УДК 342.9

Старущенко Я.В., аспірант спеціальності 081 Право
Науковий керівник: Головко К.В., д.ю.н., проф. професор кафедри конституційного і адміністративного права
(Національний авіаційний університет, м. Київ, Україна)

МЕТОДИ ВІДМИВАННЯ КОШТІВ НА БЛОКЧЕЙНІ: ЮРИДИЧНІ АСПЕКТИ

Ефективна політика та правові засади запобігання відмиванням коштів, отриманих від обігу віртуальних активів є ключем до цілісності та стабільності як міжнародної, так й національної фінансової системи та економіки.

Варто вказати, що наразі досліджуються різні методи та прийоми для відмивання коштів, отриманих від обігу віртуальних активів. Розуміння цих методів має вирішальне значення для запобігання відмивання коштів, отриманих від обігу віртуальних активів у цифрову епоху. Зокрема, до п'яти найпопулярніших методів, які використовуються злочинцями для відмивання коштів на блокчейні відносять:

1. Вкладені послуги (Nested services) – це широка категорія послуг, які працюють в межах однієї або декількох бірж. Ці послуги використовують адреси, розміщені на біржах, щоб використовувати ліквідність бірж і використовувати можливості торгівлі. Деякі біржі не вимагають високих стандартів відповідності для вкладених послуг, що дозволяє поганим акторам використовувати їх для відмивання грошей. У блокчейн-каунії ці транзакції з вкладеними послугами, схоже, були проведені їх приймаючими контрагентами (тобто біржами), а не розміщеними вкладеними послугами або адресами фізичних осіб. Найпоширенішим і сумнозвісним типом вкладених послуг є позабіржовий (OTC) брокер. Позабіржові брокери дозволяють трейдерам легко, безпечно та анонімно торгувати великою кількістю криптовалюти. Позабіржові брокери сприяють прямій торгівлі криптовалютою між двома сторонами без посередництва біржі. Ці угоди можуть бути здійснені між різними криптовалютами (наприклад, Ethereum та Bitcoin) або між криптовалютами та фіатними валютами (наприклад, криптовалютами, такими як Bitcoin, та фіатними валютами, такими як євро). Позабіржові брокери знаходять контрагентів для транзакції в обмін на комісію, але не беруть участі в переговорах. Після визначення термінів сторони передають зберігання активів через брокера. Зокрема, у Серпні 2020 Року США Міністерство юстиції (DOJ) подало скаргу на конфіскацію 280 криптовалютних адрес, причетних до відмивання криптовалюти на суму приблизно 28,7 мільйонів доларів, вкраденої з біржі хакерами, пов'язаними з Північною Кореєю, відомими як Lazarus Group. У скарзі детально описано два зломи криптобірж північнокорейських акторів, які вкрали криптовалюту на мільйони доларів і в кінцевому підсумку відмили кошти через китайських позабіржових (OTC) криптовалютних трейдерів, і слідують за відповідними діями, пов'язаними з крадіжкою 250 мільйонів доларів у криптовалюті через інші біржові зломи північнокорейських акторів [8]. Lazarus Group продовжує використовувати позабіржових трейдерів для відмивання коштів. У квітні 2023 року Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) наклало санкції на трьох осіб, у тому числі двох позабіржових криптотрейдерів, за допомогу північнокорейській групі [9].

2. Азартні платформи (Gambling platforms) популярні серед криптовалютних відмивачів грошей. Послуги з азартних ігор були вказані у звіті FATF «Віртуальні активи Червоний прапор відмивання грошей та фінансування тероризму», виданому у вересні 2020 року [10]. У цьому звіті FATF визначила дві ситуації, в яких послуги з азартних платформ можна розглядати як відмивання, зокрема: 1) кошти,

депоновані або виведені з віртуальної адреси активу або гаманця, з прямими та непрямими посиланнями на відомі підозрілі джерела, включаючи сумнівні сайти азартних ігор; 2) транзакції, що походять від або призначені для послуг онлайн-азартних ігор.

3. Мікшери (Mixers) – це послуги, які поєднують цифрові активи з багатьох адрес разом, перш ніж випускати їх з випадковими інтервалами на нові адреси призначення або гаманці, тим самим підвищуючи анонімність. Вони часто використовуються для приховування сліду коштів, перш ніж вони будуть переведені законним підприємствам або великим біржам. Варто вказати, що у березні 2023 року Міністерство юстиції США оголосило про спільне міжнародне видалення ChipMixer, сервісу з мікшування криптовалют у даркнеті, відповідальному за відмивання понад 3 мільярди доларів у криптовалюті. Операція дозволила німецькій владі вивести понад 46 мільйонів доларів у криптовалюті з серверних серверів [11]. Іншим прикладом є Tornado Cash, мікшер, який «відмив» понад 7 мільярдів доларів з 2019 по 2022 рік, допоки розробник сервісу не був заарештований голландською владою [12].

4. Фіатні біржі (Fiat exchanges) змінюють криптовалюту на готівку і можуть бути мейнстрімними, одноранговими (P2P) або несумісними (біржі, які не підкоряються або не підпадають під дію правил). Так, біржі використовували такі адреси, щоб вивести у готівку майже 23,8 мільярда доларів у криптовалюті в 2022 році, що на 68% більше, ніж у попередньому році [13].

5. Послуги зі штаб-квартирою в юрисдикціях високого ризику (Services headquartered in high-risk jurisdictions) – це послуги в юрисдикціях, визначених як такі, що мають стратегічні недоліки в своїх режимах AML або боротьби з фінансуванням тероризму (CFT). Зокрема FATF визначає юрисдикції зі слабкими заходами боротьби з відмиванням грошей (AML/CFT), які часто зовні називають «Чорним та сірим списком» [14]. Заходи FATF щодо публічного оприлюднення переліку країн зі слабкими режимами AML/CFT виявився ефективним. 18 січня 2024 року відбулася публікація делегованого Регламенту Комісії (ЄС) 2024/163 [15] про внесення змін до списку ЄС. Станом на червень 2024 року FATF розглянув 133 країни та юрисдикції та публічно визначив 108 з них такими, які мають слабкий режим AML/CFT. Наслідком цього 84 держави впровадили необхідні реформи для усунення своїх слабких сторін AML/CFT і були виключені зі списку. Європейська комісія також визначає країни, які мають стратегічні недоліки у своїх режимах AML/CFT і які становлять значну загрозу фінансовій системі Європейського Союзу [16].

Відмивання грошей та пов’язані з ним злочини (так звані «предикатні злочини») можуть загрожувати цілісності та стабільності як фінансового сектору, так і зовнішній стабільності країни в цілому. Вони можуть призвести до дестабілізації економіки, банківських криз, неефективного збору доходів, більш широких недоліків публічного адміністрування, репутаційних ризиків для міжнародних фінансових центрів та втрати кореспондентських банківських відносин. У все більш взаємопов’язаному світі шкода, завдана цими злочинами, є глобальною та впливає на цілісність і стабільність міжнародної фінансової системи.

Список використаних джерел:

1. FATF report Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

2. Suspected developer of crypto mixer Tornado Cash arrested URL: https://techcrunch.com/2022/08/12/suspected-tornado-cash-developer-arrested-in-amsterdam/

3. The Chainalysis 2024 Crypto Crime Report URL: https://go.chainalysis.com/crypto-crime-2024.html

4. «Black and grey» lists URL: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

5. Anti-money laundering and countering the financing of terrorism at international level URL: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-international-level_en