Методологічний бюлетень

Серійний номер: МінФін-AML-2026-33

Серпень 2026

“Майбутнє належить тим, хто вірить у красу своїх Мрій!”

Елеонора Рузвельт

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для суб’єктів первинного фінансового моніторингу (СПФМ), регуляторів та правоохоронних органів.

Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

Для регуляторів та правоохоронних органів є інструментом для розробки ефективних стратегій боротьби з ВК, включаючи навчання та координацію дій між різними установами для забезпечення належної співпраці та обміну інформацією.

Звіти міжнародних організацій та окремих юрисдикцій

Стратегічний аналіз ПФР Люксембургу щодо зловживання крипто-активами [1]

У серпні 2026 року Підрозділ фінансової розвідки Люксембургу (CRF) оприлюднив публічну версію стратегічного аналізу «Crypto-Asset Misuse in Financial Crime: Strategic Findings and Typologies». Документ побудований на вибірці повідомлень про підозрілу діяльність і підозрілі операції (SARs/STRs), поданих до CRF упродовж 2025 року, і має задекларовану двоєдину мету: сформувати картину поточного ландшафту підозр щодо ВК/ФТ, пов'язаних із крипто-активами, та підтримати як суб'єктів первинного фінансового моніторингу, так і компетентні органи в оцінці відповідних ризиків саме з перспективи фінансової розвідки. Принципова відмінність цього продукту від переважної більшості національних крипто-звітів полягає в джерелі даних: це не блокчейн-аналітика ринку в цілому і не результати правоохоронних проваджень, а те, що фактично побачив і задокументував приватний сектор та передав до ПФР, – тобто зріз саме детекційної спроможності системи фінансового моніторингу, а не злочинності як такої.

Методологія має вибірковий (sample-based) характер. До вибірки включено виключно повідомлення 2025 року, при цьому поняття «SARs/STRs» охоплює п'ять різних форм подання – SAR, STR, SARe та STRe (повідомлення від онлайн-провайдерів: платіжних установ, установ електронних грошей, банків, що працюють онлайн, та VASP) і TFAR (повідомлення про підозрілу діяльність, пов'язану з фінансуванням тероризму). Для формування вибірки із

[1] https://crf.public.lu/dam-assets/publications/crypto-asset-misuse-in-financial-crime-strategic-findings-and-typologies-public-crf-2026.pdf

«сотень» отриманих повідомлень застосовано комбінацію технік: пошук за ключовими словами, фільтрація за атрибутами, стратифікована вибірка та вибірка, зважена за ризиком. Аналіз має багатовимірний характер і спирається на транзакційні та фінансові дані, характеристики самих крипто-активів, клієнтські та географічні атрибути, поведінкові й темпоральні ознаки, а також елементи, що спричинили подання повідомлення. Відповідно до розподілу суб'єктів звітування, вибірка охоплює CASP/VASP (домінуюча частка), банки та кредитні установи, зокрема онлайн-банки, платіжні установи, установи електронних грошей, інвестиційні фонди та окремі визначені нефінансові установи і професії (ВНУП).

Дві методологічні застороги документа заслуговують на окрему увагу. По-перше, CRF прямо зазначає, що аналіз є ілюстративним і не повинен розумітися як вичерпний або статистично репрезентативний опис усіх отриманих повідомлень, – тобто наведені частки характеризують саме відібрану вибірку. По-друге, і це помітно лише при роботі з самим документом, усі кількісні розподіли подано у вигляді кругових діаграм без числових підписів і без зазначення абсолютного обсягу вибірки. Публічна версія таким чином передає структуру явища, але свідомо утримує масштаб: користувач отримує співвідношення типів крипто-активів і суб'єктів звітування, проте не може ані відтворити розрахунки, ані зіставити ці дані з показниками інших юрисдикцій.

Серед ключових висновків CRF виокремлює п'ять. Криптовалюти (нативні монети) зберігають домінування: понад 60 % випадків стосувалися саме криптовалют, і в 90 % із них ідеться про BTC, ETH або обидва активи. Стейблкоїни посідають друге місце – завдяки відносній ціновій стабільності та поширеності в транскордонних переказах і операціях входу/виходу з крипто-екосистеми, причому їх використання зазвичай залишається поєднаним із нативними криптовалютами. Серед повідомлень, які містили достатню інформацію про походження коштів, значна частина підозрюваних активів пов'язана зі скамом та іншими формами шахрайства. Спостерігається розмаїття продуктів і каналів: поряд із персональними рахунками на централізованих біржах (CEX) фігурують віртуальні IBAN (vIBAN), корпоративні CEX-рахунки, онлайн-банківські рахунки та рахунки електронних грошей і платіжні рахунки. Нарешті, підозріла активність є переважно транскордонною: менш ніж 10 % суб'єктів повідомлень – резиденти Люксембургу, а більшість становлять нерезиденти з держав ЄС, кошти яких лише транзитують через люксембурзькі рахунки та продукти.

Найбільш значущою методологічною складовою документа є архітектура типологій. CRF виокремлює п'ять категорій: відмивання коштів через криптоактиви; шахрайство та зловживання на базі криптоактивів; переміщення незаконних коштів через посередників; опосередкований зв’язок із незаконними адресами; прямі взаємодії з незаконними адресами. Ключове тут те, що вісь класифікації – не предикатний злочин і не тип продукту, а спосіб взаємодії суб'єкта з незаконним джерелом: безпосередній, опосередкований чи через ланцюг посередників. Дві з п'яти категорій побудовані безпосередньо на понятійному апараті блокчейн-аналітики (direct/indirect exposure, кластери адрес, peel chains), що фактично інституціоналізує результат роботи комерційних аналітичних інструментів як самостійний типологічний критерій ПФР. Для української практики це важливий прецедент: він означає, що якість типологізації на рівні ПФР дедалі більше визначається наявністю в підрозділу власної або законтрактованої блокчейн-аналітичної спроможності, без якої дві з п'яти категорій просто не можуть бути ані виявлені, ані верифіковані.

Категорія «відмивання коштів через криптоактиви» поділена на три підкатегорії. Перша – відмивання через крипто-інвестиції – стосується випадків, коли іноземні комерційні компанії, зареєстровані в Європі й задекларовані як такі, що працюють у будівництві, транспорті та оптовій торгівлі, використовували vIBAN для переказу значних сум фіатних коштів (часто в стислий проміжок часу) на власні торгові рахунки в легітимних CEX із подальшою конвертацією переважно в USDT або USDC; vIBAN у цих схемах виконував роль виключно платіжного каналу, а самі компанії пояснювали операції розрахунками за інвойсами чи управлінням казначейством при нез'ясованому джерелі фіатних коштів і невідповідності заявленої мети профілю діяльності. Друга – відмивання через інвестиції в нерухомість:

конвертація крипто-активів у фіат і використання коштів як власного внеску при купівлі об'єкта із залученням кредиту, що виявляється насамперед завдяки належній перевірці з боку банків, CASP/VASP і нотаріусів. Третя – виведення активів із професійної до особистої сфери: перерахування легітимної виручки з рахунку компанії на персональний CEX-рахунок або гаманець фізичної особи з подальшою конвертацією, часто в поєднанні з наданням недостовірної інформації про податкове резидентство, що прив'язує цю підкатегорію до податкових злочинів і привласнення активів компанії.

Категорія шахрайства та зловживань поділена на п'ять підкатегорій і містить найбільш операційно корисні деталі. У схемі «wallet hopping», ініційованої самими потерпілими, жертви переказують суми в діапазоні від 100 євро до кількох сотень тисяч євро в ETH і BTC кількома транзакціями на адреси, звідки кошти далі дробляться та конвертуються у стейблкоїни через DEX, миттєві обмінники (swapping) і некастодіальні гаманці, зрештою потрапляючи до відомих скам-кластерів. У схемах захоплення рахунку (account takeover) через фішинг і вішинг критичною операційною деталлю є попереднє внесення адрес призначення до «білого списку» – саме для зниження ймовірності блокування або додаткової верифікації; фіксується також крос-чейн активність із використанням мостів, зокрема з Ethereum на TRON. Фіктивні або високоризикові платформи виступають каталізатором подальших зловживань, зокрема відновлювального шахрайства (recovery fraud), коли жертві обіцяють повернення коштів в обмін на додатковий переказ «на оплату комісії смартконтракту», та романтичних схем із переходом жертви з мобільних застосунків знайомств на шахрайські інвестиційні сайти. У шахрайстві з фіктивними рахунками та крадіжкою особистих даних CRF окремо наголошує, що згенеровані штучним інтелектом документи та дипфейки суттєво ускладнюють виявлення на етапі верифікації, а робочим інструментом залишається виявлення кластерів рахунків за спільною адресою проживання, повторюваними IP-адресами та ідентифікаторами пристроїв.

Категорія переміщення коштів через посередників містить, ймовірно, найцінніший для транзакційного моніторингу матеріал. CRF фіксує, що майже половина випадків опосередкованого переміщення незаконних крипто-активів передбачала використання «грошових мулів». Транзитні (pass-through) CEX-рахунки характеризуються повторюваністю патернів FICO (fiat-in crypto-out), CIFO (crypto-in fiat-out) і кругових потоків, особливо в поєднанні з нещодавно створеними чи короткоживучими гаманцями та значними сумами, що проводяться спорадично в стислі проміжки часу. Окремо описано патерн FIFO (fiat-in fiat-out), коли зловмисник вносить невеликі суми фіату з банківського рахунку на CEX-рахунок і, взагалі не конвертуючи їх у крипто-активи, повертає на той самий або підконтрольний рахунок, після чого жодних логінів чи іншої активності не спостерігається, – CEX-рахунок використовується виключно як провідник, а не для торгівлі чи інвестування. У випадках, пов'язаних із наркоторгівлею, типовою є картина великих вхідних крипто-переказів або фіатних депозитів із нез'ясованих

Висновки:

- **Детекція концентрується там, де є регульований посередник:** понад 60 % випадків стосувалися криптовалют, у 90 % із них – BTC та/або ETH, а джерелом повідомлень домінували CASP/VASP. Типології поза ліцензованим периметром – DEX, обмінники без KYC – системно недооцінені.
- **vIBAN виокремлено як самостійний канал входу фіату:** компанії з будівництва, транспорту й оптової торгівлі переказували через них значні суми на власні CEX-рахунки з конвертацією в USDT/USDC під поясненням «розрахунки за інвойсами». Такі платежі варто профілювати окремо.
- **Патерни FICO, CIFO і особливо FIFO придатні до прямого перенесення в правила моніторингу:** FIFO – фіат заведено на CEX-рахунок і повернуто без жодної конвертації, після чого клієнт більше не логіниться – є самодостатнім індикатором рахунку-провідника.
- **Майже половина випадків опосередкованого переміщення включала «грошових мулів»,** а попереднє внесення адрес до «білого списку» СПФМ виявляють без блокчейн-аналітики. Натомість експозиція до підсанкційних, CSAM- і ФТ-адрес без такого інструментарію недоступна.

джерел із майже негайним виведенням на непозначені зовнішні гаманці, іноді із залученням іноземних компаній-оболонок або роздрібного бізнесу як прикриття.

Дві останні категорії розмежовують опосередковану та пряму експозицію. Опосередкована експозиція охоплює підсанкційних осіб (суми переважно низькі, багатохопові шляхи, у більшості випадків ідеться про санкційні переліки іноземних держав), адреси, пов'язані з матеріалами сексуального насильства над дітьми (шляхи навпаки короткі, окремі адреси призначення розташовані лише за один «хоп» від CEX-рахунку), кластери програм-вимагачів і викрадених коштів (довгі peel chains у поєднанні зі швидкою конвертацією у фіат і виведенням на банківський рахунок), даркнет-маркети (де багаторазове сходження високоризикових шляхів на рахунку одного суб'єкта, за оцінкою CRF, ймовірно свідчить про умисність) та адреси, пов'язані з фінансуванням тероризму, – обмежена кількість повідомлень, невеликі суми, кластери, кореневі адреси яких атрибутовано іноземним терористичним угрупованням, афілійованим із більшими міжнародними організаціями. Прямі взаємодії трапляються значно рідше, оперують малими сумами (переважно нижче 1 000 євро, а в разі оплати CSAM-контенту – у середньому менше 100 євро за операцію) і здійснюються переважно в BTC, проте, як прямо зазначає CRF, істотно підвищують правдоподібність умисної участі та відповідно посилюють обґрунтованість підозри.

У висновку CRF констатує, що ландшафт ризиків ВК/ФТ, пов'язаних із криптоактивами, розширюється одразу за трьома векторами – технічним, операційним і структурним, – тоді як профіль залучених осіб залишається переважно міжнародним. Попри домінування рахунків на централізованих біржах у вибірці 2025 року, підозріла активність дедалі частіше вказує на складнішу інфраструктуру: сервіси обміну без KYC, миттєві обмінники, децентралізовані платформи, а також інтеграцію крос-чейн мостів і мереж другого рівня (L2) у схеми відмивання. Для української системи фінансового моніторингу документ має принаймні три площини застосування: він пропонує готову типологічну сітку, сумісну з наявною методологією Держфінмоніторингу; він прямо вказує на vIBAN як недооцінений канал входу фіатних коштів у крипто-екосистему, що є актуальним у контексті запуску повноцінного регулювання ринку віртуальних активів в Україні; і він демонструє, що без блокчейн-аналітичної спроможності на рівні ПФР дві з п'яти типологічних категорій залишаються поза межами аналітичного поля.

Відмивання коштів у секторі нерухомості: ризики, економічні наслідки та нові підходи AMLA [2]

Документ AMLA присвячений комплексному аналізу вразливості сектору нерухомості до відмивання коштів, основних механізмів використання нерухомості для легалізації незаконних доходів, економічних наслідків проникнення злочинного капіталу на ринок житла, а також напрямів удосконалення системи ПВК у цій сфері. Документ має аналітичний, а не нормативний характер: AMLA наголошує, що документ узагальнює вибрану академічну літературу та політичні звіти, має сприяти професійній дискусії та не є офіційною політичною позицією AMLA чи її керівних органів. Водночас зміст документа відображає актуальний підхід до розуміння ризиків сектору нерухомості в контексті нового європейського AML-пакета та майбутньої ролі AMLA у формуванні більш узгодженого нагляду за нефінансовим сектором.

Основною тезою документа є те, що сектор нерухомості залишається особливо вразливим до відмивання коштів через поєднання декількох структурних характеристик. Йдеться передусім про значний розмір ринку, відносну стабільність вартості активів, здатність нерухомості поглинати великі обсяги капіталу, можливість отримання економічної віддачі, складність

[2] https://www.amla.europa.eu/document/download/8a29e0a5-0209-4aa1-a1be-3296d0df255c_en?filename=Thematic%20Note%20-%20Money%20Laundering%20in%20the%20Real%20Estate%20Sector.pdf

об’єктивного визначення ринкової вартості окремих об’єктів, використання складних юридичних та фінансових конструкцій, а також можливість приховувати фактичного бенефіціарного власника. Нерухомість приваблива для осіб, які відмивають кошти, ще й тому, що може використовуватися не лише як засіб збереження незаконно отриманого багатства, але й на різних етапах процесу відмивання. Злочинні доходи можуть бути вкладені в об’єкт нерухомості, після чого їх походження та фактичний власник можуть приховуватися за допомогою наступних операцій, а в результаті продажу об’єкта, отримання орендного доходу або приросту його вартості незаконні кошти можуть набувати зовнішніх ознак законного доходу. Таким чином, нерухомість здатна одночасно виконувати функції накопичення вартості, нашарування операцій та інтеграції коштів у легальну економіку.

Особливо важливою вразливістю AMLA вважає можливість розриву між юридичною та фактичною власністю на нерухоме майно. Особа або юридична структура, формально зазначена як власник об’єкта в реєстрі, не обов’язково є фізичною особою, яка в кінцевому підсумку володіє, контролює чи отримує вигоду від цього активу. Для приховування кінцевого бенефіціарного власника можуть використовуватися компанії, трасти, номінальні власники, багаторівневі корпоративні структури та інші юридичні механізми. Ризики посилюються у випадках фінансування третіми особами та транскордонних операцій, особливо коли ланцюг власності або фінансування проходить через декілька юрисдикцій із різними стандартами прозорості та різною якістю реєстрів бенефіціарної власності. Складність підтримання актуальної та достовірної інформації про фактичних власників нерухомості у різних країнах створює додаткові можливості для приховування зв’язку між активом та особою, яка фактично його контролює.

Окремим джерелом ризику є специфіка оцінки вартості нерухомості. На відміну від багатьох стандартизованих фінансових активів, кожен об’єкт нерухомості має індивідуальні характеристики, а визначення його точної ринкової вартості може бути складним і дорогим. Це створює простір для маніпулювання ціною та використання завищеної або заниженої вартості як складової схем відмивання коштів. Крім того, для реалізації таких схем можуть застосовуватися як разові операції з купівлі нерухомості, так і довгострокові фінансові конструкції з періодичними платежами. Тому оцінка ризику не повинна обмежуватися лише моментом придбання об’єкта: важливо враховувати повну структуру фінансування, подальші платежі та зміни, які відбуваються протягом життєвого циклу угоди.

AMLA значну увагу приділяє ролі професійних посередників, через яких у багатьох країнах здійснюються операції з нерухомістю. Агенти з нерухомості, нотаріуси, юристи та інші професійні учасники фактично виконують функцію «гейткіперів», оскільки мають доступ до інформації про учасників угоди, структуру власності, джерело фінансування, ціну та інші обставини операції. Агенти з нерухомості, наприклад, можуть виявляти невідповідність між профілем покупця та вартістю придбаного активу, незрозуміле джерело коштів, використання номінальних осіб, нетипову структуру угоди або аномальне ціноутворення. Водночас AMLA звертає увагу на потенційний конфлікт між функцією ПВК та комерційними інтересами посередника: агент зацікавлений у завершенні продажу й отриманні винагороди, тому за низького рівня AML-культури, слабкого нагляду або недостатнього правозастосування контрольні механізми можуть працювати неефективно. Одним із проявів цієї проблеми є відносно низький рівень повідомлення про підозрілі операції з боку окремих категорій професійних учасників ринку нерухомості.

Проблема ускладнюється значною неоднорідністю моделей оформлення угод з нерухомістю в різних країнах. У багатьох державах існують спеціальні адміністративні процедури, які передбачають перевірку особи, структури власності та, в окремих випадках, контроль або довірче зберігання коштів. Такі функції можуть виконувати нотаріуси або інші особи юридичних професій, наділені відповідними публічними повноваженнями, тоді як в інших юрисдикціях ключова роль належить брокерам, органам реєстрації чи приватним юристам. Відмінності між цими системами означають, що інтенсивність перевірок і рівень захисту від зловживань можуть істотно відрізнятися – від дуже жорстко контрольованих процедур до

моделей, близьких до прямих угод між сторонами. Відповідно різняться й рівень усвідомлення ризиків, ефективність каналів повідомлення про підозрілі операції та доступність ресурсів для виконання вимог ПВК. AMLA підкреслює, що особи, які відмивають кошти, можуть цілеспрямовано використовувати цю фрагментованість, а в найбільш негативних випадках – вступати у змову з окремими професійними учасниками. Саме тому ефективність системи ПВК залежить не лише від формальних норм, але й від того, наскільки сама архітектура ринку дозволяє такі норми ефективно застосовувати.

У документі також аналізується питання, які саме ринки та сегменти нерухомості є найбільш привабливими для осіб, які прагнуть приховати незаконно отримані активи. AMLA зазначає, що особливо привабливими можуть бути стабільні ринки з ефективним захистом права власності, належним рівнем верховенства права, розвиненою фінансовою системою та стабільним внутрішнім попитом на житло. Великі міжнародні міста також створюють більш сприятливе середовище для маскування підозрілих операцій завдяки великій кількості угод, міжнародному складу покупців і більшій можливості зберігати анонімність. Окрему увагу приділено високовартісній нерухомості. Такі об'єкти дозволяють переміщувати значні обсяги капіталу за допомогою відносно невеликої кількості операцій, їхня реальна ринкова вартість може бути більш суб'єктивною, а сам актив водночас може мати особисту споживчу цінність для власника. У наведеному AMLA дослідженні Великої Британії зазначено, що 94 % іноземних компаній, які володіють британською нерухомістю, були зареєстровані в податкових гаванях. При цьому документ обережно розмежовує різні мотиви використання таких структур і не ототожнює офшорне володіння автоматично з відмиванням коштів.

Щодо конкретних способів відмивання коштів через нерухомість AMLA зазначає, що традиційна схема придбання об'єкта безпосередньо за готівкові або інші ліквідні кошти злочинного походження з подальшим продажем чи здаванням в оренду є лише одним із можливих механізмів і сьогодні застосовується рідше через обмеження або заборони великих готівкових розрахунків. На практиці значно складніші моделі можуть передбачати використання звичайних іпотечних кредитів. Незаконні доходи можуть спрямовуватися на перший внесок, тоді як регулярне погашення іпотеки може використовуватися для поступового введення майбутніх злочинних прибутків у легальну фінансову систему. Завищення або заниження вартості нерухомості може додатково сприяти прихованим платежам або створювати можливості для спрямування коштів у погашення кредиту. У транскордонних схемах може застосовуватися формальна «позика» іноземного банку, фактичним джерелом якої є кошти самого майбутнього покупця.

До інших моделей належать операції з перепродажу нерухомості після проведення ремонтних робіт, частина яких могла оплачуватися готівкою; використання рахунків агентів з нерухомості для проведення коштів; отримання повернення коштів після формальної відмови від угоди на підставі відповідного положення договору; а також використання номінальних фізичних осіб або компаній як формальних власників майна. AMLA наголошує, що такі механізми часто не існують ізольовано, а комбінуються між собою. У результаті одна структура може одночасно приховувати джерело фінансування, фактичного покупця, бенефіціарного власника та економічну мету операції.

Особливо важливим аспектом документа є аналіз впливу відмивання коштів на функціонування самого ринку нерухомості. AMLA розглядає незаконний капітал як додатковий потік коштів у сектор, який здатний впливати одночасно на попит і пропозицію. Придбання нерухомості з метою відмивання коштів збільшує сукупний попит, що за інших рівних умов створює висхідний тиск на ціни. Якщо придбана нерухомість залишається порожньою або використовується не повністю, це одночасно зменшує ефективну пропозицію житла, ще більше посилюючи потенційне зростання цін. Таким чином, наслідки відмивання коштів можуть виходити далеко за межі безпосередньої шкоди, пов'язаної зі злочинністю, і трансформуватися у викривлення ринку житла.

Ще один важливий економічний механізм пов'язаний із мотивацією осіб, які відмивають кошти. Легальний інвестор зазвичай оцінює актив за його прибутковістю, ризиком, перспективами перепродажу та іншими економічними параметрами. Для особи, яка відмиває злочинні доходи, головною перевагою активу може бути здатність приховати походження коштів або фактичного власника. Це означає, що злочинний капітал може спрямовуватися до об'єктів, які з погляду звичайної інвестиційної логіки є менш привабливими. Такий покупець також може бути готовим сплачувати ціну вище ринкової, якщо це полегшує реалізацію схеми. Унаслідок цього відбувається неправильний розподіл капіталу, а ціни можуть відхилятися від рівня, сформованого виключно на основі легального попиту та економічної доцільності.

Водночас AMLA наголошує, що вплив злочинності на ціни нерухомості не є однозначно висхідним. Якщо незаконні доходи генеруються внаслідок насильницької злочинної діяльності, погіршення безпеки та загальної привабливості району може спричинити зниження вартості нерухомості. Відповідно кінцевий вплив залежить від характеру злочинності та від того, наскільки географічно збігаються місце отримання незаконних доходів і територія, в якій ці кошти інвестуються в нерухомість. Окремо згадуються випадки, коли нерухомість купується або орендується безпосередньо для здійснення злочинної діяльності. Такі операції можуть бути пов'язані з відмиванням коштів, хоча об'єкт у цьому разі одночасно виконує операційну функцію в межах злочинної діяльності.

Сила впливу незаконного попиту на ціни також залежить від здатності ринку швидко збільшувати пропозицію житла у відповідь на зростання попиту. AMLA зазначає, що можливості швидкого збільшення пропозиції нерухомості є обмеженими, оскільки будівництво нових об'єктів потребує часу, а географічні та регуляторні чинники можуть додатково стримувати розширення житлового фонду. У ринках із жорстко обмеженою пропозицією приріст попиту більшою мірою трансформується у зростання цін, а не у збільшення обсягів будівництва. Водночас особи, які відмивають кошти, ймовірно, концентруються не на «середньостатистичній» нерухомості, а передусім на дорогих об'єктах у великих міжнародних містах. Тому важливим, але досі не повністю дослідженим питанням залишається те, наскільки підвищення цін у преміальному сегменті поширюється на ширший ринок житла.

Емпірична частина документа демонструє, що теоретичні механізми впливу відмивання коштів на нерухомість є достатньо зрозумілими, однак точне вимірювання їх масштабу залишається складним. Насамперед немає загальновизнаної достовірної оцінки самого обсягу відмивання коштів: наведені AMLA сучасні дослідження оцінюють його приблизно в межах від 1 до 6 % ВВП залежно від країни. Якщо складно достовірно виміряти загальний обсяг відмивання коштів, то ще складніше визначити, яка його частка спрямовується саме в нерухомість і який конкретний вплив цей капітал має на ціни та доступність житла. Тому AMLA послідовно застерігає від надмірного узагальнення окремих кількісних оцінок.

Важливу частину доказової бази становлять дослідження офшорного володіння нерухомістю. Хоча використання офшорних структур може мати законні причини і не є саме по собі доказом відмивання коштів, воно демонструє економічний вплив непрозорого або важко ідентифікованого зовнішнього капіталу на локальні ринки. За даними одного з досліджень, наведених AMLA, у Великій Британії близько 1,5 % усієї житлової нерухомості та 15 % об'єктів верхнього цінового сегмента належали власникам або структурам, зареєстрованим в офшорних податкових юрисдикціях. Після референдуму щодо Brexit, який спричинив несподіване зниження офшорного попиту на британську нерухомість, найбільш залежні від такого капіталу райони Лондона зазнали відносного зниження цін до 8,2 % порівняно з прогнозованим рівнем. Автори відповідного дослідження також оцінили, що зниження попиту з боку офшорних корпорацій на 1 % пов'язувалося зі зменшенням локальних цін приблизно на 1,3 %. Інші дослідження іноземного попиту на лондонське житло також виявляли його вплив на локальні ціни та рівень вакантності об'єктів.

AMLA звертає увагу і на можливий ефект переміщення прихованого капіталу між різними видами активів. У міру того як міжнародні ініціативи з підвищення фінансової прозорості, зокрема автоматичний обмін інформацією, ускладнюють приховування багатства у традиційних офшорних фінансових активах, частина власників може переміщувати капітал у нерухомість. Через відносну непрозорість структури власності та значні можливості для використання юридичних конструкцій глобальний ринок нерухомості може ставати альтернативним каналом приховування активів. Як приклади цієї тенденції у записці наведено нові дослідження щодо Великої Британії та Дубая.

Безпосередньо щодо відмивання коштів AMLA аналізує декілька емпіричних досліджень із різними методологіями. Дослідження італійського ринку показало, що доходи від так званих «підприємницьких» злочинів, зокрема торгівлі наркотиками, збуту викрадених товарів і проституції, позитивно пов'язані з цінами на житло. Автори інтерпретують це як результат інвестування злочинних прибутків у житлову нерухомість з метою відмивання. Водночас доходи від насильницьких злочинів, таких як вимагання, мали протилежний вплив на ціни через негативний вплив злочинності на привабливість території. Позитивний ефект був сильнішим у регіонах із більшими нелегальними ринками, що додатково підтверджує можливість саме механізму відмивання коштів.

Інше дослідження стосувалося Британської Колумбії в Канаді. На основі низки модельних припущень автори дійшли оцінки, що приблизно 5 % усіх операцій з нерухомістю можуть здійснюватися з метою відмивання коштів, а відповідний додатковий попит здатний підвищувати ціни на житло приблизно на 3,7–7,5%. Проте AMLA спеціально підкреслює значну невизначеність цієї оцінки, оскільки вона сформована на основі декількох послідовних припущень щодо загального масштабу відмивання коштів, частки незаконного капіталу, яка інвестується, розподілу такого капіталу між видами активів та реакції цін на додатковий попит. Через це результат не може автоматично екстраполюватися на інші країни або ринки нерухомості.

Ще один підхід використовує повідомлення про підозрілі операції як непрямий індикатор інтенсивності потенційного відмивання коштів. На основі даних німецького ПФР щодо повідомлень, поданих агентами з нерухомості та нотаріусами, дослідники встановили позитивний зв'язок між кількістю й обсягом таких повідомлень та динамікою локальних цін на нерухомість. Зокрема, збільшення фінансового обсягу повідомлень про підозрілі операції на один мільйон євро статистично асоціювалося зі зростанням локального індексу цін на житло на 0,063%. Окреме дослідження країн ОЕСР виявило, що держави з жорсткішими ПВК-заходами демонстрували повільніше зростання цін на житло, що його автори трактували як непрямий доказ здатності ефективнішого ПВК-регулювання стримувати використання сектору нерухомості для відмивання коштів. Загальна позиція AMLA є обережною: наявні емпіричні дослідження вказують на зв'язок між показниками відмивання коштів та цінами на нерухомість, але наукова література поки не дозволяє визначити універсальний і надійно підтверджений масштаб такого впливу для різних країн.

На цій основі AMLA робить ширший висновок про те, що відмивання коштів у секторі нерухомості необхідно розглядати не лише як кримінальну або суто комплаєнс-проблему. Воно має потенційні макроекономічні та соціальні наслідки. Відмивання коштів підтримує організовану злочинність, але водночас може викривляти ринкові механізми, збільшувати вартість житла та погіршувати його доступність. Оскільки житло є базовою потребою, такі наслідки мають безпосереднє соціальне значення. Крім того, дисбаланси на ринку житла можуть зменшувати мобільність населення, ускладнювати переміщення працівників між регіонами та секторами економіки й тим самим негативно впливати на ефективність економіки загалом.

Важливу роль у відповіді на ці ризики AMLA відводить новому європейському AML-пакету. До його прийняття сектор нерухомості вже перебував у сфері AML-регулювання, а агенти з нерухомості, а за певних умов нотаріуси та інші представники незалежних юридичних

професій були охоплені відповідними обов'язками через національну імплементацію директив ЄС. Проте директивна модель залишала значний простір для відмінностей у практиці застосування вимог і нагляду між державами-членами. Новий підхід передбачає більшу гармонізацію. Регламент (ЄС) 2024/1624 переносить основні обов'язки у сфері ПВК/ФТ приватного сектору до безпосередньо застосовуваного єдиного зводу правил, тоді як Директива (ЄС) 2024/1640 спрямована на зміцнення інституційної організації національних систем та покращення доступу компетентних органів до необхідної інформації. Для сектору нерухомості це особливо важливо, оскільки його основні ризики мають структурний і транскордонний характер та пов'язані з непрозорою власністю, складними юридичними конструкціями, різним рівнем комплаєнсу серед професійних посередників і неоднорідністю наглядових практик.

AMLA очікує, що її майбутні політичні та наглядові ініціативи сприятимуть формуванню гармонізованої методології оцінки ризиків для нефінансового сектору, посиленню та зближенню наглядових практик, застосуванню ефективніших інструментів нагляду, включаючи взаємні огляди, наглядові колегії та процедури реагування на порушення, а також розвитку спільного європейського підходу до підзвітних суб'єктів, спільного аналізу та обміну даними. Ключова ідея полягає в тому, щоб пов'язати внутрішні системи контролю, оцінювання ризиків і постійний моніторинг в єдину логічну систему. Для нерухомості це означає відхід від підходу, за якого основна увага приділяється лише первинній перевірці клієнта, та перехід до аналізу всієї структури угоди: хто бере в ній участь, хто фактично отримує вигоду, звідки надходять кошти, як змінюється фінансування та чи зберігається достовірна комерційна логіка операції протягом усього процесу.

Особливого значення набуває поєднання моніторингу транзакцій із моніторингом діяльності. AMLA наголошує, що підозрілі ознаки у сфері нерухомості можуть проявлятися не тільки безпосередньо в русі коштів. Вони можуть виникати через зміну власника, структури фінансування, залучених посередників, строків або терміновості угоди, ціни, способу організації операції чи інших обставин. Отже, система контролю повинна виявляти не лише нетиповий платіж, але й аномалії у поведінці сторін та структурі самої операції. Такий підхід краще відповідає реальній природі ризиків у секторі нерухомості, де незаконне походження коштів може маскуватися за зовні звичайною фінансовою операцією, тоді як ключові індикатори ризику проявляються в юридичній чи комерційній конструкції угоди.

Висновки:

- **Потрібно перейти від разової перевірки клієнта до постійного моніторингу самої угоди:** аналізувати не лише платежі, а й зміни власника, джерела фінансування, посередників, ціну, строки та економічну логіку операції.
- **Є необхідність у посиленні ризик-орієнтованого нагляду за агентами з нерухомості, нотаріусами, юристами та іншими «гейткіперами»,** оскільки саме фрагментованість контролю й нерівномірна якість виконання AML-обов'язків створюють системні вразливості.
- **Необхідно забезпечити достовірність і практичну придатність даних про бенефіціарну власність,** особливо щодо корпоративних, трастових, номінальних і транскордонних структур, та поєднати ці дані з іншою інформацією про операцію.
- **Необхідно розглядати відмивання коштів у нерухомості як ризик не лише фінансової злочинності, а й економічної та соціальної стабільності,** оскільки незаконний капітал може підвищувати ціни, скорочувати доступність житла та викривляти розподіл інвестицій.

Документ також проводить прямий зв'язок між вразливостями сектору до відмивання коштів та ризиками невиконання або обходу цільових фінансових санкцій. Для обох типів незаконної діяльності можуть використовуватися схожі інструменти – непрозорі структури власності, посередники, номінальні особи та обмежена видимість фактичного бенефіціара активу. Саме тому AMLA розглядає прозорість бенефіціарної власності, моніторинг транзакцій і діяльності та ефективний обмін даними як

елементи, що одночасно підвищують спроможність системи протидіяти відмиванню коштів і санкційному обходу.

У підсумку тематична записка формує бачення, за яким ефективна протидія відмиванню коштів у секторі нерухомості потребує значно ширшого підходу, ніж формальне застосування стандартної належної перевірки клієнта. Необхідне поєднання ризик-орієнтованого нагляду за агентами з нерухомості, нотаріусами та іншими професійними «гейткіперами», методологій ідентифікації високоризикових суб'єктів, бізнес-моделей і операцій, постійного моніторингу взаємопов'язаних транзакцій та активності, підвищення підзвітності й публічного контролю за саморегулівними організаціями, розвитку транскордонного обміну інформацією, гармонізації AML-підходів і суттєвого покращення точності, актуальності та практичної придатності реєстрів бенефіціарної власності. Центральний висновок документа полягає в тому, що структурні характеристики ринку нерухомості – його масштаб, непрозорість, складність оцінки активів, можливість використання юридичних і транскордонних конструкцій та множинність професійних посередників – роблять цей сектор стійко привабливим для незаконного капіталу. Тому навіть із посиленням європейської AML-архітектури такі фундаментальні вразливості не зникнуть і вимагатимуть постійної уваги, якісного ризик-аналізу, ефективного нагляду та системного обміну даними.

Еволюція кримінальних мереж Європи у 2026 році [3]

Опублікований Європолом другий випуск звіту є глибоким аналітичним дослідженням, що розкриває саму природу сучасної організованої злочинності. Якщо перший звіт 2024 року встановив "код" цих мереж, визначивши їх як спритні, безкордонні, контрольовані та руйнівні (ABCD), то нове дослідження демонструє, як цей код реалізується на практиці в умовах безпрецедентного тиску правоохоронних органів.

Головний висновок є водночас і підбадьорливим, і тривожним: правоохоронна діяльність досягає значних успіхів у протидії конкретним групам, проте сама екосистема організованої злочинності демонструє вражаючу живучість і здатність до регенерації, діючи за своєрідною "блакитною картою кримінального опортунізму".

Перше, що впадає в око, – це динаміка самого переліку найбільш загрозливих мереж. З 821 мережі, ідентифікованої у 2024 році, 76% (тобто три чверті) більше не входять до актуального списку на 2026 рік. Цей факт є яскравим свідченням ефективності спільних дій правоохоронних органів країн-членів та міжнародних партнерів, які за підтримки Європолу провели близько 7000 операцій та створили близько 80 оперативних цільових груп. Масштабні міжнародні розслідування, сфокусовані на високоцінних цілях, паралельні фінансові розслідування та скоординовані обшуки в логістичних хабах дозволили заарештувати понад 1000 осіб, у тому числі понад 100 ключових лідерів.

Водночас, звіт застерігає від ейфорії: зникнення мережі з переліку не завжди означає її повну ліквідацію. Нерідко це є наслідком реструктуризації, тимчасової бездіяльності через арешти лідерів або навіть зміни в методиці оцінки загроз з боку окремих країн, що підкреслює необхідність постійного моніторингу.

Незважаючи на значні успіхи, сутність загрози залишається незмінною, а в деяких аспектах навіть посилюється. Ядро кримінальної загрози утворюють 198 мереж, які, проявивши феноменальну стійкість, зберегли свій впливовий статус. Це переважно ієрархічні, мафіозні структури з багаторічною історією, глобальним охопленням та полі-кримінальним профілем. Вони не просто виживають, а процвітають, активно використовуючи легальний бізнес для відмивання коштів, корупцію для полегшення операцій та складні контрзаходи для протидії

[3] https://www.europol.europa.eu/cms/sites/default/files/documents/Blueprint-of-criminal-opportunism.pdf

розслідуванням. Їхня здатність замінювати арештованих членів і навіть зберігати контроль з-за грат робить їх надзвичайно живучими.

Однак найбільш показовим є поява 533 нових або раніше не ідентифікованих мереж. Цей сплеск нових гравців не є випадковістю, а закономірним наслідком функціонування злочинної екосистеми: звільнені ніші швидко заповнюються, а нові можливості, особливо в цифровому середовищі, негайно експлуатуються. Це підтверджує, що боротьба з окремими мережами без впливу на системні умови, які дозволяють їм існувати, є стратегічно недостатньою.

Профіль сучасних найбільш загрозливих мереж залишається напрочуд стабільним, що вказує на існування усталених моделей злочинної діяльності. Більшість з них (63%) мають мультинаціональний склад, представляючи 118 національностей, що підкреслює їхню транскордонну природу. Примітно, що майже дві третини (64%) мереж мають чітку ієрархічну структуру, що суперечить уявленням про переважно мережеві, горизонтальні утворення. Однак навіть у цих ієрархіях відбувається розмивання кордонів: багато функцій, від логістики до фінансів, передаються на аутсорсинг спеціалізованим сервісним провайдерам або виконуються напівавтономними осередками.

Основним двигуном злочинної діяльності залишається прибуток, і наркотрафік, як і раніше, домінує, охоплюючи понад третину всіх мереж. Однак звіт фіксує важливі зрушення: стрімке зростання шахрайства (16% мереж), яке стає другою за поширеністю сферою, та значне збільшення частки чисто кібер-загроз. Це демонструє, що організована злочинність дедалі активніше переходить у цифрову площину, використовуючи її для комунікації, вербування, маркетингу незаконних послуг та, власне, скоєння злочинів.

Особливу тривогу викликає поява такого явища, як "The Com" – мережі, що об'єднує тисячі молодих людей по всьому світу в екосистему, де переплітаються сексуальна експлуатація дітей, кібератаки, насильство та навіть тероризм, що демонструє абсолютно новий рівень загрози, яка стирає межі між різними видами злочинності та екстремізму.

Найглибше аналітичне осягнення у звіті стосується розуміння злочинності не як сукупності ізольованих груп, а як "плинної кримінальної екосистеми". Це фундаментальний зсув у парадигмі, який пояснює, чому традиційні визначення організованої злочинності часто не працюють. У цій екосистемі мережі не конкурують виключно одна з одною, а й співпрацюють, створюючи тимчасові альянси, обмінюючись послугами та ресурсами. Така "конкуренція" дозволяє їм бути надзвичайно гнучкими.

Ключовим елементом цієї екосистеми є зростаюча індустрія "злочинність як послуга" (Crime-as-a-Service). З'являються високоспеціалізовані мережі, які пропонують свої послуги іншим. Це можуть бути професійні провайдери відмивання грошей, які використовують складні крипто-схеми та підпільні банківські системи; логістичні провайдери, що постачають обладнання для контрабанди (наприклад, надувні човни для Ла-Маншу), або ж "насильство як послуга", де для вбивств і залякувань вербують неповнолітніх через соціальні мережі. Ця модель не лише підвищує ефективність і стійкість всієї екосистеми, але й створює критичні вразливі місця: знешкодження одного ключового сервіс-провайдера може завдати удару одразу по багатьох злочинних мережах, що є стратегічним пріоритетом для правоохоронних органів.

Розуміння цієї екосистеми нерозривно пов'язане з концепцією "блакитної карти кримінального опортунізму". Це наступний рівень аналізу, який пояснює, чому екосистема взагалі виникає та процвітає. Її рушійною силою є систематичний пошук і експлуатація вразливостей у різних системах – цифровій, фінансовій, технологічній, геополітичній. Кримінальні мережі використовують складність сучасного світу. Вони активно застосовують AI для масштабування шахрайських кампаній, ховаються за шифрованими месенджерами (як-от MATRIX), використовують криптовалюти та техніки для обходу фінансового моніторингу. Вони розмивають межу між легальною та нелегальною економікою, широко використовуючи легальні бізнес-структури (85% мереж) в якості прикриття для своїх операцій, особливо в

таких секторах, як логістика, нерухомість та готівковий бізнес. Крім того, вони активно вербують професіоналів – адвокатів, бухгалтерів, ріелторів – які, свідомо чи ні, стають співучасниками, надаючи доступ до знань та інфраструктури. Навіть геополітичні кризи, такі як війна в Україні, створюють нові можливості – для переміщення кримінальних елементів, появи нових маршрутів контрабанди або створення "тіньових" альянсів з гібридними акторами, які використовують злочинний світ як проксі для дестабілізації.

Усвідомлення цих двох ключових висновків – плинної екосистеми та опортуністичної блакитної карти – призводить до неминучого висновку, який є лейтмотивом звіту: традиційний підхід, зосереджений виключно на "полюванні за головами" та розслідуванні окремих справ, є недостатнім. Він дає тактичні перемоги, але програє стратегічну війну, оскільки злочинний ландшафт, подібно до гідри, відрощує нові голови.

Європол закликає до системного підходу, який передбачає не лише нейтралізацію акторів, але й цілеспрямовану роботу з усунення системних вразливостей, які ці актори експлуатують. Це означає перехід до багатошарової стратегії, що включає: адміністративні заходи для боротьби з використанням легальних бізнесів; превентивні кампанії для захисту потенційних жертв та відвернення молоді від злочинного життя; інвестиції в технології та забезпечення законного доступу до даних для правоохоронних органів; посилення фінансових розслідувань та конфіскації активів; та, найважливіше, поглиблення співпраці не лише між країнами, але й між державним та приватним секторами, зокрема з технологічними компаніями та фінансовими установами.

Висновки:

- **Тактичні перемоги не гарантують стратегічного успіху.** 76% мереж зі списку 2024 року було нейтралізовано або виведено з переліку загроз, проте їхнє місце зайняли 533 нових угруповання. Злочинний ландшафт не зникає, а трансформується.
- **Ядро загрози залишається стабільним і надзвичайно стійким.** 198 ієрархічних, кримінальних мереж з глобальним охопленням, які активно використовують корупцію, легальний бізнес та передові технології, продовжують домінувати, незважаючи на тиск правоохоронців.
- **Злочинність перетворилася на "плинну екосистему" з власною інфраструктурою.** Ключовим драйвером стала модель "злочинність як послуга", де спеціалізовані провайдери (відмивачі грошей, логісти, кіллери) обслуговують одразу багато мереж, що робить систему надзвичайно живучою.
- **Боротьба з наслідками без усунення причин є неефективною.** Мережі процвітають завдяки системному опортунізму – експлуатації вразливостей у цифровій, фінансовій, правовій та геополітичній сферах. Необхідний перехід до системно-орієнтованого підходу, який передбачає "проєктування безпеки" в усі сфери.

Такий підхід, заснований на принципі "безпеки за задумом" (by design), вимагає випереджального мислення, коли законодавство, політика та технології створюються з урахуванням потенційного кримінального використання. Лише поєднуючи таку тактику з системно-орієнтованою стратегією, Європа зможе не просто наздоганяти злочинність, а випереджати її, роблячи суспільство більш стійким до загроз, які постійно еволюціонують.

Штучний інтелект як інструмент розвитку: можливостей та виклики [4]

У той час, коли темпи глобального розвитку досягли 75-річного мінімуму, штучний інтелект (ШІ) постає як безпрецедентна можливість для економік, що розвиваються. На відміну від попередніх хвиль технологічних революцій, ШІ поширюється з неймовірною швидкістю. Якщо паровому двигуну знадобилося близько 80 років, щоб досягти країн із низьким рівнем доходу, електроенергії – 40 років, а інтернету – 20 років, то країни із середнім рівнем доходу

[4] https://openknowledge.worldbank.org/server/api/core/bitstreams/7cc040bd-7442-4cae-bd0f-e416700ca68a/content

вже через пів року після запуску ChatGPT забезпечували половину його глобального трафіку. Це свідчить про те, що ШІ має потенціал для «наздоганяючого» розвитку, але реалізація цього потенціалу потребує виважених стратегічних рішень.

Вплив ШІ на розвиток визначається трьома ключовими характеристиками: його можливостями, концентрацією та комплементарними факторами. По-перше, ШІ – це технологія, здатна виконувати складні когнітивні завдання, які раніше були прерогативою висококваліфікованих спеціалістів. Це особливо важливо для країн, що розвиваються, де спостерігається гостра нестача лікарів, вчителів, агрономів та інших професіоналів. ШІ може допомогти заповнити ці прогалини, дозволяючи менш досвідченим працівникам виконувати складні завдання, або автоматизуючи частину роботи експертів, що вивільняє їхній час для більш важливих функцій.

По-друге, виробництво ШІ, його апаратне забезпечення та центри обробки даних значною мірою сконцентровані в кількох країнах, зокрема в США та Китаї. Ця концентрація створює ризик технологічної залежності для інших держав. Однак, вона ж надає можливість отримати доступ до передових технологій шляхом їх адаптації, а не створення з нуля, що потребує мільярдних інвестицій. Відкриті моделі, такі як Llama, Mistral та DeepSeek, дозволяють розробникам у всьому світі налаштовувати ШІ під місцеві потреби, мови та культуру. Доступ до таких моделей, а також стрімке зниження вартості хмарних обчислень, роблять адаптацію ШІ економічно доцільною.

По-третє, повний потенціал ШІ може бути реалізований лише за наявності відповідних комплементарних факторів, як аналогових (надійне електропостачання, доступ до інтернету, базова освіта), так і цифрових (дані для навчання, технічні навички, обчислювальні потужності). Якщо ШІ-модель навчається на даних, нерепрезентативних для конкретної країни, її ефективність буде низькою. У Нігерії, наприклад, ШІ-інструмент, навчений на даних з країн з високим рівнем доходу, надавав рекомендації щодо лабораторних тестів, які не відповідали місцевим реаліям. Без інвестицій в електроенергію, інтернет та освіту, ШІ не зможе принести користь там, де вона найбільш потрібна.

Доповідь пропонує чітку триступеневу стратегію. Першим і найважливішим кроком є впровадження (adopt) вже існуючих ШІ-рішень. Це найдоступніший шлях, який дозволяє підприємствам, фермерам та державним службовцям підвищити свою продуктивність. Проте простого впровадження недостатньо. ШІ-системи, створені в іншому середовищі, часто не працюють належним чином через мовні, культурні та інституційні відмінності.

Тому другим, і найважливішим кроком, є адаптація (adapt) ШІ до місцевих умов. Це означає навчання моделей на місцевих мовах, даних та врахування специфіки законодавства і потреб. Прикладами успішної адаптації є розробка моделей Latam-GPT для Латинської Америки та SEA-LION для Південно-Східної Азії, які краще розуміють регіональні мови та нюанси. Найбільші вигоди для країн, що розвиваються, будуть отримані саме на цьому етапі. Адаптація дозволяє створювати корисні застосунки, від чат-ботів для бізнесу до систем медичної візуалізації, без необхідності будувати гігантські моделі з нуля.

Лише після набуття досвіду в адаптації, країни можуть переходити до розвитку (advance) власних передових ШІ-технологій. Цей шлях є найскладнішим і найдорожчим, і він доступний лише для небагатьох країн, таких як Індія з її моделлю Sarvam AI чи ОАЕ з моделлю Falcon. Однак, навіть не будуючи власні моделі, країни можуть брати участь у ланцюжку створення вартості ШІ, наприклад, видобуваючи корисні копалини, виробляючи компоненти або розробляючи програмне забезпечення.

ШІ має значний потенціал для підвищення продуктивності праці, особливо для малих підприємств, які складають основу економіки країн, що розвиваються. У таких країнах частка робочих місць, які можуть бути автоматизовані, є значно нижчою (4,5%), ніж у багатих країнах (14,2%), що робить вплив ШІ на зайнятість менш руйнівним. Однак, є ризик, що без належних комплементарних факторів, ШІ може збільшити розрив у продуктивності між країнами,

оскільки більші вигоди отримують компанії, які вже були більш продуктивними та впроваджували інновації. Ланцюг створення вартості ШІ створює нові робочі місця та експортні можливості для країн, що розвиваються, проте основна частка прибутку залишається в руках провідних технологічних гігантів.

ШІ вже сьогодні демонструє вражаючі результати в публічному секторі. У внутрішніх адміністративних процесах він допомагає точніше прогнозувати стихійні лиха, ефективніше розподіляти ресурси та покращувати моніторинг. Наприклад, в Кенії ШІ-алгоритм призначає понад 10 000 судових справ на рік до посередників, зменшуючи завантаження суддів. У Бразилії ШІ аналізує дані муніципальних перевірок, щоб виявляти ризики корупції.

На передньому краї, де послуги надаються безпосередньо громадянам, ШІ може допомогти подолати нестачу кваліфікованого персоналу. Вчителі використовують ШІ для створення планів уроків та персоналізованих завдань. У сфері охорони здоров’я ШІ допомагає інтерпретувати медичні зображення. У Бангладеш ШІ-скринінг збільшив кількість пацієнтів, які перевіряються на діабетичну ретинопатію, на 40% на день. Однак, впровадження ШІ стикається з серйозними бар'єрами: обмежена доказова база, особливо для країн із низьким рівнем доходу, недостатній доступ до інтернету та навичок, а також проблеми з довірою до ШІ-рішень.

ШІ перерозподіляє владу на різних рівнях. На глобальному рівні домінування невеликої кількості країн створює залежність і може обмежувати доступ інших до критичних технологій. Стратегії «цифрового суверенітету» є дорогими та часто неефективними. Альтернативою є диверсифікація постачальників та використання відкритого програмного забезпечення. ШІ також змінює баланс сил між корпораціями та працівниками. Концентрація ринку створює «монопсонію», де компанії можуть встановлювати низьку заробітну плату та погані умови праці. Також існує загроза посилення державного нагляду та втручання в приватне життя. ШІ може використовуватися для масового стеження та поширення дезінформації, що особливо небезпечно в країнах зі слабкими інституціями.

Уряди відіграють вирішальну роль у трьох іпостасях: як рушії, користувачі та регулятори ШІ. Як рушії, вони повинні інвестувати в аналогову інфраструктуру (електрика, інтернет) та цифрові компоненти (дані, обчислення, навички), щоб створити умови для впровадження та адаптації ШІ. Вони також мають усунути інформаційні бар'єри для бізнесу та створити сприятливе підприємницьке середовище.

Висновки:

- **Унікальне вікно можливостей.** На відміну від попередніх технологічних революцій, ШІ поширюється набагато швидше. Країни, що розвиваються, мають унікальний шанс "перестрибнути" через етапи розвитку.
- **Пріоритет – адаптація, а не створення "з нуля".** Найбільший економічний ефект для країн із середнім доходом лежить у площині адаптації ШІ. Це означає створення локальних рішень на базі відкритих моделей.
- **Ризик нерівності та "витоку мізків".** ШІ може посилити нерівність, оскільки вигоди від нього отримують переважно великі, вже продуктивні компанії та висококваліфіковані працівники.
- **Держава як головний рушій змін.** Успіх у використанні ШІ визначатиметься здатністю держави виступати одночасно в трьох ролях: рушія (інвестиції в електроенергію та інтернет для шкіл та сіл), користувача (закупівля та впровадження ШІ у сервісах) та регулятора (створення чітких та гнучких правил, що стимулюють інновації).

Як користувачі, уряди повинні використовувати свою купівельну спроможність для стимулювання розробки ШІ-рішень, адаптованих до місцевих потреб. Це вимагає оцифрування даних, інвестицій у кадровий потенціал та створення чітких процедур для закупівлі, тестування та оцінки ШІ-систем.

Як регулятори, уряди повинні будувати довіру, використовуючи спочатку добровільні галузеві стандарти, а там, де вони не спрацьовують, застосовувати чинне законодавство для захисту прав громадян. Гнучкі та адаптивні правові рамки, міжнародне співробітництво та зміцнення інституційної спроможності є

ключовими для запобігання регуляторному роздробленню та захисту від можливих зловживань. Уряди країн із низьким рівнем доходу мають зосередитися на створенні довіри та використанні існуючих законів, тоді як багатші країни можуть дозволити собі розробку нових комплексних законів про ШІ. Вибір, зроблений сьогодні, визначить, чи стане ШІ каталізатором розвитку чи джерелом нових нерівностей та ризиків.

Країни, що розвиваються, не можуть дозволити собі спостерігати за технологічною революцією збоку. Вартість пасивності чи оборонної позиції надто висока, як показав досвід першої промислової революції. Більшість країн, що розвиваються, не готові до ШІ: на сьогодні лише одна з 25 країн із низьким рівнем доходу (Руанда) має національну стратегію ШІ.

Країни з найбільшим потенціалом виграшу є найменш підготовленими. Головне завдання для них – не копіювати порядки денні багатих країн, зосереджені на ризиках масового безробіття чи гонці технологій, а використовувати ШІ для вирішення своїх найнагальніших проблем: бідності, поганої освіти, слабкої охорони здоров'я. Ухвалення, адаптація та розвиток – ось перевірений шлях до процвітання. ШІ може допомогти країнам, що розвиваються, вирішити проблеми, які не піддавалися розв’язанню поколіннями, але цього можна досягти лише за умови відповідального, стратегічного та своєчасного підходу.

Регулювання

FinCEN скасував звітування про бенефіціарну власність для американських компаній [5]

11 серпня 2026 року Міністерство фінансів США оголосило остаточне правило Мережі боротьби з фінансовими злочинами (FinCEN) «Beneficial Ownership Information Reporting Requirement Revision» (RIN 1506-AB67). Правило робить постійною тимчасову норму від 26 березня 2025 року і додатково розширює перелік винятків, фактично припиняючи дію ключового обов'язку, запровадженого Законом про корпоративну прозорість (Corporate Transparency Act, CTA), – подання інформації про бенефіціарну власність (BOI) американськими юридичними особами. Правило набрало чинності з дати публікації, без стандартної тридцятиденної відстрочки, з посиланням на 5 U.S.C. 553(d)(1). Міністр фінансів Скотт Бессент охарактеризував рішення як «перемогу здорового глузду та американського малого бізнесу», а серед правових підстав, поряд із нормами Закону про банківську таємницю, прямо наведено Виконавчий указ 14192 «Unleashing Prosperity Through Deregulation».

Юридична конструкція правила заслуговує на окремий аналіз, оскільки FinCEN не скасовував і не міг скасувати CTA – це компетенція Конгресу. Замість цього регулятор скористався закладеними в самому законі повноваженнями щодо звільнення від обов'язку: 31 U.S.C. § 5336(a)(11)(B)(xxiv) (право виводити з-під визначення «звітної компанії» цілі класи суб'єктів), 31 U.S.C. § 5318(a)(7) (загальне повноваження щодо винятків у межах Закону про банківську таємницю) та 31 U.S.C. § 5336(b)(4)(A) (повноваження щодо процедур FinCEN ID). Іншими словами, ефект, еквівалентний скасуванню закону, досягнуто підзаконним інструментом у межах формально наданих повноважень. Це прецедент, що має самостійне значення для оцінки стійкості будь-якого режиму прозорості бенефіціарної власності: якщо закон делегує регуляторові широке повноваження звільняти «класи суб'єктів» без чітких законодавчих меж, обсяг режиму стає функцією політичного курсу виконавчої влади, а не законодавчого рішення.

Зміни до 31 CFR 1010.380 охоплюють шість позицій. По-перше, переозначено поняття «підзвітної компанії»: із нього виведено всі національні (domestic) суб'єкти, а новий виняток § 1010.380(c)(2)(xxiv) поширюється на «будь-який суб'єкт, створений шляхом подання документа секретареві штату» – тобто на весь масив американських корпорацій, LLC та подібних утворень. По-друге, для іноземних об'єднаних інвестиційних інструментів (foreign

[5] https://public-inspection.federalregister.gov/2026-16576.pdf

pooled investment vehicles) обов'язок звужено до осіб, які не є особами США та здійснюють суттєвий контроль; за відсутності такої особи звітування про бенефіціарних власників не подається взагалі. По-третє, іноземні звітні компанії більше не подають дані про бенефіціарних власників – осіб США. По-четверте, аналогічний виняток поширено на «заявників компанії» (company applicants), які є особами США. По-п'яте, скасовано обов'язок осіб США оновлювати або виправляти раніше подану інформацію за FinCEN ID – це звільняє приблизно 760 000 власників ідентифікаторів від тридцятиденної вимоги оновлення. По-шосте, строки подання залишено без змін, попри клопотання коментаторів.

Операційно найбільш незворотним елементом правила є не припинення збору, а знищення вже сформованого масиву. FinCEN зобов'язується видалити інформацію про бенефіціарну власність, обґрунтовано ідентифіковану як таку, що належить особам США та національним суб'єктам, – причому механізм ідентифікації прив'язаний до типу поданого документа, що посвідчує особу (американський паспорт або посвідчення водія). Видалення передбачено провести єдиним суцільним заходом за погодженням із Національним архівом, без надсилання підтверджень заявникам, а 180 днів після публікації встановлено як межу для випадкових подань, що надійдуть після набрання чинності. Відмінність між призупиненням збору та знищенням даних тут принципова: перше є зворотним політичним рішенням, друге означає, що відновлення реєстру за іншої адміністрації вимагатиме повторного збору з нуля – з відповідними витратами, часовим лагом у кілька років і повторним проходженням процедур нормотворчості.

Масштаб звуження ілюструють власні оцінки FinCEN. Після набрання чинності реєстр охоплює приблизно 28 000 іноземних звітних компаній, які не підпадають під винятки, станом на кінець 2025 року, з яких близько 13 000 вже подали звітність, а очікуваний приріст становить близько 1 800 нових реєстрацій на рік. Це слід зіставляти з десятками мільйонів суб'єктів, охоплених первісним правилом. Економічний ефект FinCEN оцінює як багатомільярдну середньорічну економію. Показово, що сам регулятор визнає невизначеність оцінок чисельності популяції з похибкою до 5 % у частині охоплення категорій винятків – тобто точність вигоди від скасування обчислено з тією ж мірою умовності, що й попередні оцінки витрат на дотримання.

Аргументація FinCEN будується навколо § 6403 CTA, який приписує Міністрові фінансів «максимально можливою мірою мінімізувати тягар для звітних компаній, пов'язаний зі збором» BOI, «з урахуванням приватних витрат на дотримання, покладених на легітимний бізнес». FinCEN наголошує, що ця вимога міститься як у розділі «Sense of Congress», так і в операційних положеннях закону, і на цій підставі кваліфікує її як юридично обов'язкову, а не декларативну. Первісне правило регулятор тепер характеризує як «ретроспективно надмірно широкий підхід», оскільки «переважна більшість» американських компаній є законними, а збір даних із них не продукував би «високо корисної» (highly useful) інформації, що виправдовувала б витрати на дотримання. З аналітичного погляду тут відбувається концептуальне зміщення: стандарт «highly useful» Закону про банківську таємницю прочитано як тест співвідношення витрат і вигід на рівні всієї популяції суб'єктів, а не як тест ризик-орієнтованого таргетування. Уразливість цієї конструкції полягає в тому, що корисність реєстру бенефіціарної власності є мережевою, а не одиничною властивістю: цінність створює можливість перевірити будь-яку компанію, і вона різко падає, коли охоплення є вибірковим і заздалегідь відомим злочинцеві – саме тому охоплення «переважно легітимних» суб'єктів є не надлишком, а умовою функціонування реєстру.

Правило містить розгорнуті відповіді на заперечення, подані під час консультацій, і саме ця частина найцікавіша для регуляторного аналізу. Аргументи про неконституційність (порушення принципу поділу влади та клаузули Take Care) відхилено з посиланням на те, що CTA прямо уповноважує Міністра звільняти суб'єктів за визначених обставин. Заперечення щодо суперечності намірам Конгресу відхилено через розмежування необов'язкових формулювань «Sense of Congress» і обов'язкових операційних приписів – хоча в частині мінімізації тягаря FinCEN застосовує протилежну логіку і спирається саме на присутність

норми в обох блоках. Щодо стандартів FATF регулятор визнав отримані застереження стосовно Рекомендації 24 і дійшов висновку, що збереження звітування іноземних компаній забезпечує досягнення цілей міжнародного співробітництва в межах витратних обмежень закону. На заперечення правоохоронного характеру – з наведенням прикладів відмивання коштів через американські компанії-оболонки та обходу санкцій – FinCEN відповів чотирма тезами: винятки погоджено письмово Міністерством юстиції та Міністерством внутрішньої безпеки; продовжують діяти вимоги Правила належної перевірки клієнтів (CDD Rule) для охоплених фінансових установ; звітування іноземних компаній збережено; а стан справ повертається до «status quo ante», що передувало первісному правилу, а не погіршується відносно нього.

Остання теза потребує критичного розгляду, оскільки вона є центральною для оцінки відповідності США стандартам FATF. Аргумент «status quo ante» коректний лише в статичному сенсі: справді, до 2024 року федерального реєстру не існувало. Проте Рекомендація 24 у редакції після перегляду 2022 року вимагає застосування багатокомпонентного підходу – використання реєстрового механізму, механізму, заснованого на діяльності компанії, та/або альтернативних механізмів, здатних забезпечити своєчасний доступ до достатньої, точної та актуальної інформації про бенефіціарну власність юридичних осіб, створених у країні. Після скасування звітування для національних суб'єктів США фактично покладаються виключно на підхід через фінансові установи, тобто на CDD Rule. Його межі відомі: він застосовується лише тоді, коли юридична особа відкриває рахунок в охопленій фінансовій установі, поріг участі залишається на рівні 25 % плюс одна контролююча особа, інформація не агрегується в доступний правоохоронним органам масив, а компанії, які взагалі не відкривають рахунків у США – типова конфігурація для оболонок, що використовуються для володіння активами чи виставлення інвойсів, – не потрапляють у жоден механізм. FinCEN окремо анонсував майбутню нормотворчість щодо CDD Rule, проте наразі це намір, а не чинна компенсаторна норма.

Для української аудиторії правило має щонайменше чотири практичні наслідки. По-перше, СПФМ втрачають перспективу використання американського реєстру як джерела верифікації структури власності контрагентів: наявність американської LLC у ланцюгу власності знову не супроводжується жодним публічним чи доступним органам записом про кінцевого бенефіціара, що повертає навантаження з установлення структури власності на саму українську установу. По-друге, американські корпоративні форми – насамперед LLC штатів Делавер, Вайомінг і Нью-Мексико – знову набувають властивостей, які історично робили їх привабливими для схем із виведення активів та обходу санкцій, що потребує підвищення рівня ризику відповідних юрисдикцій у моделях скорингу. По-третє, для позиції України у діалозі з міжнародними партнерами важливо, що йдеться про свідоме зниження рівня відповідності основній рекомендації FATF членом Групи з прямим

Висновки:

- **Ефект, еквівалентний скасуванню закону, досягнуто підзаконним актом:** FinCEN не змінював CTA, а скористався правом звільняти «класи суб'єктів» за 31 U.S.C. § 5336, вивівши з-під дії правила «будь-який суб'єкт, створений шляхом подання документа секретареві штату».
- **Незворотним є не припинення збору, а знищення масиву:** BOI осіб США видаляється єдиним заходом з ідентифікацією за типом документа – паспортом США чи посвідченням водія. Реєстр скорочується з десятків мільйонів суб'єктів до приблизно 28 000 компаній.
- **CDD Rule структурно не заміщує реєстр:** він спрацьовує лише при відкритті рахунку в охопленій установі, зберігає поріг 25 % плюс контролююча особа і не формує доступного правоохоронним органам масиву. Компанії без рахунків у США лишаються поза Рекомендацією 24 взагалі.
- **Для СПФМ негайно змінюється профіль ризику:** LLC Делаверу, Вайомінгу чи Нью-Мексико в ланцюгу власності знову не має жодного публічного запису про бенефіціара. Водночас українські компанії, зареєстровані для діяльності у США, лишаються повністю охопленими обов'язком.

визнанням отриманих застережень щодо Рекомендації 24 – це створює аргументаційний прецедент, який імовірно буде відтворюватися у внутрішніх дискусіях про дерегуляцію в інших юрисдикціях, зокрема щодо Єдиного державного реєстру та обов'язку подання структури власності. По-четверте, збереження обов'язку для іноземних звітних компаній щодо їх іноземних бенефіціарів означає, що українські юридичні особи, зареєстровані для ведення діяльності у США, залишаються у сфері дії правила в повному обсязі.

Звіти окремих інституцій та експертів

Дослідження RUSI щодо конвертації викрадених КНДР віртуальних активів у фіат [6]

Центр фінансів і безпеки Королівського об'єднаного інституту оборонних досліджень (RUSI) оприлюднив дослідницьку роботу Еллісон Оуен і д-р Ноемі Тамбе «North Korean Crypto-to-Fiat Activity». Дослідження свідомо адресує прогалину: тоді як методи відмивання КНДР безпосередньо на блокчейні задокументовано доволі докладно, поведінка пов'язаних із КНДР акторів саме на стику блокчейн-інфраструктури та традиційної фінансової системи – тобто на етапі виходу у фіат – досліджена значно гірше. Масштаб проблеми автори окреслюють однозначно: у період із січня 2024 року до вересня 2025 року КНДР викрала приблизно 2,8 млрд доларів США у віртуальних активах, і ці кошти, за припущенням дослідження, безпосередньо підтримують програму розробки зброї масового знищення. Робота має виражено практичну спрямованість: її результатом є набір індикаторів, специфічних для конвертації віртуальних активів у фіат, та чотири рекомендації щодо посилення контролів приватного сектору.

Методологія є змішаною і поєднує огляд літератури (документи FATF, регуляторні настанови, звіти міжнародних органів), 25 напівструктурованих інтерв'ю, проведених у вересні–листопаді 2025 року, та валідацію отриманих індикаторів даними блокчейн-аналітичної компанії Elliptic. Розподіл респондентів охоплює постачальників послуг з віртуальних активів (4), компанії з розслідувань у сфері віртуальних активів (4), фахівців із комплаєнсу (3), фінансові установи (3), фахівців із кібербезпеки (2), органи нагляду за VASP (2), підрозділ фінансової розвідки (1), компанії з розслідувань у сфері ПВК (1), правоохоронні органи (1), прокуратуру (1) та компанії, пов'язані з віртуальними активами (3). Автори прямо визнають ключове методологічне обмеження: розмежувати індикатори, специфічні саме для КНДР, та індикатори третіх сторін-фасилітаторів украй складно через накладання мереж відмивання. Це застереження має самостійну аналітичну вагу – воно означає, що переважна частина описаних маркерів є ознаками професійної інфраструктури відмивання загалом, а не унікальним «підписом» КНДР, і тому має цінність для СПФМ поза межами вузького контексту з ФР.

Центральним кейсом дослідження є злам біржі Bybit у лютому 2025 року на суму близько 1,5 млрд доларів США. До вересня 2025 року всі викрадені кошти було виведено та конвертовано у фіат або тверду валюту. КНДР спиралася на мережу відмивачів, позабіржових (OTC) та однорангових (P2P) трейдерів, а безпосередню роботу виконували громадяни Китаю, які, за описом респондентів, працювали цілодобово. Найбільш показова операційна деталь: транзакції дробилися на суми близько 30 тис. доларів США кожна – прямо для того, щоб окреме заморожування не мало відчутного впливу на схему в цілому. Це свідчить про калібрування структури операцій під фактичну спроможність приватного сектору реагувати, а не під формальні порогові значення, і є важливим коригуванням для тих моделей моніторингу, що орієнтуються на великі одиничні суми. Водночас 95 % викрадених у Bybit коштів пройшли через децентралізовані сервіси з використанням міксерів, мостів і власних гаманців, а частина коштів рухалася через заздалегідь налаштовані структури гаманців, що

[6] https://www.rusi.org/explore-our-research/publications/research-papers/north-korean-crypto-fiat-activity

автоматично розподіляють активи в режимі реального часу на заздалегідь визначені напрями – переважно P2P-майданчики Південної Азії та нерегульовані біржі Латинської Америки.

Дослідження детально описує інфраструктуру виходу у фіат. Ключовим елементом є позабіржові брокери та «гарантійні» майданчики. Huione Pay – камбоджійський сервіс із мобільним застосунком і фізичними відділеннями, що працює китайською мовою та обслуговує переважно громадян Китаю в Камбоджі, – був ліквідований Національним банком Камбоджі в грудні 2025 року; ще в липні 2024 року Tether заморозив близько 35 млн доларів США в USDT після надходження коштів, пов'язаних із атрибутованим КНДР зламом біржі DMM. «Гарантійні» майданчики в Telegram – зокрема Xinbi Guarantee з обігом близько 8 млрд доларів США та Huione Guarantee, відключений від платформи в травні 2025 року, – за даними Elliptic, приймали криптовалюту, що походить із атрибутованих КНДР зламів, у приватні ескроу-угоди, які ймовірно передбачають обмін на готівку. Окремо автори виділяють кореспондентські відносини між ліцензованими та неліцензованими VASP як «слабку ланку», що уможливлює змішування незаконних і законних активів: неліцензовані майданчики характеризуються поблажливим ставленням до вимог ПВК/ФТ і схильністю ставати на бік клієнта при заморожуванні операцій, чим користуються відмивачі, публічно скаржачись у Telegram на заблоковані кошти й тиснучи на репутацію платформи.

Поведінкові індикатори становлять найоригінальнішу частину роботи. Респондент від однієї з бірж зафіксував зміну тактики: якщо раніше при затриманні операції пов'язані з КНДР клієнти поводилися тихо, то тепер вони подають від 50 до 70 звернень до служби підтримки з вимогою повернення коштів. Супутні ознаки – граматично бездоганна англійська, що вказує на використання інструментів генерації відповідей, лайка китайською в разі роздратування, посилання на подарунок або спадщину як джерело коштів без будь-яких підтверджень і наративи про передавання коштів «з рук у руки», що не піддаються перевірці. Щодо «грошових мулів» дослідження фіксує переважне походження із Південно-Східної Азії – філіппінці, індонезійці та громадяни Китаю – та описує дві моделі: «від'єднану», коли продавець передає лише облікові дані й далі не контактує (висока операційна безпека, але провал біометричної перевірки), та «під'єднану», коли доступ до мула зберігається для реагування на запити біржі (дорожча, проте проходить перевірки з жестами). Наведено конкретні випадки: рахунок індонезійки використовувався для надсилання скарг корейською з подальшим переходом на англійську, а рахунок філіппінки – для тиску на біржу з метою розблокування активів КНДР після успішного проходження KYC.

Технічні маркери дослідження також деталізує. Використання Astrill VPN за замовчуванням сприймається як ознака діяльності КНДР, і лише в поодиноких випадках за ним стоїть громадянин Китаю; водночас зафіксовано перехід до ExpressVPN і Proton VPN, які через велику базу користувачів вимагають цілісної оцінки в сукупності з іншими факторами. Важливе спостереження стосується ідентифікаторів пристроїв: під час швидких обмінів актори змінюють IP-адреси, проте пристрої змінюють значно рідше, що дає біржам можливість вести чорні списки device ID та отримувати сповіщення; виразна зміна device ID натомість вказує на підключення сторонніх груп підтримки. Серед транзакційних ознак – переказ близько 7 тис. доларів США у стейблкоїнах «частинами» через P2P, автоматизований характер операцій, що вгадується за їх кількістю в стислий проміжок часу, та мовні налаштування облікового запису: англійська (США) як основна з періодичним використанням корейської як другої.

На фіатному боці схеми дослідження підтверджує усталений патерн: банківські рахунки пов'язаних із фасилітаторами КНДР відкриваються в китайських фінансових установах протягом кількох днів після зламу. Історичний приклад 2018–2019 років – новий банківський рахунок, прив'язаний до рахунку на біржі менш ніж за тиждень після викрадення коштів; у справі Тянь Іньінь ідеться про рахунок у China Guangfa Bank, а Лі Цзядун прив'язав дев'ять окремих рахунків у китайських банках. За звітом MSMT 2025 року наведено перелік із 16 китайських банків, серед яких Agricultural Bank of China, Industrial and Commercial Bank of China, China Guangfa Bank, China Construction Bank та Industrial Bank. Окремо описано канал,

що взагалі оминає банківський переказ: офіси позабіржових брокерів утримують готівку в багатьох валютах, що дозволяє отримувати кошти особисто та переміщувати їх контрабандою, уникаючи прямого депозиту від третьої особи у фінансовій установі; кур'єрські мережі рухають готівку через банкомати, а інкасаторські компанії доправляють її до установ. Згідно з MSMT, отриманий від OTC-брокерів фіат часто зараховується на підконтрольні КНДР банківські рахунки через картки UnionPay, емітовані китайськими банками. Автори також фіксують перетин із TBML: за обвинувальними актами 2023 року через компанії-прикриття закуповувалися тютюнові вироби та комунікаційне обладнання з оплатою на адресу суб'єктів в ОАЕ та Болгарії.

Розділ про практики приватного сектору містить безпосередньо застосовний матеріал. Для фінансових установ ключовою є повнота анкети при встановленні відносин: без відповідних питань установа може взагалі не ідентифікувати діяльність, пов'язану з віртуальними активами; рекомендований пакет документів включає виписки про виведення коштів із бірж та адреси гаманців, звіти блокчейн-аналізу щодо походження активів, підтвердження ліцензованого статусу VASP, історію торгівлі й депозитів, що пов'язує фіат із придбанням віртуальних активів, і пояснення клієнта щодо походження коштів. Окремо наголошено на проблемі якості даних: інформація надходить фрагментованою, неповною й непослідовною, через незахищену електронну пошту або у вигляді підготовлених вручну файлів CSV чи Excel, які легко модифікувати й які не мають контролів цілісності та стандартизованого формату. У правилах моніторингу автори наводять код категорії торговця MCC 6051, виявлення ключових слів («Bitcoin», «Binance», «wallet», «USDT»), часті дрібні платежі на численні біржі, круглі суми, що повторюються, швидкий цикл «депозит–виведення» протягом кількох годин, потоки в напрямі юрисдикцій-хабів (Сейшели, Гонконг, Кайманові Острови) та невідповідність між задекларованою професією або доходом і обсягом переказів на адресу VASP.

Для самих постачальників послуг з віртуальних активів центральним є питання «hop policy» – політики глибини простеження ланцюга операцій. Дослідження фіксує диференційований підхід: для звичайних відносин застосовується ризик-орієнтована оцінка з типовою межею близько п'яти «хопів»; для підвищеного ризику – фінансування тероризму, матеріали сексуального насильства над дітьми – простеження подовжується з визнанням того, що підсанкційні суб'єкти системно застосовують peel chains і сервіси автоматизованих переказів; у випадках ручного розгляду фіксованої межі немає взагалі, і глибина визначається доступними даними, типологією та релевантністю проміжних гаманців. Обґрунтування суто економічне: кожен додатковий «хоп» збільшує час обробки і вартість, тож безперервне глибоке простеження було б операційно неприйнятним. Окремо вказано на структурну вразливість Travel Rule: роль провайдерів часто починається і закінчується ідентифікацією контрагента, тоді як відповідальність за точність даних і додаткову перевірку залишається на VASP, а окремі провайдери обслуговують неліцензованих постачальників навіть у регульованих юрисдикціях.

Дослідження завершується чотирма рекомендаціями. Перша – регуляторам слід видати чіткі настанови щодо управління

Висновки:

- **Дроблення 1,5 млрд доларів США, викрадених у Bybit, на транші близько 30 тис. показує калібрування схеми під фактичну спроможність приватного сектору реагувати**, а не під формальні пороги: заморожування окремого траншу свідомо зроблено неболючим для схеми в цілому.
- **Найпрактичніший маркер не потребує блокчейн-аналітики:** ідентифікатори пристроїв змінюються значно рідше за IP-адреси, тож чорні списки device ID стійкіші за геолокаційний скринінг. Перехід від Astrill VPN до ExpressVPN і Proton позбавляє VPN-ознаку самодостатності.
- **Поведінкові ознаки виявилися вимірюваними:** 50-70 звернень до служби підтримки з вимогою повернення коштів, бездоганна англійська, що вказує на генерацію відповідей, посилання на подарунок чи спадщину без документів. Ці дані варто інтегрувати в систему моніторингу.

кореспондентськими відносинами між VASP, тобто домовленостями, за якими один постачальник надає іншому послуги чи доступ до фінансової інфраструктури, особливо при взаємодії з неліцензованими постачальниками. Друга – міжнародній банківській асоціації доцільно підтримати розроблення стандартизованих анкет для встановлення відносин із VASP, які фіксували б відомості про власність, структуру комплаєнсу та операційну модель. Третя – державам слід створити захищені канали обміну інформацією між фінансовими установами, регуляторами та VASP, зосереджені на ідентифікаторах бірж і підозрілих адресах гаманців; обґрунтуванням є те, що розрізненість комплаєнс-переліків і фрагментованість даних про VASP між установами унеможливлює виявлення патернів «мулів» і неліцензованих операторів. Четверта – регуляторам слід зобов'язати VASP включати специфічні посилання (references) у платіжні повідомлення при банківських переказах, ініційованих в інтересах клієнтів, зокрема ідентифікатор самого VASP, щоб банк-отримувач міг проактивно виявляти та досліджувати такі перекази. Для України остання рекомендація має найбільш безпосередню проєкцію: вона стосується не блокчейн-аналітики, а формату платіжного повідомлення, тобто інструменту, що перебуває в межах регуляторної компетенції Національного банку і не потребує ані нової технологічної інфраструктури, ані доступу до транскордонних даних.

Кокаїн і конфлікт у Сахелі: транснаціональні маршрути, збройні угруповання та системи політичного захисту в Малі, Нігері й Лівії [7]

Документ Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC) присвячений аналізу розвитку транзитної торгівлі кокаїном через центральний Сахель і Лівію та її взаємозв'язку зі збройними конфліктами, політичною нестабільністю, державними структурами, кримінальними мережами й економікою збройних угруповань. Центральна теза дослідження полягає в тому, що хоча сухопутними маршрутами через Сахель і Лівію перевозиться значно менший обсяг кокаїну, ніж морськими шляхами між Латинською Америкою, Західною Африкою та Європою, саме ці маршрути мають особливо вагомий вплив на політичну економіку та безпекове середовище регіону. Вони інтегровані у давно сформовані торговельні й контрабандні мережі, механізми політичного захисту та економіку конфліктів, завдяки чому залишаються стійкими до правоохоронного тиску, зміни політичних режимів і коливань інтенсивності збройного протистояння. Доходи від транзиту забезпечують фінансові ресурси кримінальним підприємцям, збройним формуванням і пов'язаним із державою акторам, водночас посилюючи стимули для збереження системи, у межах якої незаконна економічна діяльність може функціонувати.

Дослідження базується на значному масиві первинної та вторинної інформації. Автори використовували відкриті джерела, бази даних щодо вилучень наркотиків, моніторинг медіа і платформ відстеження конфліктів, а також багаторічні польові матеріали GI-TOC. Окремий цикл збору інформації тривав із вересня 2025 року до січня 2026 року та включав понад 150 інтерв'ю з місцевими торговцями, перевізниками, представниками правоохоронних і безпекових структур, лідерами громад, посередниками, членами збройних угруповань та пов'язаними з ними особами, безпосередніми учасниками кокаїнового трафіку, дипломатами та регіональними експертами. Дані збиралися в Малі, Нігері та різних районах Лівії та зіставлялися між кількома незалежними джерелами. Водночас автори наголошують, що основний аналітичний зріз відображає ситуацію станом на січень 2026 року, тому подальші зміни конфліктної ситуації враховані лише обмежено.

Історично Західна і Північна Африка почали набувати особливого значення як транзитний простір глобального кокаїнового ринку ще на початку 2000-х років. Кокаїн із Латинської Америки надходить до прибережних районів Західної Африки, після чого частина вантажів переміщується сухопутними коридорами через Малі та Нігер до Лівії, Марокко або Мавританії

[7] https://globalinitiative.net/wp-content/uploads/2026/08/Cocaine-and-conflict-in-Mali-Niger-and-Libya-GI-TOC-August-2026.pdf

й далі до європейських ринків. Звіт окреслює чотири основні сухопутні конфігурації, однак підкреслює, що реальна транспортна система значно складніша: маршрути перетинаються, змінюють напрямок залежно від безпекової ситуації та можуть використовуватися як для руху на північ, так і для переміщення між різними прибережними точками ввезення та вивезення. Кокаїн часто приховується серед інших товарів, а частина наркотиків залишається на регіональних ринках споживання.

Після 2019 року інтенсивність торгівлі кокаїном через Західну Африку істотно зросла. Серед головних чинників GI-TOC називає збільшення виробництва кокаїну в Латинській Америці, зростання європейського попиту, посилення правоохоронного тиску на прямі морські маршрути з Латинської Америки до Європи та покращення транспортної інфраструктури Західної Африки. Унаслідок цього злочинні мережі активніше диверсифікували логістику та стали використовувати навіть складні конфліктні території Сахелю і Лівії. Важливим спостереженням є те, що нестабільність сама по собі не зупиняє наркотрафік. Періоди гострого насильства, політичних переворотів або зміни військових союзів здатні порушувати усталені маршрути, однак мережі переважно відповідають на це перенесенням маршрутів, укладенням нових домовленостей щодо захисту та використанням інших операційних моделей.

Формування сучасної наркотрафікової інфраструктури відбувалося на основі набагато старших торговельних і контрабандних систем. У північному Малі та Нігері вони існували ще у 1990-х роках і використовувалися, зокрема, для перевезення гашишу. Поширення значно прибутковішої торгівлі кокаїном призвело до зростання конкуренції та мілітаризації контрабанди: для охорони вантажів стали залучатися озброєні формування, а контроль над маршрутами почав безпосередньо впливати на місцевий баланс сил. Одним із найбільш показових епізодів став інцидент «Air Cocaine» 2009 року, коли літак, що, за повідомленнями, перевозив кілька тонн кокаїну, приземлився на імпровізованій смузі в північному Малі. Ця справа продемонструвала не лише логістичні можливості злочинних мереж, а й масштаби можливого залучення державних посадовців до забезпечення наркотрафіку.

Початок конфлікту в північному Малі у 2012 році змінив систему перевезень, але не припинив її. Злочинні мережі почали активніше укладати ситуативні домовленості зі збройними угрупованнями, які контролювали території, а боротьба за маршрути та доходи від контрабанди дедалі більше переплиталася з самим конфліктом. Аналогічна трансформація відбулася після революції 2011 року в Лівії, коли зміна політичного режиму відкрила можливості для нових кримінальних і племінних мереж. Погіршення безпекової ситуації у Феццані та північному Нігері після 2016 року також спричинило скорочення окремих потоків, однак не їх припинення. Таким чином, досвід двох десятиліть показує високу адаптивність найбільших учасників ринку: частина ключових посередників залишається активною з початку 2000-х років, змінюючи партнерів і системи захисту відповідно до політичної ситуації.

Період 2019–2023 років, навпаки, характеризувався збільшенням транзиту. Особливо важливо, що це зростання було пов’язане не тільки із глобальним збільшенням пропозиції кокаїну, а й із відносною передбачуваністю територіального контролю та систем захисту. У північному Малі домовленості між ключовими збройними акторами дозволяли фактично розподіляти контроль над територіями і транспортними вузлами, тоді як у Малі та Нігері зберігалися механізми політичного захисту наркоторговців. У Лівії консолідація влади Лівійських арабських збройних сил (LAAF) над Феццаном і частиною Кіренаїки також створила більш передбачуване середовище для переміщення великих партій. Це формує один із принципових висновків дослідження: для великомасштабної торгівлі кокаїном критичним фактором є не стільки відсутність конфлікту, скільки наявність стабільних і передбачуваних систем захисту та контролю.

Після 2023 року ситуація суттєво змінилася одразу в усіх трьох країнах. У Малі наступ збройних сил за підтримки ПВК «Вагнер», зміна територіального контролю та припинення дії попередніх політичних домовленостей зруйнували частину усталених маршрутів у районі

Кідаля. Однак наркотрафік не припинився: перевізники почали використовувати довші та дорожчі маршрути, зокрема рух із Гао через регіон Менака в напрямку Нігеру. На початок 2026 року GI-TOC характеризує торгівлю кокаїном у північному Малі не як зруйновану, а як переконфігуровану: потоки стали більш фрагментованими та витратними, а їх географія дедалі більше визначається тим, який саме збройний актор здатний гарантувати безпечний прохід через конкретну територію.

У Нігері переворот у липні 2023 року став прикладом того, як політична зміна може реально порушити функціонування наркомереж. Зникнення усталених механізмів захисту, пов'язаних із попередньою владою, призвело до скорочення потоків, тимчасового припинення окремих маршрутів та відходу частини посередників. Деякі учасники переключилися на інші незаконні ринки, насамперед неформальну торгівлю золотом. Проте з середини 2025 року мережі почали відновлюватися вже у новій політичній конфігурації. Особливе місце в аналізі займають особи, пов'язані з Союзом нігерців за пильність і патріотизм (UNVP), яка була інтегрована в безпекову систему країни та отримала повноваження здійснювати патрулювання і контрабандні перевірки. За інформацією джерел GI-TOC, окремі пов'язані з цією структурою особи водночас могли виконувати функції захисту, супроводу та повернення незаконних вантажів. Цей випадок демонструє ризик фактичного стирання межі між протидією незаконній діяльності та її інституційним захистом.

У Лівії торгівля кокаїном розвивається в умовах політичного і територіального поділу країни. Водночас GI-TOC показує, що сама політична фрагментація не обов'язково створює перешкоди для наркотрафіку. У контрольованих LAAF районах Кіренаїки та Феццану відносна стабільність і ефективний територіальний контроль знизили ризик бандитизму та зробили транспортне середовище більш прогнозованим, у тому числі для злочинних перевезень. Пов'язані з LAAF актори, за даними дослідження, використовували своє становище для контролю та розширення прибуткових незаконних ринків, включаючи переміщення гашишу та кокаїну через південну та східну Лівію. Навіть конфлікт у Катруні у 2025 році мав переважно тимчасовий ефект: після короткострокового порушення потоків мережі перенесли частину маршрутів у район перевалу Сальвадор (Salvador Pass) і почали активніше використовувати менші населені пункти як місця зберігання.

Особливу увагу автори приділяють структурі самого кримінального середовища. Торгівля кокаїном у Малі, Нігері та Лівії формується взаємодією трьох груп: давно укорінених регіональних кримінальних посередників, пов'язаних із державою систем політичного й силового захисту та різноманітних збройних формувань. Великий транскордонний трафік контролюється відносно невеликою кількістю впливових посередників, чиї мережі здатні існувати десятиліттями, переживаючи вибори, перевороти та війни. Їх стійкість пояснюється контролем над логістикою, інтеграцією в місцевий легальний бізнес і патронажні системи, сімейними та племінними зв'язками, а також безпосереднім доступом до політичних і силових структур.

У Малі найбільші обсяги пов'язуються з мережею, яку у документі називають Tilemsi Galaxy. Вона об'єднує торговельні сім'ї з долини Tilemsi в районі Гао та зберігає відносно стабільне ядро з початку 2000-х років. Особливо суттєвим є використання цими мережами легального корпоративного сектору. Пов'язані компанії, нерідко оформлені на родичів, можуть використовуватися для перевезення наркотиків, формування зовні законних грошових потоків та легалізації доходів. У звіті також описується використання ширшої мережі компаній у Малі та сусідніх країнах, вкладення коштів у нерухомість та створення підприємств, що використовуються для прикриття незаконної діяльності. Таким чином, наркотрафік функціонує не як ізольована тіньова діяльність, а як система, що поєднує незаконні операції з легальним бізнесом, майном, транспортною інфраструктурою та політичними зв'язками.

Саме державний або квазідержавний захист автори визначають як одну з основ функціонування великомасштабної торгівлі. Порівняння Малі, Нігеру і Лівії показує, що фрагментація держави чи наявність конфлікту самі по собі не руйнують ринок, якщо

зберігаються передбачувані механізми політичного захисту. Натомість раптове руйнування таких домовленостей, як після перевороту в Нігері, може суттєво скоротити потоки, доки злочинні мережі не сформують нову систему зв'язків. Саме тому доповідь фактично зміщує аналітичний фокус із фізичних маршрутів і окремих перевізників на систему захисту, фінансування, легального бізнесу, політичного впливу та інституційних зв'язків, які роблять великомасштабний транзит можливим.

Збройні формування також відіграють важливу, хоча переважно не керівну роль. Вони здебільшого не організовують весь міжнародний ланцюг постачання, а надають конкретні послуги: захист конвоїв, транспортування, контроль територій, безпечний прохід або охорону місць зберігання. У Малі ці функції виконують як провладні, так і повстанські формування, а в Лівії – численні збройні групи, часто формально пов'язані з державними структурами. У деяких випадках винагорода за забезпечення проходу може надаватися не грошима, а частиною наркотичного вантажу або можливістю придбати його за зниженою ціною, після чого наркотики реалізуються на місцевому ринку.

Окремо аналізується роль насильницьких екстремістських організацій, насамперед JNIM та IS Sahel. GI-TOC застерігає від перебільшеного трактування так званого «нарко-джихадистського» зв'язку: ці організації не розглядаються як основні організатори транскордонного кокаїнового бізнесу. Водночас вони можуть отримувати від нього фінансову вигоду через оподаткування транзиту, забезпечення безпечного проходу або логістичну участь. Особливо помітним стало посилення ролі IS Sahel після 2023 року. Розширення територіального контролю угруповання в регіоні Менака та перенаправлення туди маршрутів із Гао створили для нього додаткові можливості отримувати платежі від наркотрафіку. За інформацією низки джерел, на окремих ділянках IS Sahel уже може бути безпосередньо інтегрований у логістику перевезень. Водночас автори уточнюють, що кокаїнова торгівля залишається лише одним із джерел доходів JNIM та IS Sahel, тоді як викрадення людей і золотодобувний сектор, імовірно, мають для їхнього фінансування більше значення.

Висновки:

- **Є необхідність у посиленні фінансових розслідувань щодо наркоторгівлі та пов'язаних із нею мереж.** Основну увагу слід приділяти не лише перевізникам, а й особам, які забезпечують політичний захист, фінансовим посередникам, які пов'язані з компаніями та активами.
- **Потрібно розширити міжнародний обмін інформацією вздовж усього маршруту кокаїну.** Необхідна тісніша координація між правоохоронними органами Латинської Америки, Західної і Північної Африки та Європи.
- **Необхідно враховувати зв'язок наркотрафіку з конфліктним фінансуванням і державними структурами.** Доходи від кокаїну підтримують окремі збройні угруповання, а великі поставки часто залежать від політичного та силового захисту.
- **Є необхідність у посиленні контролю за використанням приватної авіації.** Потрібен кращий моніторинг приватних літаків, другорядних аеродромів і транскордонних авіамаршрутів, які можуть використовуватися для перевезення великих партій кокаїну.

Ще однією характерною рисою досліджуваних мереж є їхня полікримінальність. Великі посередники одночасно можуть бути залучені до торгівлі кокаїном, канабісом, золотом, пальним, сигаретами та легального підприємництва. Це значно підвищує їхню стійкість: якщо один незаконний ринок або маршрут стає занадто ризикованим, вони можуть тимчасово перейти до іншої діяльності, не втрачаючи логістичних, фінансових та політичних зв'язків, а згодом повернутися до кокаїнового бізнесу. Саме цим частково пояснюється збереження ключових кримінальних акторів протягом десятиліть.

Окремою проблемою звіт визначає використання загальної та приватної авіації. Слабкий контроль другорядних аеродромів, наявність неформальних злітно-посадкових смуг та практика польотів із вимкненими транспондерами створюють умови для непомітного транспортування великих партій. Показовим став випадок вересня 2024 року, коли в Гвінеї-Бісау було вилучено

2,6 тонн кокаїну з приватного літака, який, за даними розслідування, спочатку мав прямувати до Бамако. Автори також вказують на використання авіації для переміщення наркотиків усередині Західної Африки. Через високу непрозорість приватної авіації та недостатній моніторинг повітряного простору GI-TOC розглядає цей напрям як значну розвідувальну прогалину та припускає його подальше розширення, особливо якщо наземні маршрути ставатимуть дедалі небезпечнішими.

У підсумку доповідь характеризує кокаїновий транзит через Сахель і Лівію не просто як проблему незаконного обігу наркотиків, а як складову ширшої економіки конфлікту та кримінально-політичної системи. Торгівля кокаїном зміцнює системи покровительства, спотворює роботу силових і державних інституцій, створює доходи для збройних акторів і підтримує взаємозалежність між кримінальними мережами, політичними елітами та структурами безпеки. У перспективі GI-TOC очікує збереження значення кокаїнових доходів для окремих збройних формувань, можливого посилення фінансової вигоди IS Sahel від контролю маршрутів, ризику подальшого проникнення кримінальних інтересів у державні структури, консолідації кримінально пов'язаних центрів впливу в Лівії та розширення використання загальної авіації. Саме тому запропонована відповідь має виходити за межі вилучення наркотиків і блокування окремих маршрутів. Автори наголошують на необхідності посилення правоохоронного та розвідувального співробітництва між Латинською Америкою, Західною і Північною Африкою та Європою, застосування адресних санкцій, обмежень на пересування і замороження активів не лише щодо безпосередніх наркоторговців, а й щодо їхніх фінансових та інших фасилітаторів, а також усунення інформаційних прогалин щодо використання приватної авіації. Фактично ключовий підхід доповіді полягає в необхідності протидіяти не лише фізичному переміщенню кокаїну, а всій екосистемі політичного захисту, фінансування, легалізації доходів, збройного контролю та інституційного сприяння, яка забезпечує стійкість транссахельського кокаїнового ринку.

Санкції Великої Британії проти Росії: нові ризики обходу обмежень та виклики для фінансового моніторингу [8]

Документ присвячений аналізу санкційного пакета Сполученого Королівства, запровадженого 6 серпня 2026 року проти 19 російських фізичних осіб, юридичних осіб і суден, а також його практичному значенню для систем фінансового моніторингу, санкційного комплаєнсу та протидії фінансовим злочинам. До пакета включено шість російських банків, шість нафтових танкерів, чотири компанії, які імпортують метали, що використовуються у військовому виробництві, дві компанії морського сектору та одну фізичну особу. При цьому автори документа наголошують, що санкційне включення саме по собі не означає встановлення факту відмивання коштів щодо кожної із зазначених осіб чи компаній. Значення цих заходів для ПВК/ФТ полягає насамперед у тому, що вони істотно змінюють ризиковий профіль операцій, пов'язаних із російськими платежами, морською торгівлею, стратегічними товарами, непрямими структурами власності та можливим обходом встановлених обмежень.

Окрему увагу приділено шести російським банкам – Ozon Bank, Realist Bank, Teleport Bank, Bank Stavr, Center-Invest та State Specialised Russian Export-Import Bank. До них застосовано заморожування активів, обмеження щодо трастових послуг, заходи з обмеження щодо обіймання посад директорів компаній, а також заборони, пов'язані з кореспондентськими відносинами та обробленням платежів. Для британських кредитних і фінансових установ це означає неможливість встановлювати або продовжувати кореспондентські відносини з такими установами та здійснювати платежі до них, від них або через них, якщо відповідна операція не підпадає під передбачений виняток або ліцензію. Водночас документ підкреслює, що

[8] https://fincrimecentral.com/uk-sanctions-russian-banks-shadow-fleet-aml/#shadow-fleet-exposure-extends-beyond-vessel-name-screening

санкційний банк може бути присутнім у транзакції не лише як безпосередній відправник чи отримувач коштів, а й як банк-посередник, кореспондент, установа відшкодування, постачальник платіжних послуг або інший непрямий учасник складного платіжного ланцюга. Додаткову складність створюють альтернативні та історичні назви банків, різні варіанти транслітерації, зміни маршрутів платежів і неповні платіжні повідомлення. Зокрема, Ozon Bank може також фігурувати як Ekom Bank, Ecom Bank або Oney Bank, Teleport Bank – як MTI Bank, a State Specialised Russian Export-Import Bank – як Exim Bank, Eximbank of Russia або Roseksim Bank. Це означає, що скринінг, побудований лише на одному офіційному англомовному найменуванні, може бути недостатнім для ефективного виявлення санкційного зв'язку.

У зв'язку з цим установам рекомендується оновлювати не лише клієнтські санкційні бази, а й платіжні фільтри, довідники банківських ідентифікаторів, репозиторії контрагентів, системи торговельного фінансування та інформацію про кореспондентські відносини. Окремо підкреслюється необхідність ретроспективного перегляду операцій, якщо раніше проводилися транзакції за участю новопризначених банків або пов'язаних із ними осіб. Водночас санкційний збіг не повинен автоматично трактуватися як доказ відмивання коштів. Натомість більш значущими з позиції фінансового моніторингу є спроби приховати участь санкційного банку, перенаправити операцію через іншу фінансову установу або використати новоствореного посередника. За відсутності зрозумілого економічного сенсу або у разі невідповідності такої поведінки встановленому профілю клієнта це може стати підставою для поглибленого аналізу на предмет можливого обходу санкцій або іншої підозрілої фінансової діяльності.

Значний блок документа присвячено так званому «тіньовому флоту». До санкційного пакета включено танкери Asteras, Perseas, Torvian, Visund, Zenturo та Arctic Express, а також Frion Ship Management LLP і Northern Engineering Limited Liability Company. У цьому контексті наголошується, що перевірка лише за назвою судна є недостатньою, оскільки судна можуть змінювати назву, прапор, зареєстрованого власника, комерційного оператора або компанію, відповідальну за управління. Більш надійним ідентифікатором вважається номер IMO, який, як правило, зберігається за судном протягом усього строку його експлуатації. Фінансові установи та інші відповідні суб'єкти повинні аналізувати не лише саме судно, а весь комерційний ланцюг перевезення, включаючи власника, оператора, технічного менеджера, фрахтувальника, платника фрахту, продавця та покупця вантажу, брокера, страховика, портового агента і банки, що забезпечують розрахунки. Таким чином, відсутність санкційного статусу у безпосереднього клієнта не усуває ризик, якщо санкційна сторона присутня на іншому рівні логістичної або фінансової структури.

Особливу увагу документ звертає на фрагментацію платежів, пов'язаних із транспортуванням нафти. Одна комерційна операція може бути розподілена між платежами за фрахт, страхування, бункерування, портові послуги, зберігання та безпосередньо за вантаж. Якщо такі платежі аналізуються окремо, без встановлення їхнього зв'язку з конкретним рейсом або вантажем, фінансова установа може не побачити загальної картини. Саме тому рекомендується поєднувати фінансову інформацію з даними про судно, маршрут, вантаж і контрагентів. Серед індикаторів підвищеного ризику визначено незрозумілі зміни власності безпосередньо перед рейсом, використання нещодавно створених компаній без усталеної історії роботи в морській галузі, багаторазову зміну прапора, непрозорі структури управління, а також проведення платежів через юрисдикції, які не мають очевидного зв'язку з походженням або пунктом призначення вантажу. Додатковими сигналами є невідповідності в ідентифікаторах суден, датах завантаження, цінах і незрозуміла роль окремих учасників операції. Документ застерігає, що кожен такий індикатор окремо не доводить протиправну поведінку, однак їх сукупність, особливо у поєднанні з російським походженням товарів або зв'язками із санкційними банками, суднами чи компаніями, може вимагати ескалації перевірки.

Важливим висновком у цьому контексті є недостатність виключно стандартної належної перевірки клієнта. Навіть якщо установа провела належну перевірку безпосереднього клієнта, додатковий санкційний або фінансовий ризик може виникнути через судно, власника вантажу, платіжного посередника чи іншу сторону, яка з'являється вже після встановлення ділових відносин. Саме тому документ обґрунтовує необхідність подієво-орієнтованого перегляду ризику, особливо після оновлення санкційних переліків або зміни істотних характеристик торговельної операції.

Ще один напрям аналізу стосується військово значущих ланцюгів постачання та ризиків непрямих платежів. До санкційного переліку включено компанії Metallkomplekt, Nikom, Technolux і Promsiz, які імпортують тантал і ніобій – метали, визначені британською владою як критично важливі для виробництва військового обладнання. Також санкції застосовано до особи – Alexander Aleksandrovich Zhdanov у зв'язку з його володінням компанією Siltron, що працює в російському хімічному секторі. Фінансовий ризик у цьому випадку не обмежується прямими платежами зазначеним особам або компаніям. Операції можуть здійснюватися через дистриб'юторів, закупівельних агентів, експедиторів, митних брокерів, афілійовані компанії або постачальників із третіх країн. Санкційна сторона може бути взагалі відсутня в рахунку-фактурі, хоча фактично отримувати товари, кошти або іншу економічну вигоду.

У таких випадках посилений аналіз повинен встановлювати фактичний предмет закупівлі, виробника товару, місце його доставки, кінцевого користувача та наявність у клієнта обґрунтованої комерційної потреби у відповідній продукції. Загальні описи на кшталт «промислові компоненти», «сировина» або «технічне обладнання» можуть бути недостатніми, якщо реальний товар має стратегічне або подвійне призначення. Для перевірки обґрунтованості операції рекомендується зіставляти рахунки-фактури, договори, транспортні документи, митну інформацію та платіжні інструкції. Особливу увагу слід приділяти розбіжностям між покупцем, вантажоодержувачем, платником та кінцевим користувачем, а також ситуаціям, коли у вже сформований ланцюг постачання раптово вводиться нещодавно створена компанія. Додатковим ризиком є зміна після встановлення ділових відносин пунктів отримання товарів або бенефіціарів платежів.

Документ окремо розглядає питання власності та контролю. Санкційні обмеження можуть поширюватися не лише на суб'єктів, прямо включених до публічного переліку, а й на юридичних осіб, якими санкційна особа прямо або опосередковано володіє чи які вона контролює. Водночас оцінка не повинна зводитися лише до механічного застосування формального порогу корпоративної власності. Наявна інформація може свідчити про фактичну можливість санкційної особи визначати діяльність юридичної особи навіть без володіння більшістю корпоративних прав. Для такої оцінки можуть бути релевантними корпоративні документи, домовленості щодо голосування, управлінські функції, фінансові відносини та інші докази фактичного впливу.

Окреме методологічне значення має розмежування санкційного та AML-реагування. Документ наголошує, що ці два процеси повинні взаємодіяти, але мають різні правові цілі. Повідомлення до Управління з імплементації фінансових санкцій Великої Британії (OFSI) стосується, зокрема, встановлення або підозри щодо підсанкційної особи, заморожених активів чи можливого порушення санкційного режиму. Натомість повідомлення про підозрілу діяльність стосується знання або підозри щодо відмивання коштів чи фінансування тероризму. Залежно від фактичних обставин одна й та сама операція може потребувати оцінки та реагування в межах обох режимів, однак застосування одного механізму звітності не замінює необхідності розгляду іншого.

У заключній частині документа підкреслюється необхідність оперативного переналаштування систем контролю з огляду на швидкість розширення санкційного режиму. На дату оголошення пакета 6 серпня 2026 року британські санкції вже охоплювали понад 3 400 фізичних осіб, юридичних осіб і суден, причому понад 500 цілей було додано протягом 2026 року. За таких умов періодичний санкційний скринінг розглядається як недостатній для установ, що

обробляють міжнародні платежі або фінансують торгівлю товарами. Першочерговими завданнями залишаються виявлення прямих санкційних збігів, заморожування відповідних активів, припинення заборонених операцій і подання необхідних повідомлень. Водночас більш складним завданням фінансового моніторингу є встановлення того, чи намагалися клієнти або посередники передбачити майбутні санкційні заходи, приховати зв'язок із санкційними особами або змінити структуру операцій з метою обходу обмежень. У цьому контексті особливої уваги потребують операції, здійснені безпосередньо перед включенням особи до санкційного переліку, раптове закриття рахунків, зміни валюти розрахунків, заміна звичного банку маловідомою фінансовою установою, відхилені платежі, вручну скасовані спрацювання систем контролю та платіжні інструкції, змінені після санкційного скринінгу.

Загальний підхід, запропонований у документі, полягає у переході від формального пошуку окремих санкційних назв до комплексного аналізу взаємопов'язаних фінансових, корпоративних, торговельних і логістичних даних. Ефективна система контролю повинна поєднувати інформацію про клієнта, бенефіціарну власність і контроль, маршрути платежів, торговельну документацію та відомості про судна. Ізольовані системи можуть виявити окремий санкційний збіг, але не розпізнати скоординоване переміщення вартості через декілька компаній, банків і транспортних активів. Тому особливого значення набуває мережевий аналіз, який дозволяє виявляти спільних директорів, адреси, контактні дані, контрагентів і платіжних посередників між формально незалежними суб'єктами. У підсумку значення розглянутого санкційного пакета для ПВК/ФТ полягає не в автоматичному ототожненні санкційного статусу з відмиванням коштів, а в необхідності значно глибше оцінювати ризики приховування, використання посередників, непрямих структур власності та контролю і можливого обходу санкцій через зовні легітимні фінансові та комерційні операції.

Висновки:

- **Актуалізація санкційного скринінгу і платіжний моніторинг.** Необхідно враховувати не лише нові санкційні банки та компанії, а й альтернативні назви, посередників, кореспондентські зв'язки та непрямі платіжні маршрути.
- **Аналіз повного ланцюга операції, а не лише безпосереднього клієнта.** Особливу увагу слід приділяти власникам і операторам суден, контрагентам, платіжним посередникам, вантажу, маршрутам постачання та кінцевим користувачам.
- **Посилення виявлення схем обходу санкцій.** Ризик-індикаторами можуть бути раптова зміна банку, посередника, валюти, маршруту платежу, власника судна, дроблення платежів або поява новостворених компаній у ланцюгу операції.
- **Забезпечення паралельного застосування санкційних та AML-процедур.** Виявлення санкційного зв'язку потребує окремої оцінки щодо заморожування активів і санкційної звітності, тоді як ознаки приховування або обходу обмежень мають додатково оцінюватися з позиції підозрілої фінансової діяльності.

Режими фінансових санкцій у Європі та ризики для неприбуткових організацій [9]

Сучасний ландшафт міжнародних фінансових санкцій формує складне та багатошарове середовище, в якому неприбуткові організації, зокрема благодійні фонди, що надають гуманітарну допомогу в зонах конфліктів, змушені діяти з надзвичайною обережністю. Фінансові санкції, будучи одним із найвпливовіших інструментів зовнішньої політики, ґрунтуються на блокуванні активів визначених осіб та забороні надання їм коштів або економічних ресурсів. Для сектору неприбуткових організацій це створює низку унікальних викликів, які виходять далеко за межі простого юридичного дотримання норм.

[9] https://www.global-amlcft.eu/financial-sanctions-europe/?cn-reloaded=1

Особливо гостро ці питання постають у контексті європейських юрисдикцій, таких як Велика Британія, Франція та Німеччина, де режими санкцій постійно розвиваються, а регуляторний тиск на неприбутковий сектор зростає, що безпосередньо впливає на оцінку ефективності в рамках Рекомендації 8 Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF).

Особливу увагу в цьому контексті привертає еволюція самої Рекомендації 8 FATF, яка зазнала суттєвих змін у листопаді 2023 року. Ці зміни стали реакцією на багаторічну практику непропорційного застосування заходів до всього неприбуткового сектору, що призводило до обмеження їхньої діяльності, втрати доступу до банківських послуг та загального зниження спроможності виконувати свої місії.

Оновлена редакція Рекомендації 8 та її Пояснювальної записки чітко наголошує на необхідності зосередженого, пропорційного та ризик-орієнтованого підходу, який не повинен перешкоджати законній діяльності неприбуткових організацій. Цей сигнал є надзвичайно важливим, оскільки він визнає системну проблему, коли надмірне регулювання, спрямоване на боротьбу з тероризмом, фактично підриває здатність цивільного суспільства діяти у найбільш вразливих регіонах світу. Запровадження FATF у липні 2025 року нової процедури, що дозволяє країнам та міжнародним фінансовим установам порушувати питання про ненавмисні наслідки застосування стандартів, які порушують діяльність неприбуткових організацій, свідчить про визнання цих ризиків на найвищому рівні та прагнення до більш збалансованого регулювання.

Взаємозв'язок між технічною відповідністю Рекомендації 8 та її ефективністю, що вимірюється через Безпосередній результат 10 (IO10), набуває критичного значення саме у контексті фінансових санкцій. IO10 оцінює, чи дійсно запобігається зловживанню неприбутковим сектором терористами, а не лише чи існують відповідні закони. У цьому сенсі перевірка санкційних списків неприбутковими організаціями стає не просто формальністю, а ключовим елементом практичної архітектури досягнення цього результату. Якщо неприбуткова організація ненавмисно переказує кошти визначеній особі, це свідчить про провал її внутрішніх процедур; але якщо держава не забезпечила належного керівництва або нагляду за сектором, це може бути розцінено як неефективність за IO10. Таким чином, режими фінансових санкцій перебувають на перетині технічних зобов'язань та реальних результатів, і саме цей аспект буде ретельно досліджуватися під час п'ятого раунду взаємних оцінок FATF, який розпочався у 2024 році із застосуванням оновленої методології, що акцентує увагу на практичних наслідках.

Розглянемо детальніше ситуацію у Сполученому Королівстві, де основою санкційного режиму є Закон про санкції та боротьбу з відмиванням грошей 2018 року. Цей закон надає Управлінню з питань впровадження фінансових санкцій (OFSI) широкі повноваження щодо адміністрування та забезпечення виконання санкцій, і, що особливо важливо, встановлює принцип суворої відповідальності без необхідності доведення умислу. Для благодійних організацій це означає, що навіть ненавмисна взаємодія з визначеними особами може мати серйозні наслідки, включно з цивільними штрафами.

Статистика OFSI демонструє зростаючу інтенсивність правозастосовної діяльності: у 2024-2025 роках було відкрито 240 активних справ, з яких 151 було ідентифіковано завдяки проактивним розслідуванням, що значно більше порівняно з попереднім періодом. Примітно, що протягом цього періоду було застосовано санкції безпосередньо до трьох благодійних організацій, що свідчить про те, що увага регулятора до цього сектору значно посилилася. Для організацій, які працюють у зонах конфліктів або в країнах, що перебувають під комплексними санкціями, ризик випадкового контакту з підсанкційними особами є структурно підвищеним, і саме цей фактор, у поєднанні з політикою банків щодо відмови від обслуговування високоризикових клієнтів, створює майже непереборні виклики для сектору.

Французький підхід до регулювання фінансових санкцій, як члена Європейського Союзу, базується на прямому застосуванні регламентів ЄС, що є обов'язковими без необхідності

національної імплементації, доповнених національним режимом замороження активів, закріпленим у Валютному та фінансовому кодексі. Генеральна дирекція казначейства (DG Trésor) підтримує національний реєстр заходів замороження, а регуляторний нагляд здійснюється спільно з Органом з питань (ACPR) та ПФР (TRACFIN). Для французьких асоціацій, які є основною правовою формою неприбуткових організацій, ключовим обов'язком є перевірка контрагентів за об'єднаним списком ЄС та національним реєстром, з подальшим повідомленням про будь-які збіги до TRACFIN.

Хоча прямі статистичні дані щодо порушень у неприбутковому секторі обмежені, загальна активність французької системи боротьби з відмиванням грошей та фінансуванням тероризму є надзвичайно високою. Про це свідчить рекордна кількість повідомлень про підозрілі операції, поданих до TRACFIN у 2023 році, що зросла на 15% порівняно з попереднім роком, а також активізація практики блокування підозрілих фінансових операцій, що свідчить про загальне посилення контролю. Це створює додаткове регуляторне навантаження на асоціації, які, навіть діючи з добрими намірами, можуть бути втягнуті у складні перевірки та звітні процедури.

Німецька система, подібно до французької, застосовує санкції ЄС безпосередньо, з додатковим національним регулюванням через Закон про зовнішню торгівлю та платежі. Проте Німеччина зробила значний крок вперед у грудні 2022 року, ухваливши Другий закон про забезпечення виконання санкцій, який суттєво посилив архітектуру правозастосування. Цей закон створив Центральний департамент із забезпечення виконання санкцій (ZfS), наділивши його повноваженнями проводити розслідування щодо заморожених активів та забезпечувати виконання заборон на надання коштів.

Адміністрування санкцій розподілено між Німецьким федеральним банком, який обробляє повідомлення від банків та розглядає заяви на отримання ліцензій, та Федеральним відомством з питань економіки та контролю за експортом (BAFA), що відповідає за економічні санкції. Важливою особливістю є те, що кримінальне переслідування за порушення санкцій здійснюється через прокуратури, і, як свідчать оприлюднені дані, уже є випадки конфіскації активів на десятки мільйонів євро.

Незважаючи на те, що взаємна оцінка FATF 2022 року визнала нагляд Німеччини за сектором неприбуткових організацій сильним та пропорційним, виклики залишаються, особливо у сфері координації численних наглядових органів та забезпечення послідовного ризик-орієнтованого підходу. Крім того, нещодавнє відкриття Європейською комісією процедури порушення через неімплементацію директиви про мінімальні стандарти кримінальних покарань за порушення санкцій вказує на те, що навіть така потужна система не є статичною і потребує постійного вдосконалення.

Аналіз цих трьох юрисдикцій виявляє три структурні теми, які формують сучасний ландшафт застосування фінансових санкцій до неприбуткового сектору. По-перше, це принцип суворої відповідальності, який діє в усіх розглянутих країнах і покладає на організації тягар забезпечення того, щоб жодні кошти не потрапили до підсанкційних осіб, незалежно від їхніх намірів. Це вимагає від неприбуткових організацій, особливо невеликих, значних ресурсів для впровадження систем перевірки та моніторингу, що часто є непосильним завданням.

По-друге, явище «дерискінгу» з боку банків, які відмовляються обслуговувати організації, що діють у високоризикових регіонах, створює серйозну перешкоду для доступу до формальної фінансової системи. Це явище, яке FATF визначила як ненавмисний наслідок надмірного застосування санкцій, безпосередньо суперечить духу оновленої Рекомендації 8, оскільки фактично виштовхує гуманітарну діяльність у неформальні канали, збільшуючи ризики, а не зменшуючи їх.

По-третє, наявність ліцензійних механізмів, які дозволяють обійти загальні заборони для гуманітарних операцій, є критичним елементом пропорційності. У кожній з країн існують такі механізми, але їхня доступність, ефективність та передбачуваність є вирішальними для того,

чи дозволяють вони організаціям діяти легально та прозоро, чи змушують їх шукати обхідні шляхи.

У підсумку, оновлена Рекомендація 8 FATF, разом із супутніми документами, задає чіткий вектор для держав: надмірне регулювання всього неприбуткового сектору є неприйнятним, і країни повинні перейти до зосередженого, пропорційного та ризик-орієнтованого нагляду. Дані правозастосування з Великої Британії, статистика операційної діяльності з Франції та посилена правозастосовна архітектура Німеччини свідчать про те, що увага до неприбуткового сектору зростає, і комплаєнс стає не просто рекомендацією, а суворою вимогою.

Водночас, ці ж режими демонструють, що ефективне досягнення Безпосереднього результату 10 неможливе без забезпечення доступності ліцензійних механізмів, чіткого керівництва з боку регуляторів та ефективної міжвідомчої координації. Майбутнє регулювання залежатиме від здатності держав знайти тонкий баланс: гарантувати цілісність фінансової системи, не дозволяючи терористам зловживати неприбутковим сектором, і водночас виправити шкоду, завдану десятиліттям непропорційного застосування стандартів FATF.

Практичний висновок для неприбуткових організацій є очевидним: регуляторне середовище стає одночасно більш вимогливим у своїх очікуваннях щодо правозастосування та більш диференційованим у своєму підході до ризиків. Це вимагає активного та інформованого залучення, регулярного моніторингу змін у нормативному середовищі та готовності інвестувати в комплаєнс-системи, які дозволять не лише вижити, але й продовжувати виконувати благородну місію з надання допомоги тим, хто її найбільше потребує, у найскладніших куточках світу.

Висновки:

- **Принцип суворої відповідальності створює непропорційний тягар для НПО.** В Англії, Франції та Німеччині відповідальність за контакти з підсанкційними особами настає незалежно від намірів, що вимагає від благодійних організацій значних комплаєнс-ресурсів і робить їх вразливими.
- **Оновлена Рекомендація 8 FATF зміщує фокус від тотального контролю до ризик-орієнтованого підходу.** Реформи 2023–2025 років чітко забороняють державам застосовувати надмірні заходи до всього сектору НПО, натомість вимагаючи адресного нагляду.
- **Правозастосовна активність щодо НПО в Європі зростає.** Дані OFSI (Велика Британія) фіксують конкретні санкційні заходи проти благодійних організацій, а Німеччина суттєво посилила інституційну спроможність через створення Центрального департаменту із забезпечення виконання санкцій (ZfS).
- **Ефективність режиму оцінюється не за наявністю законів, а за реальними результатами.** У новому раунді взаємних оцінок FATF ключовим критерієм буде те, чи дійсно система запобігає зловживанню НПО, не блокуючи при цьому законну гуманітарну діяльність, і саме цей баланс залишається найскладнішим викликом.

Нова ера цифрових активів, яку фінансові установи не можуть ігнорувати [10]

Після багатьох років регулювання, що здійснювалося переважно через правозастосовні заходи за відсутності формальних правил, американські фінансові регулятори нарешті накреслили чітку мапу.

17 березня 2026 року Комісія з цінних паперів та бірж США (SEC) і Комісія з торгівлі товарними ф'ючерсами (CFTC) опублікували Спільний тлумачний лист № 33-11412 – 68-сторінковий документ, який встановлює першу офіційну таксономію для класифікації цифрових активів згідно з федеральним законодавством США . Цей документ визначає п'ять

[10] https://fintech.global/2026/08/05/digital-asset-compliance-gaps-firms-cant-ignore/

категорій цифрових активів і чітко розмежовує юрисдикційні повноваження, що стало поворотним моментом для комплаєнс-офіцерів у всій фінансовій індустрії.

Запроваджена регуляторами класифікація ґрунтується на характеристиках, функціях і використанні цифрових активів, а не на тому, як емітенти обирають їх маркувати.

Цифрові товари, вартість яких визначається функціонуванням системи цифрових активів, а не управлінськими зусиллями, підпадають під нагляд CFTC. До цієї категорії належать Bitcoin, Ethereum, Solana, XRP, Chainlink та ще 11 активів, названих у документі.

Цифрові колекційні предмети, включно з NFT та мемкоїнами, а також цифрові інструменти, такі як токени членства та облікові дані, не вважаються цінними паперами.

Стейблкоїни, які відповідають вимогам Закону GENIUS, виокремлюються як платіжні інструменти, що регулюються банківськими органами влади.

Найбільше комплаєнс-навантаження лягає на п'яту категорію – цифрові цінні папери, які випускаються як інвестиційні контракти з очікуванням прибутку та включають токенізовані цінні папери: традиційні фінансові інструменти, такі як акції, облігації та ETF, що випускаються, торгуються та розраховуються на блокчейні.

Ринок токенізованих цінних паперів уже давно вийшов за межі концептуальних обговорень і став реальністю, з якою фінансові установи мусять рахуватися. У березні 2026 року SEC схвалила зміну правил Nasdaq, яка дозволяє торгівлю токенізованими цінними паперами. Це рішення побудоване на пілотній програмі токенізації Депозитарної трастової компанії (DTC), яка діяла на підставі листа про відсутність заперечень з грудня 2025 року. До переліку дозволених інструментів увійшли індекси Russell 1000, казначейські облігації США та провідні індексні ETF. Нью-Йоркська фондова біржа (NYSE) невдовзі пішла тим самим шляхом, уклавши партнерство з Securitize для створення нової блокчейн-платформи, а Securitize було визнано першим цифровим трансфер-агентом, уповноваженим випускати токенізовані акції та ETF. Це не просто експерименти – це промислові впровадження двома найбільшими фондовими біржами світу, які демонструють остаточний перехід токенізації з теоретичної площини в практичну .

Треті сторонні кастодіальні моделі вже забезпечують значні обсяги торгів, що робить виклики комплаєнсу ще більш нагальними. Продукт Kraken xStocks, створений на базі інфраструктури придбаної компанії Backed Finance, з моменту запуску в червні 2025 року перевищив $25 млрд сукупного обсягу торгів. Наразі продукт охоплює 100 токенізованих американських акцій та ETF із планами розширення до 500 до кінця року. Ці токени, які забезпечені базовими акціями у співвідношенні 1:1, не надають акціонерних прав, таких як голосування – власники мають лише економічний інтерес та вимоги до кредитора перед емітентом. Вони торгуються 24/5 на Kraken і 24/7 на блокчейні після виведення на гаманець. Dinari, перша платформа, яка отримала реєстрацію брокера-дилера США для токенізованих акцій, працює за аналогічною моделлю на кількох блокчейнах у партнерстві з Gemini та Flow Traders. Ondo Global Markets пропонує токенізований доступ до понад 200 американських акцій. Ці приклади ілюструють, що токенізовані цінні папери стають невід'ємною частиною фінансового ландшафту, створюючи нові операційні реалії, які вимагають негайної уваги з боку комплаєнс-підрозділів.

Найважливіший меседж, який SEC проголошує з граничною чіткістю, полягає в тому, що токенізація змінює інфраструктуру, а не регуляторний периметр. Токенізована акція залишається акцією для цілей зобов'язань щодо особистої торгівлі. Вимоги щодо обмежених списків, правила попереднього погодження угод і заборони на використання матеріальної нерозголошеної інформації застосовуються незалежно від того, чи торгується інструмент на Nasdaq чи на блокчейні.

Це створює три критичні операційні прогалини, які потребують негайного усунення. По-перше, архітектура обмежених списків: системи зіставлення тікерів не зможуть виявити токенізовані еквіваленти, які торгуються під іншими символами на майданчиках за межами

традиційного всесвіту стрічок котирувань. Списки мають базуватися на емітентах із відображенням на всі відомі форми інструментів .

По-друге, визначення підзвітних рахунків: політики, які посилаються на «брокерські рахунки», тепер мають прямо включати платформи токенізованих активів, адреси ончейн-гаманців, що використовуються для зберігання токенізованих цінних паперів, та рахунки на таких майданчиках, як Kraken xStocks, Dinari, Securitize та Ondo.

По-третє, потоки даних: традиційний моніторинг покладається на стандартизовані кастодіальні потоки, але деякі токенізовані платформи вже пропонують інтеграції, що відповідають вимогам комплаєнсу, тоді як інші вимагають ручного підтвердження, доповненого аналітикою блокчейну. Гібридний підхід залишається реалістичним на найближчі 18-24 місяців, але комплаєнс-менеджери не можуть зволікати з адаптацією своїх систем.

Цифрові активи дедалі глибше інтегруються в регульоване ядро фінансових ринків, і комплаєнс-команди стикаються з новими викликами, пов'язаними з інсайдерською інформацією, торговою активністю співробітників та конфліктами інтересів. Співробітники можуть тримати активи на десятках бірж, у кількох гаманцях і на різних блокчейнах, причому кожне джерело генерує дані в різних форматах, з різною періодичністю та різним рівнем деталізації. Комплаєнс-команда не може просто додати криптовалюти до існуючого механізму моніторингу та очікувати послідовних результатів.

Проблема фрагментації даних є однією з найбільших перешкод, оскільки один співробітник може тримати Bitcoin на одній біржі, Ethereum у браузерному гаманці, а стейблкоїни на третій платформі. Кожне джерело вимагає окремої інтеграції, і багато платформ не пропонують прямих потоків даних до інструментів моніторингу. Навіть там, де інтеграції існують, дані створюють проблеми – часові мітки транзакцій, ідентифікатори активів та типи діяльності можуть не збігатися в різних джерелах . Некастодіальні гаманці та ончейн-активність створюють особливі труднощі, оскільки співробітники, які тримають активи у таких рішеннях, контролюють власні приватні ключі, і жоден центральний орган не зберігає записи, до яких можна звернутися.

Токенізація цінних паперів створює додаткові практичні перешкоди, до яких більшість комплаєнс-програм ще не готові. Співробітники можуть не усвідомлювати, що гаманець MetaMask, Ledger або мобільний гаманець, здатний зберігати токенізовані цінні папери, кваліфікується як «покритий рахунок» . Якщо Кодекси етики не визначають це чітко, такі гаманці можуть легко бути пропущені в початкових і щорічних звітах про активи.

Смарт-контракти можуть бути розроблені для автоматичного розподілу дивідендів, обробки викупів або навіть реінвестування коштів, і кожна з цих подій з юридичної точки зору є транзакцією з цінними паперами, але без традиційної брокерської виписки вони можуть ніколи не з'явитися в квартальних звітах. Офшорні платформи створюють подібні ризики, коли співробітник, який торгує

Висновки:

- **Чіткі правила гри визначено.** SEC та CFTC затвердили офіційну класифікацію цифрових активів із чітким розмежуванням юрисдикцій, що знімає багаторічну невизначеність для фінансових установ.
- **Токенізовані цінні папери – це вже реальність.** Nasdaq та NYSE запустили торгівлю токенізованими акціями, а обсяги на платформах на кшталт Kraken xStocks перевищили $25 млрд, тому ігнорувати цей ринок більше неможливо.
- **Регуляторна сутність активу не змінюється.** Токенізована акція залишається акцією – всі вимоги щодо обмежених списків, попереднього погодження та боротьби з інсайдерською торгівлею діють незалежно від форми інструменту.
- **Існуючі комплаєнс-системи не готові.** Традиційні механізми моніторингу не враховують ончейн-адреси, альтернативні символи токенів та фрагментовані джерела даних, що створює критичні операційні прогалини.

токенізованими цінними паперами через неамериканський майданчик, може помилково вважати, що ця діяльність звільняється від звітності. Усунення цих прогалин вимагає оновлення Кодексів етики з чітким зазначенням, що токенізовані цінні папери є підзвітними цінними паперами, а блокчейн-гаманці кваліфікуються як покриті рахунки. Програми адаптації та щорічні сертифікації мають бути розширені для включення адрес гаманців, а шаблони квартальної звітності – адаптовані для включення полів для транзакцій у гаманцях і адрес контрактів. Навчання співробітників є критично важливим, оскільки без усвідомлення того, що токенізовані акції залишаються цінними паперами незалежно від форми, порушення комплаєнсу неминучі.

На завершення, запровадження п'ятикатегорійної таксономії цифрових активів забезпечує ясність, яку індустрія давно шукала . Виклик комплаєнсу тепер полягає не в неоднозначності, а в тому, чи мають комплаєнс-програми операційну спроможність бачити та контролювати інструменти, які вже торгуються.

Швидкість ринку токенізованих активів і децентралізована природа блокчейн-транзакцій вимагають нового підходу до комплаєнсу, який поєднує традиційні механізми контролю з інноваційними технологічними рішеннями.

Фінансові установи, які не адаптуються до цих змін, ризикують не лише регуляторними санкціями, але й втратою репутації та довіри клієнтів у світі, де цифрові активи стають невід'ємною частиною фінансової системи. Інвестиції в комплаєнс-інфраструктуру, здатну відстежувати цифрові активи в різних середовищах, оновлення внутрішніх політик і навчання персоналу є не просто рекомендацією, а необхідністю для виживання в новій регуляторній реальності.

Інші новини

Безпрецедентний злом Coldcard: як помилка в коді призвела до втрати 116 мільйонів доларів [11]

Інцидент, що стався наприкінці липня 2026 року з апаратним гаманцем Coldcard, є знаковим випадком, який підриває саму філософію самостійного зберігання (self-custody) віртуальних активів.

Ця атака, яка наразі оцінюється як третя за масштабом у 2026 році, продемонструвала, що навіть «холодне» зберігання, яке вважалося золотим стандартом безпеки, може бути вразливим до віддалених атак, якщо базовий процес генерації ключів має фатальні недоліки.

За даними TRM Labs та Galaxy Research, загальна сума викрадених коштів перевищує 1 816 біткойнів, що на момент атаки становило близько 116 мільйонів доларів США, а кількість постраждалих адрес сягає понад 5 200. Цей випадок змушує переглянути уявлення про надійність апаратних рішень і підкреслює критичну важливість кожного етапу створення гаманця.

Корінь проблеми сягає березня 2021 року, коли компанія Coinkite випустила версію прошивки 4.0.1. Саме в ній містилася помилка конфігурації збірки, яка мала руйнівні наслідки. Замість того, щоб використовувати апаратний генератор випадкових чисел (HRNG), який є фізичним джерелом ентропії в самому пристрої, збірка за умовчанням зверталася до слабкого програмного генератора псевдовипадкових чисел. Це призвело до катастрофічного зниження ефективної стійкості ключів зі 128 біт, як було заявлено в специфікації, до 40 біт на деяких пристроях. Така довжина ключа робить його вразливим до «brute force» (підбору ключа методом перебору) з використанням сучасних обчислювальних потужностей, причому для цього зловмисникові навіть не потрібно мати фізичного доступу до гаманця. Важливо

[11] https://www.trmlabs.com/resources/blog/the-largest-hardware-wallet-exploit-of-2026-inside-the-usd-116-million-coldcard-hack

розуміти, що оновлення прошивки виправляє цю проблему лише для майбутніх гаманців, але жодним чином не підвищує захист seed-фраз, згенерованих у вразливий період.

Атака розпочалася 30 липня 2026 року і тривала хвилями протягом чотирьох днів. Перший удар був стрімким: за 25 хвилин зловмисник вивів близько 594 BTC (майже 38 мільйонів доларів) з приблизно 500 адрес, консолідувавши їх на одній адресі. Це було лише початком. За ним послідували ще три хвилі виведення коштів, а на момент складання звіту TRM Labs четверта хвиля все ще перебувала в пулі, що свідчить про те, що остаточні цифри втрат можуть бути значно вищими.

Аналіз ланцюжків блоків, проведений експертами TRM, виявив цікаву закономірність: більшість викрадених коштів осіла на невеликій кількості адрес, підконтрольних зловмиснику. На противагу типовій поведінці професійних хакерських угруповань, на кшталт північнокорейського TraderTraitor, які починають агресивне відмивання коштів протягом кількох годин, у цьому випадку спостерігається мінімум активності. Є лише один депозит на 64.9 BTC у мікшері Wasabi та внесок 200 ETH у Tornado Cash 4 серпня. Решта транзакцій обмежується одним додатковим кроком консолідації, без спроб створення складних багаторівневих схем для приховування слідів. Така поведінка наштовхує дослідників на думку, що або зловмисники ще планують свої подальші дії, або ж до справи причетні різні групи, які діють неузгоджено.

Аналіз ончейн-даних також розкриває ще один цікавий аспект – комунікацію, що відбувається безпосередньо в блокчейні. Дослідження полів OP_RETURN показало численні спам-повідомлення, адресовані хакерам. Серед них були пропозиції відмити викрадені кошти за комісію в розмірі 7%, з контактними даними в месенджері Telegram. Це яскраво ілюструє, наскільки швидко екосистема криптовалютного шахрайства та незаконних послуг реагує на великі крадіжки, намагаючись отримати вигоду з хаосу та запропонувати свої «послуги» безпосередньо через публічний реєстр транзакцій.

Наслідки цього злому виходять далеко за межі конкретної суми втрачених коштів. Цей випадок завдає серйозного удару по довірі до концепції самостійного зберігання, яка є наріжним каменем криптовалютної філософії. Він наочно демонструє, що самостійне зберігання не усуває ризики, а лише переміщує їх з однієї площини в іншу.

Відтепер для користувачів стає очевидним, що безпека гаманця визначається не лише тим, де зберігаються приватні ключі, а й тим, як вони були згенеровані. Це підкреслює необхідність ретельного аудиту не лише вихідного коду, а й процесів збору ентропії.

У звіті TRM Labs наголошується на важливості використання мультипідписних схем, які комбінують незалежно розроблені пристрої та незалежно згенеровану ентропію, що створює значний захист за рахунок диверсифікації та зменшує залежність від єдиного слабкого місця.

Для всіх користувачів Coldcard, які створили свою seed-фразу в період з березня 2021 року до моменту виходу патчу, рекомендація однозначна: seed є скомпрометованим, незалежно від того, чи була оновлена поточна прошивка. Єдиним правильним рішенням є генерація нової адреси на пристрої з найновішою прошивкою, ретельна перевірка відбитку нового гаманця та перенесення коштів, починаючи з невеликої тестової транзакції.

Відсутність чітких слідів відмивання та різниця в побудові транзакцій між хвилями атаки залишають відкритим питання про те, хто саме стоїть за цим зломом. TRM Labs наразі утримується від атрибуції атаки конкретному угрупованню, залишаючи простір для подальшого розслідування. Цей інцидент стане предметом пильного вивчення в криптоспільноті та, безсумнівно, призведе до перегляду стандартів безпеки при розробці та використанні апаратних гаманців у майбутньому.

Ваша думка важлива!

1. Як державам протидіяти транснаціональній організованій злочинності, якщо її стійкість забезпечується не лише кримінальними мережами, а й механізмами політичного захисту та сприяння, корупцією та зв'язками з представниками державних і безпекових структур?
2. Як має змінюватися міжнародна санкційна політика, якщо суб'єкти, на яких накладено обмеження, дедалі частіше використовують непрямих посередників, альтернативні юрисдикції та багаторівневі ланцюги постачання?
3. Чи може інцидент з Coldcard стати прецедентом для посилення регуляторних вимог до виробників апаратних гаманців, зокрема щодо обов'язкового страхування від подібних програмних помилок або вимог щодо прозорого аудиту коду перед допуском пристроїв на ринок?
4. Як війна в Україні трансформує кримінальну карту Європи, створюючи нові ризики через безпрецедентні обсяги зброї, а також масштабні фінансові потоки міжнародної допомоги та переміщення капіталів, які відкривають нові можливості для шахрайства і відмивання коштів?
5. Наскільки відсутність в Україні офіційного регулювання токенізованих активів є конкурентною перевагою для залучення блокчейн-проєктів, чи навпаки – перешкодою для інтеграції українського фінансового сектору до глобальних ринків капіталу, де токенізація вже стала мейнстрімом?
6. Які вимоги до постачальників послуг, пов'язаних з обігом віртуальних активів, здатні закрити виявлений CRF розрив між vIBAN як платіжним каналом і CEX-рахунком як місцем конвертації?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-33

Бюлетень є аналітичною розробкою методологічної команди Департаменту антилегалізаційної політики Міністерства фінансів України, спрямованою на поширення кращих практик, дослідження новітніх типологій та глобальних регуляторних і правоохоронних тенденцій у сфері ПВК/ФТ/ФР. Видання призначене для підвищення інституційної спроможності всіх учасників AML системи України та сприяння ефективному управлінню ризиками ВК/ФТ/ФР з урахуванням міжнародних стандартів та актів права ЄС.

Щоб отримати доступ до інших Методологічних Бюлетенів – перейдіть за посиланням [офіційний веб-сайт Міністерства фінансів].