Кримінальне право та кримінологія

УДК 343.37:336.74:004.738.5

DOI https://doi.org/10.5281/zenodo.20755249

Протидія легалізації (відмиванню) майна, здобутого злочинним шляхом, вчиненій із застосуванням технологій криптовалютного міксування

Удовенко Ж.В.,

доктор юридичних наук, професор, кафедра кримінального та кримінального процесуального права

Національний університет «Києво-Могилянська академія»

Карандась М.В.,

студент VI курсу факультету прокуратури Національний юридичний університет імені Ярослава Мудрого

Прийнято: 21.05.2026 | Опубліковано: 30.05.2026

Анотація: У статті здійснено комплексне наукове дослідження механізмів функціонування міксерів криптовалют, які розглядаються як провідний інструмент анонімізації, обфускації (заплутування) та маскування фінансових потоків у сучасній структурі злочинності. Окрему увагу приділено аналізу ролі зазначених сервісів у процесах легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування терористичної діяльності та ухилення від сплати податкових платежів.

У роботі детально проаналізовано динаміку стрімкого зростання світового ринку криптоактивів, а також ключові тенденції його протиправного використання транснаціональними злочинними

угрупованнями. Особливу увагу приділено трансформації методів конспірації на тлі посилення глобального регуляторного тиску та імплементації жорстких нормативно-правових актів, зокрема Регламенту MiCA в Європейському Союзі та Genius Act у Сполучених Штатах Америки.

На основі ґрунтовного аналізу типологічних досліджень Державної служби фінансового моніторингу України та актуальної вітчизняної судової практики за 2024–2025 роки висвітлено практичні кейси залучення криптоміксерів до реалізації схем кібершахрайства (зокрема, за принципом «Man in the middle»), тіньового виведення капіталу та фінансування підривної діяльності спецслужбами держави-агресора.

Наукова новизна дослідження полягає в тому, що в ньому вперше у вітчизняній науці комплексно описано саме явище криптоміксерів та детально розкрито внутрішню механіку їхньої роботи. Автори простими словами пояснили суть такої діяльності та звернули увагу на те, що ці інструменти вже зараз активно використовуються на території України.

Ключові слова: криптоактиви, криптоміксери, обфускація транзакцій, децентралізовані фінансові сервіси, легалізація доходів, фінансовий моніторинг, блокчейн-аналіз, судова практика, фінансування тероризму.

Countering the Laundering of Criminally Obtained Assets Through the Use of Cryptocurrency Mixing Technologies

Abstract: The article provides a comprehensive scientific study on the functioning mechanisms of cryptocurrency mixers, which are examined as a leading tool for anonymization, obfuscation, and masking of financial flows within the modern structure of crime. Particular attention is paid to analyzing the

 ISSN: 3041-2110

role of these services in the processes of laundering (legalization) of proceeds of crime, financing of terrorist activities, and tax evasion.

The paper provides a detailed analysis of the dynamics of the rapid growth of the global crypto-assets market, as well as key trends in its illicit use by transnational organized crime groups. Specific emphasis is placed on the transformation of conspiracy methods against the backdrop of tightening global regulatory pressure and the implementation of stringent regulatory frameworks, notably the MiCA Regulation in the European Union and the Genius Act in the United States.

Based on a thorough analysis of typological studies conducted by the State Financial Monitoring Service of Ukraine and current domestic judicial practice for 2024–2025, the article highlights practical cases involving crypto mixers in cyber fraud schemes (specifically following the "Man in the middle" principle), shadow capital flight, and the financing of subversive activities by the aggressor state's intelligence services.

The scientific novelty of the study lies in the fact that it is virtually the first in domestic science to comprehensively describe the phenomenon of cryptocurrency mixers and reveal the inner mechanics of their operation in detail. The authors explained the essence of such activities in plain terms and drew attention to the fact that these tools are already being actively used within the territory of Ukraine.

Keywords: crypto-assets, cryptocurrency mixers, transaction obfuscation, decentralized financial services, money laundering, financial monitoring, blockchain analysis, judicial practice, financing of terrorism.

Постановка проблеми. Використання криптоактивів ввійшло у повсякденне життя не тільки окремих категорій громадян, а й у діяльність бізнес-середовища. Так, загальна ринкова капіталізація світового ринку

криптовалют становить 2,6 трильйона доларів США [1]. Водночас використання криптовалют для здійснення кримінальних правопорушень набуло системного характеру. Криптоактиви використовуються для ухилення від сплати податків, легалізації (відмиванні) коштів, як засіб розрахунку під час торгівлі наркотиками або під час здійснення шахрайських дій.

Слід зазначити, що останніми роками органи правопорядку значно активізували заходи протидії кримінальним правопорушенням, у яких криптовалюта використовується як засіб платежу. Водночас суттєво розширилися технічні можливості для відстеження походження криптоактивів і встановлення власників криптогаманців. У відповідь на це злочинці почали активніше використовувати інструменти, що ускладнюють ідентифікацію походження криптовалюти, зокрема криптоміксери. Вказаний функціонал зазначених сервісів спрямований на приховування кінцевого власника криптовалюти та її походження.

Необхідно звернути увагу на те, що Державна служба фінансового моніторингу України (далі – ДСФМУ) у одному зі своїх типологічних досліджень також наголосила, що одним із головних викликів для фінансової безпеки залишається активне використання віртуальних активів, які забезпечують високий рівень анонімності та значно ускладнюють виявлення незаконних фінансових потоків, пов’язаних із тероризмом. Такими є криптоміксери та DeFi-платформи - децентралізовані фінансові сервіси, які працюють без банків або бірж. Вони дозволяють фрагментувати потоки, приховувати джерела та одержувачів, обходити фінансові обмеження й нагляд [2].

Результати аналізу наукових публікацій свідчать про те, що вітчизняна наукова спільнота наразі не приділяє достатньої уваги питанню використання міксерів криптовалют. Водночас світові дослідники

здійснюють глибокий та всебічний аналіз цієї тематики. Зокрема, різні аспекти функціонування криптоміксерів детально розглянуто у працях таких науковців, як К. Бенхардт, Р. Боме, Д. Брейкер, А. Девальд, М. Мозер, А. Торрес-Аріас та А. Шоджейнасаб**.**

Метою статті є дослідження питання використання міксерів криптовалют, а також їхньої ролі як інструмента для відмивання (легалізації) коштів та ухилення від сплати податків.

Виклад основного матеріалу. За останні роки використання криптоактивів для здійснення кримінальних правопорушень стало невід'ємним елементом сучасної злочинної діяльності як в Україні, так і світу в цілому. Вказане пояснюється можливістю швидкого руху криптоактивів, труднощами ідентифікації, відстеження та арешту активів, потребою в удосконаленні механізмів фінансового моніторингу суб'єктів господарської діяльності, що надають послуги у сфері обігу криптоактивів. Так, відповідно до інформації від Chainalysis у 2025 році незаконні криптовалютні адреси отримали щонайменше 154 мільярди доларів, що на 162% більше, ніж у 2024 році. Ця тенденція зумовлена різким збільшенням вартості криптовалют, які отримані організаціями, що перебувають під санкціями, на 694% [3].

На противагу вищевказаному держави почали впроваджувати жорстку систему контролю за учасниками ринку криптовалют шляхом здійснення ретельного ліцензування надавачів послуг на вказаному ринку. Наприклад, у Європейському Союзі (далі – ЄС) у 2023 році було прийнято «Регламенту про ринки криптоактивів» (Markets in Crypto-Assets Regulation, MiCA), який став основним нормативно-правовим актом ЄС у сфері обігу криптовалют. Вказаний акт покликаний захищати інвесторів, встановити стабільність та правову визначеність на ринку криптоактивів, а також запобігти використанню криптовалют для здійснення злочинної діяльності [4]. У

Великій Британії Уряд планує запровадити повне з 2027 року регулювання криптовалют, прирівнявши їх до традиційних фінансових продуктів під наглядом Financial Conduct Authority, що також має забезпечити стабільність ринку на тлі його нестабільності [5]. У Сполучених Штатах Америки прийнятий Genius Act також вперше для країни створив рамки регулювання ринку та стандарти для учасників ринку, які хочуть провадити діяльність з обігу криптоактивів [6]. До того ж, одним з важливих аспектів Genius Act є його акцент на необхідності створення ефективної системи протидії відмиванню (легалізації) коштів, що отримані злочинним шляхом так і використанню криптоактивів для вчинення інших кримінальних правопорушень.

Водночас, з початком регулювання ринку криптоактивів та активним звітуванням учасників ринку державним регуляторам, а також постійному моніторингу органами правопорядку як і підрозділами фінансового моніторингу держав активних гравців на ринку, організовані злочинні угруповання почали використовувати механізми анонімізації криптовалютних активів, якими вони володіють для ускладнення виявлення походження таких активів та кінцевих власників органами правопорядку та суб'єктами фінансового моніторингу. Вказане стало можливим завдяки використанню «міксерів» криптовалют та «анонімних» криптовалют, що ускладнюють виявлення незаконного походження активів.

«Міксери» криптовалют є одним з механізмів, що залучаються організованими злочинними угрупованнями для анонімізації походження криптоактивів. Використання «міксерів» криптовалют за останні роки настільки виросло, що на вказаний механізм почали звертати увагу контролюючі органи держав, де крипто індустрія вже стала частиною фінансової системи. Зокрема, Управління контролю за іноземними активами при Міністерстві фінансів США у 2022 році ввело санкції проти Blender.io,

ISSN: 3041-2110

який використовується Корейською Народно-Демократичною Республікою для підтримки операцій з кібершахрайства та відмивання (легалізації) викрадених віртуальних активів [7]. Вказаний криптоміксер працював за принципом змішування транзакцій для приховування походження коштів: користувач (зокрема хакер) надсилав криптовалюту до сервісу, де вона потрапляла у спільний пул разом із коштами інших користувачів, після чого система «перемішувала» ці активи, розриваючи зв'язок між відправником і отримувачем, і повертала вже інші монети, які виглядали як не пов'язані з початковим джерелом. У цілому, Blender.io допоміг анонімізувати походження понад 500 мільйонів доларів США у біткоїнах з моменту свого створення у 2017 році. Ідентично санкції було накладено й на Tornado Cash – криптоміксер, який був використаний для відмивання (легалізації) близько 7 мільярдів доларів США з 2019 року [8]. У 2025 році Європол також повідомив, що під його координацією правоохоронні органи Федеративної Республіки Німеччина та Швейцарської Конфедерації провели операцію, яка була спрямована на ліквідацію незаконного криптовалютного міксинг-сервісу «Cryptomixer», що підозрюється у сприянні кіберзлочинності та відмиванню коштів [9].

Серед практичних спеціалістів та науковців виділяються два типи криптовалютних міксинг-сервісів – традиційні та сучасні.

Традиційні криптоміксери працюються за схемою, що визначається фіксована суму грошей, яку можна змішувати з криптоактивами із іншими транзакціями. Далі кошти різних відправників випадковим чином перерозподіляються між отримувачами. Так, спочатку сервіс створює для користувача нову випадкову адресу для внесення коштів; при кожному оновленні сторінки ця адреса змінюється. Потім відправник має зачекати, поки з'явиться щонайменше N інших користувачів із тією ж сумою, і всі вони внесуть кошти на свої адреси.

ISSN: 3041-2110

На наступному (проміжному) етапі сервіс формує транзакції, у яких ці N внесків випадково перемішуються та відправляються на N нових анонімних адрес. Це робиться для того, щоб стерти зв'язок між початковим відправником і кінцевим отримувачем. У результаті формується так звана «множина анонімності»: ймовірність правильно встановити, хто саме кому відправив кошти, становить 1 із N.

Сучасні криптоміксери, як і традиційні, працюють у три етапи. Спочатку кошти, які потрібно змішати, надсилаються на випадкову депозитну адресу, створену сервісом. Основна відмінність полягає в тому, що міксеру не потрібно чекати надходження коштів від інших користувачів — він одразу відправляє «очищені» кошти отримувачу зі своїх власних адрес, на яких уже є достатній баланс. У результаті слід повністю зникає, оскільки транзакції відправлення і отримання в блокчейні не пов'язані між собою. Крім того, через використання затримок відстеження коштів стає ще складнішим. Варто зазначити, що цей метод не має обмежень щодо суми коштів, які можуть бути відмиті [10].

Слід вказати, що криптовалютні міксери також ділять на централізовані та децентралізовані. У централізованих криптоміксерах користувачі передають свою криптовалюту міксеру, який безпосередньо змішує монети в одному пулі та повертає іншу криптовалюту такої ж вартості. Для власників акаунтів це означає необхідність високого рівня довіри до криптоміксера, адже ним володіють треті особи, які, як правило, не розкривають дані про себе. До того ж, централізований міксинг-сервіс усе одно зберігає інформацію про походження та отримувачів криптоактивів, і в разі її розкриття це нівелює приватність, яку має забезпечувати такий сервіс. Більше того, якщо міксер стане жертвою хакерської атаки або витоку даних, наприклад, усі криптоактиви можуть бути втрачені, а інформація розкрита.

ISSN: 3041-2110

У децентралізованих міксинг-сервісах пропонують альтернативу, використовуючи концепцію «доказу з нульовим розголошенням» (zero-knowledge proof), яка дозволяє підтвердити наявність криптоактивів без розкриття його їхнього походження. Користувачі об'єднуються в скоординовану групу та використовують смартконтракти для захисту своїх транзакцій. Для прикладу, уявімо 100 користувачів, кожен із яких хоче змішати один біткоїн – кожен вносить один біткоїн і отримує назад інший біткоїн тієї ж вартості. Оскільки в децентралізованих міксерах використовуються протоколи для приховування транзакцій, ніхто не знає, кому тепер належить початкова криптовалюта. Використання децентралізованих міксерів є безпечнішим, ніж централізованих, оскільки не існує записів, які можна було б розкрити третім особам.

В цілому, можна констатувати, що визначення децентралізованих міксерів частково збігається з описом традиційних криптоміксерів, що вказує на те, що незалежно від визначення опис діяльності міксинг-сервісів залишається ідентичною й залежить від інтерпретації.

Результати емпіричних досліджень щодо діяльносіт міксинг-сервісів на практиці свідчать, що такі сервіси не вимагали реєстрації користувачів або підтвердження особи. Лише один міксер дозволяв використовувати кілька вхідних адрес для надсилання біткоїнів до сервісу. Водночас 17 із 20 сервісів підтримували виплати на щонайменше дві різні вихідні адреси. Десять сервісів надавали можливість налаштовувати затримку виплат, що безпосередньо впливає на рівень анонімності транзакцій. Заявлені інтервали затримки варіювалися від миттєвих виплат до 168 годин: дев'ять сервісів пропонували затримку до 8 годин, тоді як вісім – понад 24 години. Крім того, 19 сервісів мали звичайні вебсайти (clearnet), доступні напряму через інтернет, причому 13 із них використовували зворотний проксі-сервіс Cloudflare для приховування своїх реальних серверних адрес [11, с. 3].

Слід звернути увагу, що тривалість операцій із використанням «міксерів» залежить від необхідності якісного маскування походження коштів. Наприклад, швидкі сервіси можуть завершити операції з відмивання (легалізації) віртуальних активів за 1 годину й менше, а сервіси «агресивного» маскування можуть направити кошти через 1-3 дні. Сучасні сервіси криптоміксерів використовують розширені параметри, які роблять їх більш складними. Одним із таких параметрів є випадкова затримка часу відправлення криптовалюти: більшість сервісів пропонують випадкову затримку від 1 до 1440 хвилин між отриманням і відправленням транзакцій [12, с. 49]. Це ускладнює відстеження руху коштів за часовими закономірностями. Іншим параметром є обмеження кількості адрес отримувачів, яке в сучасних міксерах зазвичай відсутнє. Також, вказане дозволяє використовувати необмежену кількість адрес, що ускладнює відстеження переказів, оскільки кошти розподіляються між багатьма отримувачами.

Важливо звернути увагу на те, як можна виявляти криптовалюти, що пройшли криптоміксери. Виявлення криптовалюти, що пройшла через міксер, базується на комплексному аналізі блокчейн-даних, оскільки такі сервіси залишають специфічні цифрові сліди. Основним інструментом перевірки є AML-сервіси (як-от Crystal, Chainalysis або AMLBot), які автоматично маркують адреси та транзакції, пов'язані з відомими пулами міксерів (наприклад, Tornado Cash або ChipMixer), присвоюючи активам високий рівень ризику (Risk Score).

Окрім спеціалізованих програм, існують характерні ознаки «міксингу», які можна помітити при ручному аналізі: надходження коштів з нових гаманців без попередньої історії, дроблення великих сум на багато дрібних рівних часток, або нетипові часові затримки між транзакціями. Хоча міксери розривають прямий зв'язок між відправником і отримувачем,

ISSN: 3041-2110

аналітичні системи відстежують непрямі патерни поведінки та накопичують бази даних «забруднених» адрес, що дозволяє біржам і регуляторам ідентифікувати такі активи як підозрілі та блокувати їх при спробі виведення в фіат. Разом з тим, на нашу думку, найкращим способом аналізу криптовалют, що підозрюються у тому, що пройшли міксер-криптовалют є здійснення комплексного аналізу: від первинного аналізу за допомогою спеціалізованих програм до здійснення OSINT перевірок та, за можливості, отримання відомостей щодо подальшого цільового використання криптовалюти. Наприклад, ознаками можливого незаконного походження криптовалют, крім відповідних алертів з аналітичних систем, що вказані вище, може бути виведення криптовалют у фіатні валюти з подальшим зняття коштів у готівку, швидкий рух такої криптовалюти, невідповідність фінансового стану особи, яка отримала таку криптовалюту, якщо її об’єм є значним.

Аналізуючи питання використання міксинг-сервісів слід звернути увагу на приклад з типологічного дослідження ДСФМУ. Вказаним органом виявлено схему використання спецслужбами російської федерації криптогаманця (USDT у мережі «Tron») для фінансування підготовки терористичних актів та інших злочинів, спрямованих проти основ національної безпеки України. Встановлено, що мультивалютний криптогаманець W застосовувався як інструмент для приховування походження активів, у тому числі злочинних. Така можливість забезпечувалася механізмами внутрішньої взаємодії гаманців на платформі, зокрема змішуванням коштів, що значно ускладнювало їх подальше відстеження. Протягом останніх семи років на криптогаманець W надходили значні обсяги віртуальних активів від переважно російських (Garantex, Grinex, Hydra) та іранських підсанкційних сервісів, криптоміксерів, а також терористичної організації Хамас. Під час аналізу ДСФМУ виявлено ланцюг

ISSN: 3041-2110

криптотранзакцій, за яким активи з криптогаманця W перераховувалися на транзитні криптогаманці, власниками яких ідентифіковано співробітників ФСБ російської федерації. Надалі кошти з кінцевих акаунтів на біржах Binance і WhiteBIT за допомогою P2P-платформ конвертувалися з USDT у гривню та надходили на карткові рахунки громадян України, яких було завербовано для вчинення терористичних актів та інших злочинів на території України [2, с. 62-63].

У вітчизняній судовій практиці також зустрічаються судові рішення, де зазначено щодо залучення міксерів-криптовалют для здійснення кримінально караної діяльності. Наприклад, в ухвалі Голосіївського районного суду м. Києва від 03.09.2025 року у справі № 752/11560/25 зазначено, що у період з 26.09.2024 по 18.10.2024 на банківський рахунок № НОМЕР_1 компанії «Buildmat Production and Delivery KFT», яка підконтрольна ОСОБА_9 , надійшли кошти в сумі 1 186 190 Євро з рахунку НОМЕР_2 компанії «UAB ACUS VAISTINE», із призначенням платежу «оплата по інвойсу» [13]. Після здійснення переказів на рахунок компанії «Buildmat Production and Delivery KFT», ОСОБА_10 та ОСОБА_11 направили до банківської установи підроблені документи про невиконання представниками зазначеної компанії своїх зобов`язань за договором та з вимогою повернення про безготівкових коштів відправнику, за результатом яких вказані кошти були повернуті на рахунки компанії «UAB ACUS VAISTINE». У подальшому віртуальні активи у розмірі 1 245 682 USDT, які надійшли від ОСОБА_9 на криптогаманці, які визначені ОСОБА_10 та ОСОБА_11 , з використанням так званих схем «міксер» з залученням ряду підконтрольних транзитних гаманців, які зокрема належать власникам обмінного сервісу «ІНФОРМАЦІЯ_5», були додані до інших віртуальних активів та виведені у готівкові кошти.

ISSN: 3041-2110

У вироку Новозаводського районного суд міста Чернігова від 28.02.2025 року у справі № 751/905/25 встановлено, що заходи конспірації, які використовували учасники організованої злочинної групи полягали у тому, щоб члени не знали, не бачили одне одного вживу та не спілкувались між собою напряму, спілкувались виключно через Інтернет месенджери, які використовують «end-to-end» шифрування трафіку («Telegram»), використання в якості платіжних інструментів криптовалюти з використанням схем виводу отриманих незаконним шляхом коштів через різноманітні «сірі» обмінні сервіси, так звані «міксери», платіжні картки так званих «дропів», тощо [14].

Ухвалою Київського районного суду м. Харкова від 31.10.2024 року у справі № 953/7018/24 встановлено, що механізм злочинної діяльності полягає у так званій схемі «Man in the middle», яка виявляється у розміщенні в українському сегменті мережі «Інтернет» оголошень спрямованих на українську аудиторію, в яких пропонується здійснити обмін готівкових грошових коштів на криптовалюту у обмінних пунктах на всій території України [15]. При цьому, шляхом використання засобів соціальної інженерії зловмисники вживають заходів, які призводять до того, що коли громадяни України прибувають для здійснення обмінної операції до обмінного пункту на території України ними особисто повідомляється як гаманець отримання криптовалюти за результатом обмінної операції - гаманець зловмисника, який надається зловмисником заздалегідь до здійснення валюто-обмінної операції. У такому випадку, потерпіла особа, громадянин України після передачі готівки до обмінного пункту отримує криптовалюту не на власний електронний гаманець, а на гаманець зловмисника, при чому гаманець зловмисника сама потерпіла особа вказує як власний, про що надає відповідні розписки до обмінного пункту. Таким чином, після передачі готівки, грошові кошти у вигляді криптовалюти надходять на гаманець

зловмисника та привласнюються останнім. В наступному, з метою унеможливлення виявлення та встановлення осіб зловмисників, останні вживають заходи спрямовані на маскування та анонімізацію криптовалютних транзакцій, які спрямовані на переведення незаконно отриманих криптовалютних активів у легальний вигляд, їх легалізацію та відмивання. З цією метою використовуються сторонні сервіси, так звані «міксери криптовалют», свап сервіси та інші заходи, які дозволяють максимально анонімізувати транзакції криптовалюти та здійснити її відмивання та легалізацію.

Отже, можна дійти висновку, що криптовалютні міксери використовуються для легалізації (відмивання) віртуальних активів, одержаних внаслідок вчинення різних кримінальних правопорушень. Крім того, ці інструменти стають ключовою ланкою в ланцюгу обфускації (заплутування) транзакцій, що дозволяє зловмисникам не лише приховувати зв'язок між джерелом походження коштів та їх кінцевим отримувачем, а й ефективно протидіяти стандартним інструментам блокчейн-аналізу, які використовують правоохоронні органи.

Висновок. Проведений аналіз свідчить, що стрімка інтеграція криптоактивів у глобальну фінансову систему супроводжується масштабною адаптацією організованої злочинності до нових цифрових реалій. Криптовалютні міксери трансформувалися з інструментів забезпечення приватності на критично важливу інфраструктуру тіньового сектору, що дозволяє зловмисникам здійснювати обфускацію транзакцій та розривати зв’язок між злочинним джерелом походження віртуальних активів і їх кінцевим отримувачем. Вивчення вітчизняної судової практики та міжнародного досвіду підтверджує, що міксинг-сервіси є ключовою ланкою у схемах легалізації доходів від наркоторгівлі, шахрайства типу «Man in the middle», кіберзлочинності та навіть фінансування тероризму

 ISSN: 3041-2110

спецслужбами держави-агресора. Попри впровадження жорстких регуляторних механізмів, таких як MiCA в ЄС чи Genius Act у США, поява децентралізованих платформ та методів «агресивного» маскування створює нові виклики для системи фінансового моніторингу. Ефективна протидія цим загрозам неможлива без комплексного підходу, який має поєднувати використання передових аналітичних програм (Crystal, Chainalysis), здійснення глибоких OSINT-перевірок та активне міжнародне співробітництво у сфері ліквідації незаконних міксинг-сервісів. Лише синхронізація правових стандартів та технічних засобів ідентифікації «забруднених» активів дозволить правоохоронним органам випереджати динамічні зміни в методах анонімізації, що використовуються для підриву національної та міжнародної фінансової безпеки.

Україна має насамперед встановити чітке нормативне регулювання обігу криптовалют та забезпечити дієвий регуляторний нагляд за гравцями цього ринку. Зокрема, необхідно надати ДСФМУ можливість отримувати від нової категорії суб'єктів первинного фінансового моніторингу — надавачів послуг у сфері криптовалюти — повну інформацію щодо віртуальних активів на їхніх гаманцях, їхнього руху та походження. Такий механізм, за аналогією з банками та небанківськими фінансовими установами, дозволить якісно виявляти схеми ухилення від сплати податків та інші кримінальні правопорушення, що вчиняються із залученням криптовалютних міксерів.

Список використаних джерел

1. CoinGecko. Charts [Електронний ресурс]. – Режим доступу: https://www.coingecko.com/uk/charts?utm_source=chatgpt.com (дата звернення: 30.04.2026).

2. Державна служба фінансового моніторингу України. Типологічне дослідження «Відмивання коштів та фінансування тероризму з

використанням віртуальних активів» [Електронний ресурс]. – Режим доступу: https://fiu.gov.ua/assets/userfiles/411/%D0%A2%D0%B8%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%20%D0%94%D0%A1%D0%A4%D0%9C%D0%A3/Typology%202025_UA.pdf (дата звернення: 30.04.2026).

3. Chainalysis. 2026 Crypto Crime Report Introduction [Електронний ресурс]. – Режим доступу: https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/ (дата звернення: 30.04.2026).

4. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010, (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [Електронний ресурс]. // EUR-Lex. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng (дата звернення: 30.04.2026).

5. Financial Conduct Authority (FCA). FCA consults on guidance on UK's future crypto regime [Електронний ресурс]. – Режим доступу: https://www.fca.org.uk/news/press-releases/fca-consults-guidance-uk-future-crypto-regime (дата звернення: 30.04.2026).

6. Національний інститут стратегічних досліджень. GENIUS Act: можливості та ризики для США, Європи та України [Електронний ресурс]. – Режим доступу: https://niss.gov.ua/doslidzhennya/ekonomika/genius-act-mozhlyvosti-ta-ryzyky-dlya-ssha-yevropy-ta-ukrayiny (дата звернення: 30.04.2026).

7. U.S. Department of the Treasury. U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats [Електронний ресурс]. – Режим доступу: https://home.treasury.gov/news/press-releases/jy0768 (дата звернення: 30.04.2026).

 ISSN: 3041-2110

8. U.S. Department of the Treasury. U.S. Treasury Sanctions Virtual Currency Mixer Tornado Cash [Електронний ресурс]. – Режим доступу: https://home.treasury.gov/news/press-releases/jy0916 (дата звернення: 30.04.2026).

9. Europol. Europol and partners shut down crypto mixer [Електронний ресурс]. – Режим доступу: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-partners-shut-down-cryptomixer (дата звернення: 30.04.2026).

10. Moser M., Bohme R., Breuker D. Mixing Detection on Bitcoin Transactions Using Statistical Analysis [Електронний ресурс]. – Режим доступу: https://scispace.com/pdf/mixing-detection-on-bitcoin-transactions-using-statistical-4x9ucqyk.pdf (дата звернення: 30.04.2026).

11. Torres-Arias A., Bönhardt C., Dewald A. Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigations [Електронний ресурс]. – Режим доступу: https://dfrws.org/wp-content/uploads/2025/03/Unmixing-the-mix-Patterns-and-challenges-in-Bitcoin-mixer-investigatios.pdf (дата звернення: 30.04.2026).

12. Shojaeinasab A. Decoding illicit Bitcoin transactions: a multi-methodological approach [Electronic resource] / A. Shojaeinasab. — Victoria : University of Victoria, 2023. — Access mode: University of Victoria Library Repository (дата звернення: 30.04.2026).

13. Ухвала Голосіївського районного суду м. Києва від 03.09.2025 у справі № 752/11560/25. URL: https://reyestr.court.gov.ua/Review/130250736 (дата звернення: 30.04.2026).

14. Вирок Новозаводського районного суду міста Чернігова від 28.02.2025 у справі № 751/905/25.

URL: https://reyestr.court.gov.ua/Review/125517822 (дата звернення: 30.04.2026).

15. Ухвала Київського районного суду м. Харкова від 31.10.2024 у справі № 953/7018/24. URL: https://reyestr.court.gov.ua/Review/122700922 (дата звернення: 30.04.2026).

ISSN: 3041-2110