



Л. М. Акімова, О. О. Акімов

Національний університет водного господарства та природокористування, м. Рівне, Україна
Міністерство оборони України, м. Київ, Україна

ІНСТРУМЕНТИ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ В ЕКОСИСТЕМІ КРИПТОАКТИВІВ

Розглянуто типології відмивання грошей з використанням криптовалют та контрзаходи, що вживають зобов'язані суб'єкти з фінансового моніторингу. Виділено основні незаконні методи відмивання грошей на етапах розміщення, нашарування та інтеграції коштів. Зокрема, на етапі розміщення криптовалюти купуються за готівку, жертви вносять кошти на криптогаманці злочинців, а також використовуються фінансові мули. Типовими методами нашарування є заплутані перекази віртуальної валюти між кількома криптогаманцями, використання програм для змішування коштів, купівля-продаж приватних монет та використання невзаємозамінних токенів, що ідентифікують право власності на цифровий об'єкт. Для інтеграції використовується обмін криптовалют на фіатну валюту або купівля фізичних активів з високою ринковою вартістю за криптовалюти. Проаналізовано методи протидії легалізації віртуальних активів як на національному рівні, так і на рівні суб'єктів звітності. Встановлено, що основним інструментом ефективної боротьби з відмиванням грошей через віртуальні активи є ліцензування постачальників послуг, пов'язаних з обігом криптовалют, та надання їм статусу первинного суб'єкта фінансового моніторингу. Такий статус вимагає від операторів ринку криптовалют застосування заходів належної перевірки клієнтів та моніторингу транзакцій, що значно ускладнює відмивання грошей на всіх трьох етапах. Досліджено поведінкові моделі, в яких звітні установи у сфері фінансового моніторингу можуть використовувати методи на основі правил та інструменти аналітики блокчейну для виявлення підозрілих транзакцій з криптовалютами. Проведено оцінювання чинних законодавчих вимог до постачальників послуг віртуальних активів в Україні. Встановлено, що українська законодавча база щодо боротьби з відмиванням грошей в екосистемі криптовалют відповідає світовій практиці. Разом з тим наголошено на наявності значної регуляторної прогалини, пов'язаної з відсутністю нагляду за надавачами послуг з використанням криптовалют з боку суб'єктів державного фінансового моніторингу.

Ключові слова: криптовалюти; фінансовий моніторинг; відмивання коштів; суб'єкт первинного фінансового моніторингу; постачальники послуг віртуальних активів; блокчейн-аналітика.

Вступ

Постановка проблеми. Для сучасних суб'єктів господарювання проблеми комплаєнс-відповідності набувають особливого значення, враховуючи потребу дотримання вимог у різних сферах корпоративної діяльності. Однією з найважливіших сфер відповідності є дотримання вимог у сфері фінансового моніторингу, серед яких можна виділити: здійснення заходів належної перевірки клієнтів, виявлення кінцевих бенефіціарних власників, здійснення скринінгових процедур та спроможність ідентифікувати фінансові операції, які містять ризик відмивання коштів або фінансування тероризму. Враховуючи стрімке зростання глобальної екосистеми криптовалют, компанії мають забезпечити використання ефективних інструментів виявлення ознак легалізації коштів за допомогою віртуальних активів. Головними чинниками, які спонукають злочинців використовувати віртуальні активи в цілях відмивання коштів, є відносна анонімність, міжнародний характер діяльнос-

ті, можливість здійснювати операції без взаємодії із суб'єктами первинного фінансового моніторингу та складність регулювання ринку.

Відносна анонімність полягає у відсутності записів про ідентифікаційні дані користувачів в переліку інформації про транзакції на блокчейні. Натомість, записи містять лише адреси криптогаманців, що створює ілюзію конфіденційності. Міжнародний характер платежів забезпечується відсутністю обмежень на транскордонні транзакції, які в традиційній економіці регулюються вимогами міжнародних платіжних систем. Як наслідок, користувачі криптогаманців мають змогу миттєво переказувати криптовалюти між різними юрисдикціями, обминаючи банківський контроль та валютний нагляд. Неліцензовані біржі криптовалют не мають статусу суб'єктів первинного фінансового моніторингу, та, відповідно, не здійснюють заходи належної перевірки клієнтів. Цей факт дає змогу злочинним елементам створювати криптогаманці для фіктивних клієнтів та

Інформація про авторів:

Акімова Людмила Миколаївна, д-р наук з державного управління, кандидат економічних наук, професор, Заслужений працівник освіти України, професор кафедри трудових ресурсів і підприємництва. Email: l_akimova@ukr.net, <https://orcid.org/0000-0002-2747-2775>

Акімов Олександр Олексійович, д-р наук з державного управління, професор, Заслужений економіст України. Email: 1970aaa@ukr.net; <https://orcid.org/0000-0002-9557-2276>

Цитування за ДСТУ: Акімова Л. М., Акімов О. О. Інструменти протидії відмиванню коштів в екосистемі криптовалют. *Ефективність державного управління* : зб. наук. пр. Вип. 3/4(84/85). Львів: НЛТУ України, 2025. С. 60–66.

Citation APA: Akimova, L. M., & Akimov, O. O. (2025). Anti-money laundering tools in the cryptoassets ecosystem management. *Efficiency of public administration*, 3/4(84/85), 60–66. <https://doi.org/10.36930/508409>

використовувати послуги фінансових мулів. Екосистема криптоактивів є достатньо новим явищем у світовій економіці, тому потрібен час для напрацювання та застосування спеціального законодавства, призначеного для регулювання системи національними наглядовими органами.

Актуальність дослідження. Сучасні ефективні національні системи фінансового моніторингу використовують як нормативний, так і технологічний інструментарій для ідентифікації відмивання незаконних доходів. Ліцензування операторів крипторинку, використання блокчейн-аналітики, застосування алгоритмів на основі правил створюють нові можливості для підвищення ефективності систем протидії відмиванню коштів у сфері криптоактивів. Актуальність дослідження зумовлена необхідністю інтеграції зазначених вище інновацій у систему фінансового моніторингу України.

Мета дослідження та основні завдання для її досягнення. Метою статті є дослідження типологій відмивання коштів з використанням криптоактивів та інструментарію, який може бути застосований звітними установами у сфері фінансового моніторингу для боротьби з цим явищем. Для досягнення мети визначено такі завдання: 1) проаналізувати способи розміщення, нашарування та інтеграції незаконно отриманих коштів в екосистемі криптоактивів; 2) ідентифікувати заходи із протидії легалізації криптоактивів на національному та первинному рівнях системи фінансового моніторингу; 3) оцінити стан регулювання ринку віртуальних активів в Україні та можливі шляхи посилення протидії відмиванню коштів.

Предмет дослідження. Предметом дослідження є інструменти, які сприяють виявленню та протидії легалізації незаконних коштів у сфері віртуальних активів.

Методи та інформаційна база дослідження

У межах дослідження було застосовано набір наукових методів, які дали змогу всебічно охарактеризувати типові схеми легалізації коштів та ефективні інструменти боротьби з їх відмиванням в екосистемі криптоактивів. За допомогою статистичного методу оброблено кількісні показники щодо обсягу активів, які надійшли на підозрілі крипто-адреси. Системний підхід дозволив дослідити взаємозв'язки між різними етапами відмивання коштів. Для вивчення нормативно-правових актів та законів, які регулюють боротьбу з відмиванням коштів на ринку криптоактивів, було застосовано метод аналізу. Зіставлення українського досвіду з практиками ефективних закордонних систем фінансового моніторингу, було забезпечено шляхом використання порів-

няльно-аналітичного методу. Логічний метод використано для формування теоретичних засад реформування сучасної системи фінансового моніторингу України.

Інформаційною базою дослідження стали звіти провідних світових компаній у сфері аналітики блокчейну, наукові публікації, законодавчі акти України та інших держав.

Аналіз останніх досліджень і публікацій

Поширення криптоактивів у міжнародній економіці спричинило значний науковий інтерес до питань регулювання постачальників послуг на цьому ринку та заходів протидії відмиванню коштів. Зокрема, в роботі Р. Самсіва [18] досліджують еволюцію термінів, пов'язаних з криптоактивами в сучасній правовій площині. У праці В. Юсупова та Р. Марчук [19] було розглянуто заходи із протидії нелегальному обігу криптоактивів в Україні. С. Wronka [11] проаналізував регулювання криптоактивів у Великій Британії та Німеччині. Окрім того, в його роботі було досліджено потенційний вплив регуляторних рамок на ринок криптоактивів. Еволюція регулювання криптоактивів у Канаді та численні невизначеності в регулюванні криптоактивів були предметом дослідження R. Clements [2]. У дослідженні M. Lehmann [8] наведено критичний аналіз положень регулювання ринку криптоактивів в Європейському Союзі та оцінювання їх потенційних наслідків.

Виокремлення не вирішених раніше частин загальної проблеми. Незважаючи на наявні наукові дослідження, питання боротьби з легалізацією коштів у системі віртуальних активів потребує подальшого розгляду. Недостатньо вивченими залишаються новітні злочинні методи легалізації криптоактивів на етапах введення, нашарування та інтеграції. Окрім цього, недостатньо дослідженими є сучасні методи реагування на ризики легалізації, що охоплюють застосування як регуляторних, так і технологічних запобіжників.

Виклад основного матеріалу дослідження з обґрунтуванням одержаних результатів

Індикативні обсяги нелегальних коштів з використанням криптоактивів, опубліковані компанією TRM Labs, яка є визнаним експертом у сфері аналітики блокчейну, вказано на рис. 1. Враховуючи постійний процес ідентифікації криптогаманців, які містять ознаки відмивання коштів, дані за 2024 р., з великою вірогідністю, буде переглянуто у звітах за наступні роки. Екстраполюючи перегляд у бік збільшення показника за 2023 р., остаточна оцінка обсягу незаконної торгівлі за 2024 р. може перевищити 75 млрд доларів США [10, с. 4].

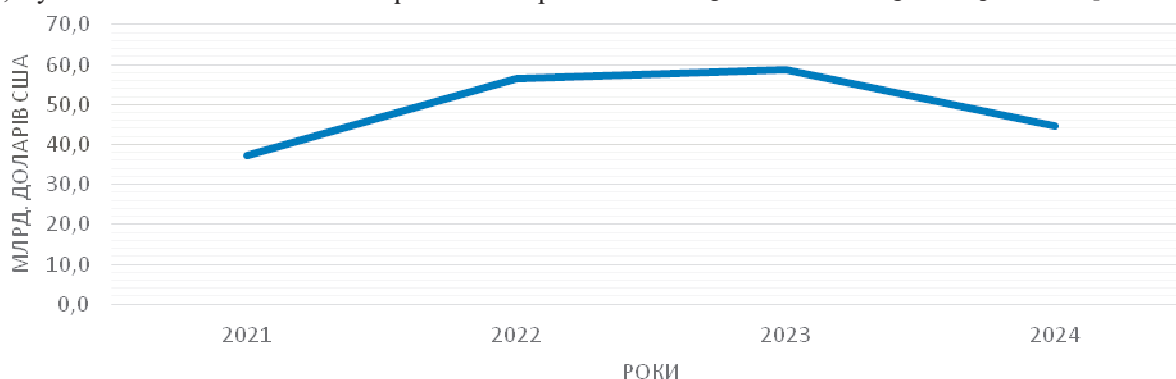


Рис. 1. Вхідний обсяг активів, які надійшли на підозрілі крипто-адреси з 2021 по 2024 роки

Джерело: сформував автор на основі [10].

На етапі введення незаконні кошти потрапляють в екосистему криптоактивів. Аналогічно до традиційної економіки, на цьому етапі головною метою злочинних елементів є розміщення незаконно набутих коштів. Типовими способами, які допомагають здійснити таке розміщення, є прямий обмін готівки на криптоактиви з використанням криптобіржі, отримання криптоактиву як оплати за незаконну діяльність, внесення готівкових коштів у криптобанкомати, розміщення криптоактивів фінансовими мулами на власних криптогаманцях.

На наступному етапі відбувається нашарування, метою якого є розірвання прямого зв'язку між походженням і призначенням коштів. Для цього використовуються способи заплутування сліду початкових активів. Типовими прикладами нашарування є здійснення швидких переказів між багатьма гаманцями і мережами, конвертація між різними видами криптоактивів або через численні біржі й платформи в різних юрисдикціях, змішування криптоактивів різних власників за допомогою "програм-змішувачів", використання монет з підвищеною приватністю.

Етап інтеграції є останнім кроком, призначеним для повернення коштів у легальну економіку. Способами інтеграції є обмін криптоактивів на фіатну валюту або інвестування в активи, що мають високу вартість.

Головним засобом протидії відмиванню коштів на етапі введення є ліцензування бірж та інших постачальників послуг на ринку криптоактивів, оскільки наявність зобов'язань щодо моніторингу транзакцій та виконання вимог стосовно ідентифікації та верифікації клієнтів створюють значний бар'єр від проникнення в екосистему нелегальних коштів. З цієї метою багато юрисдикцій, які вважають світовими фінансовими центрами, визнали постачальників послуг, пов'язаних із криптоактивами, фінансовими установами [12]. Таке визнання автоматично перетворило постачальників послуг криптоактивів на зобов'язаних суб'єктів у сфері фінансового моніторингу.

Зокрема, регламент Європейського Союзу 2023/1113 включив постачальників послуг, пов'язаних із криптоактивами (Crypto-Asset Service Providers – CASPs), до переліку зобов'язаних суб'єктів відповідно до статті 2 Директиви про боротьбу з відмиванням грошей Європейського Союзу 2015/849 [4]. Відповідно, CASPs зобов'язані розробляти та впроваджувати внутрішні політики та системи контролю у сфері боротьби з відмиванням грошей та фінансуванням тероризму (Anti-Money Laundering/Combating the Financing of Terrorism – AML/CFT), збирати та перевіряти дані про особу своїх клієнтів та бенефіціарних власників клієнтів, здійснювати моніторинг операцій з метою виявлення підозрілої діяльності, повідомляти підрозділи фінансової розвідки про наявність підозр стосовно відмивання коштів.

У США нагляд за постачальниками послуг, пов'язаних із криптоактивами (Virtual Asset Service Providers – VASPs) здійснюється як на федеральному рівні, так і на рівні окремого штату. На рівні країни VASP повинні дотримуватися вимог стосовно боротьби з відмиванням коштів згідно зі Законом про банківську таємницю (BSA) [6]. Для виконання цієї вимоги VASPs мають здійснити самостійну реєстрацію як платіжної установи на офіційному сайті підрозділу фінансової розвідки США, впровадити ефективну систему AML/CFT та подавати звіти про підозрілу діяльність. На рівні штату

установі потрібно отримати ліцензію на переказ грошових коштів або спеціалізовану ліцензію. Перед отриманням ліцензії VASP має пройти перевірку, елементами якої є аналіз фінансового стану, аудит вищого керівництва компанії, перевірка наявності процедур захисту прав споживачів.

Прикладом спеціалізованої ліцензії у США є BitLicense, яка запроваджена Департаментом фінансових послуг Нью-Йорка для компаній, що займаються бізнесом віртуальних активів у штаті Нью-Йорк [9]. Заявник повинен надати бізнес-план, деталізовану організаційну структуру, персональні дані щодо власників, керівників та ключових осіб компанії. Окрім того, потрібно надати внутрішні політики стосовно боротьби з відмиванням коштів, процедуру ідентифікації клієнтів, політику з кібербезпеки, опис внутрішньої системи управління ризиками, політику кастодіального зберігання цифрових активів клієнтів [12]. Після отримання документів Департамент фінансових послуг Нью-Йорка індивідуально оцінює фінансовий стан, прогнозований обсяг транзакцій та загальних зобов'язань компанії для визначення необхідного розміру мінімального капіталу. Заявник зобов'язаний внести гарантійний внесок або створити трастовий рахунок для захисту клієнтів. Мінімальний розмір гарантії становить 500 000 доларів США, але її значення може бути збільшене з урахуванням бізнес-моделі компанії [9]. Також постачальник послуг, пов'язаних із криптоактивами, повинен використовувати у своїй діяльності схвалену Департаментом фінансових послуг Нью-Йорка внутрішню політику лістингу нових віртуальних валют, або здійснювати операції лише з тими криптоактивами, які внесено до офіційного "Зеленого списку". Загалом, процес отримання BitLicense є надзвичайно тривалим, деталізованим та дорогим, що має на меті не допущення на ринок непрозорих компаній, схильних до здійснення ризикових операцій з криптоактивами.

Для ідентифікації компаніями криптоактивів, отриманих в якості оплати за незаконну діяльність, використовуються алгоритми на основі правил. Регульовані VASPs/CASPs повинні встановити у своїх внутрішніх документах та використовувати в системах автоматизації набір правил, згідно з якими всі транзакції в блокчейні будуть оцінюватися на ризик відмивання коштів. Прикладом такого правила може бути створення криптогаманця юридичною особою, яка раніше не здійснювала діяльність в екосистемі криптоактивів, зарахування компанією на криптогаманець значної суми коштів зі свого розрахункового рахунку в банку та швидке надсилання криптоактивів на інший нещодавно створений криптогаманець. Вказаний набір операцій може свідчити про трансфер коштів від жертви до осіб, пов'язаних з програмами-вимагачами.

Виявлення осіб, які за винагороду здійснюють транзакції з коштами злочинців (фінансових мулів), також може бути здійснене за допомогою порівняння поведінки руху активів із внутрішніми шаблонами регульованих VASPs/CASPs. Результатом цього аналізу є ідентифікація операцій структурування, за яких незаконні кошти розділяють на багато частин, кожна з яких при зарахуванні особою на криптогаманець є нижчою, ніж порогова сума, визначена законодавством певної юрисдикції. Окрім того, підхід на основі правил може виявити надходження криптоактивів, вартість яких не відповідає ри-

зик-профілю власника криптогаманця, що теж слугує індикатором використання третіх осіб з метою уникнення інформації про справжнього бенефіціара активу.

Для зменшення ризику внесення незаконно отриманих готівкових коштів в банкомати для криптоактивів (крипто-АТМ), в юрисдикціях з високими стандартами фінансового моніторингу використовують ліцензування. Оператори криптобанкоматів вважаються небанківськими фінансовими установами, внаслідок чого такі компанії мають виконувати вимоги, які передбачені для суб'єктів первинного фінансового моніторингу.

З метою ідентифікації нелегальних коштів на етапі нашарування регульовані постачальники послуг, пов'язаних із криптоактивами, використовують функціональні можливості власних інформаційних систем та спеціалізовані рішення від компаній, які здійснюють блокчейн-аналітику. Підхід на основі правил дає змогу регульованим VASPs/CASPs встановити кількісні параметри, в разі перевищення яких модуль фінансового моніторингу буде блокувати транзакцію та створювати запит на працівника звітної установи щодо необхідності аналізу підозрілої активності [17]. До таких параметрів можна віднести граничну кількість транзакцій, здійснених за участю одного криптогаманця протягом певного часу або граничну суму вартості криптоактивів, яка може бути переміщена від одного криптогаманця до іншого за певний проміжок часу.

Під час переміщення коштів через кілька міжланцюгових мостів між двома блокчейнами або між декількома різними блокчейнами одночасно, використовуються методи блокчейн-аналітики [3, с. 54-57]. Також спеціалізовану аналітику використовують для виявлення факту використання власником криптогаманця послуг "змішувачів" – сервісів, які об'єднують кошти від багатьох користувачів в один пул, а потім повертають користувачеві початкову суму внесених коштів, однак вже новими монетами, взятими з первинного пулу. Причому монети відправляються на нову адресу, яка була заздалегідь вказана користувачем. Засобом боротьби зі "змішувачами" є використання блокчейн-аналітики, що дає змогу встановити сценарій, за якого адреса криптоактиву отримує свою першу транзакцію від "змішувача". Криптогаманець, який отримує свої перші кошти через "змішувач", може бути індикатором підвищеного ризику, оскільки нові гаманці часто використовують злочинці виключно для відмивання коштів від злочинної діяльності [3, с. 65]. Такий спосіб реагування на ризик дає змогу регульованим VASPs/CASPs не здійснювати суцільний дерискінг, однак при цьому об'єктивно оцінювати рівень ризику в кожному конкретному випадку. У разі доведеного використання "змішувачів" в цілях відмивання коштів, юрисдикції можуть накладати санкції на їх діяльність, фактично блокуючи їх використання регульованими платформами криптоактивів.

До окремого виду "змішувачів" можна віднести використання криптоактивів, в яких застосовуються вбудовані криптографічні механізми. Зазначені вище криптоактиви широко відомі під назвою "приватні монети" (Privacy Coins). На відміну від більшості публічних блокчейнів, криптоактиви з криптографічними механізмами змішують справжній підпис відправника з підписами інших учасників, що робить неможливим визначення контрагента, який здійснив транзакцію. Окрім то-

го, для кожної транзакції може генеруватися одноразова адреса, що запобігає прямому зв'язку платежів із публічною адресою гаманця отримувача. Додатково, приватна монета має можливість приховувати переказану суму активів [1, с. 25]. Як наслідок, обіг криптоактивів із вбудованими криптографічними механізмами не дає змогу регульованим VASPs/CASPs, аналітичним компаніям та регуляторним органам визначити як фактичного відправника та отримувача коштів, так і обсяг підозрілих коштів, які можуть мати незаконне походження. Інструментом, який дає змогу зменшити ризик відмивання коштів, є відмова регульованих платформ криптоактивів в юрисдикціях з високими стандартами фінансового моніторингу від лістингу та торгівлі приватними монетами.

На етапі нашарування можливе використання торгівлі невзаємозамінними токенами (Non-Fungible Token – NFT) – унікальними цифровими активами, які ідентифікують право власності на цифровий об'єкт. Злочинці створюють власний NFT або купують цифровий об'єкт, який не має реальної ринкової ціни. Наступним кроком є створення багатьох криптогаманців, на які зараховуються кошти від жертв програм-вимагачів або відмиті кошти, отримані від "змішувачів". Далі відбувається фіктивне збільшення цінності NFT шляхом серії операцій купівлі-продажу цифрового об'єкта між гаманцями, які контролюють злочинні елементи. Під час кожної наступної операції купівля NFT відбувається за більшу вартість [1, с. 43]. Результатом таких дій є створення ілюзії високої ринкової вартості об'єкта, який, насправді, не має жодної цінності. Однак, кожна операція продажу залишає свій слід у блокчейні та на криптобіржі, створюючи історію торгівлі NFT та статистику зростання його ціни.

Головним способом інтеграції відмитих коштів є обмін криптоактивів на фіатну валюту. Для цього злочинні елементи намагаються здійснити переміщення криптовалют на регульовану VASP/CASP, оскільки лише ліцензовані платформи мають можливість надати юридично прозорий канал для виведення великих сум коштів у традиційну банківську систему. Інструменти блокчейн-аналітики регульованих платформ криптоактивів ідентифікують факт надходження коштів з криптогаманця на нерегульованій платформі, однак це не дає змогу зробити однозначний висновок про походження коштів від незаконної діяльності. Під час здійснення запиту щодо джерела коштів зловмисники можуть стверджувати, що криптоактиви були отримані внаслідок успішних інвестицій в нові проекти криптоактивів [16].

Відповіддю регульованих бірж на спроби використання ліцензованих платформ злочинцями в цілях інтеграції коштів є значні інвестиції в блокчейн-аналітику для ефективного виконання своїх зобов'язань у сфері AML/CFT. Інструменти такої аналітики здійснюють глибоке сканування історії транзакцій з метою проникнення крізь численні рівні змішування активів. Результатом аналізу є ідентифікація зв'язків між адресою криптогаманця, з якої надійшли кошти, та джерелами високого ризику, до яких належать гаманці, пов'язані зі "змішувачами", даркнетом або хакерськими атаками [3, с. 65].

Огляди провідних компаній з блокчейн-аналітики містять інформацію про поширене використання нерегульованих платформ криптоактивів для купівлі фіатної

валюти за відмиті кошти [10, с. 19]. Однак, нерегульовані VASPs/CASPs, зазвичай, не мають прямого доступу до традиційної банківської системи або мають статус клієнта із встановленим високим рівнем ризику. Тому за спроби здійснення транзакції банківська установа, яка є суб'єктом первинного фінансового моніторингу, може визнати таку фінансову операцію підозрілою, заблокувати переказ та надати звіт про підозрілу діяльність до підрозділу фінансової розвідки.

Альтернативним варіантом на етапі інтеграції є використання "відмитих" криптоактивів для купівлі фізичних активів високої вартості, до яких, передусім, належить нерухомість. Такий спосіб є менш ризикованим для злочинців, порівняно зі спробами отримати кошти на банківський рахунок шляхом продажу криптоактивів на регульованих або нерегульованих VASPs/CASPs. Існують юрисдикції, в яких пряме придбання нерухомості за криптовалюту є законним та регулюється відповідним законодавством. Найбільш очевидним прикладом є Республіка Ель-Сальвадор, оскільки в цій країні Bitcoin має статус законного платіжного засобу згідно зі Законом про Біткоїн (Ley Bitcoin), що набув чинності 7 вересня 2021 року [7]. В інших юрисдикціях, які намагаються стимулювати розміщення інфраструктури криптоактивів на своїх територіях, створено умови для операцій купівлі-продажу нерухомості за криптоактиви,

однак юридично такі дії визначаються як операція обміну, оскільки криптоактиви не визнаються офіційним засобом платежу. Зокрема, нотаріальні контори кантону Цуг, що входить до складу Швейцарської Конфедерації, використовуючи норми Закону про Технологію Розподіленого Реєстру, мають налагоджені процедури укладання угод з нерухомістю, в яких оплата здійснюється криптоактивами з використанням крипто-платіжного посередника [5]. Цей посередник конвертує криптоактив у швейцарський франк та забезпечує реєстрацію угоди в земельному реєстрі в офіційній валюті Швейцарської Конфедерації, однак з юридичним визнанням здійснення первинного розрахунку в криптовалюті.

Захистом від ризику відмивання коштів за розрахунок криптоактивами за нерухомість слугує наявність посередника, який володіє статусом суб'єкта первинного фінансового моніторингу та забезпечує здійснення належної перевірки клієнта та джерел походження криптоактивів перед укладенням угоди щодо об'єкту нерухомості.

У таблиці містяться узагальнені ризики відмивання коштів з використанням криптоактивів та заходи протидії, які успішно застосовують звітні суб'єкти у сфері фінансового моніторингу.

Таблиця. Типові способи відмивання коштів в екосистемі криптоактивів та заходи протидії

Етап відмивання коштів	Способи відмивання коштів	Заходи протидії
Введення	Обмін готівки на криптоактиви з використанням криптобіржі	Ліцензування бірж криптоактивів та отримання ними статусу суб'єктів первинного фінансового моніторингу. Здійснення регульованими VASPs/CASPs заходів належної перевірки до здійснення операцій з активами.
Введення	Внесення готівкових коштів у криптобанкомати	Ліцензування операторів криптобанкоматів та отримання ними статусу суб'єктів первинного фінансового моніторингу. Здійснення регульованими VASPs/CASPs заходів належної перевірки до здійснення операцій з активами.
Введення	Трансфер коштів від жертв програм-вимагачів або від інших злочинців	Застосування в інформаційних системах регульованих VASPs/CASPs алгоритмів на основі правил.
Введення	Здійснення третіми особами транзакцій з коштами, які належать кримінальним елементам	Виявлення фінансових мулів шляхом використання в інформаційних системах регульованих VASPs/CASPs алгоритмів на основі правил.
Нашарування	Швидкі перекази між багатьма гаманцями і мережами	Встановлення граничних кількісних параметрів у модулях фінансового моніторингу інформаційних систем регульованих VASPs/CASPs.
Нашарування	Конвертація між різними видами криптоактивів	Застосування блокчейн-аналітики.
Нашарування	Використання "змішувачів" криптоактивів	Застосування блокчейн-аналітики.
Нашарування	Фіктивне збільшення вартості невзаємозамінних токенів	Застосування блокчейн-аналітики.
Нашарування	Обмін традиційних криптоактивів на приватні монети	Делістинг криптоактивів із вбудованими криптографічними механізмами регульованими VASPs/CASPs.
Інтеграція	Обмін криптоактивів на фіатну валюту через регульовані VASPs/CASPs	Застосування блокчейн-аналітики.
Інтеграція	Обмін криптоактивів на фіатну валюту через нерегульовані VASPs/CASPs	Встановлення бар'єрів нерегульованим VASPs/CASPs для конвертації криптоактивів в фіатну валюту у разі відсутності інформації про джерела походження коштів.
Інтеграція	Купівля нерухомості за криптоактиви	Наявність посередника зі статусом суб'єкта первинного фінансового моніторингу, який повинен здійснювати заходи із належної перевірки клієнтів перед проведенням операцій з активами.

Примітка: створено на основі даних з [1; 3; 4; 5; 6; 7; 9; 10]

Вимоги стосовно здійснення заходів фінансового моніторингу українськими постачальниками послуг, пов'язаними з обігом віртуальних активів, містяться в

Законі України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсю-

дження зброї масового знищення" № 361-IX [13]. Відповідно до цього закону, надавачі послуг з використанням криптоактивів мають статус суб'єктів первинного фінансового моніторингу, що передбачає зобов'язання здійснювати комплекс заходів у сфері AML/CFT, ідентичний до інших учасників традиційного фінансового ринку. Зокрема, постачальники послуг, пов'язаних з обігом віртуальних активів, повинні перебувати на обліку в Державній службі фінансового моніторингу України, використовувати в своїй діяльності заходи із протидії відмиванню коштів та надавати до підрозділу фінансової розвідки звіти про підозрілі та порогові операції.

Водночас, правовідносини щодо обороту криптоактивів в Україні регулюються відповідно до Закону України "Про віртуальні активи" № 2074-IX, який було затверджено у 2022 р., однак не набув чинності [14]. У вересні 2025 р. Верховна Рада України прийняла за основу законопроект № 10225-д, який, серед іншого, має на меті усунути регуляторну прогалину, яка полягає у відсутності ефективного нагляду над постачальниками послуг, пов'язаних з обігом віртуальних активів [15]. Законопроектом пропонується розподілити нагляд за VASPs між Національною комісією з цінних паперів та фондового ринку та Національним банком України. Окрім того, проект передбачає встановлення обов'язкової процедури отримання VASP ліцензії від суб'єкта державного фінансового моніторингу та постійної відповідності ліцензійним вимогам як базову умову перебування постачальників послуг, пов'язаних з обігом віртуальних активів, на українському ринку криптоактивів. Оскільки законопроектом № 10225-д чітко визначено державні регулятори, очікується значне підвищення виконання звітними установами вимог AML/CFT, враховуючи право Національної комісії з цінних паперів та фондового ринку та Національного банку України здійснювати планові та позапланові перевірки VASPs та, у разі потреби, застосовувати суворі заходи впливу, передбачені Законом України № 361-IX.

Висновки та перспективи подальших розвідок

Розміщення нелегальних коштів відбувається шляхом купівлі криптоактивів за готівку або внесення жертвами криптоактивів на криптогаманець злочинців. З метою уникнення підозр, на етапі введення також використовуються послуги фінансових мулів, які вносять кошти через крипто-АТМ або створюють гаманці на криптобіржах на своє ім'я. Для нашарування використовуються швидкі та заплутані серії транзакцій між криптогаманцями з використанням різних бірж, конвертація в різноманітні токени, застосування "змішувачів" та приватних монет. У цілях інтеграції злочинні елементи намагаються здійснити обмін криптоактивів на фіатну валюту через регульовані або нерегульовані VASPs/CASPs. Альтернативним методом інтеграції є купівля за криптоактиви нерухомості або інших активів з високою ринковою вартістю.

Головним заходом протидії легалізації криптоактивів є ліцензування постачальників послуг, пов'язаних із криптоактивами, та отримання ними статусу суб'єктів первинного фінансового моніторингу. Для дотримання високих стандартів AML/CFT, звітні установи на ринку криптоактивів застосовують алгоритми на основі правил та інструменти блокчейн-аналітики. У разі неможливості керувати рівнем ризику регульовані VASPs/CASPs змушені використовувати дерискінг.

В Україні створено законодавчу базу стосовно боротьби з відмиванням коштів в екосистемі криптоактивів, яка відповідає міжнародним практикам. Водночас, ефективний нагляд за дотриманням вимог постачальниками послуг, пов'язаних з обігом віртуальних активів, у сфері фінансового моніторингу стане можливим лише після набуття чинності профільним законом, який регулює правовідносини на національному ринку криптоактивів.

Подальші дослідження в цій сфері варто зосередити на поглибленому аналізі міжнародної практики застосування регулятивних заходів, які уможлилювали б ефективне здійснення фінансового моніторингу постачальниками послуг, пов'язаними з обігом віртуальних активів. Особливу увагу варто приділити питанням унормування мінімальних вимог до ліцензованих операторів крипторинку щодо використання блокчейн-аналітики та застосування специфічних для цієї сфери критеріїв ризиків та індикаторів підозрілості.

References

1. Chainalysis (2025). The 2025 Crypto Crime Report. URL: <https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf>
2. Clements, R. (2021). Emerging Canadian Crypto Asset Jurisdictional Uncertainties and Regulatory Gaps. *Banking & Finance Law Review*, 37(1), pp. 25-55. URL: <https://ssrn.com/abstract=3891809>
3. Elliptic (2025). The Typologies Report: Innovating to fight financial crime in an age of rapid change. URL: <https://www.elliptic.co/blog/elliptics-typologies-report-innovating-to-fight-financial-crime-in-an-age-of-rapid-change>
4. European Commission (2023). Regulation (EU) 2023/1113 of the European Parliament and of the Council. URL: <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>
5. Federal Assembly of the Swiss Confederation (2019). Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT). URL: <https://www.news.admin.ch/news/message/attachments/60601.pdf>
6. FinCEN (1970). The Currency and Foreign Transactions Reporting Act of 1970. URL: <https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act>
7. Jurisprudencia (2021). Decreto Legislativo N° 57 (Ley Bitcoin). URL: <https://www.jurisprudencia.gob.sv/DocumentosBodega/D/2/2020-2029/2021/06/E75F3.PDF>
8. Lehmann, M. (2024). MICAR – Gold standard or regulatory poison for the crypto industry? *Common Market Law Review*, 61(3). <https://doi.org/10.54648/cola2024047>
9. New York State (2015). The official website of New York State. 23 NYCRR Part 200. URL: https://www.dfs.ny.gov/virtual_currency_businesses
10. TRM Labs (2025). Crypto Crime Report. URL: https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/68a391925a8dd785f5430482_TRM%20-Report-2025%20Crypto%20Crime%20Report.pdf
11. Wronka, C. (2024). Crypto-asset regulatory landscape: a comparative analysis of the crypto-asset regulation in the UK and Germany. *Journal of Asset Management*, 25(4), 417-426. <https://doi.org/10.1057/s41260-024-00358-z>
12. Акімова, Л. М. (2018). Механізм державного управління забезпеченням економічної безпеки в Україні: монографія. Київ: "Центр учбової літератури", 323 р.
13. Верховна Рада України (2020). Закон України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та

- фінансуванню розповсюдження зброї масового знищення" № 361-IX. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text>
14. Верховна Рада України (2023). Закон України "Про віртуальні активи" № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>
15. Верховна Рада України (2025). Проект Закону про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/56271>
16. Докієнко, Л. М., Клименко, В. В., & Акімова, Л. М. (2011). Інвестиційний менеджмент: навч. посіб. Київ: Академвидав, 405 р.
17. Клименко, В. В., Акімова, Л. М., & Докієнко, Л. М. (2015). Фінансовий ринок: навч. посіб. для студентів ВНЗ. Київ: Центр учбової літератури, 357 р.
18. Самсін Р.І. (2024). Еволюція термінів "криптовалюта", "віртуальні активи" та "криптоактиви" у сучасній правовій площині. *Київський часопис права*, 2, 213-221. <https://doi.org/10.32782/kij/2024.2.31>
19. Юсупов, В. В., & Марчук, Р. П. (2025). Протидія незаконному обігу віртуальних активів в Україні: питання правового регулювання. *Науковий вісник Ужгородського національного університету. Серія: Право*, 4(90), 367-373. <https://doi.org/10.24144/2307-3322.2025.90.4.53>

L. M. Akimova,²O. O. Akimov

The National University of Water and Environmental Engineering Rivne

²Ministry of Defence of Ukraine, Kyiv, Ukraine

ANTI-MONEY LAUNDERING TOOLS IN THE CRYPTOASSETS ECOSYSTEM

Introduction. The article examines the typologies of money laundering using crypto-assets and countermeasures taken by financial monitoring reporting entities. The main illegal methods of money laundering at the stages of placement, layering and integration of funds have been highlighted. The study contains an analysis of methods for countering the legalization of crypto assets both at the national level and at the level of reporting entities. The analysis is grounded on recent reports of leading global companies in the field of blockchain analytics, scientific publications, legislative acts of Ukraine and other countries.

Materials and Methods. The study used a set of scientific methods that allowed for a comprehensive description of typical money laundering schemes and effective anti-money laundering tools in the crypto-asset ecosystem. The statistical method was used to process quantitative indicators of the volume of assets received by suspicious crypto-addresses. The systematic approach allowed for the investigation of the relationships between different stages of money laundering. The analysis method was used to study the regulatory legal acts and laws regulating the fight against money laundering in the crypto-asset market. The comparison of Ukrainian experience with the practices of effective foreign financial monitoring systems was ensured by using the comparative analytical method. The logical method was used to form the theoretical foundations for reforming the modern financial monitoring system of Ukraine.

Analysis of Literary Sources. The problems of studying the crypto-asset market were investigated in the works of R. Samsiv, V. Yusupov, R. Marchuk, C. Wronka, R. Clements, M. Lehmann, and others. These studies were mainly aimed at the theoretical normalization of the elements of the virtual asset system and the analysis of the regulatory framework of the crypto-market.

Highlighting previously unsettled parts of the general problem. Despite the available scientific research, the issue of combating money laundering in the virtual asset system requires further consideration. The latest methods of legalizing crypto assets at the stages of introduction, layering and integration remain insufficiently studied. In addition, modern methods of responding to legalization risks, which include the use of both regulatory and technological safeguards, are insufficiently studied.

Results. The results showed that typical layering methods include obfuscated transfers of virtual currency between multiple crypto wallets, the use of money-mixing programs, the buying and selling of private coins, and the use of non-fungible tokens that identify ownership of a digital object. It has been established that the main tool for effectively combating money laundering through virtual assets is to provide service providers related to the circulation of crypto assets with the status of a primary financial monitoring entity and the use of blockchain analytics.

Discussion. The study highlights the importance of this topic for Ukraine. The national legislative framework for combating money laundering in the crypto-asset ecosystem is in line with global practice. However, there is a significant regulatory gap due to the lack of supervision of crypto-asset service providers by state financial monitoring entities.

Conclusion. The study showed that modern typologies of money laundering through the crypto-asset ecosystem are based on shortcomings in customer due diligence, technological innovations and regulatory gaps. Licensing of virtual asset market operators, blockchain analytics, rule-based algorithms and derisking create an effective system of protection against money laundering risks. The use of these tools in Ukraine will create the prerequisites for significantly increasing the efficiency of the national financial monitoring system in the virtual asset sector.

Keywords: cryptoassets; financial monitoring; money laundering; subject of primary financial monitoring; virtual asset service providers; blockchain analytics.