

МОДУЛЬ 3 — ЗАПОБІГАННЯ ПРАВОПОРУШЕННЯМ: FRAUD PREVENTION TA DUE DILIGENCE

Модуль Жан Моне ERCM — Правове регулювання криптоактивів: від основ до поглибленого рівня

Грант № 101126839 · Національний юридичний університет імені Ярослава Мудрого

У цьому модулі ми розглянемо ризик-орієнтований підхід до протидії зловживанням віртуальними активами, основні види шахрайства у цій сфері, принципи належної перевірки клієнтів (due diligence) при операціях з віртуальними активами, а також специфічні ризики P2P-платежів і бірж. Розглянемо ці питання послідовно.

РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ДО ПРОТИДІЇ ЗЛОВЖИВАННЯМ ВІРТУАЛЬНИМИ АКТИВАМИ

3.1. Поняття та принципи ризик-орієнтованого підходу

Ризик-орієнтований підхід (risk-based approach, RBA) є базовим методологічним принципом міжнародної системи протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ), закріпленим у Рекомендації 1 FATF. Його суть полягає в тому, що держави, регулятори та суб'єкти первинного фінансового моніторингу (у тому числі постачальники послуг, пов'язаних з віртуальними активами, — VASP/CASP) повинні виявляти, оцінювати й розуміти притаманні їхній діяльності ризики відмивання коштів і фінансування тероризму, а також вживати заходів, пропорційних рівню цих ризиків.

На відміну від формального («чек-лист») підходу, ризик-орієнтована модель дозволяє концентрувати обмежені ресурси комплаєнс-функції там, де ризики є найвищими, і водночас застосовувати спрощені заходи там, де ризик є низьким. Це особливо актуально для ринку віртуальних активів, який характеризується високою швидкістю транзакцій, транскордонним характером операцій, можливістю псевдонімності та використанням широкого спектра технологічних рішень (гаманці, міксери, DEX, крос-чейн мости).

Складові оцінки ризику

- Ризик клієнта (customer risk) — статус клієнта (PEP, бенефіціарний власник, юридична особа зі складною структурою власності), репутація, історія операцій.
- Ризик продукту/послуги (product risk) — анонімність-посилюючі криптовалюти (privacy coins), змішувачі (mixers/tumblers), нехостовані гаманці, деривативи на криптоактиви.
- Географічний ризик (geographic risk) — юрисдикції з високим ризиком за списками FATF, санкційні юрисдикції, країни зі слабким режимом ПВК/ФТ.
- Ризик каналу постачання (delivery channel risk) — дистанційна ідентифікація без особистого контакту, використання посередників, P2P-платформи.

На підставі комплексної оцінки цих складових суб'єкт первинного фінансового моніторингу визначає рівень заходів належної перевірки клієнта: спрощену (Simplified Due Diligence, SDD) для низькоризикових відносин, стандартну (Customer Due Diligence, CDD) для типових випадків та посилену (Enhanced Due Diligence, EDD) для клієнтів або операцій з підвищеним ризиком.

Національна оцінка ризиків та секторальні оцінки

Рекомендації FATF вимагають від держав проведення національної оцінки ризиків (National Risk Assessment, NRA), яка охоплює й сектор віртуальних активів. На підставі NRA регулятори видають секторальні настанови для VASP/CASP щодо типових індикаторів підозрілої активності, притаманних саме операціям з криптоактивами: структурування переказів нижче порогів звітності, швидке переміщення коштів через кілька гаманців («chain hopping»), використання міксерів одразу після отримання коштів, конвертація у privacy coins без очевидної економічної мети.

ОСНОВНІ ВИДИ ШАХРАЙСТВА З ВІРТУАЛЬНИМИ АКТИВАМИ

3.2. Типологія шахрайства у сфері віртуальних активів

Швидке зростання ринку віртуальних активів супроводжується появою специфічних форм шахрайства, які поєднують класичні техніки соціальної інженерії з особливостями криптовалютних розрахунків (незворотність транзакцій, відсутність центрального органу для скасування переказу, складність ідентифікації отримувача).

Кардинг (carding)

Кардинг передбачає неправомірне використання даних платіжних карток (номер картки, строк дії, CVV-код), отриманих внаслідок витоку даних, фішингу або компрометації платіжних систем, для придбання криптоактивів або поповнення рахунків на криптобіржах. Отримані таким чином криптоактиви оперативно виводяться через ланцюжок гаманців або конвертуються в інші активи з метою ускладнення простежування (розрив «paper trail»). Для CASP кардинг є значним операційним ризиком, оскільки після виявлення шахрайства ініціюється чарджбек (chargeback) з боку емітента картки, тоді як криптоактиви вже можуть бути виведені з платформи.

Фішинг (phishing)

Фішинг полягає у створенні фальшивих вебсторінок, електронних листів або повідомлень, що імітують офіційні ресурси криптобірж, гаманців або проєктів, з метою отримання приватних ключів, seed-фраз або облікових даних користувача. Різновидом є spear-phishing — таргетована атака на конкретну особу (наприклад, засновника проєкту або співробітника біржі) з використанням персоналізованої інформації, а також clone-phishing, коли зловмисник копіює легітимний ресурс і змінює лише реквізити отримувача коштів.

Вішинг (vishing)

Вішинг — це голосове шахрайство, при якому зловмисник телефонує жертві, видаючи себе за співробітника служби підтримки криптобіржі, банку або правоохоронного органу, і під приводом «захисту коштів» або «підтвердження операції» переконує жертву самостійно здійснити переказ криптоактивів на контрольовану шахраєм адресу або розкрити конфіденційні дані доступу до гаманця чи біржового акаунта.

Скамінг (scamming)

Скамінг охоплює широкий спектр шахрайських схем, зокрема: інвестиційне шахрайство (обіцянки гарантованого прибутку від «торгових платформ» або «майнінг-пулів»); романтичне шахрайство у поєднанні з інвестиційним («pig butchering» — тривале вибудовування довіри з подальшим переконанням внести кошти у фіктивну торгову платформу); rug pull — виведення ліквідності розробниками токена або DeFi-протоколу одразу після залучення коштів інвесторів; фіктивні ICO/IEO/IDO та airdrop-шахрайство, коли для отримання «безкоштовних» токенів жертву просять підключити гаманець до шкідливого смарт-контракту та надати необмежений дозвіл (approval) на списання коштів.

Спільною рисою наведених типологій є використання незворотності блокчейн-транзакцій та транскордонного характеру операцій для унеможливлення повернення коштів традиційними цивільно-правовими або кримінально-процесуальними засобами, що підвищує значення превентивних заходів на етапі встановлення ділових відносин та моніторингу операцій.

DUE DILIGENCE ПРИ ОПЕРАЦІЯХ З ВІРТУАЛЬНИМИ АКТИВАМИ

3.3. Належна перевірка клієнтів на ринку віртуальних активів

Ідентифікація та верифікація клієнта (CDD)

Стандартна процедура належної перевірки клієнта передбачає встановлення особи клієнта та перевірку його даних за офіційними документами, встановлення бенефіціарного власника для юридичних осіб і трастоподібних утворень, з'ясування мети та характеру майбутніх ділових відносин, а також перевірку клієнта за санкційними списками, переліками PEP та базами негативної інформації. У сфері віртуальних активів ця процедура доповнюється перевіркою походження криптоактивів (source of funds/source of wealth) із залученням інструментів blockchain-аналітики.

Посилена належна перевірка (EDD)

Посилена перевірка застосовується до клієнтів із підвищеним ризиком — PEP, клієнтів із юрисдикцій підвищеного ризику, операцій з нехостованими гаманцями на значні суми, а також у випадку виявлення індикаторів підозрілої активності. EDD передбачає отримання додаткових документів щодо джерела коштів, підтвердження керівництвом рішення про встановлення ділових відносин, а також посилений поточний моніторинг операцій клієнта.

Моніторинг транзакцій та blockchain-аналітика

Постійний моніторинг операцій клієнта є невід'ємною складовою CDD/EDD і передбачає виявлення нетипових патернів: структурування сум, що штучно уникають порогів звітності;

операції з адресами, пов'язаними з даркнет-майданчиками, санкційними суб'єктами або відомими шахрайськими схемами (за даними комерційних блокчейн-аналітичних рішень); різке збільшення обсягу чи частоти операцій без економічного обґрунтування. Виявлені підозрілі операції підлягають внутрішньому розслідуванню та, за наявності підстав, поданню повідомлення до підрозділу фінансової розвідки.

Travel Rule (Рекомендація 16 FATF)

«Правило подорожі» (Travel Rule), закріплене в Рекомендації 16 FATF та імplementоване в законодавстві Європейського Союзу Регламентом (ЄС) 2023/1113, зобов'язує CASP при переказі віртуальних активів супроводжувати транзакцію інформацією про платника та отримувача (ім'я, номер рахунку/адреса гаманця, а для операцій понад встановлений поріг — додаткові ідентифікаційні дані), незалежно від суми переказу в межах ЄС. Це прямо поширює на сектор віртуальних активів принцип, який десятиліттями застосовується до банківських переказів, і є ключовим інструментом простежуваності руху коштів між CASP.

P2P-ПЛАТЕЖІ ТА БІРЖІ: СПЕЦИФІЧНІ РИЗИКИ ТА ЗАХОДИ КОНТРОЛЮ

3.4. Ризики P2P-сегмента та централізованих і децентралізованих бірж

P2P-платформи (peer-to-peer), що дозволяють користувачам напряду обмінювати фіатну валюту на криптоактиви без посередництва традиційного фінансового провайдера, становлять підвищений ризик з погляду ПВК/ФТ, оскільки розрахунки часто відбуваються поза банківською системою (готівка, перекази через платіжні застосунки), а верифікація контрагента залежить від внутрішніх механізмів платформи, які істотно різняться за якістю. Типовими ризиками є використання P2P-угод для «обналичування» коштів злочинного походження («cash-out»), а також залучення «дропів» (мулів) — осіб, які за винагороду надають свої банківські рахунки або гаманці для проведення транзитних операцій.

Централізовані біржі (CEX), що виступають фінансовими посередниками та контролюють активи клієнтів, як правило, підпадають під пряме регулювання як CASP і зобов'язані впроваджувати повний комплекс заходів CDD/EDD, моніторингу та звітності. Натомість децентралізовані біржі (DEX) та протоколи, що функціонують без централізованого оператора, створюють складнощі для застосування традиційних регуляторних інструментів, оскільки відсутній суб'єкт, на якого можна покласти обов'язки з ідентифікації користувачів, — це питання залишається предметом дискусії в межах імplementації MiCA та відповідних настанов ESMA.

Ефективна система контролю на рівні CASP поєднує превентивні заходи (верифікація особи, скринінг гаманців контрагента через blockchain-аналітичні інструменти перед зарахуванням/виведенням коштів, ліміти на операції з нехостованими адресами), поточний моніторинг (виявлення патернів, характерних для «дропів» і транзитних схем) та навчання персоналу розпізнаванню типових ознак соціальної інженерії, описаних вище, з метою своєчасного попередження клієнтів про можливе шахрайство до завершення операції.

Побудова комплаєнс-функції, що поєднує ризик-орієнтований підхід, належну перевірку клієнтів і технологічні інструменти моніторингу, є визначальною умовою як для захисту користувачів віртуальних активів від шахрайства, так і для відповідності CASP регуляторним вимогам ЄС і України у процесі гармонізації національного законодавства зі стандартами MiCA.