КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1142
УДК 004.89: 004.3

Павлова Ольга Олександрівна
д.ф., доцент, завідувач кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет, Хмельницький, Україна
ORCID: 0000-0001-7019-0354
pavlovao@khmnu.edu.ua

Аскеров В'ячеслав Васильович
Асистент кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет,
Директор IT-компанії AVIVI, Хмельницький, Україна
ORCID: 0009-0009-1176-9812
vyacheslav@askerov.com

МЕТОД ПОКРАЩЕННЯ AML-ПЕРЕВІРОК У СФЕРІ КРИПТОВАЛЮТ ШЛЯХОМ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА МАШИННОГО НАВЧАННЯ

Анотація. У статті досліджено проблему підвищення ефективності AML-перевірок (Anti-Money Laundering) у сфері криптовалют в умовах стрімкого розвитку технологій блокчейн та WEB 3.0. Зростання кількості активних криптогаманців і транзакцій у децентралізованих мережах зумовлює необхідність удосконалення підходів до виявлення незаконної фінансової діяльності, зокрема операцій з відмивання коштів. Традиційні AML-механізми, що базуються на послідовному аналізі транзакцій та логічних правилах, характеризуються високими обчислювальними витратами та обмеженою адаптивністю до нових шахрайських сценаріїв. Метою роботи є розробка методу покращення AML-перевірок шляхом поєднання переваг технології блокчейн та алгоритмів машинного навчання. У статті проаналізовано сучасний стан ринку AML-сервісів, здійснено порівняння комерційних провайдерів та визначено фактори, що впливають на вартість перевірок транзакцій. Обґрунтовано гіпотезу про доцільність зміни парадигми початкової оцінки транзакцій: замість презумпції безпечності запропоновано модель попередньої умовної заборони з подальшим коригуванням рейтингу на основі результатів машинного навчання. Запропоновано математичну модель, що формалізує етапи перевірки транзакцій: початкове рейтингування, зважений аналіз параметрів, застосування ML-класифікатора, динамічне оновлення рейтингу, реакцію системи та прийняття остаточного рішення на основі порогових значень. Для верифікації методу описано теоретичний експеримент із використанням датасету транзакцій відкритих блокчейнів та застосуванням алгоритмів Logistic Regression, Random Forest і Neural Networks. Отримані результати демонструють можливість досягнення високої точності класифікації транзакцій (понад 90%) та зменшення кількості помилкових спрацьовувань. Практична цінність роботи полягає у зниженні ресурсомісткості перевірок, підвищенні адаптивності AML-систем та покращенні кібербезпеки фінансових операцій у криптовалютному середовищі.

Ключові слова: AML; криптовалюта; блокчейн; машинне навчання; аналіз транзакцій; фінансова безпека; виявлення аномалій.

ВСТУП

Згідно [1] методи з протидії відмиванню грошей (AML) складаються із законів, нормативних актів і процедур, спрямованих на те, щоб запобігти обміну злочинцями грошей, отриманих у результаті незаконної діяльності, або «брудних грошей».

Як відомо, головним завданням систем AML (Anti-Money Laundering) у сфері криптовалют є своєчасне виявлення та запобігання можливостям використання електронних активів у протизаконних операціях, що можуть нашкодити світові загалом та людству зокрема. Одним із факторів, що можуть істотно покращити процес протидії, є використання машинного навчання (ML) – реалізації сценаріїв поведінки комп'ютерних систем на основі попереднього вивчення однотипних ситуацій. Станом на зараз, методологічна база знаходиться на етапі становлення, оскільки достеменно не відомі усі

можливості ML, що практично із кожним днем розширюються стараннями великої кількості науковців та ентузіастів. Однак станом на зараз, уявлення сучасників про ML знаходяться у парадигмі природи людського мислення – раціональний пошук можливих варіантів, заснований на дедукції.

Постановка проблеми. Наразі технологія блокчейну вважається однією із найнадійніших у сфері кіберзахисту та захисту даних у фінансовій галузі, яка, за статистикою вважається найбільш схильною до зловмисних дій, в тому числі і до операцій так званого «відмивання грошей». Сучасні методи та засоби не дають достатніх гарантій щодо захисту фінансових даних, що ставить під загрозу їх безпеку. Тому постає необхідність покращення перевірок AML шляхом зміни парадигми ставлення систем до кожної окремої транзакції за допомогою використання новітніх технологій, таких як блокчейн та технології машинного навчання.

Аналіз останніх досліджень і публікацій. Згідно з останніми дослідженнями 2024 року, технології блокчейну широко застосовуються для забезпечення безпеки операцій з фінансовими даними [3-5], а також є основою фінансових стартапів у розвинутих країнах [6].

Згідно стратегії ООН щодо досягнення цілей сталого розвитку до 2030 року [7], введення в обіг криптовалюти сприяє досягненню конфепції цифрової економіки [8] та «зеленого» валютообігу [9], що дозволяє спростити процес безготівкового валютобігу між різними країнами та зробити його максимально безпечним, як для підприємств, так і для фізичних осіб.

Застосування технологій машинного навчання набуло все більшого застосування у фінансовому секторі. Відтак, у публікаціях 2024 року машинне навчання широко застосовувалось для прогнозування цін на криптовалюти [10], [11]. Проте, як показали дослідження [12], [13] та [14], застосування машинного навчання для протидії фінансовим махінаціям, таким як відмивання грошей, у сфері криптовалют, є перспективним напрямком.

Метою цієї статті є аналіз сучасного стану речей у сфері криптовалют та розробка методу та математичної моделі покращення перевірок на предмет відмивання грошей із застосуванням технології блокчейну та машинного навчання.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Сфера криптовалют активно розвивається, що сприяє економічним інноваціям, але водночас створює ризики, пов'язані з незаконною фінансовою діяльністю, включаючи відмивання коштів Anti-Money Laundering (AML). Висока анонімність, швидкість і глобальний характер криптовалют значно ускладнюють застосування традиційних методів AML-контролю. Це зумовлює необхідність розробки інноваційних підходів до виявлення та запобігання таким ризикам.

Одним із перспективних підходів є використання технології блокчейн у поєднанні з алгоритмами машинного навчання (ML). Блокчейн забезпечує прозорість, незмінність і доступність даних, що дає змогу аналізувати транзакції в реальному часі, а ML дозволяє ефективно аналізувати великі обсяги даних і виявляти приховані шаблони або аномалії, які можуть свідчити про незаконну діяльність.

Для аргументації пропонованих нами факторів покращення AML слід розглянути наявну ситуацію з розвитком даної галузі та WEB 3.0 загалом. Основні аспекти припадають на стрімке зростання ринку криптовалют та посилення ролі блокчейнів у різних сферах людського життя та діяльності: державному секторі, фінансах, наданні послуг, медицині тощо (рис.1).

Як можна побачити з рисунку 1, на рубежі 20-х років XXI століття розвиток блокчейнів переживає бурхливий сплеск. Наразі для даного дослідження не так важливі абсолютні показники, як динаміка їхнього збільшення. Також варто сказати, що саме після 2020-го року відбулися фундаментальні зміни в роботі блокчейну Ethereum, що значно розширило можливості мережі та привабило ще більшу кількість користувачів та розробників.

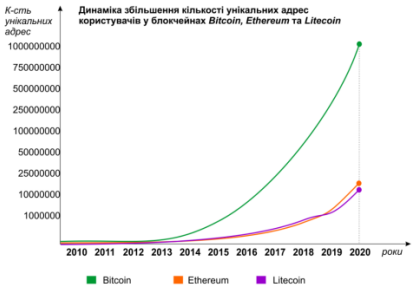

Рис. 1. Динаміка збільшення кількості унікальних адрес користувачів

Оскільки більшу цінність для нас становить інформація саме про перевірку транзакцій, необхідно звернутися до відповідних даних. На жаль, отримати статистичні дані практично неможливо з наступних причин:

1) перевірки надаються різними провайдерами, кожен з яких збирає статистику окремо;
2) кожен провайдер зацікавлений у покращенні власного сервісу, тому стежить за збереженням внутрішньої інформації;
3) неможливо узагальнити дані, оскільки кожна перевірка використовує унікальні підходи та алгоритми.

Однак, буде корисним поглянути на динаміку збільшення кількості активних крипто-гаманців у світі, що дає приблизне розуміння обсягів транзакцій. Адже якщо гаманець активний, це означає, що транзакції відбуваються, що передбачає їхню перевірку. Динаміка збільшення глобальної кількості криптогаманців у світі представлена на рис.2.

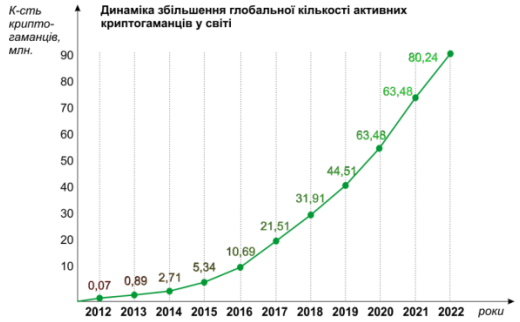

Рис. 2. Динаміка збільшення глобальної кількості активних криптогаманців у світі

МЕТОДИКА ДОСЛІДЖЕННЯ

У ході дослідження було проведено аналіз існуючих компаній, які надають послуги AML-перевірок на комерційній основі. В даному дослідженні було використано статистичний метод для порівняння актуальних пропозицій провайдерів з різних кінців світу. Значною перепоною в дослідженні виявилася маркетингова активність компаній, а саме формування привабливих для потенційних клієнтів багаторівневих пакетних послуг з різним переліком можливостей та алгоритмів. Разом із тим можна прослідкувати фактори, що впливають на ціноутворення:

1) Кількість перевірок – більша кількість прямо пропорційна вартості пакета послуг та обернено пропорційна вартості однієї перевірки;
2) Кількість користувачів – скільки гаманців може бути підключено до системи одночасно;
3) Набір алгоритмів – скільки різних сценаріїв буде застосовано для кожної окремої перевірки;
4) Комісії блокчейн – нестабільний показник вартості Gwei, що залежить від курсу криптовалют у відповідних блокчейнах;
5) Спосіб оплати – підписка чи індивідуальні умови.

Розрахунки вартості користування існуючими AML-сервісами представлені у таблиці 1.

Таблиця 1

Розрахунок вартості користування існуючими AML-сервісами

№	Компанія	Тип оплати	Вартість підписки	Вартість 1 перевірки
1	FirstAML	За місяць	$599	~ $0,7
2	ComplyCube	За місяць	$159-$449	$1,5-$0,3
3	NameScam	За перевірку	$1	$1
4	Firmcheck	За перевірку	$4,67	$4,67
5	Inscope-AML	За місяць	$600	~ $0,8
6	Artaml	За перевірку	$4,34	$4,34
7	Themis	За перевірку	$0,61	$0,61
8	AMLcloud	За місяць	$200	~$0,4
9	SwiftDil	За перевірку	$0,39	$0,39
10	APLiD	За перевірку	$4,67	$4,67

Отже, в середньому, вартість перевірки 1 транзакції знаходиться в межах $1: перевірки без використанням ML та з незначним застосуванням автоматизованих сценаріїв коштують менше зазначеної суми. Варто уточнити, що найбільша вартість близько $4,5 притаманна лише британським провайдерам, що надають послуги у Фунтах Стерлінгів та провадять майже однакову цінову політику.

Для найкращого пояснення пропонованого у роботі методу, найперше слід звернутися до головного завдання AML, а саме запобігання використання криптовалют у незаконних операціях. В такому разі справедливим є твердження, що більшість операцій з криптовалютами є законними та "корисними", оскільки вони проходять перевірку та, з рештою, відбуваються. Як вже зазначалося вище, статистика кількості заборон транзакцій за певний період від провайдерів AML практично недоступна, тим більше не вдається з'ясувати чіткі причини більшості відмов, оскільки кожен окремий результат – це сукупність величезної кількості факторів, що впливають на проміжкові оцінки та остаточний "вирок".

Однак можна зробити припущення, що більшість транзакцій все таки "корисні", оскільки в протилежному випадку людство отримало б помітну стагнацію ринку криптовалют та занепад технології блокчейн загалом. Натомість, ми спостерігаємо стабільне зростання кількості операцій у різних децентралізованих мережах за певні однакові проміжки часу, збільшення кількості власників криптогаманців та ріст емісії віртуальних активів.

Сукупність всіх показників вказує на перевагу дозволених перевірками транзакцій над забороненими. Таким чином "корисні" перекази становлять більшість, а заборонені – меншість.

Це твердження дозволяє розвинути гіпотезу про те, що обсяг даних, на яких опираються системи AML для прийняття позитивних рішень переважає сукупність інформації про "шкідливі" транзакції. В такому разі, кожна наступна перевірка базується на звірці з великим масивом даних, що потребує значних ресурсовитрат – обчислювальних, криптографічних, часових, енергетичних тощо.

За таких умов, з точки зору логіки, в загальному більшість систем AML сприймають кожну наступну транзакцію, як потенційно-безпечну, оскільки безпечних – більшість. Всі подальші дії спрямовані на пошук факторів, що можуть вказати на небезпеку переказу та знизитити оцінки етапів перевірки. Одним із методів, що використовується провайдерами, є пошук аномалій, тобто отримання нетипових для більшості результатів, що викликають підозру та слугують тригерами для додаткових чи поглиблених дій. Однак це всього лише незначна частина всього ланцюжка алгоритмів, тому загальна кількість інформації про аномалії не може задовольнити потреби в необхідній інформації розрізнених систем AML.

Провайдери AML застосовують широкий спектр методів для покращення операцій з перевірок транзакцій. Кожна з них складається з цілого комплексу заходів, що виконуються послідовно. Наразі не можна стверджувати, що алгоритми усіх перевірок уніфіковані чи стандартизовані: кожен сервіс визначає власну політику діяльності. Однак переважна більшість алгоритмів побудована на однакових засадах. AML діють за заздалегідь визначеним та логічним методом: поділ завдання на послідовні етапи та фундаментальний аналіз кожного із них з подальшим виставленням оцінок та прийняття логічного рішення. Перевірка будь-якої транзакції має такі етапи (класичний метод перевірки):

1) Початкова оцінка транзакції: кожна нова транзакція отримує початковий рейтинг на основі основних параметрів;

2) Аналіз параметрів транзакції: система розглядає різні параметри транзакції, такі як розмір, частота, зв'язки з іншими користувачами чи країнами;

3) Використання алгоритмів: Застосування алгоритмів для виявлення підозрілих ознак або шаблонів, що можуть свідчити про можливий ризик;

4) Динамічний аналіз: врахування динаміки зміни параметрів та рейтингу транзакції під час її виконання та подальшого моніторингу;

5) Відповідь системи: якщо транзакція відповідає стандартам та не виявляє незвичайної активності, то вона може бути визнана "хорошою". Натомість якщо виникає підозра на можливий незаконний характер, то рейтинг може знизитися, і можуть бути застосовані додаткові заходи перевірки;

6) Прийняття рішення: на основі оцінки та аналізу система може визначити, чи потрібно подальше вивчення, чи транзакцію можна вважати безпечною.

Можна відслідкувати, що переважна більшість всіх AML базуються на людських уявленнях про раціональність перевірки даних. З огляду на цілковиту зрозумілість завдання, що постає перед системою, ми намагаємося знайти вразливі місця перевірок, запропонувати альтернативні методи для складання алгоритмів та організації машинного навчання.

Як було зазначено вище, головна відмінність алгоритму перевірки полягає у зміні парадигми ставлення системи AML до кожної наступної транзакції. Якщо раніше попередня оцінка була основою для застосування подальших механізмів, зараз вона виконує цілком протилежну роль – заборону

транзакції та попередньої оцінки на предмет можливості, а не заборони. Для цього штучний інтелект розглядає транзакцію з різних боків та приймає рішення про послаблення негативної оцінки.

Однозначними лишаються маркери причетності криптовалюти до сумнівних та небежених операцій:

1) маркер "брудної" криптовалюти, відмічених у попередніх "шкідливих" транзакціях;
2) залишковий маркер, у випадку спроб приховання слідів після використання блендерів для криптовалют;
3) інші явні причини заборонити транзакцію на основі попередньо встановлених обставин.

Варто розуміти, що всі ці дані вже доступі та не потребують встановлення, лише перевірки. Таким чином витрати ресурсів для обчислень на цьому етапі мають бути заздалегідь меншими, ніж якби кожне подібне дослідження потрібно було робити окремо.

Надалі метод звертається до результатів машинного навчання, що базується на основі розгляду типових виявлених та попередження випадків шахрайства. Як вже було встановлено раніше, кількість "шкідливих" транзакцій становить меншість, в порівнянні з "корисними". Таким чином, для підвищення заздалегідь низької оцінки, слід опрацювати менший масив даних, ніж для зниження високої оцінки.

Для верифікації роботи методу, було складено математичне представлення кожного кроку методу.

1. Початкова оцінка транзакції

Кожна транзакція T_i отримує початковий рейтинг $R_0(T_i)$, який визначається функцією оцінювання, яка представлена формулою 1.

$$R_0(T_i) = f(P_1, P_2, \dots, P_n), \quad (1)$$

де $P_1, P_2, \dots, P_n$ – основні параметри транзакції, такі як сума, час, та інші початкові атрибути.

2. Аналіз параметрів транзакції

Для кожної транзакції система аналізує набір параметрів $P(T_i)=\{P_1, P_2, \dots, P_k\}$, таких як:

P_1: розмір транзакції,
P_2: частота операцій,
P_3: зв'язки з іншими користувачами.

Для аналізу параметрів використовуються функції, які описані відношенням 2.

$$S(T_i) = g\big(P(T_i)\big), \quad (2)$$

де $S(T_i)$ – зважені значення параметрів.

3. Використання алгоритмів машинного навчання

Вхідний вектор параметрів $S(T_i)$ передається в модель машинного навчання M за допомогою відношення 3.

$$O(T_i) = M(S\big((T_i)\big), \quad (3)$$

де $O(T_i)$ – результат класифікації, що вказує на ризик (наприклад, ймовірність приналежності до підозрілої категорії).

4. Динамічний аналіз транзакції

Рейтинг транзакції оновлюється з урахуванням динаміки параметрів, представленої формулою 4.

$$R_t(T_i) = R_t - 1(T_i) + \Delta_t, \quad (4)$$

де $\Delta_t = h(P(T_i))$ – зміни, що залежать від похідної параметрів $P(T_i)$ з часом.

5. Відповідь системи

Якщо результат класифікації $O(T_i)$ перевищує поріг ризику θ, то відповідь системи визначатиметься за формулою 5.

$$R_t(T_i) = R_t(T_i) - \delta, \quad (5)$$

де $\delta > 0$ – штраф за підозрілу активність.

Якщо ж транзакція відповідає стандартам, то відповідь системи визначатиметься за формулою 6.

$$R_t(T_i) = R_t(T_i) + \varepsilon, \quad (6)$$

де $\varepsilon > 0$ – бонус за довіру.

6. Прийняття рішення

Рішення щодо транзакції T_i приймається на основі функції 7.

$$D(T_i) = \begin{cases} \text{"потребує перевірки"}, \text{якщо } R_t(T_i) < \tau, \\ \text{"безпечна"}, \text{якщо } R_t(T_i) \geq \tau. \end{cases} \quad (7)$$

де τ – поріг безпеки для рейтингу транзакції.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведемо теоретичний експеримент з метою перевірки ефективності запропонованого методу для покращення AML-перевірок у сфері криптовалют шляхом аналізу транзакцій із використанням блокчейну та алгоритмів машинного навчання. Даний експеримент дозволяє перевірити, як добре метод працює на практиці, оцінюючи його ефективність у виявленні підозрілих транзакцій у реальному світі. Основні цілі експерименту:

1. Оцінити здатність методу виявляти підозрілі транзакції.
2. Перевірити коректність математичного представлення кожного кроку.
3. Проаналізувати точність класифікації транзакцій ("безпечна"/"потребує перевірки").

Для проведення теоретичного експерименту, нам потрібні такі компоненти:

1) Набір даних (датасет):

Склад: транзакції з відкритих блокчейнів (наприклад, Ethereum або Bitcoin).

Обсяг: 10 000 транзакцій із різними параметрами.

Маркування: транзакції поділені на "безпечні" та "підозрілі" на основі реальних кейсів або симуляцій незаконної активності.

2) Початковий рейтинг $R_0(T_i)$:

Для кожної транзакції T_i, обчислюємо початковий рейтинг $R_0(T_i)$, використовуючи параметри P_1,P_2,...,P_n як розмір, частоту, час.

Функція оцінювання $f(P_1, P_2, \dots, P_n)$ буде визначена через вагові коефіцієнти за формулою 8.

$$R_0(T_i) = \sum_{j=1}^{n} w_j P_j, \quad (8)$$

де w_j – ваговий коефіцієнт для параметра P_j.

3) Аналіз параметрів:

Використаємо функцію $g(\boldsymbol{P}(T_i))$ для створення вектора зважених значень параметрів $\boldsymbol{S}(T_i)$.

Далі перевіряємо, чи цей етап коректно формує вхідний вектор для наступного кроку.

4) Алгоритми машинного навчання:

Навчимо класифікатор *(M)* з використанням таких моделей, як Logistic Regression, Random Forest та Neural Networks.

Результат класифікації $O(T_i)$ визначатиме ризик транзакції: $O(T_i) \in [0,1]$, де значення ближче до 1 вказує на високу ймовірність ризику.

5) Динамічний аналіз $R_t(T_i)$:

Ураховуємо зміни параметрів із часом за формулою 9.

$$R_t(T_i) = R_{t-1}(T_i) + h(\boldsymbol{P}(T_i)), \quad (8)$$

Далі потрібно верифікувати, як ця модель відображає вплив часу на рейтинг.

6) Оцінка ефективності $D(T_i)$:

Визначаємо, чи транзакція потребує перевірки або безпечна, на основі кінцевого рейтингу за формулою 7 та вибираємо оптимальне значення порогу τ для мінімізації помилкових спрацьовувань.

Для оцінки результатів використовуємо наступні метрики оцінки:

1. Точність *(Accuracy):*

$$Accuracy = \frac{\text{Кількість правильних класифікацій}}{\text{Загальна кількість транзакцій}}.$$

2. Повнота (*Recall):*

$$Recall = \frac{\text{Кількість вірно визначених підозрілих транзакцій}}{\text{Загальна кількість підозрілих транзакцій}}.$$

3. Точність класифікації *(Precision):*

$$Recall = \frac{\text{Кількість вірно визначених підозрілих транзакцій}}{\text{Усі транзакції, визначені, як підозрілі}}.$$

4. F1-міра:

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}.$$

Очікувані результати експерименту:

1) Висока точність (>90%) для класифікації транзакцій.
2) Мінімізація помилкових спрацьовувань (низький False Positive Rate).
3) Демонстрація адаптивності методу до різних наборів транзакцій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження розроблено метод покращення AML-перевірок у сфері криптовалют, що базується на зміні парадигми первинної оцінки транзакцій та інтеграції технології блокчейн з алгоритмами машинного навчання. Запропоновано математичну модель формалізації процесу перевірки, яка дозволяє структуровано враховувати параметри транзакцій, результати ML-класифікації та динаміку змін у часі. Теоретичний експеримент підтвердив доцільність застосування класифікаційних моделей для підвищення точності виявлення підозрілих операцій та зменшення кількості помилкових спрацьовувань. Практичне значення результатів полягає у можливості оптимізації ресурсних витрат AML-систем, підвищенні швидкодії перевірок та забезпеченні більш адаптивного реагування на нові шахрайські сценарії у децентралізованих фінансових мережах.

Подальші дослідження авторів будуть спрямовані на проведення повномасштабного експериментального тестування методу на реальних великих датасетах блокчейн-транзакцій, інтеграцію графових нейронних мереж для аналізу складних зв'язків між гаманцями, розробку механізмів самоадаптації порогових значень на основі потокового навчання (online learning), дослідження можливостей міжблокчейнної взаємодії для формування єдиного AML-простору та оцінювання енергоефективності запропонованого підходу в умовах високонавантажених систем. Реалізація зазначених напрямків дозволить створити більш інтелектуальні, масштабовані та стійкі до новітніх кіберзагроз AML-рішення для цифрової економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. European Commission. (2024). *Anti-money laundering and countering the financing of terrorism at EU level*. https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en
2. IBM: What is anti-money laundering?
3. Kathuria, P., Goel, C., & Bassi, P. (2024).A systematic review of blockchain in fintech using network visuals.In *Finance analytics in business:Perspectives on enhancing efficiency and accuracy*(pp. 161-174).
4. Al-Qudah, A. A., Al-Okaily, M., & Yadav, M. P. P. (2024). The growth of fintech and blockchain technology in developing countries: UAE's evidence. *International Journal of Accounting & Information Management*. Advance online publication.
5. Kasmon, B., Ibrahim, S. S., Daud, D., Raja Hisham, R. R. I., & Dian Wisika Prajanti, S. (2024). FinTech application in Islamic social finance in Asia region: A systematic literature review. *International Journal of Ethics and Systems*. Advance online publication.
6. Tariq, M. U. (2024). Fintech startups and cryptocurrency in business: Revolutionizing entrepreneurship. In *Applying business intelligence and innovation to entrepreneurship* (pp. 106-124). IGI Global.
7. United Nations Development Programme (UNDP). (2024). *What are the Sustainable Development Goals?* https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku
8. Akbarovna, N. N. (2024). Opportunities for the development of cryptocurrencies in the digital economy. *Gospodarka i Innowacje*, *45*, 320-326.
9. Ali, F., Khurram, M. U., Sensoy, A., & Vo, X. V. (2024). Green cryptocurrencies and portfolio diversification in the era of greener paths. *Renewable and Sustainable Energy Reviews*, *191*, 114137.
10. Dudek, G., Fiszeder, P., Kobus, P., & Orzeszko, W. (2024). Forecasting cryptocurrencies volatility using statistical and machine learning methods: A comparative study. *Applied Soft Computing*, *151*, 111132.
11. Islam, M. Z., Islam, M. S., Al Montaser, M. A., Rasel, M. A. B., Bhowmik, P. K., & Dalim, H. M. (2024). Evaluating the effectiveness of machine learning algorithms in predicting cryptocurrency prices

under market volatility: A study based on the USA financial market. *The American Journal of Management and Economics Innovations*, *6*(12), 15-38.

12. Japinye, A. O. (2024). Integrating machine learning in anti-money laundering through crypto: A comprehensive performance review. *European Journal of Accounting, Auditing and Finance Research*, *12*(4), 54-80.
13. Kehinde, J., Ajayi, O. O., Adetayo, A., Obafemi, J. R., Akinrolabu, O. D., & Ebitigha, A. E. (2024). Machine learning model for detecting money laundering in Bitcoin blockchain transactions. *Machine Learning*, *1*(1).
14. Marasi, S., & Ferretti, S. (2024, January). Anti-money laundering in cryptocurrencies through graph neural networks: A comparative study. In *Proceedings of the IEEE 21st Consumer Communications & Networking Conference (CCNC 2024)* (pp. 272-277). IEEE.

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

Olha Pavlova
D.Sc., Associate Professor,
Head of the Department of Computer Engineering and Information Systems
Khmelnytskyi National University, Khmelnytskyi, Ukraine
ORCID: 0000-0001-7019-0354
pavlovao@khmnu.edu.ua

Viacheslav Askerov
Assistant of the Department of Computer Engineering and Information Systems
Khmelnytskyi National University,
CEO of AVIVI IT company, Khmelnytskyi, Ukraine
ORCID: 0009-0009-1176-9812
vyacheslav@askerov.com

METHOD OF IMPROVING AML CHECKS IN THE FIELD OF CRYPTOCURRENCY USING BLOCKCHAIN TECHNOLOGY AND MACHINE LEARNING

Abstract. The article investigates the problem of improving Anti-Money Laundering (AML) procedures in the cryptocurrency domain under conditions of rapid blockchain and WEB 3.0 development. The growing number of active crypto wallets and transactions in decentralized networks necessitates advanced approaches to detecting illegal financial activities, particularly money laundering operations. Traditional AML mechanisms, based on sequential transaction analysis and rule-based logic, are characterized by high computational costs and limited adaptability to emerging fraud scenarios. The aim of the study is to develop a method for enhancing AML verification by integrating blockchain technology and machine learning algorithms. The paper analyzes the current state of the AML service market, compares commercial providers, and identifies key pricing factors influencing transaction verification costs. A hypothesis is substantiated regarding the need to change the paradigm of initial transaction assessment: instead of assuming a transaction is safe by default, a model of conditional initial restriction with subsequent rating adjustment based on machine learning results is proposed. A mathematical model is introduced to formalize each verification stage: initial scoring, weighted parameter analysis, ML-based classification, dynamic rating update, system response, and final decision-making based on threshold values. To validate the proposed method, a theoretical experiment is described using a dataset of blockchain transactions and implementing Logistic Regression, Random Forest, and Neural Networks. The evaluation framework includes Accuracy, Precision, Recall, and F1-score metrics. The expected results demonstrate the potential to achieve high transaction classification accuracy (above 90%) while reducing false positive rates. The practical value of the research lies in decreasing computational resource consumption, increasing adaptability of AML systems, and strengthening cybersecurity in cryptocurrency financial operation

Keywords: AML; cryptocurrency; blockchain; machine learning; transaction analysis; financial security; anomaly detection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. European Commission. (2024). *Anti-money laundering and countering the financing of terrorism at EU level*. https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en
2. IBM: What is anti-money laundering?
3. Kathuria, P., Goel, C., & Bassi, P. (2024).A systematic review of blockchain in fintech using network visuals.In *Finance analytics in business:Perspectives on enhancing efficiency and accuracy*(pp. 161-174).
4. Al-Qudah, A. A., Al-Okaily, M., & Yadav, M. P. P. (2024). The growth of fintech and blockchain technology in developing countries: UAE's evidence. *International Journal of Accounting & Information Management*. Advance online publication.
5. Kasmon, B., Ibrahim, S. S., Daud, D., Raja Hisham, R. R. I., & Dian Wisika Prajanti, S. (2024). FinTech application in Islamic social finance in Asia region: A systematic literature review. *International Journal of Ethics and Systems*. Advance online publication.

6. Tariq, M. U. (2024). Fintech startups and cryptocurrency in business: Revolutionizing entrepreneurship. In *Applying business intelligence and innovation to entrepreneurship* (pp. 106-124). IGI Global.
7. United Nations Development Programme (UNDP). (2024). *What are the Sustainable Development Goals?* https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku
8. Akbarovna, N. N. (2024). Opportunities for the development of cryptocurrencies in the digital economy. *Gospodarka i Innowacje*, *45*, 320-326.
9. Ali, F., Khurram, M. U., Sensoy, A., & Vo, X. V. (2024). Green cryptocurrencies and portfolio diversification in the era of greener paths. *Renewable and Sustainable Energy Reviews*, *191*, 114137.
10. Dudek, G., Fiszeder, P., Kobus, P., & Orzeszko, W. (2024). Forecasting cryptocurrencies volatility using statistical and machine learning methods: A comparative study. *Applied Soft Computing*, *151*, 111132.
11. Islam, M. Z., Islam, M. S., Al Montaser, M. A., Rasel, M. A. B., Bhowmik, P. K., & Dalim, H. M. (2024). Evaluating the effectiveness of machine learning algorithms in predicting cryptocurrency prices under market volatility: A study based on the USA financial market. *The American Journal of Management and Economics Innovations*, *6*(12), 15-38.
12. Japinye, A. O. (2024). Integrating machine learning in anti-money laundering through crypto: A comprehensive performance review. *European Journal of Accounting, Auditing and Finance Research*, *12*(4), 54-80.
13. Kehinde, J., Ajayi, O. O., Adetayo, A., Obafemi, J. R., Akinrolabu, O. D., & Ebitigha, A. E. (2024). Machine learning model for detecting money laundering in Bitcoin blockchain transactions. *Machine Learning*, *1*(1).
14. Marasi, S., & Ferretti, S. (2024, January). Anti-money laundering in cryptocurrencies through graph neural networks: A comparative study. In *Proceedings of the IEEE 21st Consumer Communications & Networking Conference (CCNC 2024)* (pp. 272-277). IEEE.

Отримано редакцією журналу / Received: 05.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 25.06.26