\alpha + \beta + \gamma = 1$; $\sigma(\cdot)$ – сигмоїдна функція нормалізації.

Вагові коефіцієнти (α, β, γ) визначають внесок кожної моделі у фінальну оцінку та можуть розраховуватись емпірично на основі висновків експертів чи за результатами оцінювання якості моделей за метриками якості, наприклад, F1-score.

Зокрема, оцінка Isolation Forest s_{IF} у формулі (2) визначається на основі середньої довжини ізоляції об'єкта в ансамблі випадкових дерев [16]:

$$s_{IF}(v,t) = 2^{-\frac{E(h(x))}{c(n)}}, \quad (3)$$

де $E(h(x))$ – середня довжина шляху для об'єкта; $c(n)$– очікувана довжина шляху для нормальних точок, яка залежить від розміру вибірки n.

Оцінка LSTM s_{LSTM} [17] у формулі (2) на основі обробки впорядкованих у часі послідовностей дій користувачів (наприклад, серії SQL-запитів) формулює внутрішнє нормальне представлення поведінкового профілю та визначає різницю між нормальним і створеним профілем у часовому проміжку. Це дозволяє виявляти аномалії, які не можуть бути ідентифіковані при розгляді окремих подій протягом кількох часових проміжків *T*:

$$s_{LSTM}(v,t) = \frac{1}{T}\sum_{t=1}^{T}\left\|F_t - \hat{F}_t\right\|^2, \quad (4)$$

де F_t – вектор агрегованих ознак активності користувача за часовий інтервал Δt; $\hat{F}_t$ – прогнозоване значення вектора ознак.

При використанні Автоенкодера [17] у формулі (2) використовується реконструкційна помилка s_{AE} яка 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:

$$s_{AE}(v,t) = \frac{1}{d}\sum_{i=1}^{d}\left(x_t^{(i)} - \hat{x}_t^{(i)}\right)^2, \quad (5)$$

де $x_t^{(i)}$– реальне значення ознаки (те, що реально прийшло із запиту до БД); $\hat{x}_t^{(i)}$– відновлене значення (те, що Автоенкодер вважає "нормальним"); d – кількість ознак.

Для забезпечення коректного обчислення оцінок LSTM та Автоенкодера необхідно виконувати нормалізацію вхідних ознак, оскільки різні масштаби параметрів можуть призводити до домінування окремих компонент у значенні функції втрат. Нормалізація σ приводить значення до інтервалу [0, 1], що забезпечує узгоджене об'єднання оцінок.

Розрахунок ймовірності шляхів (π) від V_{ext} до V_{db}

Шлях π	Послідовність вузлів	Ймовірність $P(\pi) = \prod p_{uv}$
π_1	$v_{0e} \to v_1 \to v_3 \to v_4$ (DB1)	$0.7 \cdot 0.5 \cdot 0.6 = 0.21$
π_2	$v_{0e} \to v_2 \to v_3 \to v_5$ (DB2)	$0.6 \cdot 0.8 \cdot 0.7 = 0.336$

Рис. 2. Розрахунок ймовірності шляхів

Ймовірність успішного проходження атаки по кожному шляху π (рис. 2) в момент часу *t* визначається як добуток імовірностей успішного поширення атаки між відповідними вузлами, розрахованих за формулою (1):

$$P(\pi,t) = \prod_{v\in\pi} p_v(t). \quad (6)$$

Таким чином, будь-який шлях від користувача, який може бути порушником, до цільового ресурсу (бази даних) описує потенційний сценарій реалізації загрози. Для кількісного оцінювання рівня загрози запропоновано функцію ризику шляху доступу, яка враховує як структурні, так і ймовірнісні характеристики:

$$R(\pi, t) = I(\text{DB}) \cdot \exp\left(\lambda \cdot P(\pi, t) \cdot \sum_{v \in \pi} I(v)\right), \quad (7)$$

де $I(\text{DB})$ – критичність цільового ресурсу (бази даних); $P(\pi, t)$ – ймовірність реалізації шляху доступу π у момент часу t; $\sum_{v \in \pi} I(v)$ – сумарна критичність вузлів, що входять до шляху; λ – коефіцієнт чутливості моделі.

Функція (7) дозволяє враховувати накопичувальний ефект ризику при проходженні через декілька вузлів, що є характерним для багатокрокових атак. Використання експоненціальної залежності забезпечує підсилення впливу критичних сценаріїв доступу. Запропонована графова модель оцінювання ризику шляхів доступу до бази даних дозволяє не лише кількісно визначати рівень загрози, але й формувати основу для побудови адаптивного механізму реагування, орієнтованого на динамічне управління доступом у корпоративній інформаційній системі.

Механізм адаптивного реагування

На основі визначення ризику шляху за формулою (7) вводиться три рівні ризику: низький рівень – $R(\pi,t) \le \theta_1$; середній рівень – $\theta_1 < R(\pi,t) \le \theta_2$; високий рівень – $R(\pi,t) > \theta_2$. Порогові значення θ_1 та θ_2 визначаються емпірично або на основі навчання моделі та можуть адаптуватися залежно від характеристик середовища. Такий підхід дозволяє перейти від абсолютних оцінок до контекстно-залежного аналізу ризику, що є більш релевантним для сучасних систем кіберзахисту. Таким чином, система реалізує принцип risk-driven access control, за якого рішення про доступ приймаються не статично, а на основі поточного стану графової моделі взаємодії.

На основі оціненого ризику реалізується механізм адаптивного реагування, який включає три рівні впливу (рис.3).

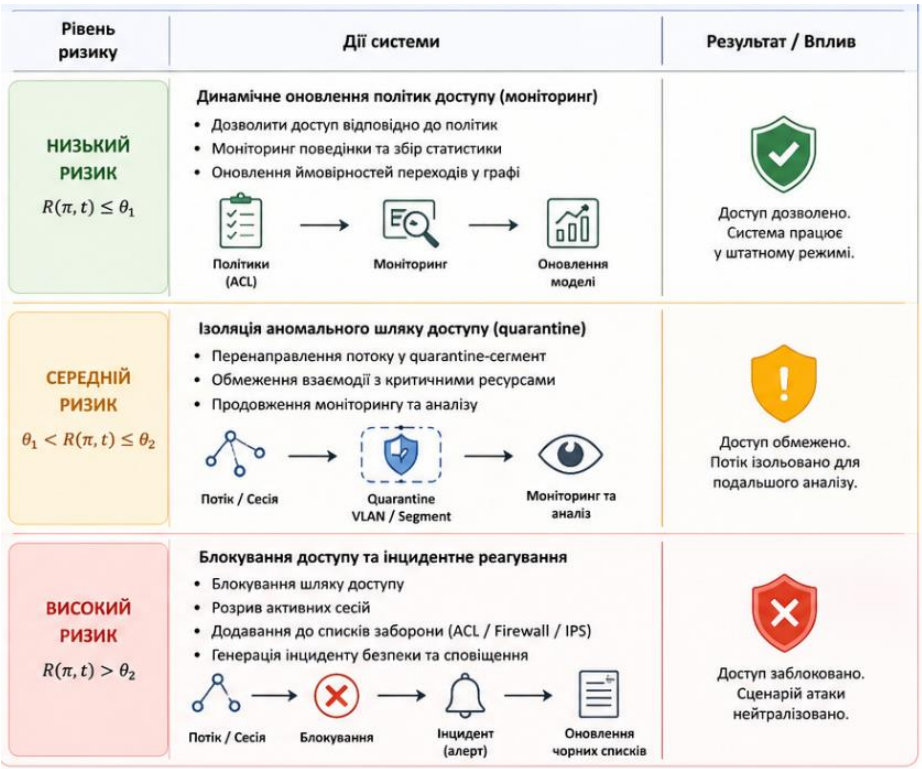

Рис. 3. Схема механізму адаптивного реагування

Таким чином, на відміну від традиційних моделей, у яких рішення приймається на основі окремих подій або атрибутів користувача, у даному підході об’єктом аналізу виступає шлях доступу π, що відображає послідовність взаємодій у системі. На основі побудованої графової моделі виконується оцінювання ризику $R(\pi,t)$, яке враховує як критичність вузлів, так і ймовірність реалізації відповідного сценарію доступу. Методи штучного інтелекту використовуються для оцінювання ймовірностей переходів та адаптації параметрів моделі до змін у поведінці системи. Отримане значення ризику використовується для динамічного прийняття рішень щодо сегментації доступу, яка реалізується на рівні потоків або сесій і включає дозволи, ізоляцію або блокування. Зворотний зв’язок забезпечує адаптацію моделі та підвищення точності виявлення аномальних сценаріїв.

Для підтвердження ефективності запропонованого методу ризик-орієнтованої сегментації доступу до корпоративних баз даних проведено експериментальне дослідження в умовах, наближених до реальної експлуатації інформаційної системи. Реалізація методу виконана мовою Python із використанням бібліотек NumPy та Pandas для обробки даних, Scikit-learn для реалізації алгоритмів машинного навчання, PyTorch для побудови нейронних мереж, NetworkX для моделювання графової структури мережі, а також Matplotlib для візуалізації результатів. Інтеграція з мережевим обладнанням здійснювалась за допомогою бібліотек Netmiko та Paramiko. Експеримент проводився на реальному мережевому обладнанні Cisco з використанням консольного доступу, що забезпечує практичну перевірку ефективності методу сегментації.

Рис. 4. Схема проведення експерименту

Для проведення експерименту в навчальній аудиторії (рис. 4) налаштована Wi-Fi мережа на маршрутизаторі Cisco 1841 із створеними VLAN (Users (10), App (20), DB (30), SOC (40),

quarantine VLAN(999) - для динамічного переміщення в нього підозрілих вузлів) та точкою доступу на AIR-CFP1602I-R-K9, 10 ПК користувачів, з них один з AlienVault OSSIM та встановленим розробленим блоком AI-контролера (що на основі штучного інтелекту обробляє мережевий трафік і поведінкові характеристики вузлів). Атакуюча платформа реалізована підготовленими сценаріями для атак на окремому ПК з встановленою Kali Linux системою, задані контрольні списки доступу ACL. У сегменті SOC розгорнуто систему моніторингу безпеки на базі AlienVault OSSIM, яка виконує збір і кореляцію подій безпеки.

AI-модуль формує оцінку аномальності $s(v,t)$, яка використовується для виявлення підозрілої активності та прийняття рішень щодо зміни політик доступу. В якості вхідних даних використовувалися лог-файли журналів доступу до бази даних та мережевих подій як легітимних сценаріїв взаємодії користувачів із системою, так і змодельованих атак різного рівня складності, зокрема: підбір облікових даних (brute-force); SQL-ін'єкції; багатокрокові сценарії доступу з елементами латерального переміщення. На основі цих даних формувався граф доступу, у якому вузли відповідали суб'єктам і ресурсам, а ребра – можливим переходам доступу. Для виявлення аномалій використовувався розроблений AI-контролер, що поєднує запропоновані алгоритми машинного навчання, а оцінювання ризику здійснювалося для шляхів доступу до бази даних.

Оцінювання ефективності здійснювалося за такими показниками: F1-score – для оцінки якості виявлення аномалій; False Positive Rate (FPR) – рівень хибних спрацювань; Attack Success Rate (ASR) – частка атак, що досягли цільового ресурсу; час реагування – затримка між виявленням аномалії та застосуванням заходів реагування.

У якості базових підходів для порівняння використано класичні методи виявлення аномалій та статичні політики контролю доступу в AlienVault без використання AI-контролера.

Отримані результати, як середні значення за 12 сценаріями і в кожному по 10 реалізацій, наведено в таблиці 1.

Таблиця 1

Порівняння ефективності підходів

Підхід	F1-score	FPR	ASR
Статичні ACL	0.72	0.18	0.48
Класичні ML-методи	0.84	0.14	0.32
Запропонований метод	0.90	0.11	0.20

Як видно з результатів, запропонований метод забезпечує підвищення якості виявлення аномалій (F1-score до 0.90) при зменшенні рівня хибних спрацювань. Водночас частка успішних атак зменшилась більш ніж удвічі порівняно з традиційними підходами.

Середній час реагування системи (час спрацювання всієї системи прийняття рішення + застосування політики) становив 180–250 мс, що підтверджує можливість її використання в режимі, наближеному до реального часу.

Отримані результати підтверджують ефективність запропонованого методу ризик-орієнтованої сегментації доступу, який забезпечує підвищення точності виявлення аномалій, зменшення частки успішних атак та своєчасне реагування на загрози. Це свідчить про доцільність його застосування у системах захисту корпоративних баз даних.

Висновки

У роботі вирішено актуальну науково-практичну задачу підвищення рівня захисту корпоративних баз даних в умовах зростання складності кіберзагроз та динамічності мережевих середовищ. Проведений аналіз сучасних підходів показав обмеженість традиційних моделей контролю доступу, які не враховують контекст взаємодії та структуру шляхів доступу до інформаційних ресурсів.

© Будзинський О.В. Захист корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту. Сучасний захист інформації, 2(66), 21–30. https://doi.org/10.31673/2409-7292.2026.027402

Запропоновано метод захисту корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту, який дозволяє враховувати як критичність вузлів, так і ймовірність переходів між ними. Основою методу є механізм адаптивного реагування, який забезпечує динамічне оновлення політик доступу, ізоляцію аномальних потоків у quarantine-сегментах та блокування небезпечних сценаріїв взаємодії залежно від рівня ризику. Особливістю підходу є те, що об’єктом впливу виступає не окремий користувач або подія, а повний шлях доступу, що дозволяє ефективно протидіяти багатокроковим атакам, зокрема латеральному переміщенню.

Практичне значення отриманих результатів полягає у можливості інтеграції запропонованого методу в сучасні системи моніторингу безпеки (SIEM/SOC) та використанні для автоматизованого управління доступом у корпоративних інформаційних системах. Використання методів штучного інтелекту забезпечує адаптивність та підвищує точність виявлення аномалій у реальному часі.

Подальші дослідження доцільно спрямувати на експериментальну валідацію запропонованого підходу на реальних наборах даних, оптимізацію обчислювальної складності алгоритмів, а також інтеграцію з технологіями Zero Trust та системами автоматизованого реагування (SOAR).

Перелік посилань

1. Savchenko, V. A., & Shapovalenko, O. D. (2020a). The main areas of artificial intelligence technologies in cybersecurity. Modern information security, 44(4), 6-11. https://doi.org/10.31673/2409-7292.2020.040611.

2. Mr. Jalindhar Banshi Kachule, Prof. Badrinath Bulepatil, Prof. Vishal Gejge & Prof. Atish Ashokrao Shriniwar. (2025). AI for Database Security Anomaly Detection: Leveraging Machine Learning for Real-Time Threat Identification. International Journal of Latest Technology in Engineering Management & Applied Science, 14(8), 1039–1045. https://doi.org/10.51583/ijltemas.2025.1408000133.

3. Пелещак, І., & Футрик, Ю. (2025). Прогнозування часових рядів за допомогою нейромережі з послідовно з'єднаними lstm блоками. Herald of Khmelnytskyi National University. Technical sciences, 347(1), 432–441. https://doi.org/10.31891/2307-5732-2025-347-59.

4. 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.

5. Pan X., Obahiaghon A., Makar B., Wilson S., Beard C. (2024). Analysis of database security. Open Access Library J. 11(04), 1–9.. URL: https://doi.org/10.4236/oalib.1111366.

6. 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.

7. 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.

8. Reddy, C., Prabhagaran, S., & Vaid, A. (2025). Adaptive Anomaly Detection in Database Transactions: Bridging Security Gaps with Reinforcement Learning. European Journal of Artificial Intelligence and Machine Learning, 4(2), 8–14. https://doi.org/10.24018/ejai.2025.4.2.53.

9. Raeiszadeh, M., Ebrahimzadeh, A., Glitho, R. H., Eker, J., & Mini, R. A. F. (2024). Real-Time Adaptive Anomaly Detection in Industrial IoT Environments. IEEE Transactions on Network and Service Management, 1. https://doi.org/10.1109/tnsm.2024.3447532.

10. Bajic, B., Rikalovic, A., Suzic, N., & Piuri, V. (2024). Toward a Human-Cyber-Physical System for Real-Time Anomaly Detection. IEEE Systems Journal, 1–12. https://doi.org/10.1109/jsyst.2024.3402978.

11. Pujol-Perich, D., Suarez-Varela, J., Ferriol, M., Xiao, S., Wu, B., Cabellos-Aparicio, A., & Barlet-Ros, P. (2021). IGNNITION: Bridging the Gap between Graph Neural Networks and Networking Systems. IEEE Network, 35(6), 171–177. https://doi.org/10.1109/mnet.001.2100266.

12. Zhong, M., Lin, M., Zhang, C., & Xu, Z. (2024). A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges. Computers & Security, 141, 103821. https://doi.org/10.1016/ j.cose. 2024.103821.

13. Caville, E., Lo, W. W., Layeghy, S., & Portmann, M. (2022). Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. Knowledge-Based Systems, 110030. https://doi.org/10.1016 /j.knosys.2022.110030.

14. Okdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. Applied Sciences, 14(22), 10487. https://doi.org/10.3390/app142210487.

© Будзинський О.В. Захист корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту. Сучасний захист інформації, 2(66), 21–30. https://doi.org/10.31673/2409-7292.2026.027402

15. Шульга, В., Іванченко, Є., Берестяна, Т., & Шкурченко, О. (2025). Методи та моделі протидії груповим кіберзагрозам на основі штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 593–606. https://doi.org/10.28925/2663-4023.2025.30.998.

16. 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. https://doi.org/10.1109/TKDE.2023.3270293.

17. Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. Computers in Industry, 131, 103498. https://doi.org/10.1016/j.compind.2021.103498.

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
E-mail: o.budzynskyi@duikt.edu.ua

PROTECTION OF CORPORATE DATABASES BASED ON RISK-ORIENTED ACCESS SEGMENTATION USING ARTIFICIAL INTELLIGENCE

The article considers the problem of increasing the level of protection of corporate databases in the face of an increasing number of complex multi-step attacks and internal threats. The limitations of traditional approaches to access control, which are based on static policies and do not take into account the context of interaction between subjects in the network, are analyzed. A method for protecting corporate databases based on risk-based access segmentation using artificial intelligence is proposed, which is based on the representation of access processes in the form of a graph model. Within the framework of the approach, the concept of a database access path is introduced and an integrated risk assessment is formed, which takes into account the criticality of nodes, the probability of transitions and the structure of interaction. Based on the obtained risk values, an adaptive response mechanism is implemented, which involves dynamic updating of access policies, isolation of anomalous flows in quarantine segments of the network and blocking of dangerous interaction scenarios. A feature of the proposed approach is the focus not on individual nodes or events, but on holistic access paths, which allows for effective detection and neutralization of complex attacks, including lateral movement and hidden behavioral anomalies. The use of artificial intelligence methods ensures the system's adaptability to changes in user behavior and the dynamics of the network environment. Verification of the method in the training environment and the obtained experimental results using the F1-score, FPR, ASR criteria confirm the effectiveness of the proposed method of risk-based access segmentation, which provides increased accuracy in anomaly detection, reduced proportion of successful attacks, and timely response to threats. The proposed approach can be integrated into modern security monitoring systems (SIEM/SOC) and used to improve the effectiveness of protecting information resources of corporate systems.

Keywords: cybersecurity, corporate databases, information protection, segmentation method, artificial intelligence, graph access models.

Надійшла до редакції (Received): 07.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Будзинський О.В. Захист корпоративних баз даних на основі ризик-орієнтованої сегментації доступу з використанням штучного інтелекту. Сучасний захист інформації, 2(66), 21–30.
https://doi.org/10.31673/2409-7292.2026.027402