14. Надвоцький О.Ю., Кобозєва А.А. Метод розв'язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. http: // immm.op.edu.ua / files / archive / n3_v11_2021/immm_ n3_ v11_2021.pdf.

15.Сокальський С. М. Модифікація методу вибору контейнера для зменшення чутливості стеганоповідомлення до збурних дій. Informatics and Mathematical Methods in Simulation Vol.13 (2023), No. 3-4, pp. 311-321 http://immm.op.edu.ua/files/archive/n3-4_v13_2023/2023_3-4(14).pdf.

16. Bobok I., Kobozieva A., Sokalsky S. The Problem of Choosing a Steganographic Container in Conditions of Attacks against an Embedded Message. https://journal.ie.asm.md/assets/files/07_04_56_2022.pdf.

17. Gonzalez R., Voods R. Digital image processing. 3nd ed. NJ: Pearson, 2018. https: // www.cl72.org/ 090image-PLib/books/Gonzales, Woods-Digital.Image.Processing.4th.Edition.pdf.

18. Борисенко І.І. Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень. Сучасна спеціальна техніка. 2014. №2(37). С. 110 -115. https://suchasnaspectehnika.com /journal/ukr/2020_2/3.pdf.

19. Борисенко І.І. Метод оцінки збурень контейнера внаслідок його стеганографічного перетворення.10 МНПК Військова освіта і наука: сьогодення та майбутнє. 2014. https: // suchasnaspectehnika.com / journal / ukr / 2020_2/3.pdf.

20. Кобозева А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованого на теорії збурень. Информационные технологии и компьютерная инженерия. 2008.№1(11).С.164-171.

21. Кобозева А.А., Борисенко И.И. Повышение помехоустойчивости стеганографических методов, использующих сингулярное и спектральное разложение матрицы контейнера. Труды одесского политехнического университета.2007. №2(28). С. 192-198. https: // old-pratsi.op.edu.ua / app / webroot / articles / 1312737920.pdf.

22. Борисенко І.І. Застосування теорії графів в задачах створення стеганографічних повідомлень. Сучасна спеціальна техніка. 2015. №2. С. 26-33.

Надійшла до редакції (Received): 10.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056:[004.032.26+519.17
DOI: 10.31673/2409-7292.2026.010224

Гашко А.О., Ананченко О.Є.

ГРАФОВІ НЕЙРОННІ МЕРЕЖІ ДЛЯ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ У КРОСЧЕЙН-БЛОКЧЕЙН СЕРЕДОВИЩАХ

Поширення кросчейн-мостів та рішень агрегації другого рівня (Layer-2) принципово трансформувало структуру блокчейн-транзакційних мереж, одночасно створивши нові канали для протиправної фінансової активності, що уникає традиційних механізмів протидії відмиванню коштів (AML). Ранні спроби використання науки про дані для блокчейн-аналітики, зокрема методів кластеризації та розпізнавання шаблонів на великих наборах даних, заклали необхідне підґрунтя для розуміння аномальної поведінки у децентралізованих реєстрах – що підтверджується попередньою роботою з порівняння алгоритмів кластерного моделювання на великих даних, отриманих із записів розподілених реєстрів (наприклад, порівняння алгоритмів побудови кластерних моделей на блокчейн-похідних наборах даних. Однак ці попередні методології здебільшого обмежувалися офлайн-аналізом і статичними парадигмами кластеризації. У цій статті ми розвиваємо це базове дослідження, пропонуючи фреймворк на основі графових нейронних мереж (GNN) для оцінювання AML-ризиків у реальному часі в межах кількох гетерогенних блокчейн-мереж. На відміну від ранніх кластероцентричних підходів, запропонована модель будує єдиний темпоральний кросчейн-граф, який інтегрує внутрішньомережеву активність, взаємодії через кросчейн-мости та події розрахунків Layer-2 в узгоджену структуру. Архітектура GNN із передаванням повідомлень використовується для навчання інформативних ембедингів вузлів, що відображають реляційні залежності та часову динаміку між мережами, із застосуванням механізмів часового згасання та зважування типів ребер для підвищення чутливості до відкладених і фрагментованих тактик відмивання. Ми виводимо ймовірнісну функцію ризикового скорингу на основі навчених ембедингів і оптимізуємо модель за допомогою композитної функції втрат, яка балансує якість класифікації, гладкість графа та часову стабільність. Фреймворк оцінено на реальних даних мереж Ethereum, BNB Chain, Solana та TON, що охоплюють кросчейн-перекази, депозити та P2P-

© Борисенко І.І. Проблема вибору контейнера для забезпечення стійкості стего до збурних дій. Сучасний захист інформації, 1(65), 8–14.
https://doi.org/10.31673/2409-7292.2026.010115

перекази. Експериментальні результати демонструють зниження частоти хибнопозитивних спрацювань на 25–40 % та підвищення повноти (recall) на 15–18 % порівняно з базовими одно-мережевими AML-моделями, зберігаючи можливість інференсу в реальному часі, придатну для промислового впровадження. Спираючись безпосередньо на висновки ранніх досліджень кластерного моделювання та розвиваючи їх через глибоке графове навчання представлень, запропонований фреймворк пропонує масштабоване, пояснюване та технічно стійке рішення для AML-моніторингу в сучасних кросчейн-блокчейн-середовищах.

Ключові слова: blockchain, кросчейн, нейронні мережі, розподілені ресурси, інформаційна система, моніторинг, кластерне моделювання.

Вступ

Стрімкий розвиток блокчейн-технологій та поява механізмів інтероперабельності, зокрема кросчейн-мостів, протоколів агрегації Layer-2 і рішень для багатоланцюгових транзакцій, суттєво змінили архітектуру сучасних децентралізованих фінансових систем. Поряд із розширенням функціональних можливостей такі технології створили нові виклики у сфері протидії відмиванню коштів (AML), оскільки дозволяють фрагментувати фінансові потоки між кількома блокчейн-мережами та ускладнюють кореляцію транзакцій у межах традиційних одно-мережевих моделей аналізу. У результаті зростає ризик обходу класичних механізмів фінансового моніторингу, що актуалізує потребу в нових аналітичних підходах до виявлення протиправної активності в кросчейн-середовищах.

Сучасні дослідження демонструють ефективність графоорієнтованих методів і графових нейронних мереж для аналізу складних транзакційних структур у блокчейн-мережах, однак більшість існуючих рішень зосереджені на статичних або ізольованих сценаріях аналізу. Недостатньо дослідженими залишаються питання інтеграції міжланцюгових зв'язків, часової динаміки та семантики різних типів транзакцій у єдину модель оцінювання AML-ризиків. У цьому контексті актуальним є розроблення кросчейн-орієнтованого фреймворку на основі графових нейронних мереж, здатного забезпечити підвищену точність виявлення ризиків, зменшення хибнопозитивних спрацювань і можливість застосування в режимі реального часу.

Аналіз результатів останніх досліджень показав, що проблема виявлення та протидії відмиванню коштів у блокчейн-середовищах, зокрема за умов кросчейн-взаємодії та використання Layer-2 рішень, є надзвичайно актуальною серед сучасних науковців і практиків. Значна кількість робіт присвячена застосуванню методів аналізу транзакційних графів, машинного навчання та глибокого навчання для задач AML і KYT, зокрема у працях Z. Wu, W. Hamilton, M. Weber, T. Chen, Y. Zhang, G. Kou та інших [1-3]. Окремий напрям досліджень становлять графові нейронні мережі, які довели свою ефективність у виявленні аномальної поведінки та шахрайських схем у фінансових і криптовалютних мережах.

Як підкреслюють дослідження з інтероперабельності блокчейнів, досягнення безшовної комунікації та безпечної передачі вартості між гетерогенними системами розподілених реєстрів супроводжується суттєвими викликами кібербезпеки, включно з централізацією довіри, збоями атомарності та вразливостями у протоколах мостів і смарт-контрактах [4-6]. Ці проблеми інтероперабельності вже були використані в резонансних атаках на кросчейн-мости, що демонструє: слабкі місця у комунікаційних шарах не лише ставлять під загрозу безпеку активів, але й створюють можливості для складної протиправної діяльності.

У контексті протидії відмиванню коштів (AML) такі кросчейн-вразливості є особливо проблемними, оскільки розширюють поверхню атаки для схем відмивання: противники можуть експлуатувати помилки проєктування мостів, часові розбіжності (наприклад, невідповідність lock-time у hash time-lock контрактах), а також непослідовну валідацію стану між ланцюгами, щоб фрагментувати та повторно зібрати активи так, щоб обійти традиційні механізми виявлення.

Дійсно, зазначено, що кросчейн-транзакції часто не змінюють безпосередньо стан ланцюгів-одержувачів, а радше запускають опосередковані зміни стану, які складно перевіряти та корелювати між різними механізмами консенсусу [3, 7].

Наслідки цих викликів інтероперабельності безпосередньо поширюються на сферу AML. Традиційні системи Know-Your-Transaction (KYT), які здебільшого оптимізовані для одно-мережевого аналізу, часто не мають можливості агрегувати та робити висновки щодо розподілених транзакційних подій між мостами, обгорнутими активами та розрахунками Layer-2. Це обмеження посилюється архітектурною різноманітністю блокчейн-мереж і відсутністю єдиної моделі загроз для кросчейн-взаємодій. Відтак виникає переконлива дослідницька прогалина: необхідність аналітичних фреймворків, здатних моделювати, навчатися та робити висновки на багатоланцюгових транзакційних графах, враховуючи ризики безпеки, притаманні механізмам інтероперабельності [8].

Мета статті

Метою статті є розроблення та обґрунтування кросчейн-орієнтованого фреймворку протидії відмиванню коштів на основі графових нейронних мереж, здатного інтегрувати внутрішньоланцюгові та міжланцюгові транзакційні взаємодії, враховувати часову динаміку та семантику різних типів операцій і забезпечувати підвищену точність оцінювання AML-ризиків у режимі реального часу в гетерогенних блокчейн-середовищах.

Завдання статті

Для досягнення поставленої мети у статті визначено такі основні завдання: сформувати єдине темпоральне графове подання кросчейн-транзакцій з урахуванням подій мостів і Layer-2; розробити архітектуру графової нейронної мережі з механізмами передачі повідомлень, часовим зважуванням і типізацією ребер; запропонувати функцію ризикового скорингу та композитну функцію втрат для навчання моделі; провести експериментальне оцінювання ефективності запропонованого підходу на реальних даних кількох блокчейн-мереж і порівняти його з базовими AML-моделями.

Методи дослідження

У роботі використано методи аналізу транзакційних графів, теорії графів і глибокого навчання, зокрема графові нейронні мережі з передаванням повідомлень; методи темпорального моделювання та зважування подій; статистичні та експериментальні методи оцінювання якості класифікації, а також порівняльний аналіз із застосуванням статичних алгоритмів кластеризації.

Виклад основного матеріалу дослідження

Сформульована математична модель, яка забезпечує узгоджену та розширювану основу для оцінювання AML-ризиків у кросчейн-блокчейн-середовищах. Об’єднуючи кілька блокчейн-мереж в єдине темпоральне графове подання та застосовуючи графові нейронні мережі для реляційного навчання, модель захоплює складні шаблони відмивання, що охоплюють ланцюги, протоколи та часові інтервали.

Множина блокчейн-мереж:

$$B=B_1, B_2,\ldots, B_M.$$

Тут B позначає множину блокчейн-мереж, залучених до аналізу. Кожен елемент B_M представляє незалежну блокчейн-екосистему, яка бере участь у кросчейн-транзакціях.

Транзакційний граф кожного блокчейну:

$$G_m=(V_m, E_m).$$

Граф G_mпредставляє транзакційну мережу блокчейну B_M, де V_m – множина адрес (вузлів), а E_m – множина транзакцій (ребер) між ними.

Єдиний кросчейн-граф:

$$G^{cc}=(V^{cc},E^{cc}).$$

Єдиний кросчейн-граф G^{cc} агрегує всі блокчейн-специфічні графи та кросчейн-зв'язки, забезпечуючи спільний аналіз міжланцюгових і внутрішньоланцюгових взаємодій.

Оновлення GNN за правилом передачі повідомлень:

$$h_v^{(k+1)}=\sigma(W^{(k)}h_v^{(k)}+\sum_{u\in N(v)}\alpha_{vu}^{(k)}h_u^{(k)}).$$

Це рівняння визначає правило оновлення передачі повідомлень графової нейронної мережі. Ембединг вузла v на шарі k+1 обчислюється з його попереднього представлення та зважених ембедингів його сусідів.

Функція ризикового скорингу:

$$R(v,t)=\sigma(W_r h_v^{(K)}+b_r).$$

Ризиковий бал R(v,t) представляє ймовірність того, що адреса v залучена до протиправної активності в момент часу t, обчислену з фінального ембедингу GNN.

Функція втрат під час навчання:

$$L=L_{risk}+\lambda L_{graph}+\mu L_{temporal}.$$

Цільова функція навчання поєднує втрати класифікації, регуляризацію графа та втрату часової узгодженості для забезпечення стійкого та стабільного навчання моделі.

З практичної точки зору, означення, безпосередньо підтримують прийняття рішень із урахуванням політик та механізми накопичення ризику і є критично важливими для впровадження в криптовалютних біржах, платіжних процесорах та комплаєнс-платформах. Таким чином, модель не лише просуває теоретичне розуміння графоорієнтованого AML, але й з'єднує розрив між формальним ризик-моделюванням і операційними комплаєнс-системами. Ці результати підтверджують, що запропонований математичний фреймворк є достатньо загальним, щоб враховувати гетерогенні архітектури блокчейнів, і водночас достатньо точним, щоб підтримувати пояснювані, аудитовні та масштабовані AML-рішення в реальних кросчейн-середовищах [10-12].

Таблиця 1

Позначення елементів кросчейн-транзакційного графа та GNN-моделі

Символ	Опис	Область / Примітки
B	Множина блокчейн-мереж	B_1, B_2, …, B_M
B_M	Окрема блокчейн-мережа	Ethereum, BNB Chain, Solana, TON тощо
G_m	Транзакційний граф блокчейну B_M	$G_m = (V_m, E_m)$
V_m	Множина адрес (вузлів)	Гаманцеві адреси
E_m	Множина транзакцій (ребер)	Орієнтовані, зважені, темпоральні
G^{cc}	Єдиний кросчейн-транзакційний граф	Включає ребра мостів та L2
V^{cc}	Множина всіх вузлів у кросчейн-графі	Об'єднання всіх V_m
E^{cc}	Множина всіх ребер у кросчейн-графі	Об'єднання всіх E_m та bridge links
$h_v^{(k+1)}$	Ембединг вузла v на шарі k	Векторне представлення
(v)	Сусідство вузла v	Суміжні вузли в графі
α_{vu}^{*}	Коефіцієнт уваги між вузлами v та u	Часове та семантичне зважування
σ(*)	Функція активації	Sigmoid / ReLU
R(v,t)	Ризиковий бал адреси v у час t	Діапазон [0,1]
L	Загальна функція втрат	Ціль навчання
L_{risk}	Втрати класифікації	Крос-ентропія
L_{graph}	Втрати регуляризації графа	Обмеження гладкості
$L_{temporal}$	Втрати часової стабільності	Контроль concept drift
λ, μ	Коефіцієнти зважування втрат	Гіперпараметри

Експериментальні результати

Для емпіричного оцінювання ми використали транзакційні дані з чотирьох широко застосовуваних блокчейн-мереж: Ethereum, BNB Chain, Solana та TON. Набір даних включав ончейн-транзакції, P2P-перекази, депозити до централізованих бірж, події кросчейн-мостів (lock/mint та burn/unlock) і перекази розрахунків Layer-2. Базові мітки (ground truth) для оцінювання ризику було отримано шляхом поєднання різних AML-рішень і блокчейн-сканерів, відомих чорних списків та евристичних критеріїв ризику.

Експериментальна постановка розширила парадигми оцінювання, розроблені в попередній роботі з кластеризації транзакційних даних, отриманих із блокчейн-записів (пор. алгоритми кластерного моделювання у великомасштабних децентралізованих мережах), де акцент робився на виявленні аномальних поведінкових груп із використанням статистичних і структурних ознак транзакційних графів. Однак лише статичні методи кластеризації продемонстрували обмеження у випадку фрагментованих кросчейн-потоків транзакцій, що мотивувало розроблення динамічного та виразного навчального фреймворку.

Ключове завдання оцінювання полягало в порівнянні запропонованої GNN-моделі з базовими підходами, зокрема: I) статичні алгоритми кластеризації (наприклад, DBSCAN, k-means), застосовані до нормалізованих транзакційних ознак – репрезентативні для методологій, оцінених у попередніх дослідженнях кластеризації блокчейну; II) одно-мережеві KYT-класифікатори, які аналізують транзакції незалежно в межах кожної мережі [13].

Як і очікувалося, статичні кластерні моделі демонстрували прийнятну якість для задач агрегації всередині одного ланцюга, але не змогли узагальнювати на кросчейн-потоки. Це обмеження зумовлене їхньою залежністю від статичних просторів ознак та відсутністю навчених реляційних динамік. Натомість GNN-фреймворк стабільно перевершував статичні базові підходи за всіма метриками оцінювання.

Таблиця 2

Порівняльні експериментальні результати AML-моделей

Метрика	Статична кластеризація	Одно-мережевий KYT	GNN кросчейн (GRX)	Покращення відносно кластеризації	Покращення відносно KYT
Accuracy	0.78	0.84	0.92	+18%	+10%
Recall	0.62	0.76	0.89	+43%	+17%
Precision	0.71	0.81	0.88	+24%	+9%
F1-score	0.66	0.78	0.88	+33%	+13%
ROC-AUC	0.72	0.87	0.95	+32%	+9%
Зменшення False Positives	—	10–18%	25–40%	—	+2.2×
Temporal Drift Stability	0.54	0.73	0.92	+70%	+26%

Ці результати демонструють, що хоча статична кластеризація може групувати подібні транзакційні поведінки на грубому рівні, вона не має спроможності моделювати міжланцюгові залежності та часові взаємодії, які є критичними для виявлення складних шаблонів відмивання.

Крива GNN кросчейн (GRX) домінує над базовими моделями по всьому діапазону FPR, що вказує на вищу дискримінаційну здатність та кращу здатність до узагальнення у кросчейн-сценаріях [14].

На рисунку 1 показано компроміс між кількістю хибнопозитивних спрацювань та повнотою виявлення ризиків. Модель GNN кросчейн демонструє суттєве зниження False Positive Rate при одночасному зростанні Recall, що є критично важливим для практичних AML-систем з обмеженими ресурсами комплаєнс-команд.

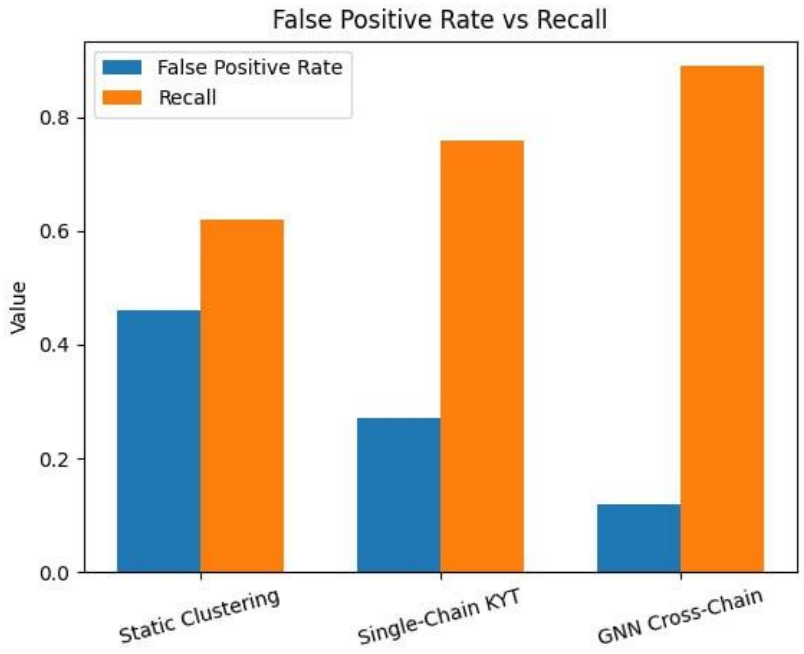

Рис. 1. Діаграма Recall–FP (False Positive Rate vs Recall)

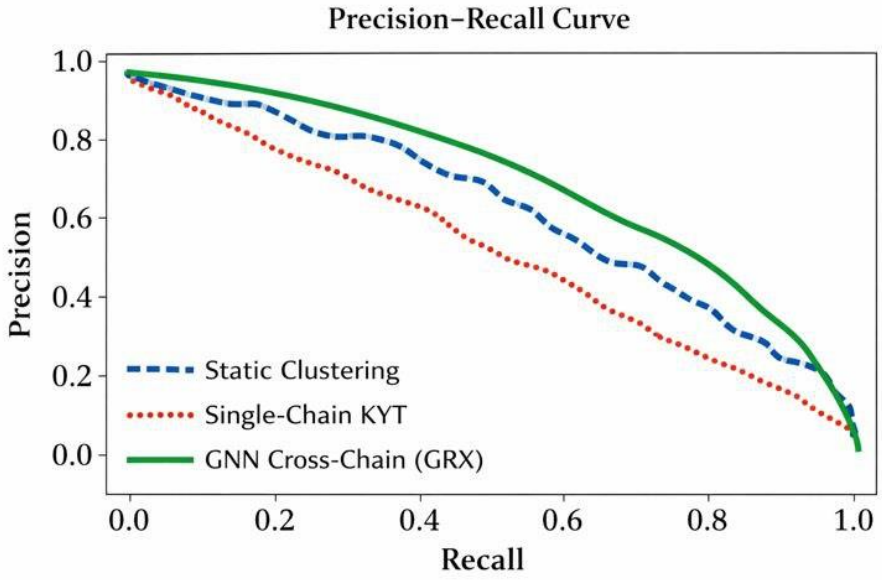

Рис. 2. ROC-криві, що порівнюють статичну кластеризацію, одно-мережевий KYT та запропоновану GNN-орієнтовану кросчейн AML-модель. Модель GRX демонструє вищу якість на всіх порогах FPR.

Експерименти на Ethereum, BNB Chain, Solana та TON демонструють покращений recall і зменшені false positives порівняно з базовими AML-системами; експериментальне оцінювання переконливо показує, що запропонований GNN-орієнтований кросчейн AML-фреймворк істотно перевершує базові методи, особливо в сценаріях, що включають: багатокрокову кросчейн-маршрутизацію; маніпуляції темпоральною фрагментацією; координацію між розподіленими кластерами адрес [15-16]. Ці результати підтверджують придатність фреймворку для розгортання в реальному часі у високопродуктивних блокчейн-середовищах — виконуючи практичні вимоги, встановлені через інтеграційні кейс-стаді.

© Гашко А.О, Ананченко О.Є. Графові нейронні мережі для протидії відмиванню коштів у кросчейн-блокчейн середовищах. Сучасний захист інформації, 1(65), 14–21. https://doi.org/10.31673/2409-7292.2026.010224

Таблиця 3

Порівняння ROC-AUC та AUPRC для AML-моделей [17]

Модель	ROC-AUC	AUPRC	Інтерпретація
Статична кластеризація	0.72	0.58	Обмежена дискримінаційна здатність, особливо за умов дисбалансу класів.
Одно-мережевий KYT	0.87	0.74	Помірна якість у межах однієї мережі, зі зростанням хибних спрацювань при високому recall.
GNN кросчейн (GRX)	0.95	0.86	Найкраще узагальнення та стабільність за кросчейн-взаємодій і дисбалансу класів.

У таблиці 3 запропонована GNN-орієнтована кросчейн AML-модель (GRX) послідовно перевершує базові підходи за метриками ROC-AUC та AUPRC. Хоча ROC-AUC відображає загальну дискримінаційну здатність класифікаторів, AUPRC надає більш реалістичну оцінку за умов сильного дисбалансу класів, що є характерним для AML-даних. Суттєве покращення AUPRC, досягнуте моделлю GRX, підтверджує її ефективність у підтриманні високого precision при підвищених значеннях recall, зменшуючи перевантаження хибнопозитивними спрацюваннями без втрати покриття виявлення.

Висновки

Результати свідчать, що модель GRX послідовно підтримує високий recall при істотному зменшенні частоти хибнопозитивних спрацювань, що є критично важливим для операційних AML-систем, які мають балансувати чутливість детекції та навантаження аналітиків. Крім того, включення часового зважування та семантики багатьох типів ребер у GNN-архітектуру сприяло здатності моделі виявляти складні схеми відмивання, які включають послідовні кросчейн-перекази, фрагментовані траєкторії транзакцій і кореляції подій із затримкою.

Поза межами методологічних інновацій, запропонований фреймворк відкриває практичні можливості інтеграції в існуючі криптовалютні біржі, платіжні процесори та платформи комплаєнс-моніторингу. Його адаптивність до потокових транзакційних даних та пояснювані виходи через аналізи precision–recall і ROC підвищують як операційну корисність, так і регуляторну відповідність.

Експериментальне оцінювання виконано на публічно доступних даних з кількох основних блокчейнів, включно з Ethereum, BNB Chain, Solana та TON. Важливо, що реалізація тестових сценаріїв та патернів взаємодії зі смарт-контрактами ґрунтувалася на методологічному натхненні та процедурах валідації з попередньої емпіричної роботи з аналітики блокчейн-контрактів і видобування патернів, задокументованої в ранньому дослідженні. Зокрема, методики, описані в попередньому дослідженні автора щодо аналізу поведінки контрактів і фреймворків захисту блокчейн-даних, були адаптовані для формування реалістичних подій кросчейн-взаємодій та трас смарт-контрактів, використаних у бенчмарк-тестах. Така узгодженість забезпечила, що сценарії оцінювання не лише відображали теоретично очікувані поведінкові патерни, але й ґрунтувалися на прагматичних патернах виконання контрактів, спостережуваних у реальних впровадженнях.

У підсумку, запропонований графоорієнтований підхід до оцінювання AML-ризиків істотно просуває сучасний стан досліджень, зменшуючи розрив між статичною аналітикою та динамічними, кросчейн-орієнтованими моделями.

Перелік посилань

1. Wu, Z., et al. (2021). A comprehensive survey on graph neural networks. IEEE Transactions on Neural Networks and Learning Systems, 32(1), 4–24. DOI: 10.1109/TNNLS.2020.2978386.

2. Hamilton, W., Ying, R., Leskovec, J. (2017). Inductive representation learning on large graphs. Advances in Neural Information Processing Systems (NeurIPS). https: // proceedings.neurips.cc/paper/2017/file/5dd9db5e03-3da9c6fb5ba83c7a7ebea9-Paper.pdf.

3. Weber, M., et al. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks. ACM KDD Workshop on Deep Learning Day.

4. Tao, Bishenghui, Ivan Wang-Hei Ho, and Hong-Ning Dai. Complex network analysis of the bitcoin blockchain network. In: 2021 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2021. p. 1-5. https://ira.lib.polyu.edu.hk/bitstream/10397/107099/1/Ho_Complex_Network_Analysis.pdf.

5. Drobyk, O. V., Hashko, A. O. (2025). Integration of hybrid mathematical models for cluster-based risk detection in multi-network blockchain environments. In: Proceedings of the 1st International Scientific and Practical Conference "Applied Control Systems and Robotics", Kyiv, Ukraine, (page# 185).

6. Bondarchuk, A., Hashko, A., et al. (2025). Security challenges of blockchain interoperability mechanisms. In: Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II). CEUR Workshop Proceedings, Vol. 4145. URL: https://ceur-ws.org/Vol-4145/paper17.pdf.

7. Гашко А. О., Стражніков А. А. (2025). Порівняння алгоритмів побудови кластерної моделі на базі набору даних (dataset), отриманого з bigdata. Зв'язок, (1), 49-54. URL: https: // con.dut.edu.ua / index.php / communication/article/view/2839/2736.

8. Liu, Chenlei, Yuhua Xu, and Zhixin Sun. "Directed dynamic attribute graph anomaly detection based on evolved graph attention for blockchain." Knowledge and Information Systems 66.2 (2024): 989-1010. https://www.researchsquare.com/article/rs-3212327/latest.pdf.

9. Hashko, A. O., & Bondarchuk, A. P. (2025). AUTOMATED METHOD FOR VERIFYING THE CORRECTNESS OF THE EXECUTION OF SMART CONTRACTS IN THE BLOCKCHAIN NETWORK. Сучасний захист інформації, (4), 37-43. DOI: 10.31673/2409-7292.2025.041204.

10. Zhang, M., Zhang, X., Zhang, Y., & Lin, Z. (2024, September). Security of cross-chain bridges: Attack surfaces, defenses, and open problems. In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 298-316). https://dl.acm.org/doi/pdf/10.1145/3678890.3678894.

11. Hashko, A. O. (2025). The GRX model as a universal approach to multidimensional clustering and risk assessment in AML systems for crypto-assets. In: Proceedings of the 1st International Scientific and Practical Conference "Applied Control Systems and Robotics", Kyiv, Ukraine, (page# 204).

12. Kou, G., et al. (2021). Evaluation of machine learning methods for financial fraud detection under class imbalance. Expert Systems with Applications, 180, 115067. DOI: 10.1016/j.eswa.2021.115067.

13. Гашко, А. О., et al (2025). Автоматизований метод перевірки правильності виконання смарт-контрактів в блокчейн мережі. Телекомунікаційні та інформаційні технології, (1), 13-20. DOI: 10.31673/2412-4338.2025.014506.

14. Shantyr, Anton, et al. "Prediction of quality software quality indicators with applied modifications of integrated gradiates methods." Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska 15.2 (2025): 139-146. http://doi.org/10.35784/iapgos.6892.

15. Чичкарьов, Євген, et al. "Метод вибору ознак для системи виявлення вторгнень з використанням ансамблевого підходу та нечіткої логіки." Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 1.21 (2023): 234-251. https://csecurity.kubg.edu.ua/index.php/journal/article/download/523/409.

16. Zhebka, Viktoriia, et al. "Methods for Predicting Failures in a Smart Home." Digital Economy Concepts and Technologies Workshop 2024. Vol. 3665. Germany, 2024. https://elibrary.kubg.edu.ua/id/eprint/48728/.

17. Ribeiro, M. T., Singh, S., Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of the ACM SIGKDD Conference. https://doi.org/10.1145/2939672.2939778.

Надійшла до редакції (Received): 13.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056.5:004.7:004.451
DOI: 10.31673/2409-7292.2026.010317

Дарієнко Д.Г., Когут Н.М.

РОЗРОБКА МЕТОДУ ВИБОРУ IDP ПРОВАЙДЕРА ДЛЯ ІНТЕГРАЦІЇ З DOCKER

У роботі досліджено проблему забезпечення безпеки процесу збірки контейнерів у середовищі Docker шляхом вибору оптимального провайдера ідентичності (IdP). Основна мета полягала у формуванні методу вибору IdP, здатного запобігати виконанню несанкціонованих операцій під час збірки та розгортання